Šis tekstas yra skirtas tik informacijai ir teisinės galios neturi. Europos Sąjungos institucijos nėra teisiškai atsakingos už jo turinį. Autentiškos atitinkamų teisės aktų, įskaitant jų preambules, versijos skelbiamos Europos Sąjungos oficialiajame leidinyje ir pateikiamos svetainėje „EUR-Lex“. Oficialūs tekstai tiesiogiai prieinami naudojantis šiame dokumente pateikiamomis nuorodomis

►B

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2016/799

2016 m. kovo 18 d.

kuriuo įgyvendinamas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 165/2014 ir nustatomi tachografų ir jų komponentų konstrukcijos, bandymo, įrengimo, naudojimo ir remonto reikalavimai

(Tekstas svarbus EEE)

(OL L 139, 2016 5 26, p. 1)

pataisytas:

►C1 Klaidų ištaisymas, OL L 146, 2016 6 3, p. 31 (2016/799)

►C2 Klaidų ištaisymas, OL L 27, 2017 2 1, p. 169 (2016/799)

▼B

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2016/799

2016 m. kovo 18 d.

kuriuo įgyvendinamas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 165/2014 ir nustatomi tachografų ir jų komponentų konstrukcijos, bandymo, įrengimo, naudojimo ir remonto reikalavimai

(Tekstas svarbus EEE)

1 straipsnis

Dalykas ir taikymo sritis

1. Šiuo reglamentu nustatomos nuostatos, būtinos, kad būtų vienodai taikomi šie aspektai, susiję su tachografais:

a) transporto priemonės buvimo vietos registravimas tam tikrais vairuotojo kasdienio darbo laiko momentais;

b) išmaniojo tachografo duomenų galimo klastojimo arba jų netinkamo naudojimo nuotolinis ankstyvas nustatymas;

c) sąsaja su intelektinėmis transporto sistemomis;

d) tachografų, įskaitant apsaugos mechanizmus, tipo patvirtinimo procedūrų administraciniai ir techniniai reikalavimai.

2. Išmaniųjų tachografų ir jų komponentų konstrukcija, bandymas, įrengimas, tikrinimas, naudojimas ir remontas turi atitikti šio reglamento 1C priede nustatytus techninius reikalavimus.

3. Tachografai, kurie nėra išmanieji tachografai, turi ir toliau atitikti konstrukcijos, bandymo, įrengimo, tikrinimo, eksploatavimo ir remonto reikalavimus, nustatytus atitinkamai Tarybos reglamento (EEB) Nr. 3821/85 ([1]) 1 priede arba 1B priede.

4. Siekiant iš anksto nustatyti sukčiavimo atvejus, pagal Europos Parlamento ir Tarybos direktyvos 96/53/EB 10d straipsnį nuotolinio ankstyvo nustatymo įrenginiu turi būti perduodami ir masės duomenys, kuriuos pateikia transporto priemonėje įrengta svėrimo sistema.

2 straipsnis

Apibrėžtys

Šiame reglamente vartojami Reglamento (ES) Nr. 165/2014 2 straipsnyje apibrėžti terminai.

Kitų vartojamų terminų apibrėžtys:

1) skaitmeninis tachografas, arba pirmosios kartos tachografas – skaitmeninis tachografas, kuris nėra išmanusis tachografas;

2) išorinis GNSS įrenginys – įrenginys, kuriame yra GNSS imtuvas (kai transporto priemonės blokas nėra vientisas blokas), taip pat kiti komponentai, kurių reikia į likusią transporto priemonės bloko dalį siunčiamiems buvimo vietos duomenims apsaugoti;

([1]) 1985 m. gruodžio 20 d. Tarybos reglamentas (EEB) Nr. 3821/85 dėl kelių transporto priemonėse naudojamų tachografų (OL L 370, 1985 12 31, p. 8).

▼B

3) informacijos aplankas – elektroninės ar popierinės formos aplankas, kuriame yra visa informacija, kurią gamintojas arba jo atstovas pateikia tipo patvirtinimo institucijai tachografo arba jo komponento tipui patvirtinti, įskaitant Reglamento (ES) Nr. 165/2014 12 straipsnio 3 dalyje nurodytus sertifikatus, šio reglamento 1C priede nurodytų bandymų rezultatus, taip pat brėžinius, fotografijas ir kitus svarbius dokumentus;

4) informacijos paketas – elektroninės ar popierinės formos informacijos aplankas, papildytas kitais dokumentais; informacijos aplanką tais dokumentais papildo tipo patvirtinimo institucija, vykdydama savo funkcijas; jie apima patvirtinus tipą išduodamą tachografo ar jo komponento EB tipo patvirtinimo pažymėjimą;

5) informacijos paketo rodyklė – dokumentas, kuriame pateiktas sunumeruotas informacijos paketo turinys ir nurodytos visos svarbios šio paketo dalys. To dokumento formatas turi būti toks, kad aiškiai skirtųsi EB tipo patvirtinimo etapai, taip pat to paketo persvarstymo ir atnaujinimo datos;

6) nuotolinio ankstyvo nustatymo įrenginys – transporto priemonės bloko įranga, naudojama tikslinėms patikroms kelyje atlikti;

7) išmanusis tachografas, arba antrosios kartos tachografas – skaitmeninis tachografas, atitinkantis Reglamento (ES) Nr. 165/2014 8, 9 ir 10 straipsniuose ir šio reglamento 1C priede nustatytus reikalavimus;

8) tachografo komponentas, arba komponentas – bet kuris iš šių elementų: transporto priemonės blokas, judesio jutiklis, tachografo kortelė, registracijos lapas, išorinis GNSS įrenginys ir nuotolinio ankstyvo nustatymo įrenginys;

9) tipo patvirtinimo institucija – valstybės narės institucija, atsakinga už tachografo arba jo komponentų tipo patvirtinimą, leidimų išdavimą, tipo patvirtinimo pažymėjimų išdavimą ir prireikus jų panaikinimą; ji palaiko ryšį su kitų valstybių narių tipo patvirtinimo institucijomis ir užtikrina, kad gamintojai vykdytų savo pareigą užtikrinti atitiktį šio reglamento reikalavimams.

3 straipsnis

Su vietos nustatymu susietos paslaugos

1. Gamintojai užtikrina, kad išmanieji tachografai būtų suderinami su buvimo vietos nustatymo paslaugomis, kurias teikia GALILEO ir Europos geostacionarinė navigacinė tinklo sistema (EGNOS).

2. Be to, gamintojai gali nuspręsti užtikrinti suderinamumą ne tik su 1 dalyje nurodytomis sistemomis, bet ir su kitomis palydovinės navigacijos sistemomis.

▼B

4 straipsnis

Tachografo ir jo komponentų tipo patvirtinimo tvarka

1. Gamintojas arba jo atstovas pateikia tachografo arba bet kurio jo komponento ar komponentų grupės tipo patvirtinimo paraišką tipo patvirtinimo institucijai, kurią paskiria kiekviena valstybė narė. Paraišką sudaro informacijos aplankas, kuriame pateikiama informacija apie kiekvieną atitinkamą komponentą, jei reikia, kitų komponentų, kurių reikia tachografui sukomplektuoti, tipo patvirtinimo pažymėjimai, taip pat bet kokie kiti susiję dokumentai.

2. Valstybė narė patvirtina visų tachografų, komponentų arba komponentų grupių, atitinkančių jiems taikomus 1 straipsnio 2 arba 3 dalyje nurodytus administracinius ir techninius reikalavimus, tipą. Tokiu atveju tipo patvirtinimo institucija pareiškėjui išduoda tipo patvirtinimo pažymėjimą, atitinkantį šio reglamento II priede nustatytą pavyzdį.

3. Tipo patvirtinimo institucija gali paprašyti gamintojo arba jo atstovo pateikti papildomos informacijos.

4. Gamintojas arba jo atstovas tipo patvirtinimo institucijai, taip pat įstaigoms, atsakingoms už Reglamento (ES) Nr. 165/2014 12 straipsnio 3 dalyje nurodytų sertifikatų išdavimą, pateikia tiek tachografų arba tachografo komponentų, kiek būtina tipo tvirtinimo procedūrai tinkamai įvykdyti.

5. Jei gamintojas arba jo atstovas pageidauja, kad būtų patvirtintas tam tikrų tachografo komponentų ar komponentų grupių tipas, jis tipo patvirtinimo institucijoms pateikia kitus komponentus, kurių tipas jau patvirtintas, taip pat kitas būtinas viso tachografo konstrukcijos dalis, kad institucijos galėtų atlikti reikiamus bandymus.

5 straipsnis

Tipo patvirtinimo pakeitimai

1. Gamintojas arba jo atstovas nedelsdamas praneša tipo patvirtinimo institucijoms, atlikusioms pirminį tipo patvirtinimą, apie bet kokius informacijos pakete nurodytos programinės arba techninės tachografo įrangos arba jam gaminti naudojamų medžiagų pobūdžio pakeitimus ir pateikia paraišką dėl tipo patvirtinimo pakeitimo.

2. Tipo patvirtinimo institucijos gali peržiūrėti arba pratęsti galiojantį tipo patvirtinimą arba, atsižvelgiant į pakeitimų pobūdį ir charakteristikas, išduoti naują tipo patvirtinimą.

Peržiūra atliekama, jei tipo patvirtinimo institucija mano, kad programinės arba techninės tachografo įrangos arba jam gaminti naudojamų medžiagų pobūdžio pakeitimai yra nereikšmingi. Tokiais atvejais tipo patvirtinimo institucija išduoda peržiūrėtus informacijos paketo dokumentus, nurodydama pakeitimų pobūdį ir jų patvirtinimo datą. Šiam reikalavimui įvykdyti pakanka atnaujinto informacijos paketo suvestinės redakcijos, prie kurios pridedamas išsamus padarytų pakeitimų aprašas.

▼B

Pratęsiama, jei tipo patvirtinimo institucija mano, kad programinės arba techninės tachografo įrangos arba jam gaminti naudojamų medžiagų pobūdžio pakeitimai yra reikšmingi. Tokiais atvejais ji gali pareikalauti atlikti naujus bandymus ir apie tai praneša atitinkamai gamintojui arba jo atstovui. Jei šių bandymų rezultatai atitinka reikalavimus, tipo patvirtinimo institucija išduoda patikslintą tipo patvirtinimo pažymėjimą, kuriame nurodomas pratęsimo numeris. Tipo patvirtinimo pažymėjime nurodomos pratęsimo priežastys ir išdavimo data.

3. Informacijos paketo rodyklėje nurodoma tipo patvirtinimo paskutinio pratęsimo ar peržiūros data arba atnaujinto tipo patvirtinimo paskutinės suvestinės redakcijos data.

4. Naujas tipo patvirtinimas būtinas, kai dėl prašomų patvirtinto tipo tachografo arba jo komponentų pakeitimų turėtų būti išduodamas naujas saugumo sertifikatas ar sąveikumo sertifikatas.

6 straipsnis

Įsigaliojimas

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

Jis taikomas nuo 2016 m. kovo 2 d.

Tačiau priedai taikomi nuo 2019 m. kovo 2 d., išskyrus 16 priedėlį, kuris taikomas nuo 2016 m. kovo 2 d.

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

▼B

I C PRIEDAS

Gamybos, bandymo, instaliavimo ir apžiūros reikalavimai

ĮVADAS	
1	APIBRĖŽTYS
2	BENDROSIOS TACHOGRAFO CHARAKTERISTIKOS IR FUNKCIJOS
2.1	Bendrosios charakteristikos
2.2	Funkcijos
2.3	Veikimo režimai
2.4	Saugumas
3	TACHOGRAFO KONSTRUKCIJOS IR FUNKCINIAI REIKALAVIMAI
3.1	Kortelės įstatymo ir ištraukimo stebėsena
3.2	Greičio ir atstumo matavimas ir buvimo vietos nustatymas
3.2.1	Nuvažiuoto atstumo matavimas
3.2.2	Greičio matavimas
3.2.3	Buvimo vietos nustatymas
3.3	Laiko matavimas
3.4	Vairuotojo veiklos stebėsena
3.5	Važiavimo būsenos stebėsena
3.6	Vairuotojo įvedami duomenys
3.6.1	Vietos, kurioje prasideda ir (arba) baigiasi dienos darbo laikotarpiai, duomenų įvedimas
3.6.2	Duomenų apie vairuotojo veiklą įvedimas rankiniu būdu ir vairuotojo sutikimas dėl ITS sąsajos
3.6.3	Informacijos apie ypatingas būsenas įvedimas
3.7	Įmonės užraktų valdymas
3.8	Kontrolės veiklos stebėsena
3.9	Įvykių ir (arba) trikčių aptikimas
3.9.1	„Įstatyta negaliojanti kortelė“
3.9.2	„Kortelių nesuderinamumo“ įvykis
3.9.3	„Dalinio laiko sutapimo“ įvykis
3.9.4	„Važiavimo be reikiamos kortelės“ įvykis
3.9.5	„Kortelė įstatyta važiuojant“
3.9.6	„Netinkamai užbaigtas paskutinis kortelės naudojimo seansas“
3.9.7	„Greičio viršijimo“ įvykis
3.9.8	„Maitinimo nutrūkimo“ įvykis
3.9.9.	„Ryšio su nuotolinio ryšio įrenginiu klaida“
3.9.10.	„Iš GNSS imtuvo negauta informacijos apie buvimo vietą“

▼B

3.9.11.	„Ryšio su išoriniu GNSS įrenginiu klaida“
3.9.12.	„Duomenų apie judėjimą klaida“
3.9.13.	„Transporto priemonės judėjimo nesuderinamumo“ įvykis
3.9.14.	„Bandymo pažeisti apsaugą“ įvykis
3.9.15.	„Nesuderinto laiko“ įvykis
3.9.16.	Kortelės triktis
3.9.17.	Tachografo triktis
3.10	Savidiagnostika ir savitikra
3.11	Atmintyje laikomų duomenų nuskaitymas
3.12	Informacijos įrašymas ir laikymas duomenų atmintyje
3.12.1	Įrangos identifikavimo duomenys
3.12.1.1	Transporto priemonės bloko identifikavimo duomenys
3.12.1.2	Judesio jutiklio identifikavimo duomenys
3.12.1.3	Pasaulinės palydovinės navigacijos sistemos identifikavimo duomenys
3.12.2	Raktai ir pažymėjimai
3.12.3	Duomenys apie vairuotojo arba dirbtuvių kortelės įstatymą ir ištraukimą
3.12.4	Duomenys apie vairuotojo veiklą
3.12.5	Vietos, kur prasideda ir baigiasi dienos darbo laikotarpiai ir (arba) nepertraukiamo vairavimo trukmė pasiekia 3 valandas
3.12.6	Odometro duomenys
3.12.7	Išsamūs duomenys apie greitį
3.12.8	Duomenys apie įvykius
3.12.9	Duomenys apie triktis
3.12.10	Duomenys apie kalibravimą
3.12.11	Duomenys apie laiko koregavimą
3.12.12	Duomenys apie kontrolės veiklą
3.12.13	Duomenys apie įmonės užraktus
3.12.14	Duomenys apie duomenų perkėlimo veiklą
3.12.15	Duomenys apie ypatingas būsenas
3.12.16	Tachografo kortelių duomenys
3.13	Tachografo kortelėse įrašytos informacijos nuskaitymas
3.14	Informacijos įrašymas į tachografo korteles ir laikymas
3.14.1	Informacijos įrašymas į pirmosios kartos tachografo korteles ir laikymas
3.14.2	Informacijos įrašymas į antrosios kartos tachografo korteles ir laikymas
3.15	Rodymas ekrane
3.15.1	Numatytasis rodinys
3.15.2	Perspėjamasis rodinys

▼B

3.15.3	Naudojimasis meniu
3.15.4	Kiti rodiniai
3.16	Spausdinimas
3.17	Perspėjimai
3.18	Duomenų perkėlimas į išorines laikmenas
3.19	Nuotolinis ryšys tikslinėms patikroms kelyje atlikti
3.20	Duomenų persiuntimas į papildomus išorinius įtaisus
3.21	Kalibravimas
3.22	Kalibravimo tikrinimas kelyje
3.23	Laiko koregavimas
3.24	Eksploatacinės savybės
3.25	Medžiagos
3.26	Ženklai
4	TACHOGRAFO KORTELIŲ KONSTRUKCIJOS IR FUNKCINIAI REIKALAVIMAI
4.1	Regimieji duomenys
4.2	Saugumas
4.3	Standartai
4.4	Aplinkos ir elektrinės specifikacijos
4.5	Duomenų laikymas
4.5.1	Elementariosios rinkmenos, kurių paskirtis – identifikavimas ir kortelės tvarkymas
4.5.2	Lustinės kortelės identifikacija
4.5.2.1	Lusto identifikacija
4.5.2.2	DIR (tik antrosios kartos tachografo kortelėse)
4.5.2.3	ATR informacija (sąlyginė, tik antrosios kartos tachografo kortelėse)
4.5.2.4	Didesnio ilgio informacija (sąlyginė, tik antrosios kartos tachografo kortelėse)
4.5.3	Vairuotojo kortelė
4.5.3.1	Tachografo taikomoji programa (tinkama pirmosios ir antrosios kartos transporto priemonės blokams)
4.5.3.1.1	Taikomosios programos identifikacija
4.5.3.1.2	Raktai ir pažymėjimai
4.5.3.1.3	Kortelės identifikacija
4.5.3.1.4	Kortelės turėtojo identifikacija
4.5.3.1.5	Duomenų perkėlimas iš kortelės
4.5.3.1.6	Informacija apie vairuotojo pažymėjimą
4.5.3.1.7	Duomenys apie įvykius
4.5.3.1.8	Duomenys apie triktis
4.5.3.1.9	Duomenys apie vairuotojo veiklą

▼B

4.5.3.1.10	Duomenys apie naudotas transporto priemones
4.5.3.1.11	Vietos, kur prasideda ir (arba) baigiasi dienos darbo laikotarpiai
4.5.3.1.12	Duomenys apie kortelės naudojimo seansą
4.5.3.1.13	Duomenys apie kontrolės veiklą
4.5.3.1.14	Duomenys apie ypatingas būsenas
4.5.3.2	Antrosios kartos tachografo taikomoji programa (netinkama pirmosios kartos transporto priemonės blokui)
4.5.3.2.1	Taikomosios programos identifikacija
4.5.3.2.2	Raktai ir pažymėjimai
4.5.3.2.3	Kortelės identifikacija
4.5.3.2.4	Kortelės turėtojo identifikacija
4.5.3.2.5	Duomenų perkėlimas iš kortelės
4.5.3.2.6	Informacija apie vairuotojo pažymėjimą
4.5.3.2.7	Duomenys apie įvykius
4.5.3.2.8	Duomenys apie triktis
4.5.3.2.9	Duomenys apie vairuotojo veiklą
4.5.3.2.10	Duomenys apie naudotas transporto priemones
4.5.3.2.11	Vietos, kur prasideda ir (arba) baigiasi dienos darbo laikotarpiai
4.5.3.2.12	Duomenys apie kortelės naudojimo seansą
4.5.3.2.13	Duomenys apie kontrolės veiklą
4.5.3.2.14	Duomenys apie ypatingas būsenas
4.5.3.2.15	Naudotų transporto priemonės blokų duomenys
4.5.3.2.16	Duomenys apie vietas, kur nepertraukiamo vairavimo trukmė pasiekia tris valandas
4.5.4	Dirbtuvių kortelė
4.5.4.1	Tachografo taikomoji programa (tinkama pirmosios ir antrosios kartos transporto priemonės blokams)
4.5.4.1.1	Taikomosios programos identifikacija
4.5.4.1.2	Raktai ir pažymėjimai
4.5.4.1.3	Kortelės identifikacija
4.5.4.1.4	Kortelės turėtojo identifikacija
4.5.4.1.5	Duomenų perkėlimas iš kortelės
4.5.4.1.6	Duomenys apie kalibravimą ir laiko koregavimą
4.5.4.1.7	Duomenys apie įvykius ir triktis
4.5.4.1.8	Duomenys apie vairuotojo veiklą
4.5.4.1.9	Duomenys apie naudotas transporto priemones
4.5.4.1.10	Duomenys apie dienos darbo laikotarpių pradžią ir (arba) pabaigą
4.5.4.1.11	Duomenys apie kortelės naudojimo seansą
4.5.4.1.12	Duomenys apie kontrolės veiklą

▼B

4.5.4.1.13	Duomenys apie ypatingas būsenas
4.5.4.2	2-osios kartos tachografo taikomoji programa (netinkama pirmosios kartos transporto priemonės blokui)
4.5.4.2.1	Taikomosios programos identifikacija
4.5.4.2.2	Raktai ir pažymėjimai
4.5.4.2.3	Kortelės identifikacija
4.5.4.2.4	Kortelės turėtojo identifikacija
4.5.4.2.5	Duomenų perkėlimas iš kortelės
4.5.4.2.6	Duomenys apie kalibravimą ir laiko koregavimą
4.5.4.2.7	Duomenys apie įvykius ir triktis
4.5.4.2.8	Duomenys apie vairuotojo veiklą
4.5.4.2.9	Duomenys apie naudotas transporto priemones
4.5.4.2.10	Duomenys apie dienos darbo laikotarpių pradžią ir (arba) pabaigą
4.5.4.2.11	Duomenys apie kortelės naudojimo seansą
4.5.4.2.12	Duomenys apie kontrolės veiklą
4.5.4.2.13	Naudotų transporto priemonės blokų duomenys
4.5.4.2.14	Duomenys apie vietas, kur nepertraukiamo vairavimo trukmė pasiekia tris valandas
4.5.4.2.15	Duomenys apie ypatingas būsenas
4.5.5	Kontrolės kortelė
4.5.5.1	Tachografo taikomoji programa (tinkama pirmosios ir antrosios kartos transporto priemonės blokams)
4.5.5.1.1	Taikomosios programos identifikacija
4.5.5.1.2	Raktai ir pažymėjimai
4.5.5.1.3	Kortelės identifikacija
4.5.5.1.4	Kortelės turėtojo identifikacija
4.5.5.1.5	Duomenys apie kontrolės veiklą
4.5.5.2	2-osios kartos tachografo taikomoji programa (netinkama pirmosios kartos transporto priemonės blokui)
4.5.5.2.1	Taikomosios programos identifikacija
4.5.5.2.2	Raktai ir pažymėjimai
4.5.5.2.3	Kortelės identifikacija
4.5.5.2.4	Kortelės turėtojo identifikacija
4.5.5.2.5	Duomenys apie kontrolės veiklą
4.5.6	Įmonės kortelė
4.5.6.1	Tachografo taikomoji programa (tinkama pirmosios ir antrosios kartos transporto priemonės blokams)
4.5.6.1.1	Taikomosios programos identifikacija
4.5.6.1.2	Raktai ir pažymėjimai
4.5.6.1.3	Kortelės identifikacija

▼B

4.5.6.1.4 Kortelės turėtojo identifikacija

4.5.6.1.5 Duomenys apie įmonės veiklą

4.5.6.2 2-osios kartos tachografo taikomoji programa (netinkama pirmosios kartos transporto priemonės blokui)

4.5.6.2.1 Taikomosios programos identifikacija

4.5.6.2.2 Raktai ir pažymėjimai

4.5.6.2.3 Kortelės identifikacija

4.5.6.2.4 Kortelės turėtojo identifikacija

4.5.6.2.5 Duomenys apie įmonės veiklą

5 TACHOGRAFO ĮRENGIMAS

5.1 Įrengimas

5.2 Įrengimo plokštelė

5.3 Plombavimas

6 TIKRINIMAI, PATIKROS IR REMONTAS

6.1 Montuotojų, dirbtuvių ir transporto priemonių gamintojų patvirtinimas

6.2 Naujų arba suremontuotų prietaisų tikrinimas

6.3 Įrengimo patikra

6.4 Periodinės patikros

6.5 Paklaidų matavimas

6.6 Remontas

7 KORTELĖS IŠDAVIMAS

8 TACHOGRAFŲ IR TACHOGRAFO KORTELIŲ TIPO PATVIRTINIMAS

8.1 Bendrosios nuostatos

8.2 Saugumo sertifikatas

8.3 Veikimo sertifikatas

8.4 Sąveikumo sertifikatas

8.5 Tipo patvirtinimo pažymėjimas

8.6 Išimtinė procedūra: pirmieji sąveikumo sertifikatai, skirti 2-osios kartos tachografams ir tachografo kortelėms

ĮVADAS

Pirmosios kartos skaitmeninių tachografų sistema diegiama nuo 2006 m. gegužės 1 d. Vidaus transporte ji gali būti naudojama iki naudojimo laikotarpio pabaigos. Tarptautiniame transporte, praėjus 15 metų po šio Komisijos reglamento įsigaliojimo, kiekvienoje transporto priemonėje turės būti įrengtas šiame reglamente nustatytus reikalavimus atitinkantis antrosios kartos išmanusis tachografas.

Šiame priede pateikiami antrosios kartos tachografų ir tachografo kortelių reikalavimai. Nuo įdiegimo dienos antrosios kartos tachografai montuojami pirmą kartą registruojamose transporto priemonėse ir išduodamos antrosios kartos tachografų kortelės.

Siekiant skatinti sklandų antrosios kartos tachografų sistemos diegimą,

▼B

— antrosios kartos tachografų kortelės turi būti tinkamos naudoti ir pirmosios kartos transporto priemonių blokuose,

— nereikalaujama, kad galiojančios pirmosios kartos tachografų kortelės būtų pakeistos įdiegimo dieną.

Tai leis vairuotojams išsaugoti savo vairuotojo kortelę ir ja naudotis abiejose sistemose.

Tačiau antrosios kartos tachografai turi būti kalibruojami naudojant tik antrosios kartos dirbtuvių korteles.

Šiame priede pateikiami visi reikalavimai, susiję su pirmosios ir antrosios kartos tachografų sistemų sąveika.

15 priedėlyje pateikiama papildomos informacijos apie šių abiejų sistemų vienalaikio naudojimo administravimą.

Priedėlių sąrašas

1 priedėlis.	DUOMENŲ ŽINYNAS
2 priedėlis.	TACHOGRAFO KORTELIŲ SPECIFIKACIJA
3 priedėlis.	PIKTOGRAMOS
4 priedėlis.	SPAUDINIAI
5 priedėlis.	RODINYS
6 priedėlis.	PRIEKINĖ KALIBRAVIMO IR DUOMENŲ PERKĖLIMO JUNGTIS
7 priedėlis.	DUOMENŲ PERKĖLIMO PROTOKOLAI
8 priedėlis.	KALIBRAVIMO PROTOKOLAS
9 priedėlis.	TIPO PATVIRTINIMAS. BŪTINŲJŲ BANDYMŲ SĄRAŠAS
10 priedėlis.	SAUGUMO REIKALAVIMAI
11 priedėlis.	BENDRIEJI APSAUGOS MECHANIZMAI
12 priedėlis.	BUVIMO VIETOS NUSTATYMAS NAUDOJANTIS PASAULINE PALYDOVINĖS NAVIGACIJOS SISTEMA (GNSS)
13 priedėlis.	ITS SĄSAJA
14 priedėlis.	NUOTOLINIO RYŠIO FUNKCIJA
15 priedėlis.	PERĖJIMAS PRIE NAUJOS ĮRANGOS. SKIRTINGŲ KARTŲ ĮRANGOS VIENALAIKIO NAUDOJIMO ADMINISTRAVIMAS
16 priedėlis.	M1 IR N1 KLASIŲ TRANSPORTO PRIEMONIŲ ADAPTERIAI

1 APIBRĖŽTYS

Šiame priede:

a) aktyvinimas –

etapas, kuriuo, panaudojus dirbtuvių kortelę, tachografas pradeda visiškai veikti ir atlieka visas, įskaitant apsaugos, funkcijas;

b) autentiškumo tikrinimas –

nurodytos tapatybės nustatymo ir tikrinimo funkcija;

c) autentiškumas –

savybė, rodanti, kad informaciją pateikusios šalies tapatybę galima patikrinti;

d) savidiagnostika –

operatoriaus arba išorinės įrangos reikalavimu atliekami patikrinimai;

▼B

e) kalendorinė diena –

laikas nuo 00.00 val. iki 24.00 val. Visos kalendorinės dienos nustatomos pagal UTC (suderintąjį pasaulinį laiką);

f) išmaniojo tachografo kalibravimas –

duomenų atmintyje laikomų transporto priemonės parametrų atnaujinimas arba patvirtinimas. Transporto priemonės parametrai – transporto priemonės identifikacija (VIN, transporto priemonės registracijos numeris ir registracijos valstybė narė) ir transporto priemonės charakteristikos (w, k, l, padangų dydis, greičio ribotuvo nuostatis (jei yra), UTC laikas, odometro rodmuo); kalibruojant tachografą, duomenų atmintyje taip pat turi būti išsaugota informacija apie uždėtų plombų, susijusių su tipo patvirtinimu, rūšis ir identifikatorius;

bet koks tik UTC laiko atnaujinimas ar patvirtinimas laikomas laiko koregavimu, o ne kalibravimu, jei tai neprieštarauja 409 reikalavimui;

tachografui sukalibruoti reikia dirbtuvių kortelės;

g) kortelės numeris –

unikalus iš 16 rašmenų sudarytas numeris tachografo kortelei valstybėje narėje identifikuoti. Kortelės numerį sudaro kortelių numeracijos indeksas (jei naudojamas), kortelės keitimo indeksas ir kortelės atnaujinimo indeksas;

taigi kortelė identifikuojama ją išdavusios valstybės narės kodu ir kortelės numeriu;

h) kortelių numeracijos indeksas –

kortelės numerio 14-as rašmuo, naudojamas atskirti skirtingoms kortelėms, išduotoms įmonei, dirbtuvėms ar kontrolės institucijai, turinčioms teisę gauti keletą tachografo kortelių. Įmonei, dirbtuvėms ar kontrolės institucijai priskiriamas unikalus numeris, kurį sudaro pirmi 13 kortelės numerio rašmenų;

i) kortelės atnaujinimo indeksas –

kortelės numerio 16-as rašmuo, didinamas kaskart, kai tachografo kortelė atnaujinama;

j) kortelės keitimo indeksas –

kortelės numerio 15-as rašmuo, didinamas kaskart, kai tachografo kortelė pakeičiama;

k) transporto priemonės būdingasis koeficientas –

skaitmeninė charakteristika, rodanti išėjimo signalo, skleidžiamo transporto priemonės dalies, kuria transporto priemonė yra sujungta su tachografu (pavarų dėžės išėjimo velenas arba ašis), vertę, kol įprastomis bandymo sąlygomis, nurodytomis 414 reikalavimo apraše, transporto priemonė nuvažiuoja vieną kilometrą. Būdingasis koeficientas išreiškiamas impulsais kilometrui (w = … imp/km);

l) įmonės kortelė –

transporto įmonei, kuri turi eksploatuoti transporto priemones su įmontuotu tachografu, valstybės narės institucijų išduota tachografo kortelė, pagal kurią identifikuojama transporto įmonė ir kuri suteikia galimybę rodyti, perkelti į kitas laikmenas ir spausdinti tachografe laikomus duomenis, kuriuos užblokavo ta transporto įmonė;

▼B

m) tachografo konstanta –

skaitmeninė charakteristika, rodanti įvesties signalo vertę, reikalingą nuvažiuotam 1 km nuotoliui rodyti ir registruoti; ši konstanta išreiškiama impulsais kilometrui (k =… imp/km);

n) nepertraukiamo vairavimo trukmė, kurią apskaičiuoja tachografas ([1]) –

nepertraukiamo vairavimo trukmė apskaičiuojama kaip bendroji tam tikro vairuotojo vairavimo trukmė nuo paskutinio ne trumpesnio kaip 45 minučių PASIRENGIMO DIRBTI, PERTRAUKOS / POILSIO arba NEŽINOMO ([2]) laikotarpio (šis laikotarpis gali būti padalytas pagal Europos Parlamento ir Tarybos reglamentą (EB) Nr. 561/2006 ([3])). Skaičiuojant atsižvelgiama į vairuotojo kortelės atmintyje įrašytus duomenis apie ankstesnę veiklą (jei reikia). Jeigu vairuotojas neįstato kortelės į kortelės lizdą, skaičiuojama remiantis su atitinkamu lizdu susijusiais duomenų atminties įrašais apie pastarąjį laikotarpį, kai kortelė nebuvo įstatyta į kortelės lizdą;

o) kontrolės kortelė –

tachografo kortelė, kurią valstybės narės institucijos išduoda kompetentingai nacionalinei kontrolės institucijai ir pagal kurią identifikuojama kontrolės įstaiga (pasirinktinai – ir kontroliuojančio pareigūno tapatybė) bei kuri suteikia prieigą prie nuskaityti, spausdinti ir (arba) perkelti į kitas laikmenas norimų duomenų, laikomų atmintyje arba vairuotojo kortelėse, ir – pasirinktinai – dirbtuvių kortelėse laikomų duomenų.

Ji taip pat suteikia galimybę pasinaudoti kalibravimo tikrinimo kelyje funkcija ir užtikrina prieigą prie nuotolinio ankstyvo nustatymo ryšio skaitytuvo duomenų;

p) bendroji poilsio trukmė, kurią apskaičiuoja tachografas ([1]) –

bendroji poilsio trukmė apskaičiuojama kaip bendroji tam tikro vairuotojo ne trumpesnių kaip 15 minučių PASIRENGIMO DIRBTI, PERTRAUKOS / POILSIO arba NEŽINOMO ([2]) laikotarpių trukmė nuo paskutinio ne trumpesnio kaip 45 minučių PASIRENGIMO DIRBTI, PERTRAUKOS / POILSIO arba NEŽINOMO ([3]) laikotarpio (tas laikotarpis gali būti padalytas pagal Reglamentą (EB) Nr. 561/2006).

Skaičiuojant atsižvelgiama į vairuotojo kortelės atmintyje įrašytus duomenis apie ankstesnę veiklą (jei reikia). Skaičiuojant neatsižvelgiama į neigiamos trukmės nežinomus laikotarpius (nežinomo laikotarpio pradžia yra ankstesnė nei jo pabaiga), susidarančius dėl dviejų skirtingų tachografų laiko dalinio sutapimo.

([1]) Šiuo būdu apskaičiuota nepertraukiamo vairavimo trukmė ir bendroji poilsio trukmė yra parametrai, pagal kuriuos tachografas apskaičiuoja perspėjimo dėl nepertraukiamo vairavimo trukmės parametrą. Vien jais remiantis teisinių išvadų dėl minėtųjų trukmių daryti negalima. Nepertraukiamo vairavimo trukmė ir bendroji poilsio trukmė gali būti apskaičiuojamos ir kitais būdais, pakeičiant šias apibrėžtis, jei jos tampa neaktualios dėl to, kad yra atnaujinamos kituose susijusiuose teisės aktuose.

([2]) NEŽINOMI laikotarpiai – laikotarpiai, kai vairuotojo kortelė nebuvo įstatyta į tachografą ir duomenys apie vairuotojo veiklą nebuvo įvesti ranka.

([3]) 2006 m. kovo 15 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 561/2006 dėl tam tikrų su kelių transportu susijusių socialinių teisės aktų suderinimo ir iš dalies keičiantis Tarybos reglamentus (EEB) Nr. 3821/85 ir (EB) Nr. 2135/98 bei panaikinantis Reglamentą (EEB) Nr. 3820/85 (OL L 102, 2006 4 11, p. 1).

▼B

Jeigu vairuotojas neįstato kortelės į kortelės lizdą, skaičiuojama remiantis su atitinkamu lizdu susijusiais duomenų atminties įrašais apie pastarąjį laikotarpį, kai kortelė nebuvo įstatyta į kortelės lizdą;

q) duomenų atmintis –

tachografe sumontuotas elektroninis duomenų kaupiklis;

r) skaitmeninis parašas –

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

s) duomenų perkėlimas –

transporto priemonės bloko arba tachografo kortelės atmintyje užregistruotų visų duomenų rinkinių arba jų dalies kopijavimas kartu su skaitmeniniu parašu su sąlyga, kad, vykdant šį procesą, išsaugoti duomenys nėra pakeičiami ar ištrinami.

Išmaniųjų tachografų transporto priemonių blokų gamintojai ir įrangos, kuri suprojektuota ir skirta duomenų rinkmenoms perkelti, gamintojai imasi visų deramų priemonių, kad užtikrintų, kad transporto įmonės arba vairuotojai tokius duomenis galėtų perkelti kuo greičiau.

Gali būti nebūtina perkelti išsamią greičio rinkmeną norint nustatyti atitiktį Reglamentui (EB) Nr. 561/2006, tačiau ji gali būti naudojama kitais tikslais, pavyzdžiui, eismo įvykiui tirti.

t) vairuotojo kortelė –

valstybės narės valdžios institucijų tam tikram vairuotojui išduota tachografo kortelė, pagal kurią nustatoma vairuotojo tapatybė ir kuri yra skirta duomenims apie vairuotojo veiklą laikyti;

u) padangų efektyvusis apskritimo ilgis –

atstumų, kuriuos nuvažiuoja vieną kartą visiškai apsisukdamas kiekvienas transporto priemonę varantis ratas (varantieji ratai), vidurkis. Šie atstumai matuojami standartinėmis bandymo sąlygomis, nustatytomis 414 reikalavimo apraše, ir išreiškiami „l = … mm“. Transporto priemonių gamintojams leidžiama, užuot matavus šiuos atstumus, atlikti teorinius skaičiavimus, atsižvelgiant į parengtos važiuoti nepakrautos transporto priemonės didžiausią leidžiamą ašių apkrovą ([1]). Tokio teorinio skaičiavimo metodiką tvirtina kompetentinga valstybės narės institucija ir jis gali būti atliekamas tik prieš tachografo aktyvinimą;

v) įvykis –

išmaniojo tachografo aptiktas neįprastas veikimas, kurio priežastis gali būti mėginimas sukčiauti;

w) išorinis GNSS įrenginys –

įrenginys, kuriame yra GNSS imtuvas (kai transporto priemonės blokas nėra vientisas blokas), taip pat kiti komponentai, kurių reikia į likusią transporto priemonės bloko dalį siunčiamiems buvimo vietos duomenims apsaugoti;

([1]) 2012 m. gruodžio 12 d. Komisijos reglamentas (ES) Nr. 1230/2012, kuriuo įgyvendinamas Europos Parlamento ir Tarybos reglamentas (EB) Nr. 661/2009 dėl variklinių transporto priemonių, jų priekabų ir joms skirtų sistemų, sudėtinių dalių bei atskirų techninių mazgų tipo patvirtinimo, atsižvelgiant į jų bendrąją saugą, reikalavimų ir iš dalies keičiama Europos Parlamento ir Tarybos direktyva 2007/46/EB (OL L 353, 2012 12 21, p. 31), su paskutiniais pakeitimais.

▼B

x) triktis –

išmaniojo tachografo aptiktas neįprastas veikimas, kurio priežastis gali būti įrangos veikimo sutrikimas arba gedimas;

y) GNSS imtuvas –

elektroninis įrenginys, kuriuo priimami ir skaitmeniniu būdu apdorojami vienos ar kelių pasaulinių palydovinių navigacijos sistemų (GNSS) signalai, siekiant pateikti buvimo vietos, greičio ir laiko informaciją;

z) įrengimas –

tachografo sumontavimas transporto priemonėje;

aa) sąveikumas –

sistemų ir susijusių verslo procesų pajėgumas keistis duomenimis ir dalytis informacija;

bb) sąsaja –

infrastruktūra tarp atskirų sistemų, užtikrinanti sistemų sujungimo ir sąveikos priemones;

cc) buvimo vieta –

transporto priemonės geografinės koordinatės tam tikru laiko momentu;

dd) judesio jutiklis –

tachografo dalis, generuojanti signalą, atitinkantį transporto priemonės važiavimo greitį ir (arba) nuvažiuotą atstumą;

ee) negaliojanti kortelė –

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

ff) atvirasis standartas –

standartas, nustatytas standartų specifikacijos dokumente, kuris yra nemokamas arba parduodamas už simbolinį mokestį ir kurį galima kopijuoti, platinti ar naudoti nemokamai arba už simbolinį mokestį;

gg) nekontroliuojama –

kai pagal Reglamento (EB) Nr. 561/2006 nuostatas tachografo naudoti nereikalaujama;

hh) greičio viršijimas –

leidžiamo transporto priemonės greičio viršijimas, apibrėžiamas kaip bet kuris ilgesnis kaip 60 sekundžių laikotarpis, kuriuo išmatuotas transporto priemonės greitis viršija greičio ribotuvo, nurodyto Tarybos direktyvoje 92/6/EEB [1] (su paskutiniais pakeitimais), nustatytą vertę;

ii) periodinė patikra –

operacijos, atliekamos norint patikrinti, ar tachografas veikia tinkamai, ar jo nuostačiai atitinka transporto priemonės parametrus ir ar prie tachografo nėra pritvirtinta klastojimo įtaisų;

[1] 1992 m. vasario 10 d. Tarybos direktyva 92/6/EEB dėl tam tikrų kategorijų variklinių transporto priemonių greičio ribotuvų įrengimo ir naudojimo Bendrijoje (OL L 57, 1992 3 2, p. 27).

▼B

jj) spausdintuvas –

tachografo komponentas, kuriuo spausdinami laikomų duomenų spaudiniai;

kk) nuotolinis ankstyvo nustatymo ryšys –

ryšys, užmezgamas tarp nuotolinio ankstyvo nustatymo ryšio įrenginio ir nuotolinio ankstyvo nustatymo ryšio skaitytuvo per tikslines patikras kelyje, kuriomis siekiama nuotoliniu būdu nustatyti galimą tachografo duomenų klastojimą arba netinkamą tachografo naudojimą;

ll) nuotolinio ryšio įrenginys –

transporto priemonės bloko įranga, naudojama tikslinėms patikroms kelyje atlikti;

mm) nuotolinio ankstyvo nustatymo ryšio skaitytuvas –

sistema, kurią kontroliuojantys pareigūnai naudoja tikslinėms patikroms kelyje;

nn) atnaujinimas –

naujos tachografo kortelės išdavimas baigus galioti arba sugedus senajai ir ją grąžinus išduodančiajai institucijai. Atnaujinimas užtikrina, kad vienu metu nebus dviejų galiojančių kortelių;

oo) remontas –

judesio jutiklio, transporto priemonės bloko arba laido remontas, dėl kurio reikia atjungti jo maitinimo šaltinį arba jį patį atjungti nuo kitų tachografo komponentų, arba atidaryti judesio jutiklį ar transporto priemonės bloką;

pp) kortelės keitimas –

naujos tachografo kortelės išdavimas vietoj senosios, kuri paskelbta pamesta, pavogta ar sugedusi ir nebuvo grąžinta išduodančiajai institucijai. Keitimas niekada neužtikrina, kad vienu metu nebus dviejų galiojančių kortelių;

qq) saugumo sertifikavimas –

bendraisiais kriterijais grindžiamo sertifikavimo įstaigos atliekamas sertifikavimas, kai tikrinama, ar tachografas (ar komponentas) arba tachografo kortelė atitinka atitinkamų apsaugos profilių apraše nustatytus saugumo reikalavimus;

rr) savitikra –

tachografo periodiškai ir automatiškai atliekami patikrinimai triktims aptikti;

ss) laiko matavimas –

suderintojo pasaulinio laiko ir datos (UTC) nuolatinis registravimas skaitmeninėmis priemonėmis;

tt) laiko koregavimas –

reguliarus automatinis laiko koregavimas su ne didesne nei vienos minutės paklaida arba kalibravimo metu atliktas koregavimas;

uu) padangų dydis –

(išorinių varančiųjų ratų) padangų matmenų nuoroda pagal Tarybos direktyvą 92/23/EEB ([1]) su paskutiniais pakeitimais;

([1]) 1992 m. kovo 31 d. Tarybos direktyva 92/23/EEB dėl motorinių transporto priemonių ir jų priekabų padangų bei jų montavimo (OL L 129, 1992 5 14, p. 95).

▼B

vv) transporto priemonės identifikacija –

numeriai, pagal kuriuos identifikuojama transporto priemonė: transporto priemonės registracijos numeris su registracijos valstybės narės žymeniu ir transporto priemonės identifikavimo numeris (VIN) ([1]);

ww) savaitė (atliekant tachografo skaičiavimus) –

laikotarpis nuo pirmadienio 00.00 val. iki sekmadienio 24.00 val. pagal UTC;

xx) dirbtuvių kortelė –

tachografo kortelė, kurią valstybės narės valdžios institucijos išduoda paskirtam tachografo gamintojo, montuotojo, transporto priemonės gamintojo ar tos valstybės narės patvirtintų dirbtuvių personalui, pagal kurią nustatoma kortelės turėtojo tapatybė ir kuri suteikia galimybę tachografus bandyti, kalibruoti ir aktyvinti ir (arba) perkelti duomenis iš jų;

yy) adapteris –

įtaisas, kuris nuolat siunčia transporto priemonės greičio ir (arba) nuvažiuoto atstumo signalą ir nėra naudojamas nepriklausomam judėjimui aptikti ir kuris yra:

— įrengtas ir naudojamas tik M1 ir N1 klasių transporto priemonėse (kaip nurodyta Europos Parlamento ir Tarybos direktyvos 2007/46/EB ([2]) su paskutiniais pakeitimais II priede), kurios pradėtos eksploatuoti nuo 2006 m. gegužės 1 d.,

— įrengtas transporto priemonėse, kuriose mechaniškai neįmanoma įrengti kitos rūšies judesio jutiklio, kuris kitais atžvilgiais atitiktų šio priedo ir jo 1–15 priedėlių reikalavimus,

— įrengtas tarp transporto priemonės bloko ir tos dalies, kurioje gaunami integruotų jutiklių ar kitų sietuvų generuojami greičio ir (arba) atstumo impulsai,

— transporto priemonės bloko atžvilgiu adapterio veikimas yra toks pat, koks būtų prie transporto priemonės bloko prijungus judesio jutiklį, atitinkantį šio priedo ir 1–16 priedėlių nuostatas;

naudojant tokį adapterį anksčiau minėtose transporto priemonėse turi būti įmanoma sumontuoti ir tinkamai naudoti transporto priemonės bloką, atitinkantį visus šio priedo reikalavimus;

tokiose transporto priemonėse išmanųjį tachografą sudaro laidai, adapteris ir transporto priemonės blokas;

([1]) 1975 m. gruodžio 18 d. Tarybos direktyva 76/114/EEB dėl valstybių narių įstatymų, reglamentuojančių motorinių transporto priemonių ir jų priekabų identifikavimo lenteles, įrašus, tų lentelių tvirtinimo vietą ir būdus, suderinimo (OL L 24, 1976 1 30, p. 1).

([2]) 2007 m. rugsėjo 5 d. Europos Parlamento ir Tarybos direktyva 2007/46/EB, nustatanti motorinių transporto priemonių ir jų priekabų bei tokioms transporto priemonėms skirtų sistemų, sudėtinių dalių ir atskirų techninių mazgų patvirtinimo pagrindus (Pagrindų direktyva) (OL L 263, 2007 10 9, p. 1).

▼B

zz) duomenų nepažeistumas –

laikomų duomenų tikslumas ir nuoseklumas, kai tarp dviejų duomenų įrašo atnaujinimo momentų duomenys niekaip nekeičiami. Nepažeistumas reiškia, kad duomenys yra tiksli pirminės versijos kopija, pvz., kad jie nebuvo iškraipyti įrašymo į tachografo kortelę ar specializuotą įrangą ir jų nuskaitymo metu arba juos perduodant bet kuriuo ryšio kanalu;

aaa) duomenų privatumas –

visos techninės priemonės, kurių imtasi siekiant tinkamai įgyvendinti principus, nustatytus Europos Parlamento ir Tarybos direktyva 95/46/EB ([1]) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir Europos Parlamento ir Tarybos direktyva 2002/58/EB ([2]);

bbb) išmaniojo tachografo sistema –

tachografas, tachografo kortelės ir visi tiesiogiai ar netiesiogiai sąveikaujantys įrenginiai jų gamybos, montavimo, naudojimo, bandymo ir kontrolės metu, pavyzdžiui, kortelės, nuotolinio ryšio skaitytuvas, kita duomenų perkėlimo, duomenų analizės, kalibravimo, saugumo elementų generavimo, tvarkymo arba diegimo įranga ir pan.;

ccc) įdiegimo data –

36 mėnesiai po Europos Parlamento ir Tarybos reglamento (ES) Nr. 165/2014 ([3]) 11 straipsnyje nurodytų išsamių nuostatų įsigaliojimo.

Tai data, nuo kurios:

— *pirmą kartą registruojamose transporto priemonėse turi būti sumontuotas tachografas, sujungtas su vietos nustatymo paslauga, pagrįsta palydovine navigacijos sistema,*

— *jis turi būti pritaikytas transporto priemonei važiuojant persiųsti duomenis kompetentingoms kontrolės institucijoms, atliekančioms tikslines patikras kelyje,*

— *jame gali būti įrengta standartinė sąsaja, leidžianti tachografo užregistruotus arba sukurtus duomenis per išorinį įrenginį naudoti veikimo režimu;*

ddd) apsaugos profilis –

dokumentas, naudojamas atliekant sertifikavimą pagal bendruosius kriterijus, kuriame pateikta nuo įgyvendinimo nepriklausanti informacijos saugumo užtikrinimo reikalavimų specifikacija;

([1]) 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (OL L 281, 1995 11 23, p. 31).

([2]) 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002 7 31, p. 37).

([3]) 2014 m. vasario 4 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 165/2014 dėl kelių transporto priemonėse naudojamų tachografų, kuriuo panaikinamas Tarybos reglamentas (EEB) Nr. 3821/85 dėl kelių transporto priemonėse naudojamų tachografų ir iš dalies keičiamas Europos Parlamento ir Tarybos reglamentas (EB) Nr. 561/2006 dėl tam tikrų su kelių transportu susijusių socialinių teisės aktų suderinimo (OL L 60, 2014 2 28, p. 1).

▼B

eee) GNSS tikslumas –

tachografui registruojant buvimo vietą pagal pasaulinės palydovinės navigacijos sistemos (GNSS) duomenis, horizontaliojo tikslumo paklaida (HDOP), apskaičiuojama kaip mažiausia HDOP visose pasiekiamose GNSS.

2 BENDROSIOS TACHOGRAFO CHARAKTERISTIKOS IR FUNKCIJOS

2.1 **Bendrosios charakteristikos**

Tachografo paskirtis – įrašyti, laikyti, rodyti, spausdinti ir pateikti su vairuotojo veikla susijusius duomenis.

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

01) Tachografą sudaro laidai, judesio jutiklis ir transporto priemonės blokas.

02) Judesio jutiklių ir transporto priemonės blokų sąsaja turi atitikti reikalavimus, nustatytus 11 priedėlyje.

03) Transporto priemonės blokas turi būti prijungtas prie pasaulinės palydovinės navigacijos sistemos (-ų), kaip nurodyta 12 priedėlyje.

04) Transporto priemonės blokas turi užmegzti ryšį su nuotolinio ankstyvo nustatymo ryšio skaitytuvais, kaip nurodyta 14 priedėlyje.

05) Transporto priemonės bloke gali būti ITS sąsaja, nurodyta 13 priedėlyje.

Tachografas gali būti prijungtas prie kitų įrenginių per papildomas sąsajas ir (arba) per neprivalomą ITS sąsają.

06) Prijungti prie tachografo arba jame įdiegti bet kokias – patvirtintas ar kitokias – funkcijas, įtaisą ar įtaisus leidžiama tik tada, jei jie netrikdo ir negali sutrikdyti tinkamo ir saugaus tachografo veikimo ir nepažeidžia šio reglamento reikalavimų.

Tachografo naudotojų tapatybė nustatoma pagal tachografo korteles.

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

Tachografas įrašo ir saugo duomenis savo duomenų atmintyje, nuotolinio ryšio įrenginyje ir tachografo kortelėse.

Tai daroma vadovaujantis 1995 m. spalio 24 d. Direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ([1]), 2002 m. liepos 12 d. Direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ([2]) ir Reglamento (ES) Nr. 165/2014 7 straipsniu.

([1]) OL L 281, 1995 11 23, p. 31.
([2]) OL L 201, 2002 7 31, p. 37.

▼B

2.2 **Funkcijos**

08) Tachografas turi atlikti tokias funkcijas:

— stebėti kortelių įstatymo ir ištraukimo veiksmus,

— matuoti greitį ir atstumą ir nustatyti buvimo vietą,

— matuoti laiką (trukmę),

— stebėti vairuotojo veiklą,

— stebėti važiavimo būseną,

— leisti vairuotojui ranka įvesti tokius duomenis:

— vietų, kuriose prasideda ir (arba) baigiasi dienos darbo laikotarpiai, duomenis,

— duomenis apie vairuotojo veiklą,

— duomenis apie ypatingas būsenas,

— valdyti įmonės užraktus,

— stebėti kontrolės veiklą,

— aptikti įvykius ir (arba) triktis,

— atlikti 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,

— užmegzti nuotolinį ryšį, kad būtų galima atlikti tikslines patikras kelyje,

— persiųsti duomenis į papildomus įrenginius,

— kalibruoti,

— atlikti kalibravimo patikrą kelyje,

— koreguoti laiką.

2.3 **Veikimo režimai**

09) Tachografas turi veikti keturiais veikimo režimais:

— naudojimo režimu,

— kontrolės režimu,

— kalibravimo režimu,

— įmonės režimu.

10) Priklausomai nuo to, kokia galiojanti tachografo kortelė įstatoma į kortelių sąsajos įtaisą, tachografas turi persijungti į atitinkamą veikimo režimą, kaip nurodyta toliau. Nustatant veikimo režimą, nesvarbu, kurios kartos kortelė įstatoma į lizdą, jei ji yra galiojanti. Pirmosios kartos dirbtuvių kortelė visada laikoma negaliojančia, kai ji įstatoma į antrosios kartos transporto priemonės bloką.

▼B

Veikimo režimas		Vairuotojo kortelės lizdas				
		Kortelės nėra	Vairuotojo kortelė	Kontrolės kortelė	Dirbtuvių kortelė	Įmonės kortelė
Porininko kortelės lizdas	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 (*)

(*) Šiais atvejais tachografas naudoja tik į vairuotojo kortelės lizdą įstatytą kortelę.

11) Tachografas turi atmesti įstatytas negaliojančias korteles; galima tik pamatyti, išspausdinti ir perkelti informaciją iš kortelių, kurių galiojimo laikas pasibaigęs.

12) Visos 2.2 punkte išvardytos funkcijos turi veikti bet kuriuo veikimo režimu, išskyrus tokius atvejus:

— kalibravimo funkcija galima naudotis tik kalibravimo režimu,

— kalibravimo tikrinimo kelyje funkcija galima naudotis tik kontrolės režimu,

— įmonės užraktų valdymo funkcija galima naudotis tik įmonės režimu,

— kontrolės veiklos stebėjimo funkcija galima naudotis tik kontrolės režimu,

— duomenų perkėlimo funkcija neveikia naudojimo režimu (išskyrus 193 reikalavimo apraše nustatytus atvejus), išskyrus duomenų perkėlimą iš vairuotojo kortelės, kai į transporto priemonės bloką neįstatyta jokia kitos rūšies kortelė.

13) Tachografas turi gebėti parodyti duomenis ekrane, išvesti juos į spausdintuvą ar išorines sąsajas, išskyrus tokius atvejus:

— naudojimo režimu bet kokia įstatytos tachografo kortelės neatitinkanti asmens tapatybės informacija (pavardė ir vardas) užtamsinama, o įstatytos tachografo kortelės numerio neatitinkantis numeris užtamsinamas iš dalies (užtamsinamas kiekvienas nelyginis rašmuo skaičiuojant iš kairės į dešinę);

— įmonės režimu gali būti pateikti tik laikotarpių, kai nėra užrakto, vairuotojo duomenys (102, 105 ir 108 reikalavimai) arba tik kai jokia kita įmonė (identifikuojama pagal pirmuosius 13 įmonės kortelės numerio skaitmenų) neturi užrakto;

— kai į tachografą neįstatyta jokia kortelė, gali būti išvesti tik einamosios ir aštuonių ankstesnių kalendorinių dienų su vairuotoju susiję duomenys;

— asmens duomenys iš transporto priemonės bloko negali būti išvesti per jo ITS sąsają, nebent įsitikinama, kad vairuotojas, su kuriuo susiję duomenys, yra davęs sutikimą;

▼B

— transporto priemonės blokų įprasta naudojimo trukmė yra 15 metų, skaičiuojant nuo transporto priemonės bloko pažymėjimų išdavimo dienos, tačiau transporto priemonės blokus galima naudoti dar tris mėnesius – vien tik duomenims iš jų perkelti.

2.4 **Saugumas**

Sistemos apsaugos paskirtis – apsaugoti duomenų atmintį taip, kad būtų neįmanoma neteisėtai naudotis duomenimis bei juos klastoti, ir aptikti bet kokius mėginimus tai padaryti, saugoti duomenų, perduodamų tarp judesio jutiklio ir transporto priemonės bloko, tarp tachografo ir tachografo kortelių bei tarp tachografo ir išorinio GNNS įrenginio, nepažeistumą ir autentiškumą, taip pat saugoti duomenų, nuotolinio ankstyvo nustatymo ryšiu perduodamų kontrolei vykdyti, konfidencialumą, nepažeistumą ir autentiškumą ir tikrinti perkeliamų duomenų nepažeistumą ir autentiškumą.

14) Kad sistema būtų saugi, toliau nurodyti komponentai turi atitikti jų apsaugos profilių aprašuose nustatytus saugumo reikalavimus, kaip reikalaujama 10 priedėlyje:

— transporto priemonės blokas,

— tachografo kortelė,

— judesio jutiklis,

— išorinis GNSS įrenginys (šis profilis būtinas ir taikomas tik konfigūracijai su išoriniu GNSS įrenginiu).

3 TACHOGRAFO KONSTRUKCIJOS IR FUNKCINIAI REIKALAVIMAI

3.1 **Kortelės įstatymo ir ištraukimo stebėsena**

15) Tachografas turi stebėti kortelių sąsajos įtaisus ir registruoti kortelių įstatymo ir ištraukimo veiksmus.

16) Įstačius kortelę, tachografas turi nustatyti, ar įstatyta kortelė yra galiojanti, ir jei ji yra galiojanti – nustatyti, kokios rūšies ir kurios kartos kortelė įstatyta.

Kortelė pripažįstama negaliojančia, jei į tachografą anksčiau jau buvo įstatyta kortelė su tuo pačiu numeriu, kurios atnaujinimo indeksas didesnis.

Kortelė pripažįstama negaliojančia, jei į tachografą anksčiau jau buvo įstatyta kortelė su tuo pačiu numeriu ir atnaujinimo indeksu, kurios keitimo indeksas didesnis.

17) Pirmosios kartos tachografų korteles tachografas turi laikyti negaliojančiomis, jei dirbtuvės yra atsisakiusios galimybės naudoti pirmosios kartos tachografų korteles, vadovaudamosi 15 priedėliu (reik. MIG003).

18) Pirmosios kartos dirbtuvių kortelės, įstatytos į antrosios kartos tachografą, laikomos negaliojančiomis.

▼B

19) Tachografo konstrukcija turi būti tokia, kad tinkamai įstatyta į sąsajos įtaisą kortelė būtų užfiksuojama.

20) Tachografo kortelę turi būti įmanoma išimti tik transporto priemonei sustojus ir įrašius į jas reikiamus duomenis. Kortelę įmanoma išimti tik naudotojui atlikus konkretų veiksmą

3.2 **Greičio ir atstumo matavimas ir buvimo vietos nustatymas**

21) Pagrindinis nuvažiuoto atstumo ir greičio matavimo duomenų šaltinis yra judesio jutiklis (gali būti integruotas adapteryje).

22) Naudojant šią funkciją, pagal judesio jutiklio generuojamus impulsus nuolat matuojamas transporto priemonės nuvažiuotas atstumas ir pateikiamas odometro rodmuo.

23) Naudojant šią funkciją, pagal judesio jutiklio generuojamus impulsus nuolat matuojamas transporto priemonės greitis ir pateikiamas jo rodmuo.

24) Greičio matavimo funkcija taip pat teikia informaciją apie tai, ar transporto priemonė juda, ar stovi. Transporto priemonė laikoma judančia, jei bent 5 sekundes gaunamas didesnio kaip 1 imp/s dažnio signalas iš judesio jutiklio; priešingu atveju transporto priemonė laikoma stovinčia.

25) Bet kurioje transporto priemonėje, kurioje yra sumontuotas šio reglamento nuostatas atitinkantis tachografas, esantys greitį rodantys įtaisai (spidometrai) ir nuvažiuotą atstumą rodantys įtaisai (odometrai) turi atitikti reikalavimus dėl didžiausių leidžiamųjų paklaidų, nustatytų šiame priede (žr. 3.2.1 ir 3.2.2 punktus).

26) Siekiant nustatyti, ar neklastojami judėjimo duomenys, judesio jutiklio informacija turi būti patvirtinama pagal transporto priemonės judėjimo informaciją, gaunamą iš GNSS imtuvo arba (pasirinktinai) iš kito (-ų) nuo judesio jutiklio nepriklausomo (-ų) šaltinio (-ių).

27) Naudojant šią funkciją nustatoma transporto priemonės buvimo vieta, kad būtų galima automatiškai užregistruoti:

— vietą, kurioje prasideda vairuotojo ir (arba) vairuotojo poriniko dienos darbo laikotarpis;

— vietą, kurioje vairuotojo nepertraukiamo vairavimo trukmė pasiekia trijų valandų kartotinį;

— vietą, kurioje baigiasi vairuotojo ir (arba) vairuotojo poriniko dienos darbo laikotarpis.

3.2.1 *Nuvažiuoto atstumo matavimas*

28) Nuvažiuotas atstumas gali būti matuojamas:

— susumuojant į priekį ir atbulomis nuvažiuotą atstumą arba

— skaičiuojant tik į priekį nuvažiuotą atstumą.

29) Tachografas turi matuoti atstumą nuo 0 iki 9 999 999,9 km.

▼B

30) Atstumas matuojamas su tokia paklaida (ne mažesnis kaip 1 000 m atstumas):

— iki sumontavimo – ± 1 %,

— sumontavus ir atliekant periodines patikras – ± 2 %,

— naudojant – ± 4 %.

31) Atstumas turi būti matuojamas 0,1 km ar mažesnėmis atkarpomis.

3.2.2 *Greičio matavimas*

32) Tachografas turi matuoti 0–220 km/h greitį.

33) Siekiant užtikrinti, kad greitis būtų rodomas su ne didesne kaip ± 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 4 000–25 000 imp/km, tachografas turi matuoti 20–180 km/h greitį su ± 1 km/h paklaida (kai greitis pastovus).

Pastaba. Dėl duomenų laikymo įrangos tikslumo galima papildoma ± 0,5 km/h tachografo registruojamo greičio paklaida.

34) Greitis turi būti teisingai išmatuojamas su leidžiama paklaida ne vėliau kaip praėjus 2 sekundėms po greičio kitimo pabaigos, kai jis kinta ne didesne kaip 2 m/s^2 sparta.

35) Greitis turi būti matuojamas 1 km/h ar didesniu tikslumu.

3.2.3 *Buvimo vietos nustatymas*

36) Tachografu nustatoma absoliučioji transporto priemonės padėtis, naudojant GNSS imtuvą.

37) Absoliučioji padėtis nustatoma kaip geografinė platuma ir ilguma laipsniais ir minutėmis, 1/10 minutės tikslumu.

3.3 **Laiko matavimas**

38) Laikas turi būti matuojamas nuolat ir skaitmeniniu būdu parodoma data bei laikas pagal UTC.

39) Tachografo sistemoje (įrašuose, keičiantis duomenimis) duomenų ir visų 4 priedėlyje „Spaudiniai“ nurodytų spaudinių data turi būti registruojama pagal UTC laiką ir datą.

40) Vietos laikui nustatyti turi būti įmanoma pakeisti rodomą laiką pusės valandos žingsniu. Neleidžiama jokių kitų pakeitimų, išskyrus neigiamus arba teigiamus pusės valandos kartotinius.

41) Tipo patvirtinimo sąlygomis laiko matavimo paklaida gali būti ne didesnė kaip ±2 s per dieną, jei laikas nekoreguojamas.

▼B

42) Laikas turi būti matuojamas 1 sekundės ar didesniu tikslumu.

43) Tipo patvirtinimo sąlygomis laiko matavimo neturi sutrikdyti išorinio maitinimo nebuvimas trumpesnį kaip 12 mėnesių laikotarpį.

3.4 **Vairuotojo veiklos stebėsena**

44) Naudojant šią funkciją, nuolat stebima atskirai vieno vairuotojo ir vieno vairuotojo porininko veikla.

45) Vairuotojo veiklos rūšys yra tokios: VAIRAVIMAS, DARBAS, PASIRENGĘS DIRBTI ir PERTRAUKA / POILSIS.

46) Vairuotojas ir (arba) vairuotojo porininkas turi galėti rankiniu būdu pasirinkti veiklos rūšis DARBAS, PASIRENGĘS DIRBTI ir PERTRAUKA / POILSIS.

47) Kai transporto priemonė važiuoja, automatiškai parenkama vairuotojo veiklos rūšis VAIRAVIMAS, o vairuotojo porininko – PASIRENGĘS DIRBTI.

48) Kai transporto priemonė sustoja, automatiškai parenkama vairuotojo veiklos rūšis DARBAS.

49) Pirmasis veiklos pakeitimas į POILSĮ arba PASIRENGIMĄ DIRBTI ne vėliau kaip praėjus 120 sekundžių nuo automatinio pakeitimo į DARBĄ dėl to, kad transporto priemonė sustojo, laikomas įvykusiu transporto priemonei stovint (todėl pakeitimas į DARBO nustatymą gali būti atšaukiamas).

50) Ši funkcija turi teikti informaciją apie veiklos pasikeitimus registravimo funkcijoms vienos minutės tikslumu.

51) Jei kuriuo nors kalendorinės minutės momentu užregistruota, kad prieš pat tą minutę ir tuoj pat po jos vykdoma VAIRAVIMO veikla, visa ta minutė turi būti laikoma VAIRAVIMU.

52) Jei pagal 051 reikalavimą kalendorinė minutė nelaikoma VAIRAVIMU, visa ta minutė laikoma tos rūšies veikla, kuri tą minutę truko ilgiausiai (arba vėliausiąja iš vienodai trukusių veiklos rūšių).

53) Naudojant šią funkciją taip pat nuolat stebima vairuotojo nepertraukiamo vairavimo trukmė ir bendroji poilsio trukmė.

3.5 **Važiavimo būsenos stebėsena**

54) Naudojant šią funkciją nuolat automatiškai stebima važiavimo būsena.

55) Kai į tachografą įstatomos dvi galiojančios vairuotojo kortelės, turi būti parenkama ĮGULOS važiavimo būsena, o visais kitais atvejais – VIENO VAIRUOTOJO važiavimo būsena.

3.6 **Vairuotojo įvedami duomenys**

3.6.1 *Vietos, kurioje prasideda ir (arba) baigiasi dienos darbo laikotarpiai, duomenų įvedimas*

56) Naudojantis šia funkcija, galima įvesti vietos, kuriose, pasak vairuotojo ir (arba) vairuotojo porininko, prasideda ir (arba) baigiasi darbo dienos laikotarpiai, duomenis.

▼B

57) Vietos apibrėžiamos kaip šalis ir, jei reikia papildomai, regionas; jų duomenys įvedami arba patvirtinami rankiniu būdu.

58) Ištraukiant vairuotojo kortelę, tachografas turi pasiūlyti vairuotojui (porininkui) įrašyti vietą, kurioje baigėsi dienos darbo laikotarpis.

59) Vairuotojas turi įrašyti esamą transporto priemonės vietą, o šis įrašas laikomas laikinu.

60) Vietų, kuriose prasideda ir (arba) baigiasi dienos darbo laikotarpiai, duomenis įvesti turi būti įmanoma naudojantis meniu komandomis. Jei per vieną kalendorinę minutę atliekama daugiau negu viena tokia įvestis, per tą laiką registruojami tik paskutinės vietos, kurioje prasideda laikotarpis, ir paskutinės vietos, kurioje jis baigiasi, duomenys.

3.6.2 *Duomenų apie vairuotojo veiklą įvedimas rankiniu būdu ir vairuotojo sutikimas dėl ITS sąsajos*

61) Įstačius vairuotojo (arba dirbtuvių) kortelę (ir tik tuo metu) tachografas turi leisti rankiniu būdu įvesti veiklos duomenis. Rankiniu būdu įvedant veiklos duomenis nurodomas tos laiko zonos, kuri tuo metu nustatyta transporto priemonės bloke (UTC skirtumas), vietos laikas ir data.

Įstatant vairuotojo ar dirbtuvių kortelę, kortelės turėtojui primenama:

— paskutinio kortelės ištraukimo data ir laikas,

— (neprivaloma) tuo metu transporto priemonės bloke nustatytas vietos laiko skirtumas.

Pirmą kartą įstačius vairuotojo kortelę arba dirbtuvių kortelę, dar nežinomą transporto priemonės blokui, kortelės turėtojas turi būti paragintas duoti sutikimą dėl asmens duomenų, susijusių su tachografu, išvesties per neprivalomą ITS sąsają.

Bet kuriuo metu, kai vairuotojo (arba dirbtuvių) kortelė yra kortelės lizde, vairuotojo (arba dirbtuvių) sutikimą galima aktyvinti arba atšaukti naudojantis meniu komandomis.

Turi būti įmanoma įvesti veiklos duomenis su tokiais apribojimais:

— veiklos rūšis turi būti DARBAS, PASIRENGĘS DIRBTI arba PERTRAUKA / POILSIS,

— kiekvienos veiklos pradžios ir pabaigos laikas turi patekti į laikotarpį nuo paskutinio kortelės ištraukimo iki dabartinio įdėjimo,

— skirtingų rūšių veiklos laikas negali iš dalies sutapti.

Jei reikia, rankiniu būdu įvesti duomenis turi būti įmanoma pirmą kartą įstačius anksčiau nenaudotą vairuotojo (arba dirbtuvių) kortelę.

▼B

Veiklos duomenų įvedimo rankiniu būdu procedūra turi apimti tiek vienas po kito atliekamų veiksmų, kiek reikia kiekvienos veiklos rūšiai ir pradžios bei pabaigos laikui nustatyti. Kortelės turėtojas turi turėti galimybę nenurodyti jokios veiklos bet kurią laikotarpio nuo paskutinio kortelės ištraukimo iki dabartinio kortelės įdėjimo dalį.

Rankiniu būdu įvesdamas duomenis, kai įstatoma kortelė, kortelės turėtojas turi galimybę nurodyti:

— vietą, kurioje baigėsi ankstesnis dienos darbo laikotarpis, susijusią su atitinkamu laiku (taip pakeičiamas įrašas, padarytas paskutinį kartą ištraukiant kortelę),

— vietą, kurioje prasideda einamasis dienos darbo laikotarpis, susijusią su atitinkamu laiku.

Jei kortelės turėtojas nenurodo vietos, kurioje prasideda arba baigėsi dienos darbo laikotarpis, rankiniu būdu įvesdamas duomenis, kai įstatoma kortelė, laikoma, kad jo darbo laikotarpis nuo paskutinio kortelės ištraukimo nepasikeitė. Kitas vietos, kurioje baigėsi ankstesnis dienos darbo laikotarpis, įrašas pakeičia laikiną įrašą, padarytą paskutinį kartą ištraukiant kortelę.

Jei įvedami vietos duomenys, jie įrašomi susijusioje tachografo kortelėje.

Duomenų įvedimas rankiniu būdu nutraukiamas, jei:

— kortelė ištraukiama arba

— transporto priemonė juda, o kortelė yra vairuotojo kortelės lizde.

Be to, duomenų įvedimas rankiniu būdu gali būti nutrauktas, pavyzdžiui, po tam tikro laikotarpio, kurį naudotojas yra neaktyvus. Jei duomenų įvedimas rankiniu būdu nutraukiamas, tachografas patvirtina visus iki galo įvestus vietos ir veiklos duomenis (jei vieta ir laikas arba veiklos rūšis, pradžios ir pabaigos laikas yra aiškūs).

Jei antra vairuotojo ar dirbtuvių kortelė įstatoma tuo metu, kai rankiniu būdu įvedami anksčiau įstatytos kortelės veiklos duomenys, turi būti galima rankiniu būdu įvedamus tos ankstesnės kortelės duomenis įvesti iki galo ir tik tada pradėti antrosios kortelės duomenų įvedimą rankiniu būdu.

Kortelės turėtojas turi turėti galimybę įvesti duomenis rankiniu būdu, laikydamasis tokios minimalios procedūros:

— rankiniu būdu chronologine seka įvesti laikotarpio nuo paskutinio kortelės ištraukimo iki dabartinio įdėjimo veiklos duomenis.

— Pirmosios veiklos pradžios laikas yra kortelės ištraukimo laikas. Iš anksto nustatoma, kad kiekvieno vėlesnio įrašo pradžios laikas yra iškart po ankstesnio įrašo pabaigos laiko. Kiekvienai veiklai parenkama veiklos rūšis ir pabaigos laikas.

▼B

Procedūra užbaigiama, kai rankiniu būdu įvestos veiklos pabaigos laikas sutampa su kortelės įdėjimo laiku. Tada tachografas gali leisti kortelės turėtojui keisti bet kokius rankiniu būdu įvestus veiklos duomenis, kol neatliekamas patvirtinimas pasirenkant specialią komandą. Vėliau toks pakeitimas draudžiamas.

3.6.3 *Informacijos apie ypatingas būsenas įvedimas*

62) Tachografas turi leisti vairuotojui tikruoju laiku įvesti informaciją apie tokias dvi ypatingas būsenas:

— NEKONTROLIUOJAMA (pradžia, pabaiga)

— KĖLIMAS KELTU / VEŽIMAS TRAUKINIU (pradžia, pabaiga).

Pasirinkus būseną NEKONTROLIUOJAMA, būsenos KĖLIMAS KELTU / VEŽIMAS TRAUKINIU pasirinkti negalima.

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

Pasirinkus būseną NEKONTROLIUOJAMA negalima:

— važiuoti be reikiamos kortelės;

— rodyti perspėjimus, susijusius su nepertraukiamo vairavimo trukme.

Būsenos KĖLIMAS KELTU / VEŽIMAS TRAUKINIU pradžia nustatoma prieš išjungiant variklį kelte / traukinyje.

Būsena KĖLIMAS KELTU / VEŽIMAS TRAUKINIU baigiasi, kai:

— vairuotojas rankiniu būdu nustato būsenos KĖLIMAS KELTU / VEŽIMAS TRAUKINIU pabaigą;

— vairuotojas ištraukia kortelę.

Būsena KĖLIMAS KELTU / VEŽIMAS TRAUKINIU baigiasi, kai ji nustoja galioti pagal taisykles, nustatytas Reglamente (EB) Nr. 561/2006.

3.7 **Įmonės užraktų valdymas**

63) Naudojant šią funkciją galima valdyti užraktus, kuriuos įmonė nustato, kad įmonės režimu prieiti prie duomenų leistų tik sau.

64) Įmonės užraktus sudaro pradžios data / laikas (užrakinimas) ir pabaigos data / laikas (atrakinimas), susieti su įmonės identifikacija pagal įmonės kortelės numerį (užrakinant).

65) Užraktus galima užrakinti ir atrakinti tik tikruoju laiku.

66) Atrakinti užraktą gali tik ta įmonė, kuri jį užrakino (identifikuojama pagal pirmuosius 13 įmonės kortelės rašmenų), arba

67) kitai įmonei užrakinus savo užraktą, ankstesnės įmonės užraktas turi būti automatiškai atrakinamas.

▼B

68) Jei įmonė užrakina naują užraktą, o ankstesnis užraktas buvo tos pačios įmonės, tuomet daroma prielaida, kad ankstesnis užraktas nebuvo atrakintas, ir jis lieka užrakintas.

3.8 **Kontrolės veiklos stebėsena**

69) Naudojantis šia funkcija stebima RODYMO EKRANE, SPAUSDINIMO, transporto priemonės bloko ir kortelės DUOMENŲ PERKĖLIMO ir KALIBRAVIMO TIKRINIMO KELYJE veikla kontrolės režimu.

70) Naudojantis šia funkcija taip pat stebima GREIČIO VIRŠIJIMO KONTROLĖS veikla kontrolės režimu. Laikoma, kad įvykdyta greičio viršijimo kontrolė, kai tachografui veikiant kontrolės režimu į spausdintuvą arba ekraną perduodamas greičio viršijimo pranešimas arba iš transporto priemonės bloko atminties perkeliami duomenys apie įvykius ir triktis.

3.9 **Įvykių ir (arba) trikčių aptikimas**

71) Naudojantis šia funkcija aptinkami toliau nurodyti įvykiai ir (arba) triktys.

3.9.1 *„Įstatyta negaliojanti kortelė“*

72) Šis įvykis užfiksuojamas įstačius bet kokią negaliojančią kortelę, jau pakeistą vairuotojo kortelę ir (arba) pasibaigus įstatytos kortelės galiojimo laikui.

3.9.2 *„Kortelių nesuderinamumo“ įvykis*

73) Šis įvykis užfiksuojamas, kai kartu įstatomos dvi galiojančios kortelės, kurių derinys toliau esančioje lentelėje pažymėtas X.

Kortelių nesuderinamumas		Vairuotojo kortelės lizdas				
		Kortelės nėra	Vairuotojo kortelė	Kontrolės kortelė	Dirbtuvių kortelė	Įmonės kortelė
Porininko kortelės lizdas	Kortelės nėra					
	Vairuotojo kortelė				X	
	Kontrolės kortelė			X	X	X
	Dirbtuvių kortelė		X	X	X	X
	Įmonės kortelė			X	X	X

3.9.3 *„Dalinio laiko sutapimo“ įvykis*

74) Šis įvykis užfiksuojamas, kai vairuotojo kortelės paskutinio ištraukimo data ir laikas, užfiksuoti kortelės atmintyje, yra vėlesni už tachografo, į kurį kortelė įstatyta, rodomą datą ir laiką.

3.9.4 *„Važiavimo be reikiamos kortelės“ įvykis*

75) Šis įvykis užfiksuojamas, kai kartu įstatomos dvi kortelės, kurių derinys toliau esančioje lentelėje pažymėtas X, ir kai vairuotojo veiklos rūšis pasikeičia į VAIRAVIMĄ arba kai esant vairuotojo veiklai VAIRAVIMAS pasikeičia veikimo režimas.

▼B

Važiavimas be reikiamos kortelės		Vairuotojo kortelės lizdas				
		Kortelės nėra (arba ji yra negaliojanti)	Vairuotojo kortelė	Kontrolės kortelė	Dirbtuvių kortelė	Įmonės kortelė
Porininko kortelės lizdas	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

3.9.5 *„Kortelė įstatyta važiuojant“*

76) Šis įvykis užfiksuojamas, jei į kurį nors lizdą įstatoma tachografo kortelė, kai vairuotojo veikla yra VAIRAVIMAS.

3.9.6 *„Netinkamai užbaigtas paskutinis kortelės naudojimo seansas“*

77) Šis įvykis užfiksuojamas, kai įstačius kortelę į lizdą tachografas nustato, kad, nepaisant 3.1 punkto nuostatų, ankstesnis kortelės naudojimo seansas užbaigtas netinkamai (kortelė ištraukta nebaigus į ją įrašyti visų reikiamų duomenų). Šis įvykis fiksuojamas tik vairuotojo ir dirbtuvių kortelėse.

3.9.7 *„Greičio viršijimo“ įvykis*

78) Šis įvykis užfiksuojamas kaskart, kai viršijamas greitis.

3.9.8 *„Maitinimo nutrūkimo“ įvykis*

79) Šis įvykis užfiksuojamas tachografui veikiant ne kalibravimo arba kontrolės režimu, jei judesio jutiklio ir (arba) transporto priemonės bloko maitinimas nutrūksta ilgesniam kaip 200 milisekundžių laikotarpiui. Maitinimo nutrūkimo trukmės slenkstinę vertę nustato gamintojas. Šis įvykis neturi būti fiksuojamas dėl įtampos kritimo užvedant variklį.

3.9.9. *„Ryšio su nuotolinio ryšio įrenginiu klaida“*

80) Šis įvykis užfiksuojamas **tachografui veikiant ne kalibravimo režimu**, kai nuotolinio ryšio įrenginys nepatvirtina sėkmingai gavęs iš transporto priemonės bloko išsiųstus nuotolinio ryšio duomenis, atlikus daugiau kaip tris šių duomenų siuntimo bandymus.

3.9.10. *„Iš GNSS imtuvo negauta informacijos apie buvimo vietą“*

81) Šis įvykis užfiksuojamas **tachografui veikiant ne kalibravimo režimu**, kai iš GNSS imtuvo (vidinio ar išorinio) ilgiau kaip tris bendros vairavimo trukmės valandas negaunama informacijos apie buvimo vietą.

3.9.11. *„Ryšio su išoriniu GNSS įrenginiu klaida“*

82) Šis įvykis užfiksuojamas **tachografui veikiant ne kalibravimo režimu**, kai, transporto priemonei važiuojant, ryšys tarp išorinio GNSS įrenginio ir transporto priemonės bloko nutrūksta ilgesniam nei 20 minučių laikotarpiui.

▼B

3.9.12. *„Duomenų apie judėjimą klaida“*

83) Šis įvykis užfiksuojamas **tachografui veikiant ne kalibravimo režimu**, kai nutrūksta įprastas duomenų srautas tarp judesio jutiklio ir transporto priemonės bloko ir (arba) įvyksta duomenų nepažeistumo arba autentiškumo tikrinimo klaida keičiantis duomenimis tarp judesio jutiklio ir transporto priemonės bloko.

3.9.13. *„Transporto priemonės judėjimo nesuderinamumo“ įvykis*

84) Šis įvykis užfiksuojamas **tachografui veikiant ne kalibravimo režimu**, kai nesutampa judėjimo jutiklio informacija apie judėjimą ir vidinio GNSS imtuvo ar išorinio GNSS įrenginio arba kitų autonominių šaltinių informacija apie judėjimą, kaip nustatyta 12 priedėlyje. Šis įvykis nefiksuojamas, kai transporto priemonė keliama keltu arba vežama traukiniu, kai parinkta būsena NEKONTROLIUOJAMA arba kai iš GNSS imtuvo negaunama informacijos apie buvimo vietą.

3.9.14. *„Bandymo pažeisti apsaugą“ įvykis*

85) Šis įvykis užfiksuojamas tachografui veikiant ne kalibravimo režimu, kai įvyksta bet koks kitas įvykis, darantis poveikį judesio jutiklio, transporto priemonės bloko ir (arba) išorinio GNSS įrenginio saugumui, kurio reikalavimai nustatyti 10 priedėlyje.

3.9.15. *„Nesuderinto laiko“ įvykis*

86) Šis įvykis užfiksuojamas **tachografui veikiant ne kalibravimo režimu**, kai transporto priemonės blokas aptinka didesnį nei 1 minutės transporto priemonės bloko nustatyto laiko ir GNSS imtuvo laiko neatitikimą. Šis įvykis fiksuojamas kartu su transporto priemonės bloko vidinio laikrodžio rodmeniu ir atliekamas automatinis laiko koregavimas. Užfiksavęs nesuderinto laiko įvykį, transporto priemonės blokas nefiksuoja kitų nesuderinto laiko įvykių per kitas 12 valandų. Šis įvykis nefiksuojamas, jei per pastarąsias 30 dienų GNSS imtuvas neaptiko galiojančio GNSS signalo. Tačiau, jeigu iš GNSS imtuvo vėl gaunama informacija apie buvimo vietą, atliekamas automatinis laiko koregavimas.

3.9.16. *Kortelės triktis*

87) Ši triktis užfiksuojama, kai naudojama tachografo kortelė sugenda.

3.9.17. *Tachografo triktis*

88) Ši triktis užfiksuojama, kai tachografui veikiant ne kalibravimo režimu įvyksta bet kuri iš šių trikčių:

— transporto priemonės bloko vidinė triktis,

— spausdintuvo triktis,

— ekrano triktis,

— duomenų perkėlimo triktis,

— jutiklio triktis,

— GNSS imtuvo ar išorinio GNSS įrenginio triktis,

— nuotolinio ryšio įrenginio triktis.

▼B

3.10 **Savidiagnostika ir savitikra**

89) Tachografas turi pats aptikti triktis atlikdamas savidiagnostiką ir savitikrą, kaip nurodyta lentelėje.

Tikrinamas mazgas	Savitikra	Savidiagnostika
Programinė įranga		Vientisumas
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
Nuotolinio ryšio įrenginys	Tinkamas veikimas	Tinkamas veikimas
GNSS įrenginys	Tinkamas veikimas	Tinkamas veikimas

3.11 **Atmintyje laikomų duomenų nuskaitymas**

90) Tachografas turi gebėti nuskaityti bet kokius savo duomenų atmintyje laikomus duomenis.

3.12 **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 vairuotojo porininkus, šešis kortelių įstatymo ir ištraukimo ciklus ir 256 veiklos rūšies pasikeitimus. Taigi 365 dienos apima informaciją ne mažiau kaip apie 2 190 vairuotojų (porininkų), 2 190 kortelių įstatymo ir ištraukimo ciklų ir 93 440 veiklos rūšių pasikeitimų;

— vidutinis buvimo vietų skaičius per dieną yra ne mažiau kaip šešios buvimo vietos, kuriose prasideda dienos darbo laikotarpis, šešios buvimo vietos, kuriose vairuotojo nepertraukiamo vairavimo trukmė pasiekia trijų valandų kartotinį, ir šešios buvimo vietos, kuriose baigiasi dienos darbo laikotarpis, tad 365 dienos apima ne mažiau kaip 6 570 buvimo vietų;

— jei nenurodyta kitaip, laikas registruojamas vienos minutės tikslumu;

— odometro rodmens vertės registruojamos vieno kilometro tikslumu;

— greitis registruojamas 1 km/h tikslumu;

— buvimo vieta (platuma ir ilguma) registruojama laipsniais ir minutėmis, 1/10 minutės tikslumu, atitinkamu GNSS tikslumu ir gavimo laiku.

▼B

91) Duomenų atmintyje laikomiems duomenims tipo patvirtinimo sąlygomis neturi pakenkti išorinio maitinimo nebuvimas trumpiau nei 12 mėnesių. Be to, 14 priedėlyje apibrėžtame išoriniame nuotolinio ryšio įrenginyje laikomiems duomenims neturi pakenkti išorinio maitinimo nebuvimas trumpiau nei 28 dienas.

92) Tachografo duomenų atmintyje turi būti galima netiesiogiai arba tiesiogiai registruoti toliau nurodytą informaciją.

3.12.1 *Įrangos identifikavimo duomenys*

3.12.1.1 Transporto priemonės bloko identifikavimo duomenys

93) Tachografo duomenų atmintyje laikomi tokie transporto priemonės bloko identifikavimo duomenys:

— gamintojo pavadinimas,

— gamintojo adresas,

— komponento šifras,

— serijos numeris,

— transporto priemonės bloko karta,

— informacija apie galimybę naudoti pirmosios kartos tachografo korteles,

— programinės įrangos versijos numeris,

— programinės įrangos įdiegimo data,

— įrangos pagaminimo metai,

— patvirtinimo numeris.

94) Transporto priemonės bloko gamintojas visam laikui įrašo transporto priemonės bloko identifikavimo duomenis, išskyrus programinės įrangos duomenis ir patvirtinimo numerį, kurie gali keistis atnaujinant programinę įrangą, ir informaciją apie galimybę naudoti pirmosios kartos tachografo korteles.

3.12.1.2 Judesio jutiklio identifikavimo duomenys

95) Judesio jutiklio atmintyje laikomi tokie identifikavimo duomenys:

— gamintojo pavadinimas,

— serijos numeris,

— patvirtinimo numeris,

— įterptojo apsaugos komponento identifikatorius (pvz., vidinės mikroschemos (mikroprocesoriaus) komponento šifras),

— operacinės sistemos identifikatorius (pvz., programinės įrangos versijos numeris).

96) Judesio jutiklio identifikavimo duomenis jame visam laikui įrašo judesio jutiklio gamintojas.

97) Transporto priemonės bloko duomenų atmintyje turi būti galima registruoti ir laikyti toliau nurodytus 20 naujausių siejimo su judesio jutikliais atvejų duomenis (jei per vieną kalendorinę dieną siejama keletą kartą, išsaugomi tik pirmojo ir paskutinio siejimo tą dieną duomenys).

▼B

Turi būti registruojami tokie kiekvieno tokio siejimo duomenys:

— judesio jutiklio identifikavimo duomenys:

— serijos numeris,

— patvirtinimo numeris;

— judesio jutiklio siejimo duomenys:

— siejimo data.

3.12.1.3 Pasaulinės palydovinės navigacijos sistemos identifikavimo duomenys

98) Išorinio GNSS įrenginio atmintyje laikomi tokie identifikavimo duomenys:

— gamintojo pavadinimas,

— serijos numeris,

— patvirtinimo numeris,

— įterptojo apsaugos komponento identifikatorius (pvz., vidinės mikroschemos (mikroprocesoriaus) komponento šifras),

— operacinės sistemos identifikatorius (pvz., programinės įrangos versijos numeris).

99) Išorinio GNSS įrenginio identifikavimo duomenis jame visam laikui įrašo išorinio GNSS įrenginio gamintojas.

100) Transporto priemonės bloko duomenų atmintyje turi būti galima registruoti ir laikyti toliau nurodytus 20 naujausių jungimo su išoriniais GNSS įrenginiais atvejų duomenis (jei per vieną kalendorinę dieną jungiama keletą kartą, išsaugomi tik pirmojo ir paskutinio jungimo tą dieną duomenys).

Turi būti registruojami tokie kiekvieno tokio jungimo duomenys:

— išorinio GNSS įrenginio identifikavimo duomenys:

— serijos numeris,

— patvirtinimo numeris;

— išorinio GNSS įrenginio jungimo duomenys:

— jungimo data.

3.12.2 *Raktai ir pažymėjimai*

101) Tachografe turi būti galima laikyti tiek kriptografinių raktų ir pažymėjimų, kiek nurodyta 11 priedėlio A ir B dalyse.

3.12.3 *Duomenys apie vairuotojo arba dirbtuvių kortelės įstatymą ir ištraukimą*

102) Tachografo duomenų atmintyje užregistruojami ir laikomi tokie vairuotojo arba dirbtuvių kortelės kiekvieno įstatymo ir ištraukimo ciklo duomenys:

— kortelės turėtojo pavardė ir vardas (-ai), įrašyti kortelės atmintyje,

— kortelės numeris, ją išdavusi valstybė narė ir kortelės galiojimo pabaigos data, įrašyti kortelės atmintyje,

— kortelės karta,

▼B

— įkišimo data ir laikas,

— transporto priemonės odometro rodmens vertė įstatant kortelę,

— lizdas, į kurį įstatyta kortelė,

— ištraukimo data ir laikas,

— transporto priemonės odometro rodmens vertė ištraukiant kortelę,

— tokia kortelės atmintyje įrašyta informacija apie transporto priemonę, kuria anksčiau naudojosi vairuotojas:

— transporto priemonės registracijos numeris ir registracijos valstybė narė,

— transporto priemonės bloko karta (jei žinoma),

— kortelės ištraukimo data ir laikas,

— ženklas, rodantis, ar įstatęs kortelę jos turėtojas rankiniu būdu įvedė veiklos rūšis, ar ne.

103) Duomenų atmintyje šie duomenys saugomi ne trumpiau kaip 365 dienas.

104) Kai atmintinės talpa išnaudojama, nauji duomenys rašomi ant seniausiųjų įrašų.

3.12.4 *Duomenys apie vairuotojo veiklą*

105) Pasikeitus vairuotojo ir (arba) vairuotojo porininko veiklai ir (arba) važiavimo būsenai ir (arba) įstačius arba ištraukus vairuotojo arba dirbtuvių kortelę, tachografo duomenų atmintyje užregistruojami ir laikomi tokie duomenys:

— važiavimo būsena (ĮGULA, VIENAS VAIRUOTOJAS),

— kortelės lizdas (VAIRUOTOJO, VAIRUOTOJO PORININKO),

— kortelės būsena atitinkamame lizde (ĮSTATYTA, NEĮSTATYTA),

— veiklos rūšis (VAIRAVIMAS, PASIRENGĘS DIRBTI, DARBAS, PERTRAUKA / POILSIS),

— pasikeitimo data ir laikas.

ĮSTATYTA reiškia, kad į lizdą įstatyta galiojanti vairuotojo ar dirbtuvių kortelė. NEĮSTATYTA, priešingai, reiškia, kad į lizdą neįstatyta galiojanti vairuotojo ar dirbtuvių kortelė (pvz., įstatyta įmonės kortelė arba neįstatyta jokia kortelė).

Vairuotojo rankiniu būdu įvesta informacija apie veiklą duomenų atmintyje neregistruojama.

106) Duomenų atmintyje duomenys apie vairuotojo veiklą saugomi ne trumpiau kaip 365 dienas.

107) Kai atmintinės talpa išnaudojama, nauji duomenys rašomi ant seniausiųjų įrašų.

▼B

3.12.5 *Vietos, kur prasideda ir baigiasi dienos darbo laikotarpiai ir (arba) nepertraukiamo vairavimo trukmė pasiekia 3 valandas*

108) Tachografo duomenų atmintyje užregistruojami ir laikomi tokie duomenys:

— buvimo vieta, kurioje prasideda vairuotojo ir (arba) vairuotojo porininko dienos darbo laikotarpis;

— buvimo vieta, kurioje vairuotojo nepertraukiamo vairavimo trukmė pasiekia trijų valandų kartotinį;

— buvimo vieta, kurioje baigiasi vairuotojo ir (arba) vairuotojo porininko dienos darbo laikotarpis.

109) Jei tuo metu negaunama transporto priemonės buvimo vietos duomenų iš GNSS imtuvo, tachografas turi naudoti naujausius turimus buvimo vietos duomenis ir su jais susijusius datos ir laiko duomenis.

110) Kartu su kiekvienos buvimo vietos duomenimis tachografo duomenų atmintyje užregistruojami ir laikomi tokie duomenys:

— vairuotojo (porininko) kortelės numeris ir ją išdavusi valstybė narė,

— kortelės karta,

— įrašo data ir laikas,

— įrašo rūšis (pradžia, pabaiga arba 3 valandų nepertraukiamo vairavimo trukmė),

— atitinkamos GNSS tikslumas, data ir laikas, kai tinkama,

— transporto priemonės odometro rodmens vertė.

111) Duomenų atmintyje buvimo vietos, kurioje prasideda ir baigiasi dienos darbo laikotarpiai ir (arba) nepertraukiamo vairavimo trukmė pasiekia 3 valandas, duomenis turi būti galima saugoti ne trumpiau kaip 365 dienas.

112) Kai atmintinės talpa išnaudojama, nauji duomenys rašomi ant seniausiųjų įrašų.

3.12.6 *Odometro duomenys*

113) Tachografo duomenų atmintyje užregistruojama transporto priemonės odometro rodmens vertė ir data kiekvienos kalendorinės dienos vidurnaktį.

114) Duomenų atmintyje odometro vidurnakčio rodmens vertes turi būti galima išlaikyti ne trumpiau kaip 365 dienas.

115) Kai atmintinės talpa išnaudojama, nauji duomenys rašomi ant seniausiųjų įrašų.

3.12.7 *Išsamūs duomenys apie greitį*

116) Tachografo duomenų atmintyje užregistruojama ir laikoma ne mažiau kaip paskutinių 24 valandų transporto priemonės judėjimo informacija apie momentinį transporto priemonės greitį kiekvieną sekundę ir atitinkama data bei laikas.

3.12.8 *Duomenys apie įvykius*

Šioje poskyryje nurodytais tikslais laikas registruojamas vienos sekundės tikslumu.

117) Tachografo duomenų atmintyje užregistruojami ir laikomi toliau nurodyti duomenys apie kiekvieną aptiktą įvykį pagal atitinkamas duomenų laikymo taisykles.

▼B

Įvykis	Duomenų laikymo taisyklės	Užregistruojami duomenys apie kiekvieną įvykį
Įstatyta negaliojanti kortelė	— 10 paskutinių įvykių	— Įvykio data ir laikas — Įvykį sukėlusios kortelės rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Panašių įvykių tą dieną skaičius
Kortelių nesuderinamumas	— 10 paskutinių įvykių	— Įvykio pradžios data ir laikas — Įvykio pabaigos data ir laikas — Abiejų nesuderinamų kortelių rūšis, numeriai, jas išdavusi valstybė narė ir kortelės karta
Važiavimas be reikiamos kortelės	— Ilgiausiai trukęs įvykis per kiekvieną iš paskutinių 10 dienų, kuriomis jis įvyko — Penki ilgiausiai trukę įvykiai per paskutines 365 dienas	— Įvykio pradžios data ir laikas — Įvykio pabaigos data ir laikas — Kortelės, kuri buvo kortelės lizde įvykio pradžioje ir (arba) pabaigoje, rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Panašių įvykių tą dieną skaičius
Kortelė įstatyta važiuojant	— Paskutinis įvykis per kiekvieną iš paskutinių 10 dienų, kuriomis jis įvyko	— Įvykio data ir laikas — Kortelės rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Panašių įvykių tą dieną skaičius
Netinkamai užbaigtas paskutinis kortelės naudojimo seansas	— 10 paskutinių įvykių	— Kortelės įstatymo data ir laikas — Kortelės rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Paskutiniai iš kortelės nuskaityti seanso duomenys: — Kortelės įstatymo data ir laikas — Transporto priemonės registracijos numeris, registracijos valstybė narė ir transporto priemonės bloko karta
Greičio viršijimas (1)	— Svarbiausias įvykis per kiekvieną iš paskutinių 10 dienų, kuriomis jis įvyko (t. y. įvykis, kai greitis viršytas daugiausiai) — Penki svarbiausi įvykiai per paskutines 365 dienas — Pirmasis po paskutinio kalibravimo įvykęs įvykis	— Įvykio pradžios data ir laikas — Įvykio pabaigos data ir laikas — Didžiausias įvykio metu išmatuotas greitis — Įvykio metu išmatuoto greičio aritmetinis vidurkis — Vairuotojo kortelės rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta (kai tinkama) — Panašių įvykių tą dieną skaičius

▼B

Įvykis	Duomenų laikymo taisyklės	Užregistruojami duomenys apie kiekvieną įvykį
Maitinimo nutrūkimas (2)	— Ilgiausiai trukęs įvykis per kiekvieną iš paskutinių 10 dienų, kuriomis jis įvyko — Penki ilgiausiai trukę įvykiai per paskutines 365 dienas	— Įvykio pradžios data ir laikas — Įvykio pabaigos data ir laikas — Kortelės, kuri buvo kortelės lizde įvykio pradžioje ir (arba) pabaigoje, rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Panašių įvykių tą dieną skaičius
Ryšio su nuotolinio ryšio įrenginiu klaida	— Ilgiausiai trukęs įvykis per kiekvieną iš paskutinių 10 dienų, kuriomis jis įvyko — Penki ilgiausiai trukę įvykiai per paskutines 365 dienas	— Įvykio pradžios data ir laikas — Įvykio pabaigos data ir laikas — Kortelės, kuri buvo kortelės lizde įvykio pradžioje ir (arba) pabaigoje, rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Panašių įvykių tą dieną skaičius
Iš GNSS imtuvo negauta informacijos apie buvimo vietą	— Ilgiausiai trukęs įvykis per kiekvieną iš paskutinių 10 dienų, kuriomis jis įvyko — Penki ilgiausiai trukę įvykiai per paskutines 365 dienas	— Įvykio pradžios data ir laikas — Įvykio pabaigos data ir laikas — Kortelės, kuri buvo kortelės lizde įvykio pradžioje ir (arba) pabaigoje, rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Panašių įvykių tą dieną skaičius
Duomenų apie judėjimą klaida	— Ilgiausiai trukęs įvykis per kiekvieną iš paskutinių 10 dienų, kuriomis jis įvyko — Penki ilgiausiai trukę įvykiai per paskutines 365 dienas	— Įvykio pradžios data ir laikas — Įvykio pabaigos data ir laikas — Kortelės, kuri buvo kortelės lizde įvykio pradžioje ir (arba) pabaigoje, rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Panašių įvykių tą dieną skaičius
Transporto priemonės judėjimo nesuderinamumas	— Ilgiausiai trukęs įvykis per kiekvieną iš paskutinių 10 dienų, kuriomis jis įvyko — Penki ilgiausiai trukę įvykiai per paskutines 365 dienas	— Įvykio pradžios data ir laikas — Įvykio pabaigos data ir laikas — Kortelės, kuri buvo kortelės lizde įvykio pradžioje ir (arba) pabaigoje, rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — 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) — Kortelės, kuri buvo kortelės lizde įvykio pradžioje ir (arba) pabaigoje, rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Įvykio rūšis

▼B

Įvykis	Duomenų laikymo taisyklės	Užregistruojami duomenys apie kiekvieną įvykį
Nesuderintas laikas	— Ilgiausiai trukęs įvykis per kiekvieną iš paskutinių 10 dienų, kuriomis jis įvyko — Penki ilgiausiai trukę įvykiai per paskutines 365 dienas	— Tachografo data ir laikas — GNSS data ir laikas — Kortelės, kuri buvo kortelės lizde įvykio pradžioje ir (arba) pabaigoje, rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Panašių įvykių tą dieną skaičius

(1) Tachografo duomenų atmintyje užregistruojami ir laikomi tokie duomenys:

— paskutinės GREIČIO VIRŠIJIMO KONTROLĖS data ir laikas,

— pirmojo greičio viršijimo po tos GREIČIO VIRŠIJIMO KONTROLĖS data ir laikas,

— greičio viršijimo įvykių po paskutinės GREIČIO VIRŠIJIMO KONTROLĖS skaičius.

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

3.12.9 *Duomenys apie triktis*

Šiame poskyryje nurodytais tikslais laikas registruojamas vienos sekundės tikslumu.

118) Tachografo duomenų atmintyje užregistruojami ir laikomi toliau nurodyti duomenys apie kiekvieną aptiktą triktį pagal atitinkamas duomenų laikymo taisykles.

Triktis	Duomenų laikymo taisyklės	Užregistruojami duomenys apie kiekvieną triktį
Kortelės triktis	— 10 paskutinių vairuotojo kortelės trikčių	— Trikties pradžios data ir laikas — Trikties pabaigos data ir laikas — Kortelės rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta
Tachografo triktys	— 10 paskutinių kiekvienos rūšies trikčių — Pirmoji triktis po paskutinio kalibravimo	— Trikties pradžios data ir laikas — Trikties pabaigos data ir laikas — Trikties rūšis — Kortelės, kuri buvo kortelės lizde, kai įvyko ir (arba) baigėsi triktis, rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta

3.12.10 *Duomenys apie kalibravimą*

119) Tachografo duomenų atmintyje užregistruojami ir laikomi tokie duomenys:

— žinomi kalibravimo parametrai aktyvinimo momentu,

▼B

— pats pirmasis kalibravimas po aktyvinimo,

— pats pirmasis kalibravimas šioje transporto priemonėje (identifikuojamoje pagal jos VIN),

— 20 paskutinių kalibravimo atvejų (jei per vieną kalendorinę dieną kalibruojama kelis kartus, užregistruojami duomenys tik apie paskutinį kalibravimą).

120) Registruojami tokie kiekvieno kalibravimo duomenys:

— kalibravimo tikslas (aktyvinimas, pirmasis įrengimas, įrengimas, periodinė patikra),

— dirbtuvių pavadinimas ir adresas,

— dirbtuvių kortelės numeris, kortelę išdavusi valstybė narė ir kortelės galiojimo pabaigos data,

— transporto priemonės identifikacija,

— atnaujinti arba patvirtinti parametrai (w, k, l, padangų dydis, greičio ribotuvo nuostatis, odometro rodmenys (sena ir nauja vertės), data ir laikas (sena ir nauja vertės),

— visų uždėtų plombų rūšys ir identifikatoriai.

121) Be to, tachografo duomenų atmintyje užregistruojama ir laikoma informacija apie tai, ar jame galima naudoti pirmosios kartos tachografo korteles (ar ši galimybė aktyvinta, ar ne).

122) Judesio jutiklio atmintyje registruojami ir laikomi tokie duomenys apie judesio jutiklio įrengimą:

— pirmasis susiejimas su transporto priemonės bloku (data, laikas, transporto priemonės bloko patvirtinimo numeris, serijos numeris),

— paskutinis susiejimas su transporto priemonės bloku (data, laikas, transporto priemonės bloko patvirtinimo numeris, serijos numeris).

123) Išorinio GNSS įrenginio atmintyje registruojami ir laikomi tokie duomenys apie jo įrengimą:

— pirmasis sujungimas su transporto priemonės bloku (data, laikas, transporto priemonės bloko patvirtinimo numeris, serijos numeris),

— paskutinis sujungimas su transporto priemonės bloku (data, laikas, transporto priemonės bloko patvirtinimo numeris, serijos numeris).

3.12.11 *Duomenys apie laiko koregavimą*

124) Tachografo duomenų atmintyje užregistruojami ir laikomi duomenys apie laiko koregavimą, atliktą kalibravimo režimu neįprasto kalibravimo metu (f apibrėžtis):

— paskutinis laiko koregavimas,

— paskutiniai penki atvejai, kai laikas pakoreguotas daugiausiai.

125) Turi būti registruojami tokie duomenys apie kiekvieną laiko koregavimą:

— data ir laikas, senoji vertė,

— data ir laikas, naujoji vertė,

— dirbtuvių pavadinimas ir adresas,

— dirbtuvių kortelės numeris, kortelę išdavusi valstybė narė, kortelės karta ir kortelės galiojimo pabaigos data.

▼B

3.12.12 *Duomenys apie kontrolės veiklą*

126) Tachografo duomenų atmintyje užregistruojami ir laikomi tokie duomenys apie 20 pastarųjų kontrolės veiklos atvejų:

— kontrolės data ir laikas,

— kontrolės kortelės numeris, kortelę išdavusi valstybė narė ir kortelės karta,

— kontrolės rūšis (rodymas ekrane, spausdinimas, duomenų perkėlimas iš transporto priemonės bloko, duomenų perkėlimas iš kortelės ir (arba) kalibravimo tikrinimas kelyje).

127) Jei perkeliami duomenys, turi būti užregistruojamos pirmosios ir paskutinės dienų, kurių duomenys perkeliami, datos.

3.12.13 *Duomenys apie įmonės užraktus*

128) Tachografo duomenų atmintyje užregistruojami ir laikomi tokie duomenys apie 255 pastaruosius įmonės užraktus:

— užrakinimo data ir laikas,

— atrakinimo data ir laikas,

— įmonės kortelės numeris, kortelę išdavusi valstybė narė ir kortelės karta,

— įmonės pavadinimas ir adresas.

Duomenys, kurie buvo anksčiau užrakinti užraktu, kuris pašalintas iš atminties dėl minėto limito, laikomi neužrakintais.

3.12.14 *Duomenys apie duomenų perkėlimo veiklą*

129) Tachografo duomenų atmintyje užregistruojami ir laikomi tokie duomenys apie duomenų iš atminties perkėlimą į išorines laikmenas įmonės arba kalibravimo režimu:

— duomenų perkėlimo data ir laikas,

— įmonės arba dirbtuvių kortelės numeris, kortelę išdavusi valstybė narė ir kortelės karta,

— įmonės arba dirbtuvių pavadinimas.

3.12.15 *Duomenys apie ypatingas būsenas*

130) Tachografo duomenų atmintyje užregistruojami ir laikomi tokie duomenys apie ypatingas būsenas:

— įrašo data ir laikas,

— ypatingos būsenos rūšis.

131) Duomenų atmintyje duomenis apie ypatingas būsenas turi būti įmanoma saugoti ne trumpiau kaip 365 dienas (darant prielaidą, kad per dieną vidutiniškai prasideda ir baigiasi viena būsena). Kai atmintinės talpa išnaudojama, nauji duomenys rašomi ant seniausiųjų įrašų.

3.12.16 *Tachografo kortelių duomenys*

132) Tachografo atmintyje laikomi tokie duomenys, susiję su įvairiomis tachografo kortelėmis, naudotomis transporto priemonės bloke:

— tachografo kortelės numeris ir serijos numeris,

— tachografo kortelės gamintojas,

▼B

— tachografo kortelės rūšis,

— tachografo kortelės versija.

133) Tachografo atmintyje turi būti galima išsaugoti ne mažiau kaip 88 tokius įrašus.

3.13 **Tachografo kortelėse įrašytos informacijos nuskaitymas**

134) Tachografas turi gebėti nuskaityti iš pirmosios ir antrosios kartos tachografo kortelių duomenis, būtinus:

— kortelės rūšiai, turėtojui, anksčiau naudotai transporto priemonei, paskutinio kortelės ištraukimo datai bei laikui ir tuo metu pasirinktai veiklai identifikuoti,

— patikrinti, ar paskutinis kortelės naudojimo seansas buvo užbaigtas tinkamai,

— vairuotojo nepertraukiamo vairavimo trukmei, bendrajai poilsio trukmei ir ankstesnės bei einamosios savaičių bendrajai poilsio trukmei ir bendrajai vairavimo trukmei apskaičiuoti,

— reikiamiems spaudiniams su vairuotojo kortelės atmintyje įrašytais duomenimis išspausdinti,

— duomenims iš vairuotojo kortelės į išorines laikmenas perkelti.

Šis reikalavimas taikomas tik pirmosios kartos tachografo kortelėms, jei dirbtuvės nėra atsisakiusios jų naudoti.

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

3.14 **Informacijos įrašymas į tachografo korteles ir laikymas**

3.14.1 *Informacijos įrašymas į pirmosios kartos tachografo korteles ir laikymas*

136) Jei dirbtuvės nėra atsisakiusios naudoti pirmosios kartos tachografų kortelių, tachografas turi užregistruoti ir laikyti duomenis lygiai taip pat, kaip tai darytų pirmosios kartos tachografas.

137) Vos tik įstačius vairuotojo arba dirbtuvių kortelę, tachografas kortelės atmintyje turi nustatyti kortelės naudojimo seanso duomenis.

138) Tachografas turi atnaujinti galiojančiose vairuotojo, dirbtuvių, įmonės ir (arba) kontrolės kortelėse laikomus duomenis, įrašydamas visą kortelės turėtojui svarbią naują informaciją, susijusią su tuo laikotarpiu, kuriuo kortelė yra kortelės lizde. Šiose kortelėse laikomi duomenys nurodyti 4 skyriuje.

139) Tachografas turi atnaujinti galiojančiose vairuotojo ir (arba) dirbtuvių kortelėse laikomus vairuotojo veiklos ir vietos duomenis (nustatytus 4.5.3.1.9 ir 4.5.3.1.11 punktuose), užregistruodamas veiklos ir vietos duomenis, kuriuos kortelės turėtojas įrašė rankiniu būdu.

140) Vairuotojo ir dirbtuvių kortelėse neturi būti laikomi duomenys apie įvykius, nenustatytus pirmosios kartos tachografams.

▼B

141) Tachografo kortelių duomenys turi būti atnaujinami taip, kad, kai reikia, atsižvelgiant į faktinę kortelių atmintinės talpą naujausi duomenys pakeistų seniausius.

142) Įvykus įrašymo klaidai tachografas turi ne daugiau kaip tris kartus mėginti įrašyti duomenis iš naujo, o jei tai nepavyksta — paskelbti kortelę sugedusia ir negaliojančia.

143) Prieš išimant vairuotojo kortelę ir įrašius joje visus reikiamus duomenis, tachografas turi nustatyti į pradinę padėtį kortelės naudojimo seanso duomenis.

3.14.2 *Informacijos įrašymas į antrosios kartos tachografo korteles ir laikymas*

144) Antrosios kartos tachografo kortelėse turi būti 2 skirtingos kortelių taikomosios programos, iš kurių pirmoji turi būti lygiai tokia pati, kaip pirmosios kartos tachografo kortelių programa TACHO, o antroji – TACHO_G2, kaip nurodyta 4 skyriuje ir 2 priedėlyje.

145) Vos tik įstačius vairuotojo arba dirbtuvių kortelę, tachografas kortelės atmintyje turi nustatyti kortelės naudojimo seanso duomenis.

146) Tachografas turi atnaujinti galiojančių vairuotojo, dirbtuvių, įmonės ir (arba) kontrolės kortelių abiejose programose laikomus duomenis, įrašydamas visą kortelės turėtojui svarbią informaciją, susijusią su tuo laikotarpiu, kuriuo kortelė yra kortelės lizde. Šiose kortelėse laikomi duomenys nurodyti 4 skyriuje.

147) Tachografas turi atnaujinti galiojančiose vairuotojo ir (arba) dirbtuvių kortelėse laikomus duomenis apie vairuotojo veiklos vietas ir buvimo vietą (nustatytus 4.5.3.1.9, 4.5.3.1.11, 4.5.3.2.9 ir 4.5.3.2.11 punktuose), užregistruodamas veiklos ir vietos duomenis, kuriuos kortelės turėtojas įrašė rankiniu būdu.

148) Tachografo kortelių duomenys turi būti atnaujinami taip, kad, kai reikia, atsižvelgiant į faktinę kortelių atmintinės talpą naujausi duomenys pakeistų seniausius.

149) Įvykus įrašymo klaidai tachografas turi ne daugiau kaip tris kartus mėginti įrašyti duomenis iš naujo, o jei tai nepavyksta — paskelbti kortelę sugedusia ir negaliojančia.

150) Prieš išimant vairuotojo kortelę ir įrašius abiejose kortelės programose visus reikiamus duomenis, tachografas turi nustatyti į pradinę padėtį kortelės naudojimo seanso duomenis.

3.15 **Rodymas ekrane**

151) Ekrane turi tilpti ne mažiau kaip 20 rašmenų.

152) Rašmuo turi būti ne mažesnis kaip 5 mm aukščio ir 3,5 mm pločio.

153) Ekrane turi būti galima atvaizduoti rašmenis, nurodytus 1 priedėlio 4 skyriuje „Ženklų rinkiniai“. Ekrane rašmenys gali būti vaizduojami supaprastintai (pvz., diakritiniai rašmenys gali būti rodomi be diakritinių ženklų arba vietoj mažųjų raidžių rodomos didžiosios).

▼B

154) Ekrano apšvietimas neturi akinti.

155) Rodmenys turi būti matomi iš tachografo išorės.

156) Tachografo ekrane rodomi:

— numatytieji duomenys,

— perspėjimų informacija,

— naudojimosi meniu informacija,

— kiti naudotojo pageidaujami duomenys.

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

157) 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.

158) Transporto priemonei judant ekranas turi būti visada įjungtas.

159) Tachografas gali turėti rankiniu būdu arba automatiškai valdomą funkciją ekranui IŠJUNGTI, kai transporto priemonė stovi.

Rodymo ekrane formatas nustatytas 5 priedėlyje.

3.15.1 *Numatytasis rodinys*

160) Kai nereikia rodyti jokios kitos informacijos, tachografo ekrane be atskiro reikalavimo rodomas:

— vietos laikas (UTC laikas + vairuotojo nustatytas laiko skirtumas),

— veikimo režimas,

— vykdoma vairuotojo veikla ir vykdoma vairuotojo porininko veikla,

— su vairuotoju susijusi informacija:

— jei vykdoma veikla yra VAIRAVIMAS – jo nepertraukiamo vairavimo trukmė ir tuometė bendroji poilsio trukmė,

— jei vykdoma veikla yra ne VAIRAVIMAS – šios veiklos trukmė (nuo jos pasirinkimo momento) ir tuometė bendroji poilsio trukmė.

161) Su kiekvienu vairuotoju susiję duomenys turi būti pateikiami aiškiai, paprastai ir nedviprasmiškai. Jeigu su vairuotoju ir vairuotoju porininku susijusios informacijos negalima parodyti vienu metu, tachografas be atskiro reikalavimo turi rodyti su vairuotoju susijusią informaciją, o naudotojas turi galimybę pasirinkti su vairuotojo porininku susijusios informacijos rodinį.

162) Jeigu dėl ekrano pločio negalimas numatytasis veikimo režimo rodinys, tachografas trumpam turi parodyti naują veikimo režimą, kai jis pasirenkamas.

▼B

163) Įstačius kortelę tachografas turi trumpam parodyti kortelės turėtojo pavardę (pavadinimą).

164) Kai pasirenkama būsena NEKONTROLIUOJAMA arba KĖLIMAS KELTU / VEŽIMAS TRAUKINIU, numatytajame rodinyje turi būti rodoma atitinkama piktograma, žyminti, kad atitinkama būsena pradėta (leidžiama tuo pačiu metu nerodyti vykdomos vairuotojo veiklos).

3.15.2 *Perspėjamasis rodinys*

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

3.15.3 *Naudojimasis meniu*

166) Tachografo komandomis turi būti galima pasinaudoti per atitinkamą meniu sistemą.

3.15.4 *Kiti rodiniai*

167) Turi būti galima pasirinkti, kad ekrane būtų rodoma:

— UTC data bei laikas ir vietos laiko skirtumas,

— bet kurio iš šešių spaudinių turinys, pateikiamas tokiu pačiu formatu, kaip ir patys spaudiniai,

— vairuotojo nepertraukiamo vairavimo trukmė ir bendroji poilsio trukmė,

— vairuotojo porininko nepertraukiamo vairavimo trukmė ir bendroji poilsio trukmė,

— ankstesnės ir einamosios savaitės vairuotojo bendroji vairavimo trukmė,

— ankstesnės ir einamosios savaitės vairuotojo porininko bendroji vairavimo trukmė,

neprivaloma:

— esama vairuotojo porininko veiklos trukmė (nuo jos pasirinkimo momento),

— einamosios savaitės vairuotojo bendroji vairavimo trukmė,

— einamojo dienos darbo laikotarpio vairuotojo porininko bendroji vairavimo trukmė,

— einamojo dienos darbo laikotarpio vairuotojo bendroji vairavimo trukmė.

168) Spaudinio turinys turi būti rodomas nuosekliai, eilutė po eilutės. Jei ekrano plotis yra mažesnis kaip 24 rašmenys, visa informacija naudotojui turi būti pateikiama tinkamais būdais (keletu eilučių, bėgančiąja eilute ir pan.).

Ekrane gali būti nerodomos spaudinio eilutės, skirtos užpildyti ranka.

▼B

3.16 **Spausdinimas**

169) Tachografas turi gebėti spausdinti informaciją iš savo duomenų atminties ir (arba) iš tachografo kortelių tokių septynių rūšių spaudiniuose:

— vairuotojo veiklos kasdienis spaudinys iš kortelės,

— vairuotojo veiklos kasdienis spaudinys iš transporto priemonės bloko,

— įvykių ir trikčių spaudinys iš kortelės,

— įvykių ir trikčių spaudinys iš transporto priemonės bloko,

— techninių duomenų spaudinys,

— greičio viršijimo spaudinys,

— tam tikro transporto priemonės bloko tachografo kortelės duomenų istorija (žr. 3.12.16 punktą).

Šių spaudinių formatas ir turinys išsamiai apibūdinti 4 priedėlyje.

Spaudinių pabaigoje gali būti pateikiami papildomi duomenys.

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

170) „Vairuotojo veiklos kasdienį spaudinį iš kortelės“ ir „Įvykių ir trikčių spaudinį iš kortelės“ turi būti įmanoma išspausdinti tik tuomet, kai į tachografą įstatyta vairuotojo arba dirbtuvių kortelė. Prieš spausdindamas tachografas turi atnaujinti atitinkamoje kortelėje laikomus duomenis.

171) Tam, kad išspausdintų „Vairuotojo veiklos kasdienį spaudinį iš kortelės“ arba „Įvykių ir trikčių spaudinį iš kortelės“, tachografas:

— automatiškai pasirenka vairuotojo kortelę arba dirbtuvių kortelę, jei yra įstatyta tik viena iš jų;

— jei yra įstatytos abi šios kortelės – nurodo komandą reikiamai kortelei pasirinkti arba pasirenka į vairuotojo kortelės lizdą įstatytą kortelę.

172) Spausdintuvas turi gebėti spausdinti 24 rašmenis vienoje eilutėje.

173) Rašmuo turi būti ne mažesnis kaip 2,1 mm aukščio ir 1,5 mm pločio.

174) Spausdintuvu turi būti įmanoma atspausdinti rašmenis, nurodytus 1 priedėlio 4 skyriuje „Ženklų rinkiniai“.

175) Spausdintuvai turi būti tokios konstrukcijos, kad spaudiniai būtų pakankamai ryškūs ir juos skaitant nekiltų dviprasmybių.

176) Spaudinių matmenys ir įrašai juose turi nesikeisti įprastomis drėgnio (10–90 %) ir temperatūros sąlygomis.

177) Tachografuose naudojamas patvirtinto tipo spausdinimo popierius paženklinamas tinkamu tipo patvirtinimo ženklu ir nurodoma, kurios (-ių) rūšies (-ių) tachografuose tas popierius gali būti naudojamas.

▼B

178) Įprastomis laikymo sąlygomis (šviesos intensyvumo, drėgnio ir temperatūros požiūriu) laikomi spaudiniai turi išlikti aiškiai įskaitomi ir identifikuojami bent dvejus metus.

179) Spaudiniai turi atitikti bent bandymo specifikacijas, nustatytas 9 priedėlyje.

180) Be to, šiuose dokumentuose turi būti galima įrašyti įrašus ranka, pvz., vairuotojas gali pasirašyti.

181) Jei spausdinimo metu baigiasi popierius, įdėjus naujo popieriaus, tachografas turi gebėti pradėti spausdinti spaudinį iš naujo arba tęsti spausdinimą su vienareikšmiška nuoroda į anksčiau atspausdintą dalį

3.17 **Perspėjimai**

182) Tachografas turi perspėti vairuotoją, kai aptinka įvykį ir (arba) triktį.

183) Perspėjimas dėl maitinimo nutrūkimo gali būti atidėtas iki maitinimas vėl bus tiekiamas.

184) Tachografas turi perspėti vairuotoją likus 15 minučių iki maksimalaus nepertraukiamo vairavimo laikotarpio pabaigos ir jam pasibaigus.

185) Perspėjimai turi būti regimieji. Kartu gali būti pateikiami ir papildomi girdimieji perspėjimai.

186) Regimieji perspėjimai turi būti aiškiai atpažįstami naudotojui, būti vairuotojo regos lauke ir aiškiai įskaitomi tiek dieną, tiek naktį.

187) Regimųjų perspėjimų komponentai gali būti įmontuoti tachografe ir (arba) nuotoliniai.

188) Pastaruoju atveju jie turi būti paženklinti raide T.

189) Perspėjimas turi trukti ne mažiau kaip 30 sekundžių, nebent naudotojas, spustelėdamas vieną ar kelis tam tikrus tachografo klavišus, patvirtintų, jog jį pastebėjo. Po pirmojo patvirtinimo neturi būti panaikintas perspėjimo priežasties rodinys, nurodytas kitoje pastraipoje.

190) Perspėjimo priežastis turi būti rodoma tachografo ekrane tol, kol naudotojas, paspausdamas tam tikrą klavišą arba pasirinkdamas tam tikrą tachografo komandą, patvirtina, kad ją mato.

191) Gali būti pateikiami papildomi perspėjimai, jei vairuotojas negali jų supainioti su pirmiau minėtais.

3.18 **Duomenų perkėlimas į išorines laikmenas**

192) Pateikus užklausą, tachografas turi gebėti per kalibravimo / duomenų perkėlimo jungtį perkelti duomenis iš savo atminties arba vairuotojo kortelės į išorines laikmenas. Prieš perkeldamas duomenis tachografas turi atnaujinti atitinkamoje kortelėje laikomus duomenis.

▼B

193) Be to, tachografas, veikdamas bet kuriuo režimu, gali persiųsti duomenis kitomis priemonėmis įmonei, kurios tapatumas patvirtintas tuo pačiu ryšio kanalu (papildoma funkcija). Tokiu atveju turi galioti įmonės režimo duomenų prieigos teisės.

194) Perkeliant duomenų negalima kaip nors pakeisti ar ištrinti.

195) Kalibravimo / duomenų perkėlimo jungties elektrinė sąsaja nurodyta 6 priedėlyje.

196) Duomenų perkėlimo protokolai nustatyti 7 priedėlyje.

3.19 **Nuotolinis ryšys tikslinėms patikroms kelyje atlikti**

197) Kai įjungtas uždegimas, transporto priemonės blokas kas 60 sekundžių nuotolinio ryšio įrenginyje turi išsaugoti naujausius duomenis, reikalingus tikslinėms patikroms kelyje atlikti. Tokie duomenys turi būti užšifruoti ir pasirašyti, kaip nustatyta 11 ir 14 priedėliuose.

198) Nuotoliniu būdu tikrintinus duomenis turi būti galima nuskaityti nuotolinio ryšio skaitytuvu per belaidį ryšį, kaip nustatyta 14 priedėlyje.

199) Tikslinėms patikroms kelyje atlikti reikalingi šie duomenys:

— paskiausias mėginimas pažeisti apsaugą,

— ilgiausias maitinimo sutrikimas,

— jutiklio triktis,

— duomenų apie judėjimą klaida,

— transporto priemonės judėjimo nesuderinamumas,

— važiavimas be galiojančios kortelės,

— informacija, apie tai, kad kortelė į lizdą įstatyta važiuojant,

— duomenys apie laiko koregavimą,

— kalibravimo data, įskaitant paskutinių dviejų kalibravimo įrašų datas,

— transporto priemonės registracijos numeris,

— tachografo įrašytas važiavimo greitis.

3.20 **Duomenų persiuntimas į papildomus išorinius įtaisus**

200) Tachografe gali būti įrengta standartinė sąsaja, leidžianti tachografo užregistruotus arba sukurtus duomenis naudoti veikimo arba kalibravimo režimu naudojant išorinį įrenginį.

13 priedėlyje nustatyta ir standartizuota neprivaloma ITS sąsaja. Gali būti naudojamos ir kitos panašios sąsajos, jei jos visiškai atitinka 13 priedėlio reikalavimus dėl būtiniausių duomenų sąrašo, saugumo ir vairuotojo sutikimo.

ITS duomenims, prieinamiems per šią sąsają, taikomi šie reikalavimai:

— šie duomenys yra atrinkti turimi duomenys iš tachografo duomenų žinyno (1 priedėlis);

▼B

— šių atrinktų duomenų poaibis pažymėtas kaip „asmens duomenys“;

— „asmens duomenų“ poaibiu galima naudotis tik jei vairuotojas yra davęs sutikimą (ir tuo galima įsitikinti), kad jo asmens duomenys gali būti išsiųsti iš transporto priemonės tinklo;

— bet kuriuo metu, kai vairuotojo kortelė yra kortelės lizde, vairuotojo sutikimą galima aktyvinti arba atšaukti naudojantis meniu komandomis;

— duomenų rinkinys ir poaibis transliuojami naudojant *Bluetooth* belaidžio ryšio protokolą transporto priemonės kabinos spinduliu ir atnaujinami kas minutę;

— išorinio įtaiso siejimas su ITS sąsaja bus apsaugotas specialiu atsitiktiniu bent 4 skaitmenų PIN, kuris užregistruojamas ir pateikiamas kiekvieno transporto priemonės bloko ekrane;

— bet kokiomis aplinkybėmis ITS sąsaja negali trikdyti ar paveikti transporto priemonės bloko tinkamo veikimo ir saugumo.

Be pasirinktų turimų duomenų rinkinio, laikomo minimaliu sąrašu, gali būti persiunčiami ir kiti duomenys, jei jie negali būti laikomi asmens duomenimis.

Tachografas turi pranešti kitiems išoriniams įrenginiams apie vairuotojo sutikimą.

Kai transporto priemonės uždegimas įjungtas, minėti duomenys transliuojami nuolat.

201) Tachografuose, siekiant užtikrinti suderinamumą, ir toliau gali būti įrengta nuoseklioji ryšio sąsaja, nurodyta Reglamento (EEB) Nr. 3821/85 su paskutiniais pakeitimais 1B priede. Bet kuriuo atveju vairuotojo sutikimo vis tiek reikia, jei perduodami asmens duomenys.

3.21 **Kalibravimas**

202) Kalibravimo funkcija turi leisti:

— automatiškai susieti judesio jutiklį su transporto priemonės bloku,

— automatiškai sujungti išorinį GNSS įrenginį (jei yra) su transporto priemonės bloku,

— skaitmeniniu būdu priderinti tachografo konstantą (k) prie transporto priemonės būdingojo koeficiento (w),

— koreguoti rodomą laiką įstatytos dirbtuvių kortelės galiojimo laikotarpiu,

— koreguoti esamą odometro rodmens vertę,

— atnaujinti duomenų atmintyje laikomus judesio jutiklio identifikavimo duomenis,

— atnaujinti duomenų atmintyje laikomus išorinio GNSS įrenginio (jei yra) identifikavimo duomenis,

▼B

— atnaujinti informaciją apie visų uždėtų plombų rūšis ir identifikatorius,

— atnaujinti arba patvirtinti kitus tachografui žinomus parametrus: transporto priemonės identifikaciją, w, l, padangų dydį ir greičio ribotuvo nuostatį (jei yra).

203) Be to, kalibravimo funkcija turi užtikrinti galimybę uždrausti tachografe naudoti pirmosios kartos tachografo korteles, jei įvykdytos 15 priedėlyje nustatytos sąlygos.

204) Susiejant judesio jutiklį su transporto priemonės bloku atliekami bent šie veiksmai:

— atnaujinami judesio jutiklio atmintyje laikomi jo įrengimo duomenys (jei reikia);

— iš judesio jutiklio į transporto priemonės bloko duomenų atmintį nukopijuojami reikiami judesio jutiklio identifikavimo duomenys.

205) Sujungiant išorinį GNSS įrenginį su transporto priemonės bloku atliekami bent šie veiksmai:

— atnaujinami išorinio GNSS įrenginio atmintyje laikomi jo įrengimo duomenys (jei reikia);

— iš išorinio GNSS įrenginio į transporto priemonės bloko duomenų atmintį nukopijuojami reikiami išorinio GNSS įrenginio identifikavimo duomenys, įskaitant jo serijos numerį.

Po sujungimo patikrinama GNSS informacija apie buvimo vietą.

206) Naudojantis kalibravimo funkcija turi būti galima įvesti reikiamus duomenis per kalibravimo /duomenų perkėlimo jungtį laikantis 8 priedėlyje nustatyto kalibravimo protokolo. Naudojantis kalibravimo funkcija reikiamus duomenis galima įvesti ir kitais būdais.

3.22 **Kalibravimo tikrinimas kelyje**

207) Kalibravimo tikrinimo kelyje funkcija, pateikus užklausą, leidžia nuskaityti prie transporto priemonės bloko prijungto judesio jutiklio (gali būti integruotas į adapterį) ir išorinio GNSS įrenginio (jei yra) serijos numerius.

208) Juos nuskaityti turi būti įmanoma bent jau transporto priemonės bloko ekrane, naudojantis meniu komandomis.

209) Naudojantis kalibravimo tikrinimo kelyje funkcija, taip pat turi būti galima per K linijos sąsają pasirinkti 6 priedėlyje nustatyto kalibravimo įvesties / išvesties signalo linijos įvesties / išvesties režimą. Tai daroma per seansą *ECUAdjustmentSession*, kaip nurodyta 8 priedėlio 7 skirsnyje „Bandomųjų impulsų valdymas. Įvesties ir išvesties valdymo funkcinis blokas“.

3.23 **Laiko koregavimas**

210) Laiko koregavimo funkcija turi leisti automatiškai koreguoti rodomą laiką. Laikui koreguoti tachografe naudojami du laiko šaltiniai: 1) transporto priemonės bloko vidaus laikrodis, 2) GNSS imtuvas.

▼B

211) Transporto priemonės bloko vidaus laikrodžio laiko nuostatis automatiškai koreguojamas ne ilgesniais kaip 12 valandų intervalais. Jei toks intervalas baigiasi, o GNSS signalo negaunama, laikas nustatomas iš karto, kai tik transporto priemonės blokas gali gauti laiko informaciją iš GNSS imtuvo, atsižvelgiant į transporto priemonės uždegimo sąlygas. Atskaitos laikas, pagal kurį automatiškai nustatomas transporto priemonės bloko vidaus laikrodžio laikas, gaunamas iš GNSS imtuvo. Nesuderinto laiko įvykis užfiksuojamas, jei rodomas laikas daugiau nei viena (1) minute skiriasi nuo GNSS imtuvo pateiktos informacijos.

212) Kalibravimo režimu laiko koregavimo funkcija taip pat turi leisti priverstinai koreguoti rodomą laiką.

3.24 **Eksploatacinės savybės**

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

214) Tachografas turi visiškai tinkamai veikti esant 10–90 % drėgniui.

215) Išmaniajame tachografe naudojamos plombos turi atlaikyti tas pačias sąlygas, kaip ir tachografo komponentai, prie kurių jos pritvirtintos.

216) Tachografas turi būti apsaugotas nuo viršįtampio, maitinimo poliškumo pakeitimo ir trumpojo jungimo.

217) Judesio jutikliai turi:

— reaguoti į magnetinį lauką, kuris neleidžia nustatyti transporto priemonės judėjimo. Tokiomis aplinkybėmis transporto priemonės blokas įrašo ir laiko atmintyje jutiklio triktį (88 reikalavimas), arba

— turėti jutimo elementą, kuris apsaugotas nuo magnetinių laukų arba yra jiems atsparus.

218) Tachografas ir išorinis GNSS įrenginys turi atitikti JT EEK taisyklę Nr. 10 ir turi būti apsaugoti nuo elektrostatinių išlydžių ir trumpalaikių srovių.

3.25 **Medžiagos**

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

220) Įprastomis naudojimo sąlygomis visos įrangos vidaus dalys turi būti apsaugotos nuo drėgmės ir dulkių.

221) Transporto priemonės bloko ir išorinio GNSS įrenginio apsaugos klasė turi būti IP 40, o judesio jutiklio – IP 64 pagal standartą IEC 60529:1989, įskaitant A1:1999 ir A2:2013.

222) Tachografas turi atitikti jam taikomas ergonominio dizaino technines specifikacijas.

▼B

223) Tachografas turi būti apsaugotas nuo atsitiktinio pažeidimo.

3.26 **Ženklai**

224) Jei tachografas rodo transporto priemonės odometro rodmenį ir greitį, jo ekrane turi būti tokie užrašai:

— greta nuotolį rodančio skaičiaus turi būti nurodyti atstumo matavimo vienetai, žymimi santrumpa „km“,

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

Tachografas gali būti nustatytas rodyti greitį myliomis per valandą, tada ir greičio matavimo vienetus žyminti santrumpa turi būti „mph“. Tachografas gali būti nustatytas rodyti nuotolį myliomis, tada ir atstumo matavimo vienetus žyminti santrumpa turi būti „mi“.

225) Ant kiekvieno atskiro 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.

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

4 TACHOGRAFO KORTELIŲ KONSTRUKCIJOS IR FUNKCINIAI REIKALAVIMAI

4.1 **Regimieji duomenys**

Kortelės priekyje:

227) Kortelę išduodančios valstybės narės valstybine kalba arba kalbomis didžiosiomis raidėmis išspausdinti žodžiai „Vairuotojo kortelė“, „Kontrolės kortelė“, „Dirbtuvių kortelė“ arba „Įmonės kortelė“.

228) Kortelę išduodančios valstybės narės pavadinimas (neprivalomas).

229) Kortelę išduodančios valstybės narės skiriamasis ženklas, išspausdintas negatyvo atvaizdu mėlyname stačiakampyje ir apsuptas dvylikos geltonų žvaigždučių. Skiriamieji ženklai nurodyti toliau.

B	Belgija	LV	Latvija
BG	Bulgarija	L	Liuksemburgas
CZ	Čekijos Respublika	LT	Lietuva
CY	Kipras	M	Malta
DK	Danija	NL	Nyderlandai
D	Vokietija	A	Austrija
EST	Estija	PL	Lenkija

▼B

GR	Graikija	P RO SK SLO	Portugalija Rumunija Slovakija Slovėnija
E	Ispanija	FIN	Suomija
F HR H	Prancūzija Kroatija Vengrija	S	Švedija
IRL	Airija	UK	Jungtinė Karalystė
I	Italija		

230) Informacija, nurodoma išduodamoje kortelėje 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)	Kontrolieriaus pavardė (jei taikoma)	Kortelės turėtojo pavardė (jei taikoma)
3.	Vairuotojo gimimo data	Kontrolieriaus vardas (-ai) (jei taikoma)	Kortelės turėtojo vardas (-ai) (jei taikoma)
4a.	Kortelės įsigaliojimo data		
4b.	Kortelės galiojimo pabaigos data		
4c.	Išduodančiosios institucijos pavadinimas (gali būti spausdinamas kitoje pusėje)		
4d.	Kitas nei pateiktasis 5 antraštėje numeris administravimo reikmėms (neprivaloma)		
5a.	Vairuotojo pažymėjimo (galiojančio išduodant vairuotojo kortelę) numeris	—	—
5b.	Kortelės numeris		
6.	Vairuotojo nuotrauka	Kontrolieriaus nuotrauka (neprivaloma)	Montuotojo nuotrauka (neprivaloma)
7.	Kortelės turėtojo parašas (neprivaloma)		
8.	Kortelės turėtojo nuolatinė gyvenamoji vieta arba pašto adresas (neprivaloma)	Kontrolės institucijos pašto adresas	Įmonės arba dirbtuvių pašto adresas

231) Datos rašomos formatu „dd/mm/yyyy“ arba „dd.mm.yyyy“ (diena, mėnesis, metai).

Kitoje kortelės pusėje:

232) Pateikiamas kortelės priekyje sunumeruotų punktų paaiškinimas.

▼B

233) Kortelės turėtojui davus specialų rašytinį sutikimą, gali būti įrašyta ir su kortelės administravimu nesusijusi informacija, jei tai niekaip nepakeistų tachografo kortelės naudojimo paskirties.

234) Tachografų kortelių fono dominuojanti spalva turi būti tokia:

— vairuotojo kortelės: balta,

— kontrolės kortelės: mėlyna,

— dirbtuvių kortelės: raudona,

— įmonės kortelės: geltona.

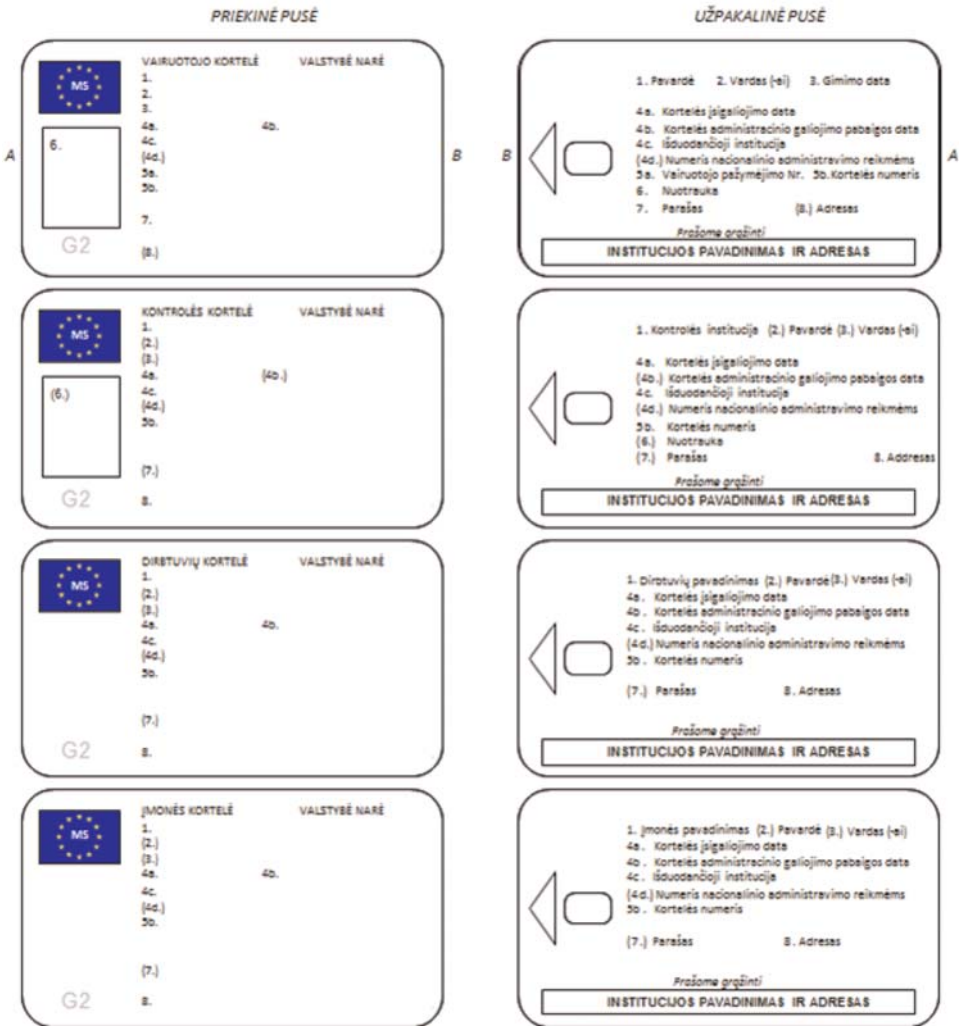
235) Tachografo kortelės turi turėti bent tokius apsaugos nuo klastojimo ir nuo neteisėto keitimo elementus:

— apsauginio dizaino foną su smulkiu ornamentiniu raštu ir spalvotais spaudiniais,

— nuotraukos plote apsauginio dizaino fonas ir nuotrauka turi iš dalies sutapti,

— bent vieną dvispalvę mikrospaudos eilutę.

BENDRIJOS VAIRUOTOJO KORTELĖS PAVYZDYS



▼B

236) Pasikonsultavusios su Komisija, valstybės narės gali naudoti papildomas spalvas ir ženklus, pvz., nacionalinius simbolius ir apsaugos elementus, jei tai nepažeidžia kitų šio priedo nuostatų.

237) Reglamento (ES) Nr. 165/2014 26 straipsnio 4 dalyje nurodytos laikinos kortelės turi atitikti šio priedo nuostatas.

4.2 **Saugumas**

Sistemos apsaugos paskirtis – užtikrinti tarp kortelių ir tachografo perduodamų duomenų nepažeistumą bei autentiškumą, iš kortelių perkeliamų duomenų nepažeistumą bei autentiškumą, užtikrinti, kad įrašyti tam tikrą informaciją į korteles galėtų tik tachografas, taip pat iššifruoti tam tikrus duomenis, užkirsti kelią bet kokiai galimybei klastoti kortelėse laikomus duomenis, apsaugoti nuo neteisėto keitimo ir aptikti bet kokius mėginimus tai padaryti.

238) Tam, kad sistema būtų saugi, tachografo kortelės turi atitikti saugumo reikalavimus, nustatytus10 ir 11 priedėliuose.

239) Informaciją iš tachografo kortelių turi būti įmanoma nuskaityti ir kita įranga, pvz., asmeniniais kompiuteriais.

4.3 **Standartai**

240) Tachografo kortelės turi atitikti tokių standartų reikalavimus:

— ISO/IEC 7810. Atpažinimo kortelės. Fizikinės charakteristikos.

— ISO/IEC 7816. Atpažinimo kortelės. Lustinės kortelės.

  — 1 dalis. Fizikinės charakteristikos.

  — 2 dalis. Kontaktų matmenys ir vieta (ISO/IEC 7816-2: 2007).

  — 3 dalis. Elektrinis sietuvas ir siuntimo protokolai (ISO/IEC 7816-3: 2006).

  — 4 dalis. Struktūra, saugumas ir mainų komandos (ISO/IEC 7816-4: 2013 + Cor 1:2014).

  — 6 dalis. Tarpsektoriniai duomenų mainų elementai (ISO/IEC 7816-6: 2004 + Cor 1:2006).

  — 8 dalis. Saugumo operacijų komandos (ISO/IEC 7816-8: 2004).

— Tachografo kortelės bandomos pagal ISO/IEC 10373-3:2010 „Atpažinimo kortelės. Bandymo metodai. 3 dalis. Lustinės kortelės su kontaktais ir atitinkami sietuvų įtaisai.“

4.4 **Aplinkos ir elektrinės specifikacijos**

241) Tachografo kortelės turi gebėti tinkamai veikti visomis Bendrijos teritorijai būdingomis klimato sąlygomis ir bent jau temperatūroje nuo – 25 °C iki + 70 °C, o trumpam – iki + 85 °C temperatūroje. „Trumpam“ reiškia ne ilgiau kaip 4 valandas kiekvienąkart ir ne daugiau kaip 100 kartų per visą kortelės naudojimo laiką.

242) Tachografo kortelės turi tinkamai veikti esant 10–90 % drėgniui.

▼B

243) Pagal aplinkos ir elektrines specifikacijas naudojamos tachografo kortelės turi tinkamai veikti penkerius metus.

244) Naudojamos kortelės turi atitikti EEK taisyklę Nr. 10, susijusią su elektromagnetiniu suderinamumu, ir turi būti apsaugotos nuo elektrostatinių išlydžių.

4.5 **Duomenų laikymas**

Šiame poskyryje:

— jei nenurodyta kitaip, laikas registruojamas vienos minutės tikslumu;

— odometro rodmens vertės registruojamos vieno kilometro tikslumu;

— greitis registruojamas 1 km/h tikslumu;

— buvimo vietos duomenys (platuma ir ilguma) registruojami laipsniais ir minutėmis, 1/10 minutės tikslumu.

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

Jei nenurodyta kitaip, duomenų laikymas tachografo kortelėse organizuojamas taip, kad jei išnaudojama tam tikriems įrašams numatyta atminties talpa, nauji duomenys pakeistų seniausiuosius.

245) Šiame poskyryje nurodyta mažiausia įvairių taikomųjų programų duomenų rinkmenoms skirtos atmintinės talpa. Tachografo kortelės turi gebėti nurodyti tachografui faktinę šioms duomenų rinkmenoms skirtos atmintinės talpą.

246) Visi su kitomis galimomis kortelės taikomosiomis programomis susiję papildomi duomenys, kurie gali būti laikomi tachografo kortelėse, turi būti laikomi vadovaujantis Direktyva 95/46/EB, Direktyva 2002/58/EB ir Reglamento (ES) Nr. 165/2014 7 straipsniu.

247) Tachografo kortelės kiekviena pagrindinė rinkmena (MF) turi turėti ne daugiau kaip penkias elementariąsias rinkmenas (EF) kortelei tvarkyti, programai ir lustui identifikuoti ir dvi specialiąsias rinkmenas (DF):

— *DF Tachograph*, kurioje yra taikomoji programa, prieinama pirmosios kartos transporto priemonės blokams, taip pat esanti pirmosios kartos tachografo kortelėse;

— *DF Tachograph_G2*, kurioje yra taikomoji programa, prieinama tik antrosios kartos transporto priemonės blokams, esanti tik antrosios kartos tachografo kortelėse.

Visa informacija apie tachografo kortelių struktūrą pateikiama 2 priedėlyje.

4.5.1 *Elementariosios rinkmenos, kurių paskirtis – identifikavimas ir kortelės tvarkymas*

4.5.2 *Lustinės kortelės identifikacija*

248) Tachografo kortelės atmintyje laikomi tokie lustinės kortelės identifikavimo duomenys:

— laikrodžio sustabdymas,

▼B

— kortelės serijos numeris (įskaitant pagaminimo žymenis),

— kortelės tipo patvirtinimo numeris,

— kortelės indivilizuotojo identifikacija (ID),

— įmontuotojo ID,

— IC identifikatorius.

4.5.2.1 Lusto identifikacija

249) Tachografo kortelių atmintyje laikomi tokie integrinio grandyno (IC) identifikavimo duomenys:

— IC serijos numeris,

— IC pagaminimo žymenys.

4.5.2.2 DIR (tik antrosios kartos tachografo kortelėse)

250) Tachografo kortelių atmintyje laikomi programos identifikavimo duomenų objektai, nurodyti 2 priedėlyje.

4.5.2.3 ATR informacija (sąlyginė, tik antrosios kartos tachografo kortelėse)

251) Tachografo kortelės atmintyje laikomas šis didesnio ilgio duomenų objektas:

— jei tachografo kortelėje galimi didesnio ilgio laukai, didesnio ilgio duomenų objektas, nurodytas 2 priedėlyje.

4.5.2.4 Didesnio ilgio informacija (sąlyginė, tik antrosios kartos tachografo kortelėse)

252) Tachografo kortelės atmintyje laikomi šie didesnio ilgio duomenų objektai:

— jei tachografo kortelėje galimi didesnio ilgio laukai, didesnio ilgio duomenų objektai, nurodyti 2 priedėlyje.

4.5.3 *Vairuotojo kortelė*

4.5.3.1 Tachografo taikomoji programa (tinkama pirmosios ir antrosios kartos transporto priemonės blokams)

4.5.3.1.1 Taikomosios programos identifikacija

253) Vairuotojo kortelės atmintyje laikomi šie taikomosios programos identifikavimo duomenys:

— tachografo taikomosios programos identifikacija,

— tachografo kortelės identifikavimo rūšis.

4.5.3.1.2 Raktai ir pažymėjimai

254) Vairuotojo kortelėje turi būti galima laikyti tiek kriptografinių raktų ir pažymėjimų, kiek nurodyta 11 priedėlio A dalyje.

▼B

4.5.3.1.3 Kortelės identifikacija

255) Vairuotojo kortelės atmintyje laikomi šie kortelės identifikavimo duomenys:

— kortelės numeris,

— kortelę išdavusi valstybė narė, kortelę išdavusios institucijos pavadinimas, išdavimo data,

— kortelės įsigaliojimo ir galiojimo pabaigos data.

4.5.3.1.4 Kortelės turėtojo identifikacija

256) Vairuotojo kortelės atmintyje laikomi šie jos turėtojo identifikavimo duomenys:

— turėtojo pavardė,

— turėtojo vardas (-ai),

— gimimo data,

— pageidaujama kalba.

4.5.3.1.5 Duomenų perkėlimas iš kortelės

257) Vairuotojo kortelės atmintyje laikoma ši informacija apie duomenų perkėlimą:

— paskutinio duomenų perkėlimo iš kortelės data ir laikas (skirti ne kontrolei).

258) Vairuotojo kortelės atmintyje turi būti galima išsaugoti vieną tokį įrašą.

4.5.3.1.6 Informacija apie vairuotojo pažymėjimą

259) Vairuotojo kortelės atmintyje laikomi šie duomenys apie vairuotojo pažymėjimą:

— pažymėjimą išdavusi valstybė narė, jį išdavusios institucijos pavadinimas,

— vairuotojo pažymėjimo (galiojančio išduodant kortelę) numeris.

4.5.3.1.7 Duomenys apie įvykius

Šiame poskyryje nurodytais tikslais laikas registruojamas vienos sekundės tikslumu.

260) Vairuotojo kortelės atmintyje laikoma informacija apie šiuos įvykius, tachografo aptiktus, kai kortelė buvo kortelės lizde:

— dalinis laiko sutapimas (kai tai atsitiko dėl kortelės),

— kortelė įstatyta važiuojant (jei įstatyta ta kortelė),

— netinkamai užbaigtas paskutinis kortelės naudojimo seansas (kai naudota ta kortelė),

— maitinimo nutrūkimas,

— duomenų apie judėjimą klaida,

— mėginimai pažeisti apsaugą.

261) Vairuotojo kortelės atmintyje laikoma ši informacija apie minėtus įvykius:

— įvykio kodas,

— įvykio pradžios (arba kortelės įstatymo, jei įvykis vyko tuo metu) data ir laikas,

▼B

— įvykio pabaigos (arba kortelės ištraukimo, jei įvykis vyko tuo metu) data ir laikas,

— transporto priemonės, kurioje įvykis įvyko, registracijos numeris ir registracijos valstybės narė.

Pastaba. Jei įvyko dalinio laiko sutapimo įvykis:

— 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 įstatymo į dabartinę transporto priemonę data ir laiku;

— transporto priemonės duomenys turi atitikti dabartinę transporto priemonę, kurioje įvyko įvykis.

Pastaba. Jei įvyko įvykis „netinkamai užbaigtas paskutinis kortelės naudojimo seansas“:

— įvykio pradžios data ir laikas turi sutapti su kortelės, kurios naudojimo seansas užbaigtas netinkamai, įstatymo data ir laiku;

— įvykio pabaigos data ir laikas turi sutapti su seanso, kurio metu įvykis buvo aptiktas, kortelės įstatymo data ir laiku;

— transporto priemonės duomenys turi atitikti transporto priemonę, kurioje seansas buvo netinkamai užbaigtas.

262) Vairuotojo kortelės atmintyje turi būti galima išsaugoti duomenis apie šešis paskutinius kiekvienos rūšies įvykius (t. y. iš viso 36 įvykius).

4.5.3.1.8 Duomenys apie triktis

Šiame poskyryje nurodytais tikslais laikas registruojamas vienos sekundės tikslumu.

263) Vairuotojo kortelės atmintyje turi būti galima laikyti informaciją apie tokias triktis, tachografo aptiktas, kai kortelė buvo kortelės lizde:

— kortelės triktį (kai tai atsitiko dėl kortelės),

— tachografo triktį.

264) Vairuotojo kortelės atmintyje laikoma ši informacija apie minėtas triktis:

— trikties kodas,

— trikties pradžios (arba kortelės įstatymo, jei triktis vyko tuo metu) data ir laikas,

— trikties pabaigos (arba kortelės ištraukimo, jei triktis vyko tuo metu) data ir laikas,

— transporto priemonės, kurioje įvyko triktis, registracijos numeris ir registracijos valstybė narė.

265) Vairuotojo kortelės atmintyje turi būti galima išsaugoti duomenis apie dvylika paskutinių kiekvienos rūšies trikčių (t. y. iš viso 24 triktis).

▼B

4.5.3.1.9 Duomenys apie vairuotojo veiklą

266) Vairuotojo kortelės atmintyje laikomi tokie kiekvienos kalendorinės dienos, kurią kortelė buvo naudota arba kurią vairuotojas rankiniu būdu įvedė duomenis apie veiklą, duomenys:

— data,

— kortelės buvimo tą dieną skaitiklio rodmens vertė (kuri kiekvieną naudojimo dieną padidėja vienetu),

— visas tą dieną vairuotojo nuvažiuotas atstumas,

— vairuotojo būsena 00.00 val.,

— informacija apie tai, ar vairuotojas pakeitė veiklos rūšį ir (arba) važiavimo būseną ir (arba) įstatė į lizdą ar ištraukė savo kortelę:

— važiavimo būsena (ĮGULA, VIENAS VAIRUOTOJAS),

— kortelės lizdas (VAIRUOTOJO, VAIRUOTOJO PORININKO),

— kortelės būsena (ĮSTATYTA, NEĮSTATYTA),

— veiklos rūšis (VAIRAVIMAS, PASIRENGĘS DIRBTI, DARBAS, PERTRAUKA / POILSIS),

— pasikeitimo laikas.

267) Vairuotojo kortelės atmintyje turi būti galima išsaugoti duomenis apie vairuotojo ne mažiau kaip 28 dienų veiklą (vidutinę vairuotojo veiklą sudaro 93 veiklos pasikeitimai per dieną).

268) 261, 264 ir 266 reikalavimuose išvardyti duomenys turi būti laikomi taip, kad veiklos duomenis būtų galima gauti chronologine tvarka, net jei laikas iš dalies sutaptų.

4.5.3.1.10 Duomenys apie naudotas transporto priemones

269) Vairuotojo kortelės atmintyje laikomi tokie duomenys apie kiekvieną kalendorinę dieną, kurią kortelė buvo naudota, ir apie kiekvieną tam tikros transporto priemonės naudojimo laikotarpį tą dieną (laikotarpis apima visus kortelės įstatymo ir ištraukimo ciklus transporto priemonėje):

— pirmojo transporto priemonės panaudojimo data ir laikas (t. y. pirmojo per tą transporto priemonės naudojimo laikotarpį kortelės įstatymo data ir laikas, o jei naudojimo laikotarpis tuo metu tęsiasi – 00.00 val.),

— transporto priemonės odometro rodmens vertė tuo metu,

— paskutiniojo transporto priemonės panaudojimo data ir laikas (t. y. paskutiniojo kortelės ištraukimo tą transporto priemonės naudojimo laikotarpį data ir laikas, o jei naudojimo laikotarpis tuo metu tęsiasi – 23.59 val.),

▼B

— transporto priemonės odometro rodmens vertė tuo metu,

— transporto priemonės registracijos numeris ir registracijos valstybė narė.

270) Vairuotojo kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 84 tokius įrašus.

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

271) Vairuotojo kortelės atmintyje laikomi šie vairuotojo įvedami duomenys, susiję su vietomis, kur prasideda ir (arba) baigiasi dienos darbo laikotarpiai:

— įrašo data ir laikas (arba su įrašu susijusi data ir laikas, kai įrašoma rankiniu būdu),

— įrašo rūšis (pradžia ar pabaiga, įrašo aplinkybės),

— įrašyta šalis ir regionas,

— transporto priemonės odometro rodmens vertė.

272) Vairuotojo kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 42 poras tokių įrašų.

4.5.3.1.12 Duomenys apie kortelės naudojimo seansą

273) Vairuotojo kortelės atmintyje laikomi tokie duomenys, susiję su transporto priemone, kurioje buvo pradėtas einamasis kortelės naudojimo seansas:

— seanso pradžios (t. y. kortelės įstatymo) data ir laikas vienos sekundės tikslumu,

— transporto priemonės registracijos numeris ir registracijos valstybė narė.

4.5.3.1.13 Duomenys apie kontrolės veiklą

274) Vairuotojo kortelės atmintyje laikomi tokie duomenys apie kontrolės veiklą:

— kontrolės data ir laikas,

— kontrolės kortelės numeris ir ją išdavusi valstybė narė,

— kontrolės rūšis (rodymas ekrane, spausdinimas, duomenų perkėlimas iš transporto priemonės bloko ir (arba) duomenų perkėlimas iš kortelės),

— laikotarpis, kurio duomenys perkelti (jei perkeliami duomenys),

— transporto priemonės, kurioje buvo atliekama kontrolė, registracijos numeris ir registracijos valstybė narė.

Pastaba. Duomenų perkėlimas iš kortelės registruojamas tik tada, kai tai atliekama tachografu.

275) Vairuotojo kortelės atmintyje turi būti galima išsaugoti vieną tokį įrašą.

4.5.3.1.14 Duomenys apie ypatingas būsenas

276) Vairuotojo kortelės atmintyje laikomi tokie su ypatingomis būsenomis susiję duomenys, įrašyti, kai kortelė buvo kortelės lizde (nesvarbu, kuriame):

— įrašo data ir laikas,

— ypatingos būsenos rūšis.

▼B

277) Vairuotojo kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 56 tokius įrašus.

4.5.3.2 Antrosios kartos tachografo taikomoji programa (netinkama pirmosios kartos transporto priemonės blokui)

4.5.3.2.1 Taikomosios programos identifikacija

278) Vairuotojo kortelės atmintyje laikomi šie taikomosios programos identifikavimo duomenys:

— tachografo taikomosios programos identifikacija,

— tachografo kortelės identifikavimo rūšis.

4.5.3.2.2 Raktai ir pažymėjimai

279) Vairuotojo kortelėje turi būti galima laikyti tiek kriptografinių raktų ir pažymėjimų, kiek nurodyta 11 priedėlio B dalyje.

4.5.3.2.3 Kortelės identifikacija

280) Vairuotojo kortelės atmintyje laikomi šie kortelės identifikavimo duomenys:

— kortelės numeris,

— kortelę išdavusi valstybė narė, kortelę išdavusios institucijos pavadinimas, išdavimo data,

— kortelės įsigaliojimo ir galiojimo pabaigos data.

4.5.3.2.4 Kortelės turėtojo identifikacija

281) Vairuotojo kortelės atmintyje laikomi šie jos turėtojo identifikavimo duomenys:

— turėtojo pavardė,

— turėtojo vardas (-ai),

— gimimo data,

— pageidaujama kalba.

4.5.3.2.5 Duomenų perkėlimas iš kortelės

282) Vairuotojo kortelės atmintyje laikoma ši informacija apie duomenų perkėlimą:

— paskutinio duomenų perkėlimo iš kortelės data ir laikas (skirti ne kontrolei).

283) Vairuotojo kortelės atmintyje turi būti galima išsaugoti vieną tokį įrašą.

4.5.3.2.6 Informacija apie vairuotojo pažymėjimą

284) Vairuotojo kortelės atmintyje laikomi šie duomenys apie vairuotojo pažymėjimą:

— pažymėjimą išdavusi valstybė narė, jį išdavusios institucijos pavadinimas,

— vairuotojo pažymėjimo (galiojančio išduodant kortelę) numeris.

4.5.3.2.7 Duomenys apie įvykius

Šiame poskyryje nurodytais tikslais laikas registruojamas vienos sekundės tikslumu.

▼B

285) Vairuotojo kortelės atmintyje laikoma informacija apie šiuos įvykius, tachografo aptiktus, kai kortelė buvo kortelės lizde:

— dalinis laiko sutapimas (kai tai atsitiko dėl kortelės),

— kortelė įstatyta važiuojant (jei įstatyta ta kortelė),

— netinkamai užbaigtas paskutinis kortelės naudojimo seansas (kai naudota ta kortelė),

— maitinimo nutrūkimas,

— ryšio su nuotolinio ryšio įrenginiu klaida,

— iš GNSS imtuvo negauta informacijos apie buvimo vietą,

— ryšio su išoriniu GNSS įrenginiu klaida,

— duomenų apie judėjimą klaida,

— transporto priemonės judėjimo nesuderinamumas,

— mėginimai pažeisti apsaugą,

— nesuderintas laikas.

286) Vairuotojo kortelės atmintyje laikoma ši informacija apie minėtus įvykius:

— įvykio kodas,

— įvykio pradžios (arba kortelės įstatymo, jei įvykis vyko tuo metu) data ir laikas,

— įvykio pabaigos (arba kortelės ištraukimo, jei įvykis vyko tuo metu) data ir laikas,

— transporto priemonės, kurioje įvykis įvyko, registracijos numeris ir registracijos valstybės narė.

Pastaba. Jei įvyko dalinio laiko sutapimo įvykis:

— 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 įstatymo į dabartinę transporto priemonę data ir laiku;

— transporto priemonės duomenys turi atitikti dabartinę transporto priemonę, kurioje įvyko įvykis.

Pastaba. Jei įvyko įvykis „netinkamai užbaigtas paskutinis kortelės naudojimo seansas“:

— įvykio pradžios data ir laikas turi sutapti su kortelės, kurios naudojimo seansas užbaigtas netinkamai, įstatymo data ir laiku;

— įvykio pabaigos data ir laikas turi sutapti su seanso, kurio metu įvykis buvo aptiktas, kortelės įstatymo data ir laiku;

▼B

— transporto priemonės duomenys turi atitikti transporto priemonę, kurioje seansas buvo netinkamai užbaigtas.

287) Vairuotojo kortelės atmintyje turi būti galima išsaugoti duomenis apie šešis paskutinius kiekvienos rūšies įvykius (t. y. iš viso 66 įvykius).

4.5.3.2.8 Duomenys apie triktis

Šiame poskyryje nurodytais tikslais laikas registruojamas vienos sekundės tikslumu.

288) Vairuotojo kortelės atmintyje turi būti galima laikyti informaciją apie tokias triktis, tachografo aptiktas, kai kortelė buvo kortelės lizde:

— kortelės triktį (kai tai atsitiko dėl kortelės),

— tachografo triktį.

289) Vairuotojo kortelės atmintyje laikoma ši informacija apie minėtas triktis:

— trikties kodas,

— trikties pradžios (arba kortelės įstatymo, jei triktis vyko tuo metu) data ir laikas,

— trikties pabaigos (arba kortelės ištraukimo, jei triktis vyko tuo metu) data ir laikas,

— transporto priemonės, kurioje įvyko triktis, registracijos numeris ir registracijos valstybė narė.

290) Vairuotojo kortelės atmintyje turi būti galima išsaugoti duomenis apie dvylika paskutinių kiekvienos rūšies trikčių (t. y. iš viso 24 triktis).

4.5.3.2.9 Duomenys apie vairuotojo veiklą

291) Vairuotojo kortelės atmintyje laikomi tokie kiekvienos kalendorinės dienos, kurią kortelė buvo naudota arba kurią vairuotojas rankiniu būdu įvedė duomenis apie veiklą, duomenys:

— data,

— kortelės buvimo tą dieną skaitiklio rodmens vertė (kuri kiekvieną naudojimo dieną padidėja vienetu),

— visas tą dieną vairuotojo nuvažiuotas atstumas,

— vairuotojo būsena 00.00 val.,

— informacija apie tai, ar vairuotojas pakeitė veiklos rūšį ir (arba) važiavimo būseną ir (arba) įstatė į lizdą ar ištraukė savo kortelę:

— važiavimo būsena (ĮGULA, VIENAS VAIRUOTOJAS),

— kortelės lizdas (VAIRUOTOJO, VAIRUOTOJO PORININKO),

— kortelės būsena (ĮSTATYTA, NEĮSTATYTA),

— veiklos rūšis (VAIRAVIMAS, PASIRENGĘS DIRBTI, DARBAS, PERTRAUKA / POILSIS),

▼B

— pasikeitimo laikas.

292) Vairuotojo kortelės atmintyje turi būti galima išsaugoti duomenis apie vairuotojo ne mažiau kaip 28 dienų veiklą (vidutinę vairuotojo veiklą sudaro 93 veiklos pasikeitimai per dieną).

293) 286, 289 ir 291 reikalavimuose išvardyti duomenys turi būti laikomi taip, kad veiklos duomenis būtų galima gauti chronologine tvarka, net jei laikas iš dalies sutaptų.

4.5.3.2.10 Duomenys apie naudotas transporto priemones

294) Vairuotojo kortelės atmintyje laikomi tokie duomenys apie kiekvieną kalendorinę dieną, kurią kortelė buvo naudota, ir apie kiekvieną tam tikros transporto priemonės naudojimo laikotarpį tą dieną (laikotarpis apima visus kortelės įstatymo ir ištraukimo ciklus transporto priemonėje):

— pirmojo transporto priemonės panaudojimo data ir laikas (t. y. pirmojo per tą transporto priemonės naudojimo laikotarpį kortelės įstatymo data ir laikas, o jei naudojimo laikotarpis tuo metu tęsiasi – 00.00 val.),

— transporto priemonės odometro rodmens vertė pirmojo panaudojimo metu,

— paskutiniojo transporto priemonės panaudojimo data ir laikas (t. y. paskutiniojo kortelės ištraukimo tą transporto priemonės naudojimo laikotarpį data ir laikas, o jei naudojimo laikotarpis tuo metu tęsiasi – 23.59 val.),

— transporto priemonės odometro rodmens vertė paskutiniojo panaudojimo metu,

— transporto priemonės registracijos numeris ir registracijos valstybė narė,

— transporto priemonės VIN.

295) Vairuotojo kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 84 tokius įrašus.

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

296) Vairuotojo kortelės atmintyje laikomi šie vairuotojo įvedami duomenys, susiję su vietomis, kur prasideda ir (arba) baigiasi dienos darbo laikotarpiai:

— įrašo data ir laikas (arba su įrašu susijusi data ir laikas, kai įrašoma rankiniu būdu),

— įrašo rūšis (pradžia ar pabaiga, įrašo aplinkybės),

— įrašyta šalis ir regionas,

— transporto priemonės odometro rodmens vertė,

— transporto priemonės buvimo vieta,

— GNSS tikslumas, data ir laikas, kai buvo nustatyta buvimo vieta.

297) Vairuotojo kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 84 poras tokių įrašų.

▼B

4.5.3.2.12 Duomenys apie kortelės naudojimo seansą

298) Vairuotojo kortelės atmintyje laikomi tokie duomenys, susiję su transporto priemone, kurioje buvo pradėtas einamasis kortelės naudojimo seansas:

— seanso pradžios (t. y. kortelės įstatymo) data ir laikas vienos sekundės tikslumu,

— transporto priemonės registracijos numeris ir registracijos valstybė narė.

4.5.3.2.13 Duomenys apie kontrolės veiklą

299) Vairuotojo kortelės atmintyje laikomi tokie duomenys apie kontrolės veiklą:

— kontrolės data ir laikas,

— kontrolės kortelės numeris ir ją išdavusi valstybė narė,

— kontrolės rūšis (rodymas ekrane, spausdinimas, duomenų perkėlimas iš transporto priemonės bloko ir (arba) duomenų perkėlimas iš kortelės),

— laikotarpis, kurio duomenys perkelti (jei perkeliami duomenys),

— transporto priemonės, kurioje buvo atliekama kontrolė, registracijos numeris ir registracijos valstybė narė.

Pastaba. Laikantis saugumo reikalavimų, duomenų perkėlimas iš kortelės registruojamas tik tada, kai tai atliekama tachografu.

300) Vairuotojo kortelės atmintyje turi būti galima išsaugoti vieną tokį įrašą.

4.5.3.2.14 Duomenys apie ypatingas būsenas

301) Vairuotojo kortelės atmintyje laikomi tokie su ypatingomis būsenomis susiję duomenys, įrašyti, kai kortelė buvo kortelės lizde (nesvarbu, kuriame):

— įrašo data ir laikas,

— ypatingos būsenos rūšis.

302) Vairuotojo kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 56 tokius įrašus.

4.5.3.2.15 Naudotų transporto priemonės blokų duomenys

303) Vairuotojo kortelės atmintyje laikomi tokie duomenys, susiję su įvairiais transporto priemonės blokais, kuriuose naudota kortelė:

— transporto priemonės bloko naudojimo laikotarpio pradžios (t. y. pirmojo per laikotarpį kortelės įstatymo į transporto priemonės bloką) data ir laikas,

— transporto priemonės bloko gamintojas,

— transporto priemonės bloko rūšis,

— transporto priemonės bloko programinės įrangos versijos numeris.

304) Vairuotojo kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 84 tokius įrašus.

▼B

4.5.3.2.16 Duomenys apie vietas, kur nepertraukiamo vairavimo trukmė pasiekia tris valandas

305) Vairuotojo kortelės atmintyje laikomi tokie duomenys, susiję su transporto priemonės buvimo vieta, kurioje vairuotojo nepertraukiamo vairavimo trukmė pasiekia trijų valandų kartotinį:

— data ir laikas, kai kortelės turėtojo nepertraukiamo vairavimo trukmė pasiekia trijų valandų kartotinį,

— transporto priemonės buvimo vieta,

— GNSS tikslumas, data ir laikas, kai buvo nustatyta buvimo vieta.

306) Vairuotojo kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 252 tokius įrašus.

4.5.4 *Dirbtuvių kortelė*

4.5.4.1 Tachografo taikomoji programa (tinkama pirmosios ir antrosios kartos transporto priemonės blokams)

4.5.4.1.1 Taikomosios programos identifikacija

307) Dirbtuvių kortelės atmintyje laikomi šie taikomosios programos identifikavimo duomenys:

— tachografo taikomosios programos identifikacija,

— tachografo kortelės identifikavimo rūšis.

4.5.4.1.2 Raktai ir pažymėjimai

308) Dirbtuvių kortelėje turi būti galima laikyti tiek kriptografinių raktų ir pažymėjimų, kiek nurodyta 11 priedėlio A dalyje.

309) Dirbtuvių kortelės atmintyje turi būti galima laikyti asmeninės identifikacijos numerį (PIN kodą).

4.5.4.1.3 Kortelės identifikacija

310) Dirbtuvių kortelės atmintyje laikomi tokie kortelės identifikavimo duomenys:

— kortelės numeris,

— kortelę išdavusi valstybė narė, kortelę išdavusios institucijos pavadinimas, išdavimo data,

— kortelės įsigaliojimo ir galiojimo pabaigos data.

4.5.4.1.4 Kortelės turėtojo identifikacija

311) Dirbtuvių kortelės atmintyje laikomi tokie jos turėtojo identifikavimo duomenys:

— dirbtuvių pavadinimas,

— dirbtuvių adresas,

— turėtojo pavardė,

— turėtojo vardas (-ai),

— pageidaujama kalba.

4.5.4.1.5 Duomenų perkėlimas iš kortelės

312) Dirbtuvių kortelės atmintyje turi būti galima laikyti duomenų perkėlimo iš kortelės įrašus taip pat, kaip vairuotojo kortelėje.

▼B

4.5.4.1.6 Duomenys apie kalibravimą ir laiko koregavimą

313) Dirbtuvių kortelės atmintyje turi būti galima saugoti įrašus apie kalibravimą ir (arba) laiko koregavimą, atliktą tada, kai kortelė buvo įstatyta į tachografą.

314) Kiekviename įraše apie kalibravimą turi būti tokie duomenys:

— kalibravimo tikslas (aktyvinimas, pirmasis įrengimas, įrengimas, periodinė patikra),

— transporto priemonės identifikacija,

— atnaujinti arba patvirtinti parametrai (w, k, l, padangų dydis, greičio ribotuvo nuostatis, odometro rodmenys (sena ir nauja vertės), data ir laikas (sena ir nauja vertės),

— tachografo identifikacija (transporto priemonės bloko komponento šifras, transporto priemonės bloko serijos numeris, judesio jutiklio serijos numeris).

315) Dirbtuvių kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 88 tokius įrašus.

316) Dirbtuvių kortelės atmintyje laikoma informacija, rodanti, kiek kartų iš viso atliktas kalibravimas naudojant šią kortelę.

317) Dirbtuvių kortelės atmintyje laikoma informacija, rodanti, kiek kartų atliktas kalibravimas po paskutinio duomenų perkėlimo iš jos.

4.5.4.1.7 Duomenys apie įvykius ir triktis

318) Dirbtuvių kortelės atmintyje turi būti galima laikyti įrašus apie įvykius ir triktis taip pat, kaip vairuotojo kortelėje.

319) Dirbtuvių kortelės atmintyje turi būti galima laikyti duomenis apie tris paskutinius kiekvienos rūšies įvykius (t. y. iš viso 18 įvykių) ir apie šešias paskutines kiekvienos rūšies triktis (t. y. iš viso 12 trikčių).

4.5.4.1.8 Duomenys apie vairuotojo veiklą

320) Dirbtuvių kortelės atmintyje turi būti galima laikyti duomenis apie vairuotojo veiklą taip pat, kaip vairuotojo kortelėje.

321) Dirbtuvių kortelės atmintyje turi būti galima išsaugoti duomenis bent apie vairuotojo vienos dienos vidutinę veiklą.

4.5.4.1.9 Duomenys apie naudotas transporto priemones

322) Dirbtuvių kortelės atmintyje turi būti galima laikyti įrašus apie naudotas transporto priemones taip pat, kaip vairuotojo kortelėje.

323) Dirbtuvių kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 4 tokius įrašus.

4.5.4.1.10 Duomenys apie dienos darbo laikotarpių pradžią ir (arba) pabaigą

324) Dirbtuvių kortelės atmintyje turi būti galima laikyti įrašus apie dienos darbo laikotarpių pradžią ir (arba) pabaigą taip pat, kaip vairuotojo kortelėje.

325) Dirbtuvių kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip tris poras tokių įrašų.

▼B

4.5.4.1.11 Duomenys apie kortelės naudojimo seansą

326) Dirbtuvių kortelės atmintyje turi būti galima laikyti duomenų apie kortelės naudojimo seansą įrašus taip pat, kaip vairuotojo kortelėje.

4.5.4.1.12 Duomenys apie kontrolės veiklą

327) Dirbtuvių kortelės atmintyje turi būti galima laikyti duomenų apie kontrolės veiklą įrašus taip pat, kaip vairuotojo kortelėje.

4.5.4.1.13 Duomenys apie ypatingas būsenas

328) Dirbtuvių kortelė atmintyje turi būti galima laikyti duomenis, susijusius su ypatingomis būsenomis, taip pat, kaip vairuotojo kortelėje.

329) Dirbtuvių kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 2 tokius įrašus.

4.5.4.2 2-osios kartos tachografo taikomoji programa (netinkama pirmosios kartos transporto priemonės blokui)

4.5.4.2.1 Taikomosios programos identifikacija

330) Dirbtuvių kortelės atmintyje laikomi šie taikomosios programos identifikavimo duomenys:

— tachografo taikomosios programos identifikacija,

— tachografo kortelės identifikavimo rūšis.

4.5.4.2.2 Raktai ir pažymėjimai

331) Dirbtuvių kortelėje turi būti galima laikyti tiek kriptografinių raktų ir pažymėjimų, kiek nurodyta 11 priedėlio B dalyje.

332) Dirbtuvių kortelės atmintyje turi būti galima laikyti asmeninės identifikacijos numerį (PIN kodą).

4.5.4.2.3 Kortelės identifikacija

333) Dirbtuvių kortelės atmintyje laikomi tokie kortelės identifikavimo duomenys:

— kortelės numeris,

— kortelę išdavusi valstybė narė, kortelę išdavusios institucijos pavadinimas, išdavimo data,

— kortelės įsigaliojimo ir galiojimo pabaigos data.

4.5.4.2.4 Kortelės turėtojo identifikacija

334) Dirbtuvių kortelės atmintyje laikomi tokie jos turėtojo identifikavimo duomenys:

— dirbtuvių pavadinimas,

— dirbtuvių adresas,

— turėtojo pavardė,

— turėtojo vardas (-ai),

— pageidaujama kalba.

4.5.4.2.5 Duomenų perkėlimas iš kortelės

335) Dirbtuvių kortelės atmintyje turi būti galima laikyti duomenų perkėlimo iš kortelės įrašus taip pat, kaip vairuotojo kortelėje.

▼B

4.5.4.2.6 Duomenys apie kalibravimą ir laiko koregavimą

336) Dirbtuvių kortelės atmintyje turi būti galima saugoti įrašus apie kalibravimą ir (arba) laiko koregavimą, atliktą tada, kai kortelė buvo įstatyta į tachografą.

337) Kiekviename įraše apie kalibravimą turi būti tokie duomenys:

— kalibravimo tikslas (aktyvinimas, pirmasis įrengimas, įrengimas, periodinė patikra),

— transporto priemonės identifikacija,

— atnaujinti arba patvirtinti parametrai (w, k, l, padangų dydis, greičio ribotuvo nuostatis, odometro rodmenys (sena ir nauja vertės), data ir laikas (sena ir nauja vertės),

— tachografo identifikacija (transporto priemonės bloko komponento šifras, transporto priemonės bloko serijos numeris, judesio jutiklio serijos numeris, nuotolinio ryšio įrenginio serijos numeris ir išorinio GNSS įrenginio (jei yra) serijos numeris,

— visų uždėtų plombų rūšys ir identifikatoriai,

— informacija apie tai, ar transporto priemonės bloke galima naudoti pirmosios kartos tachografo korteles (ar tokia galimybė aktyvinta, ar ne).

338) Dirbtuvių kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 88 tokius įrašus.

339) Dirbtuvių kortelės atmintyje laikoma informacija, rodanti, kiek kartų iš viso atliktas kalibravimas naudojant šią kortelę.

340) Dirbtuvių kortelės atmintyje laikoma informacija, rodanti, kiek kartų atliktas kalibravimas po paskutinio duomenų perkėlimo iš jos.

4.5.4.2.7 Duomenys apie įvykius ir triktis

341) Dirbtuvių kortelės atmintyje turi būti galima laikyti įrašus apie įvykius ir triktis taip pat, kaip vairuotojo kortelėje.

342) Dirbtuvių kortelės atmintyje turi būti galima laikyti duomenis apie tris paskutinius kiekvienos rūšies įvykius (t. y. iš viso 33 įvykius) ir apie šešias paskutines kiekvienos rūšies triktis (t. y. iš viso 12 trikčių).

4.5.4.2.8 Duomenys apie vairuotojo veiklą

343) Dirbtuvių kortelės atmintyje turi būti galima laikyti duomenis apie vairuotojo veiklą taip pat, kaip vairuotojo kortelėje.

344) Dirbtuvių kortelės atmintyje turi būti galima išsaugoti duomenis bent apie vairuotojo vienos dienos vidutinę veiklą.

4.5.4.2.9 Duomenys apie naudotas transporto priemones

345) Dirbtuvių kortelės atmintyje turi būti galima laikyti įrašus apie naudotas transporto priemones taip pat, kaip vairuotojo kortelėje.

346) Dirbtuvių kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 4 tokius įrašus.

▼B

4.5.4.2.10 Duomenys apie dienos darbo laikotarpių pradžią ir (arba) pabaigą

347) Dirbtuvių kortelės atmintyje turi būti galima laikyti įrašus apie dienos darbo laikotarpių pradžią ir (arba) pabaigą taip pat, kaip vairuotojo kortelėje.

348) Dirbtuvių kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip tris poras tokių įrašų.

4.5.4.2.11 Duomenys apie kortelės naudojimo seansą

349) Dirbtuvių kortelės atmintyje turi būti galima laikyti duomenų apie kortelės naudojimo seansą įrašus taip pat, kaip vairuotojo kortelėje.

4.5.4.2.12 Duomenys apie kontrolės veiklą

350) Dirbtuvių kortelės atmintyje turi būti galima laikyti duomenų apie kontrolės veiklą įrašus taip pat, kaip vairuotojo kortelėje.

4.5.4.2.13 Naudotų transporto priemonės blokų duomenys

351) Dirbtuvių kortelės atmintyje laikomi tokie duomenys, susiję su įvairiais transporto priemonės blokais, kuriuose naudota kortelė:

— transporto priemonės bloko naudojimo laikotarpio pradžios (t. y. pirmojo per laikotarpį kortelės įstatymo į transporto priemonės bloką) data ir laikas,

— transporto priemonės bloko gamintojas,

— transporto priemonės bloko rūšis,

— transporto priemonės bloko programinės įrangos versijos numeris.

352) Dirbtuvių kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 4 tokius įrašus.

4.5.4.2.14 Duomenys apie vietas, kur nepertraukiamo vairavimo trukmė pasiekia tris valandas

353) Dirbtuvių kortelės atmintyje laikomi tokie duomenys, susiję su transporto priemonės buvimo vieta, kurioje vairuotojo nepertraukiamo vairavimo trukmė pasiekia trijų valandų kartotinį:

— data ir laikas, kai kortelės turėtojo nepertraukiamo vairavimo trukmė pasiekia trijų valandų kartotinį,

— transporto priemonės buvimo vieta,

— GNSS tikslumas, data ir laikas, kai buvo nustatyta buvimo vieta.

354) Dirbtuvių kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 18 tokių įrašų.

4.5.4.2.15 Duomenys apie ypatingas būsenas

355) Dirbtuvių kortelės atmintyje turi būti galima laikyti duomenis, susijusius su ypatingomis būsenomis, taip pat, kaip vairuotojo kortelėje.

356) Dirbtuvių kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 2 tokius įrašus.

▼B

4.5.5 *Kontrolės kortelė*

4.5.5.1 Tachografo taikomoji programa (tinkama pirmosios ir antrosios kartos transporto priemonės blokams)

4.5.5.1.1 Taikomosios programos identifikacija

357) Kontrolės kortelės atmintyje laikomi šie taikomosios programos identifikavimo duomenys:

— tachografo taikomosios programos identifikacija,

— tachografo kortelės identifikavimo rūšis.

4.5.5.1.2 Raktai ir pažymėjimai

358) Kontrolės kortelėje turi būti galima laikyti tiek kriptografinių raktų ir pažymėjimų, kiek nurodyta 11 priedėlio A dalyje.

4.5.5.1.3 Kortelės identifikacija

359) Kontrolės kortelės atmintyje laikomi šie kortelės identifikavimo duomenys:

— kortelės numeris,

— kortelę išdavusi valstybė narė, kortelę išdavusios institucijos pavadinimas, išdavimo data,

— kortelės įsigaliojimo ir galiojimo pabaigos data (jei yra).

4.5.5.1.4 Kortelės turėtojo identifikacija

360) Kontrolės kortelės atmintyje laikomi tokie jos turėtojo identifikavimo duomenys:

— kontrolės institucijos pavadinimas,

— kontrolės institucijos adresas,

— turėtojo pavardė,

— turėtojo vardas (-ai),

— pageidaujama kalba.

4.5.5.1.5 Duomenys apie kontrolės veiklą

361) Kontrolės kortelės atmintyje laikomi šie duomenys apie kontrolės veiklą:

— kontrolės data ir laikas,

— kontrolės rūšis (rodymas ekrane, spausdinimas, duomenų perkėlimas iš transporto priemonės bloko, duomenų perkėlimas iš kortelės ir (arba) kalibravimo tikrinimas kelyje),

— laikotarpis, kurio duomenys perkelti (jei perkeliami duomenys),

— transporto priemonės, kurioje buvo atliekama kontrolė, registracijos numeris ir registracijos valstybė narė,

— patikrintos vairuotojo kortelės numeris ir ją išdavusi valstybė narė.

362) Kontrolės kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 230 tokių įrašų.

▼B

4.5.5.2 2-osios kartos tachografo taikomoji programa (netinkama pirmosios kartos transporto priemonės blokui)

4.5.5.2.1 Taikomosios programos identifikacija

363) Kontrolės kortelės atmintyje laikomi šie taikomosios programos identifikavimo duomenys:

— tachografo taikomosios programos identifikacija,

— tachografo kortelės identifikavimo rūšis.

4.5.5.2.2 Raktai ir pažymėjimai

364) Kontrolės kortelėje turi būti galima laikyti tiek kriptografinių raktų ir pažymėjimų, kiek nurodyta 11 priedėlio B dalyje.

4.5.5.2.3 Kortelės identifikacija

365) Kontrolės kortelės atmintyje laikomi šie kortelės identifikavimo duomenys:

— kortelės numeris,

— kortelę išdavusi valstybė narė, kortelę išdavusios institucijos pavadinimas, išdavimo data,

— kortelės įsigaliojimo ir galiojimo pabaigos data (jei yra).

4.5.5.2.4 Kortelės turėtojo identifikacija

366) Kontrolės kortelės atmintyje laikomi tokie jos turėtojo identifikavimo duomenys:

— kontrolės institucijos pavadinimas,

— kontrolės institucijos adresas,

— turėtojo pavardė,

— turėtojo vardas (-ai),

— pageidaujama kalba.

4.5.5.2.5 Duomenys apie kontrolės veiklą

367) Kontrolės kortelės atmintyje laikomi šie duomenys apie kontrolės veiklą:

— kontrolės data ir laikas,

— kontrolės rūšis (rodymas ekrane, spausdinimas, duomenų perkėlimas iš transporto priemonės bloko, duomenų perkėlimas iš kortelės ir (arba) kalibravimo tikrinimas kelyje),

— laikotarpis, kurio duomenys perkelti (jei perkeliami duomenys),

— transporto priemonės, kurioje buvo atliekama kontrolė, registracijos numeris ir registracijos valstybė narė,

— patikrintos vairuotojo kortelės numeris ir ją išdavusi valstybė narė.

368) Kontrolės kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 230 tokių įrašų.

▼B

4.5.6 *Įmonės kortelė*

4.5.6.1 Tachografo taikomoji programa (tinkama pirmosios ir antrosios kartos transporto priemonės blokams)

4.5.6.1.1 Taikomosios programos identifikacija

369) Įmonės kortelės atmintyje laikomi šie taikomosios programos identifikavimo duomenys:

— tachografo taikomosios programos identifikacija,

— tachografo kortelės identifikavimo rūšis.

4.5.6.1.2 Raktai ir pažymėjimai

370) Įmonės kortelėje turi būti galima laikyti tiek kriptografinių raktų ir pažymėjimų, kiek nurodyta 11 priedėlio A dalyje.

4.5.6.1.3 Kortelės identifikacija

371) Įmonės kortelės atmintyje laikomi šie kortelės identifikavimo duomenys:

— kortelės numeris,

— kortelę išdavusi valstybė narė, kortelę išdavusios institucijos pavadinimas, išdavimo data,

— kortelės įsigaliojimo ir galiojimo pabaigos data (jei yra).

4.5.6.1.4 Kortelės turėtojo identifikacija

372) Įmonės kortelės atmintyje laikomi šie jos turėtojo identifikavimo duomenys:

— įmonės pavadinimas,

— įmonės adresas.

4.5.6.1.5 Duomenys apie įmonės veiklą

373) Įmonės kortelės atmintyje laikomi šie duomenys apie įmonės veiklą:

— veiklos data ir laikas,

— veiklos rūšis (transporto priemonės bloko užrakinimas ir (arba) atrakinimas ir (arba) duomenų perkėlimas iš transporto priemonės bloko ir (arba) duomenų perkėlimas iš kortelės),

— laikotarpis, kurio duomenys perkelti (jei perkeliami duomenys),

— transporto priemonės registracijos numeris ir valstybės narės registracijos institucija,

— kortelės numeris ir kortelę išdavusi valstybė narė (jei perkeliami duomenys iš kortelės).

374) Įmonės kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 230 tokių įrašų.

▼B

4.5.6.2 2-osios kartos tachografo taikomoji programa (netinkama pirmosios kartos transporto priemonės blokui)

4.5.6.2.1 Taikomosios programos identifikacija

375) Įmonės kortelės atmintyje laikomi šie taikomosios programos identifikavimo duomenys:

— tachografo taikomosios programos identifikacija,

— tachografo kortelės identifikavimo rūšis.

4.5.6.2.2 Raktai ir pažymėjimai

376) Įmonės kortelėje turi būti galima laikyti tiek kriptografinių raktų ir pažymėjimų, kiek nurodyta 11 priedėlio B dalyje.

4.5.6.2.3 Kortelės identifikacija

377) Įmonės kortelės atmintyje laikomi šie kortelės identifikavimo duomenys:

— kortelės numeris,

— kortelę išdavusi valstybė narė, kortelę išdavusios institucijos pavadinimas, išdavimo data,

— kortelės įsigaliojimo ir galiojimo pabaigos data (jei yra).

4.5.6.2.4 Kortelės turėtojo identifikacija

378) Įmonės kortelės atmintyje laikomi šie jos turėtojo identifikavimo duomenys:

— įmonės pavadinimas,

— įmonės adresas.

4.5.6.2.5 Duomenys apie įmonės veiklą

379) Įmonės kortelės atmintyje laikomi šie duomenys apie įmonės veiklą:

— veiklos data ir laikas,

— veiklos rūšis (transporto priemonės bloko užrakinimas ir (arba) atrakinimas ir (arba) duomenų perkėlimas iš transporto priemonės bloko ir (arba) duomenų perkėlimas iš kortelės),

— laikotarpis, kurio duomenys perkelti (jei perkeliami duomenys),

— transporto priemonės registracijos numeris ir valstybės narės registracijos institucija,

— kortelės numeris ir kortelę išdavusi valstybė narė (jei perkeliami duomenys iš kortelės).

380) Įmonės kortelės atmintyje turi būti galima išsaugoti ne mažiau kaip 230 tokių įrašų.

5 TACHOGRAFO ĮRENGIMAS

5.1 **Įrengimas**

381) Nauji tachografai montuotojams arba transporto priemonių gamintojams pristatomi neaktyvinti ir juose turi būti nustatytos reikiamos galiojančios visų 3.21 skyriuje išvardytų kalibravimo parametrų numatytosios vertės. Jei jokia konkreti vertė netinkama, raidinių parametrų atveju įrašoma klaustukų eilutė, o skaitmeninių parametrų atveju – 0. Dalių, kurios svarbios tachografo saugumui, tiekimas gali būti ribojamas, jei to reikalaujama atliekant saugumo sertifikavimą.

▼B

382) Prieš tachografo aktyvinimą turi būti galima pasinaudoti kalibravimo funkcija net ir ne kalibravimo režimu.

383) Dar neaktyvintas tachografas neturi registruoti ir saugoti duomenų, nurodytų 3.12.3, 3.12.9 ir 3.12.12–3.12.15 punktuose.

384) Montuodamas tachografą transporto priemonės gamintojas nustato visus žinomus parametrus.

385) Transporto priemonių gamintojai arba montuotojai turi aktyvinti sumontuotą tachografą ne vėliau kaip iki tada, kai transporto priemonė pradedama naudoti pagal Reglamentą (EB) Nr. 561/2006.

386) Tachografas aktyvinamas automatiškai, pirmą kartą įstačius į bet kurį kortelių sąsajos įtaisą galiojančią dirbtuvių kortelę.

387) Specialios judesio jutiklio ir transporto priemonės bloko susiejimo operacijos (jei jų reikia) atliekamos automatiškai prieš aktyvinimą arba jo metu.

388) Specialios išorinio GNSS įrenginio ir transporto priemonės bloko sujungimo operacijos (jei jų reikia) atliekamos automatiškai prieš aktyvinimą arba jo metu.

389) Aktyvintas tachografas turi imti visiškai tinkamai veikti ir taikyti prieigos prie duomenų teises.

390) Aktyvintas tachografas turi persiųsti nuotolinio ryšio įrenginiui apsaugotus duomenis, reikalingus tikslinėms patikroms kelyje atlikti.

391) Aktyvinto tachografo registravimo ir duomenų laikymo funkcijos turi tinkamai veikti.

392) Po įrengimo atliekamas kalibravimas. Atliekant kalibravimą pirmą kartą, nebūtina įrašyti transporto priemonės registracijos numerio, jei patvirtintos dirbtuvės, turinčios atlikti kalibravimą, jo nežino. Tokiomis aplinkybėmis, prieš pradedant naudoti transporto priemonę pagal Reglamentą (EB) Nr. 561/2006 ([1]), transporto priemonės savininkui tik tuo metu turi būti įmanoma įrašyti transporto priemonės registracijos numerį naudojant savo įmonės kortelę (pavyzdžiui, naudojantis transporto priemonės bloko žmogaus ir mašinos sąsajos tam tikros meniu struktūros komandomis). Bet koks šio įrašo atnaujinimas ar patvirtinimas turi būti įmanomas tik naudojant dirbtuvių kortelę.

393) Norint sumontuoti išorinį GNSS įrenginį, reikia jį sujungti su transporto priemonės bloku ir po to patikrinti GNSS informaciją apie buvimo vietą.

394) Tachografas turi būti įrengtas tokioje transporto priemonės vietoje, kad reikiamomis jo funkcijomis vairuotojas galėtų naudotis sėdėdamas savo sėdynėje.

([1]) OL L 102, 2006 4 11, p. 1.

▼B

5.2 **Įrengimo plokštelė**

395) Patikrinus sumontuotą tachografą, ant jo pritvirtinama aiškiai matoma ir lengvai prieinama įrengimo plokštelė, kurioje pateikta informacija yra išgraviruota arba neištrinamai išspausdinta. Kai tai neįmanoma, plokštelė tvirtinama ant transporto priemonės B statramsčio taip, kad būtų aiškiai matoma. Jei transporto priemonė neturi B statramsčio, įrengimo plokštelė turėtų būti tvirtinama ant transporto priemonės durų rėmo vairuotojo pusėje ir bet kuriuo atveju turi būti aiškiai matoma.

Po kiekvienos patikros, kurią atlieka patvirtintas montuotojas ar dirbtuvės, ankstesnės plokštelės vietoje tvirtinama nauja plokštelė.

396) Plokštelėje pateikiama bent tokia informacija:

— patvirtinto montuotojo pavardė ar dirbtuvių pavadinimas, adresas ar firmos pavadinimas;

— transporto priemonės būdingasis koeficientas: „w = … imp/km“;

— tachografo konstanta: „k = … imp/km“;

— padangų efektyvusis apskritimo ilgis: „l = … mm“;

— padangų dydis;

— transporto priemonės būdingojo koeficiento ir padangų efektyviojo apskritimo ilgio išmatavimo data;

— transporto priemonės identifikavimo numeris;

— informacija apie tai, ar (ne)įrengtas išorinis GNSS įrenginys;

— išorinio GNSS įrenginio serijos numeris;

— nuotolinio ryšio įrenginio serijos numeris;

— visų uždėtų plombų serijos numeriai;

— transporto priemonės vieta, kurioje įrengtas adapteris, jei jis yra;

— transporto priemonės vieta, kurioje įrengtas judesio jutiklis, jei jis neprijungtas prie pavarų dėžės arba jei nenaudojamas adapteris;

— laido, jungiančio adapterį ir transporto priemonės vietą, iš kurios gaunami impulsai, spalva;

— adapteryje įtaisyto judesio jutiklio serijos numeris.

397) Antroji, papildoma plokštelė gali būti naudojama tik M1 ir N1 transporto priemonėse, kuriose įrengtas adapteris pagal Komisijos reglamentą (EB) Nr. 68/2009 ([1]) su paskutiniais pakeitimais, ir kai neįmanoma įtraukti visos būtinos 396 reikalavime nurodytos informacijos. Tokiais atvejais šioje papildomoje plokštelėje įrašoma informacija bent pagal keturias paskutines 396 reikalavimo įtraukas.

([1]) 2009 m. sausio 23 d. Komisijos reglamentas (EB) Nr. 68/2009, kuriuo devintąjį kartą su technikos pažanga derinamas Tarybos reglamentas (EEB) Nr. 3821/85 dėl kelių transporto priemonėse naudojamų tachografų (OL L 21, 2009 1 24, p. 3).

▼B

Jei naudojama antroji, papildoma plokštelė, ji tvirtinama greta pirmosios, pagrindinės plokštelės, nurodytos 396 reikalavime; jos apsaugos lygis turi būti toks pat. Be to, antrojoje plokštelėje taip pat nurodoma tachografą įrengusio patvirtinto montuotojo pavardė ir adresas arba dirbtuvių pavadinimas bei adresas ir įrengimo data.

5.3 **Plombavimas**

398) Užplombuojamos šios dalys:

— visos jungtys, kurias atjungus galima būtų padaryti neaptinkamų pakeitimų arba neaptinkamai dingtų duomenys (pvz., tai gali būti taikoma judesio jutiklio sujungimui su pavarų dėže, adapteriui M1 ir N1 klasių transporto priemonėse, išorinio GNSS įrenginio jungčiai arba transporto priemonės blokui);

— įrengimo plokštelė, nebent ji būtų pritvirtinta taip, kad jos neįmanoma nuimti nesugadinus jos žymenų.

399) Pirmiau išvardytas plombas leidžiama nuimti:

— avarijos atveju,

— įrengiant, reguliuojant ar remontuojant greičio ribotuvą arba kokį nors kitą kelių eismo saugą užtikrinantį įtaisą, jeigu tachografas tebeveikia patikimai, be sutrikimų ir iš karto sumontavus greičio ribotuvą arba kokį nors kitą kelių eismo saugą užtikrinantį įtaisą, o kitais atvejais – per septynias dienas, jį iš naujo užplombuoja patvirtintas montuotojas arba dirbtuvės (laikantis 6 skyriaus nuostatų).

400) Kiekvieną kartą nuėmus plombas turi būti surašomas aktas, kuriame nurodomos plombų nuėmimo priežastys ir kuris turi būti pateiktas kompetentingai institucijai.

401) Plombos turi turėti gamintojo priskirtą identifikavimo numerį. Šis numeris turi būti unikalus ir skirtis nuo bet kurio kito plombos numerio, kurį suteikė kitas plombų gamintojas.

Šis unikalus identifikavimo numeris yra: neištrinamas ženklas MM NNNNNN, kur MM – unikalus gamintojo identifikavimo kodas (registruojamas EK tvarkomoje duomenų bazėje), o NNNNNN – plombos raidinis skaitinis kodas, nepasikartojantis gamintojo registre.

402) Ant plombos turi būti laisvos vietos, kurioje patvirtinti montuotojai, dirbtuvės ar transporto priemonių gamintojai galėtų pridėti specialų ženklą pagal Reglamento (ES) Nr. 165/2014 22 straipsnio 3 dalį.

Šis ženklas neturi uždengti plombos identifikavimo numerio.

403) Plombų gamintojai registruojasi specialioje duomenų bazėje ir paskelbia savo plombų identifikavimo numerius laikydamiesi tvarkos, kurią nustato Europa Komisija.

404) Taikant Reglamentą (ES) Nr. 165/2014, patvirtintos dirbtuvės ir transporto priemonių gamintojai turi naudoti tik pirmiau nurodytoje duomenų bazėje registruotų plombų gamintojų plombas.

▼B

405) Plombų gamintojai ir platintojai registruoja plombas, parduotas naudoti pagal Reglamentą (ES) Nr. 165/2014, kad jas būtų galima atsekti, ir turi būti pasirengę prireikus pateikti šiuos įrašus kompetentingoms nacionalinėms institucijoms.

406) Plombų identifikavimo numeriai turi būti matomi įrengimo plokštelėje.

6 TIKRINIMAI, PATIKROS IR REMONTAS

Reikalavimai dėl atvejų, kuriais leidžiama nuimti plombas, kaip nurodyta Reglamento (ES) Nr. 165/2014 22 straipsnio 5 dalyje, nustatyti šio priedo 5.3 skyriuje.

6.1 **Montuotojų, dirbtuvių ir transporto priemonių gamintojų patvirtinimas**

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

— montavimo darbus,

— tikrinimus,

— patikras,

— remontą.

Dirbtuvių kortelės išduodamos tik tokiems montuotojams ir (arba) dirbtuvėms, kuriems yra leista aktyvinti 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 saugumui, kurio reikalavimai nustatyti 10 priedėlyje.

6.2 **Naujų arba suremontuotų prietaisų tikrinimas**

407) Kiekvienas naujas ar suremontuotas įtaisas turi būti patikrinamas, ar tinkamai veikia, tiksliai rodo bei registruoja ir yra sukalibruotas laikantis 3.2.1, 3.2.2, 3.2.3 ir 3.3 skyriuose nustatytų ribų, ir turi būti užplombuojamas pagal 5.3 skyriaus nuostatas.

6.3 **Įrengimo patikra**

408) Visa transporto priemonėje montuojama sistema (įskaitant patį tachografą) turi atitikti 3.2.1, 3.2.2, 3.2.3 ir 3.3 skyrių nuostatas dėl didžiausių leidžiamųjų nuokrypų.

6.4 **Periodinės patikros**

409) Transporto priemonėse sumontuota įranga turi būti periodiškai tikrinama kiekvienąkart, kai atliekamas jos remontas, pasikeičia transporto priemonės būdingasis koeficientas ar padangų efektyvusis apskritimo ilgis, įrangos UTC laiko rodmuo skiriasi nuo tikrojo laiko daugiau kaip 20 minučių arba pasikeičia transporto priemonės registracijos numeris, arba bent kartą per dvejus metus (24 mėnesius) po paskutinės patikros.

410) Tokios patikros metu tikrinama:

— ar tachografas, įskaitant duomenų laikymo tachografo kortelėse funkciją ir ryšį su nuotolinio ryšio skaitytuvais, veikia tinkamai;

▼B

— ar įranga atitinka 3.2.1 ir 3.2.2 skyrių nuostatas dėl didžiausių leidžiamųjų nuokrypų;

— ar įranga atitinka 3.2.3 ir 3.3 skyrių nuostatas;

— ar tachografas yra su tipo patvirtinimo ženklu;

— ar pritvirtinta 396 reikalavime nurodyta įrengimo plokštelė ir 225 reikalavime nurodyta plokštelė;

— padangų dydis ir tikrasis jų apskritimo ilgis;

— ar prie įrangos nėra prijungta klastojimo įtaisų;

— ar tinkamai uždėtos plombos, ar jų būklė gera, ar jų identifikavimo numeriai galioja (EK duomenų bazėje registruotas plombų gamintojas) ir ar jų identifikavimo numeriai atitinka ženklus įrengimo plokštelėje (žr. 401 reikalavimą).

411) Jei nustatoma, kad nuo paskutinės patikros įvyko vienas iš 3.9 skyriuje (Įvykių ir (arba) trikčių aptikimas) išvardytų įvykių, ir tachografų gamintojai ir (arba) nacionalinės institucijos mano, kad įrangos saugumui kyla pavojus, dirbtuvės turi:

a. palyginti pavarų dėžėje įtaisyto judesio jutiklio identifikavimo duomenis ir susieto judesio jutiklio, užregistruoto transporto priemonės bloke, identifikavimo duomenis;

b. patikrinti, ar įrengimo plokštelėje nurodyta informacija atitinka transporto priemonės bloke įrašytą informaciją;

c. patikrinti, ar judesio jutiklio serijos numeris ir patvirtinimo numeris, jei nurodytas ant judesio jutiklio korpuso, atitinka įrašytą tachografo duomenų atmintyje laikomą informaciją;

d. palyginti išorinio GNSS įrenginio (jei yra) plokštelėje nurodytus ir transporto priemonės duomenų atmintyje laikomus identifikavimo duomenis.

412) Dirbtuvės savo patikros ataskaitose turi registruoti visus duomenis, susijusius su pažeistomis plombomis ar klastojimo įtaisais. Dirbtuvės tokias ataskaitas saugo bent dvejus metus ir jas pateikia kompetentingos institucijos prašymu.

413) Per šias patikras tachografas sukalibruojamas ir prevencijos tikslais pakeičiamos plombos, už kurias yra atsakingos dirbtuvės.

6.5 **Paklaidų matavimas**

414) Tachografą sumontavus ir eksploatuojant, paklaidos nustatomos toliau nurodytomis sąlygomis, laikytinomis standartinėmis badymo sąlygomis:

— parengta važiuoti nepakrauta transporto priemonė;

— padangų slėgis atitinka gamintojo instrukcijas;

▼B

— padangų nusidėvėjimas ne didesnis, nei leidžiama pagal nacionalinę teisę;

— transporto priemonės judėjimas:

— savo varikliu varoma transporto priemonė važiuoja tiesia linija lygiu keliu 50 km/h ±5 km/h greičiu. Matavimo atstumas turi būti ne trumpesnis kaip 1 000 m;

— bandymą galima atlikti ir kitais būdais, pvz., bandymo stendu, jei jų rezultatų tikslumas panašus.

6.6 **Remontas**

415) Dirbtuvės turi gebėti perkelti duomenis iš tachografo, kad galėtų juos pateikti atitinkamai transporto įmonei.

416) 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 dvejus metus.

7 KORTELĖS IŠDAVIMAS

Valstybių narių nustatyta kortelių išdavimo tvarka turi atitikti toliau nurodytus reikalavimus.

417) Pirmą kartą išduodant tachografo kortelę pareiškėjui, numeracijos indeksas (jei naudojamas), keitimo indeksas ir atnaujinimo indeksas turi būti 0.

418) Visų vienai kontrolės institucijai, vienoms dirbtuvėms ar vienai transporto įmonei išduodamų neasmeninių kortelių pirmieji 13 skaitmenų yra tokie patys, o numeracijos indeksai skiriasi.

419) Vietoj esamos tachografo kortelės išduodamos ją pakeičiančios kortelės numeris turi būti toks pats, kaip ir pakeistosios, tik keitimo indeksas padidinamas viena pozicija (tokia seka: 0, …, 9, A, …, Z).

420) Vietoj esamos tachografo kortelės išduodamos ją pakeičiančios kortelės galiojimo pabaigos data turi būti tokia pati, kaip ir pakeistosios.

421) Vietoj esamos tachografo kortelės išduodamos ją atnaujinančios kortelės numeris turi būti toks pats, kaip ir pakeistosios, tik keitimo indeksas vėl turi būti 0, o atnaujinimo indeksas padidinamas viena pozicija (tokia seka: 0, …, 9, A, …, Z).

422) Jei esama tachografo kortelė administravimo duomenims pakeisti keičiama toje pačioje valstybėje narėje, laikomasi atnaujinimo taisyklių, jei kitoje valstybėje narėje – pirmojo išdavimo taisyklių.

423) Neasmeninių dirbtuvių ar kontrolės kortelių eilutėje „kortelės turėtojo pavardė“ įrašomas dirbtuvių ar kontrolės institucijos pavadinimas arba montuotojo ar kontroliuojančiojo pareigūno pavardė, jei valstybė narė taip nusprendžia.

▼B

424) Siekdamos užtikrinti išduodamų vairuotojų kortelių unikalumą, valstybės narės keičiasi duomenimis elektroniniu būdu, vadovaudamosi Reglamento (ES) Nr. 165/2014 31 straipsniu.

8 TACHOGRAFŲ IR TACHOGRAFO KORTELIŲ TIPO PATVIRTINIMAS

8.1 **Bendrosios nuostatos**

Šiame skyriuje žodis „tachografas“ reiškia tachografą arba jo komponentus. Judesio jutiklį, išorinį GNSS įrenginį arba nuotolinio ryšio įrenginį su transporto priemonės bloku jungiančių laidų tipo patvirtinti nereikalaujama. Tachografo naudojamas popierius laikomas tachografo komponentu.

Bet kuris gamintojas gali paprašyti patvirtinti jo komponento tipą kartu su bet kuriuo judesio jutiklio, išorinio GNSS įrenginio tipu ir atvirkščiai, jei kiekvienas komponentas atitinka šio priedo reikalavimus. Arba gamintojai gali prašyti patvirtinti viso tachografo tipą.

425) Tachografas pateikiamas tvirtinti kartu su visais integruotais papildomais įtaisais.

426) Tvirtinant tachografo ir tachografo kortelių tipą atliekami saugumo, veikimo ir sąveikumo bandymai. Jei šių bandymų rezultatai teigiami, tai nurodoma atitinkamame sertifikate.

427) Valstybių narių tipo patvirtinimo institucijos suteikia tipo patvirtinimo pažymėjimą tik gavusios tipo patvirtinimo paraiškoje nurodyto tachografo arba tachografo kortelės:

— saugumo sertifikatą,

— veikimo sertifikatą ir

— sąveikumo sertifikatą.

428) Apie bet kokius programinės arba techninės tachografo įrangos arba medžiagų, iš kurių jis gaminamas, pakeitimus iš anksto pranešama institucijai, patvirtinusiai tachografo tipą. Ši institucija patvirtina gamintojui pratęsianti tipo patvirtinimą arba gali pareikalauti atnaujintų veikimo, saugumo ir (arba) sąveikumo sertifikatų.

429) Tachografo programinės įrangos naujovinimo *in situ* tvarką turi patvirtinti institucija, patvirtinusi tachografo tipą. Dėl programinės įrangos naujovinimo neturi būti pakeisti ir ištrinti jokie tachografe laikomi duomenys apie vairuotojo veiklą. Programinė įranga naujovinama tik įrangos gamintojo atsakomybe.

430) Negalima atsisakyti patvirtinti programinės įrangos pakeitimų, kuriais atnaujinamas anksčiau patvirtinto tipo tachografas, jeigu tokie pakeitimai susiję tik su tomis funkcijomis, kurios šiame priede nenustatytos. Tachografo programinės įrangos naujovinimas gali neapimti naujų ženklų rinkinių, jei tai techniškai neįmanoma.

▼B

8.2 **Saugumo sertifikatas**

431) Saugumo sertifikatas išduodamas laikantis šio priedo 10 priedėlio nuostatų. Tachografo komponentai, kuriuos reikia sertifikuoti, yra transporto priemonės blokas, judesio jutiklis, išorinis GNSS įrenginys ir tachografo kortelės.

432) Išimtinėmis aplinkybėmis, kai saugumo sertifikavimo institucijos atsisako sertifikuoti naują įrangą remdamosi tuo, kad apsaugos mechanizmai yra pasenę, tipas ir toliau patvirtinamas tik tomis konkrečiomis išimtinėmis aplinkybėmis ir tik tada, kai nėra jokio kito sprendimo, atitinkančio reglamento nuostatas.

433) Tokiomis aplinkybėmis atitinkama valstybė narė nedelsdama informuoja Europos Komisiją, kuri per dvylika kalendorinių mėnesių nuo tipo patvirtinimo pradeda procedūrą, siekdama užtikrinti, kad saugumo lygis ir vėl būtų toks, koks buvo pradžioje.

8.3 **Veikimo sertifikatas**

434) Kiekvienas pareiškėjas, pageidaujantis gauti tipo patvirtinimo pažymėjimą, pateikia valstybės narės tipo patvirtinimo institucijai visą jos pareikalautą medžiagą ir dokumentus.

435) Gamintojai per mėnesį nuo prašymo gavimo turi pateikti tinkamus gaminių, kurių tipą pageidauja patvirtinti, pavyzdžius ir susijusius dokumentus, kurių reikalauja laboratorijos, paskirtos atlikti veikimo bandymus. Visas su tokiu prašymu susijusias išlaidas padengia prašantysis subjektas. Laboratorijos užtikrina visos informacijos, kuri yra komercinė paslaptis, konfidencialumą.

436) Veikimo sertifikatas gamintojui išduodamas tik tada, jei visų 9 priedėlyje nurodytų veikimo bandymų rezultatai yra teigiami.

437) Veikimo sertifikatą išduoda tipo patvirtinimo institucija. Sertifikate nurodomas jo gavėjo pavadinimas, modelio identifikacija, išsamus atliktų bandymų sąrašas ir gauti rezultatai.

438) Bet kurio tachografo komponento veikimo sertifikate taip nurodomi visų kitų jį sertifikuojant išbandytų suderinamų patvirtinto tipo tachografo komponentų tipo patvirtinimo numeriai.

439) Bet kurio tachografo komponento veikimo sertifikate taip nurodomas ISO ar CEN standartas, pagal kurį buvo sertifikuota funkcinė sąsaja.

8.4 **Sąveikumo sertifikatas**

440) Sąveikumo bandymus atlieka viena Europos Komisijos įgaliota laboratorija, už kurią yra atsakinga Komisija.

441) Laboratorija registruoja gamintojų pateikiamus sąveikumo bandymų prašymus chronologine jų gavimo tvarka.

442) Prašymai oficialiai registruojami tik pateikus laboratorijai:

— visą sąveikumo bandymams reikalingą medžiagą ir dokumentus,

▼B

— atitinkamą saugumo sertifikatą,

— atitinkamą veikimo sertifikatą.

Gamintojui pranešama prašymo užregistravimo data.

443) Laboratorija neatlieka tachografo ar tachografo kortelių, kuriems nesuteiktas saugumo sertifikatas ir veikimo sertifikatas, veikimo bandymų, išskyrus išimtines aplinkybes, aprašytas 432 reikalavime.

444) Visi prašantys atlikti sąveikumo bandymus gamintojai įsipareigoja palikti už tokius bandymus atsakingai laboratorijai visą bandymams atlikti pateiktą medžiagą ir reikiamus dokumentus.

445) Sąveikumo bandymai pagal šio priedo 9 priedėlio nuostatas turi būti atliekami su visų rūšių tachografais arba tachografo kortelėmis:

— kurių tipo patvirtinimas tebegalioja,

— kurių tipas kol kas nepatvirtintas (laukiama sprendimo) ir kurie turi galiojantį sąveikumo sertifikatą.

446) Sąveikumo bandymai apima bet kurios kartos tachografus arba tachografo korteles, kurie vis dar naudojami.

447) Laboratorija sąveikumo sertifikatą gamintojui išduoda tik sėkmingai atlikusi visus reikiamus sąveikumo bandymus.

448) Jei vieno ar daugiau tachografų arba tachografo kortelių sąveikumo bandymų rezultatai yra neigiami, sąveikumo sertifikatas neišduodamas, kol gamintojas nepadarys reikiamų pakeitimų ir sąveikumo bandymų rezultatai nebus teigiami. 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 saugumo ir veikimo sertifikatai tebegalioja.

449) Sąveikumo sertifikatas galioja šešis mėnesius. Pasibaigus šiam laikotarpiui jis atšaukiamas, jei gamintojas negauna atitinkamo tipo patvirtinimo pažymėjimo. Gamintojas jį pateikia valstybės narės tipo patvirtinimo institucijai, išdavusiai veikimo sertifikatą.

450) Bet kuris sąveikumo trūkumą lėmęs elementas neturi būti naudojamas pelnui gauti arba padėti užimti dominuojančią padėtį.

8.5 **Tipo patvirtinimo pažymėjimas**

451) Valstybės narės tipo patvirtinimo institucija gali išduoti tipo patvirtinimo pažymėjimą, kai tik gauna tris reikiamus sertifikatus.

▼B

452) Bet kurio tachografo komponento tipo patvirtinimo pažymėjime taip pat nurodomi kitų suderinamų patvirtinto tipo tachografų tipo patvirtinimo numeriai.

453) Gamintojui išduodamo tipo patvirtinimo pažymėjimo kopija išsiunčiama už sąveikumo bandymus atsakingai laboratorijai.

454) Už sąveikumo bandymus atsakinga laboratorija turi turėti svetainę internete, kurioje skelbiamas ir atnaujinamas tokių tachografų ir tachografo kortelių modelių sąrašas:

— dėl kurių buvo užregistruoti sąveikumo bandymų prašymai;

— kuriems buvo išduotas sąveikumo sertifikatas (kad ir laikinas);

— kuriems buvo išduotas tipo patvirtinimo pažymėjimas.

8.6 **Išimtinė procedūra: pirmieji sąveikumo sertifikatai, skirti 2-osios kartos tachografams ir tachografo kortelėms**

455) Keturis mėnesius po to, kai patvirtinama, kad pirmoji 2-osios kartos tachografo ir 2-osios kartos tachografo kortelių (vairuotojo, dirbtuvių, kontrolės ir įmonės kortelių) pora yra sąveiki, visi pagal tuo laikotarpiu užregistruotus prašymus išduoti sąveikumo sertifikatai (įskaitant ir patį pirmąjį) yra laikinieji.

456) Jei šiam laikotarpiui pasibaigus visi atitinkami gaminiai yra sąveikūs, visi atitinkami sąveikumo sertifikatai tampa nuolatiniais.

457) Jei per šį laikotarpį aptinkama sąveikumo trūkumų, už sąveikumo bandymus atsakinga laboratorija, padedama visų susijusių gamintojų, turi nustatyti jų priežastis ir pasiūlyti gamintojams padaryti reikiamus pakeitimus.

458) Jei pasibaigus šiam laikotarpiui lieka sąveikumo nesklandumų, už sąveikumo bandymus atsakinga laboratorija, kartu su susijusiais gamintojais ir atitinkamus veikimo sertifikatus išdavusiomis tipo patvirtinimo institucijomis turi rasti sąveikumo trūkumų priežastis ir nustatyti, kokius pakeitimus turi padaryti kiekvienas susijęs gamintojas. Techninių sprendimų ieškoma ne ilgiau kaip du mėnesius, o jei per tą laiką bendro sprendimo nerandama, Komisija, pasikonsultavusi su laboratorija, atsakinga už sąveikumo bandymus, nusprendžia, kuris tachografas (-ai) ir kortelės gauna nuolatinį sąveikumo sertifikatą, ir nurodo priežastis.

459) Sąveikumo bandymų prašymai, užregistruoti laboratorijoje nuo keturių mėnesių laikotarpio, išdavus pirmąjį laikinojo sąveikumo sertifikatą, pabaigos iki 455 reikalavime nurodyto Komisijos sprendimo priėmimo datos, atidedami iki bus išspręsti pradiniai sąveikumo nesklandumai. Vėliau tokie prašymai nagrinėjami chronologine jų registracijos tvarka.

▼B

1 priedėlis

DUOMENŲ ŽINYNAS

TURINYS

1. ĮVADAS

1.1. Duomenų tipų apibrėžčių metodas

1.2. Nuorodos

2. DUOMENŲ TIPŲ APIBRĖŽTYS

2.1. ActivityChangeInfo

2.2. Adresas

2.3. AESKey

2.4. AES128Key

2.5. AES192Key

2.6. AES256Key

2.7. BCDString

2.8. CalibrationPurpose

2.9. CardActivityDailyRecord

2.10. CardActivityLengthRange

2.11. CardApprovalNumber

2.12. CardCertificate

2.13. CardChipIdentification

2.14. CardConsecutiveIndex

2.15. CardControlActivityDataRecord

2.16. CardCurrentUse

2.17. CardDriverActivity

2.18. CardDrivingLicenceInformation

2.19. CardEventData

2.20. CardEventRecord

2.21. CardFaultData

2.22. CardFaultRecord

2.23. CardIccIdentification

2.24. CardIdentification

2.25. CardMACertificate

2.26. CardNumber

2.27. CardPlaceDailyWorkPeriod

2.28. CardPrivateKey

2.29. CardPublicKey

▼B

2.30. CardRenewalIndex

2.31. CardReplacementIndex

2.32. CardSignCertificate

2.33. CardSlotNumber

2.34. CardSlotsStatus

2.35. CardSlotsStatusRecordArray

2.36. CardStructureVersion

2.37. CardVehicleRecord

2.38. CardVehiclesUsed

2.39. CardVehicleUnitRecord

2.40. CardVehicleUnitsUsed

2.41. Certificate

2.42. CertificateContent

2.43. CertificateHolderAuthorisation

2.44. CertificateRequestID

2.45. CertificationAuthorityKID

2.46. CompanyActivityData

2.47. CompanyActivityType

2.48. CompanyCardApplicationIdentification

2.49. CompanyCardHolderIdentification

2.50. ControlCardApplicationIdentification

2.51. ControlCardControlActivityData

2.52. ControlCardHolderIdentification

2.53. ControlType

2.54. CurrentDateTime

2.55. CurrentDateTimeRecordArray

2.56. DailyPresenceCounter

2.57. Datef

2.58. DateOfDayDownloaded

2.59. DateOfDayDownloadedRecordArray

2.60. Distance

2.61. DriverCardApplicationIdentification

▼B

2.62. DriverCardHolderIdentification

2.63. DSRCSecurityData

2.64. EGFCertificate

2.65. EmbedderIcAssemblerId

2.66. EntryTypeDailyWorkPeriod

2.67. EquipmentType

2.68. EuropeanPublicKey

2.69. EventFaultRecordPurpose

2.70. EventFaultType

2.71. ExtendedSealIdentifier

2.72. ExtendedSerialNumber

2.73. FullCardNumber

2.74. FullCardNumberAndGeneration

2.75. Generation

2.76. GeoCoordinates

2.77. GNSSAccuracy

2.78. GNSSContinuousDriving

2.79. GNSSContinuousDrivingRecord

2.80. GNSSPlaceRecord

2.81. HighResOdometer

2.82. HighResTripDistance

2.83. HolderName

2.84. InternalGNSSReceiver

2.85. K-ConstantOfRecordingEquipment

2.86. KeyIdentifier

2.87. KMWCKey

2.88. Language

2.89. LastCardDownload

2.90. LinkCertificate

2.91. L-TyreCircumference

2.92. MAC

2.93. ManualInputFlag

2.94. ManufacturerCode

2.95. ManufacturerSpecificEventFaultData

2.96. MemberStateCertificate

▼B

2.97. MemberStateCertificateRecordArray

2.98. MemberStatePublicKey

2.99. Name

2.100. NationAlpha

2.101. NationNumeric

2.102. NoOfCalibrationRecords

2.103. NoOfCalibrationsSinceDownload

2.104. NoOfCardPlaceRecords

2.105. NoOfCardVehicleRecords

2.106. NoOfCardVehicleUnitRecords

2.107. NoOfCompanyActivityRecords

2.108. NoOfControlActivityRecords

2.109. NoOfEventsPerType

2.110. NoOfFaultsPerType

2.111. NoOfGNSSCDRecords

2.112. NoOfSpecificConditionRecords

2.113. OdometerShort

2.114. OdometerValueMidnight

2.115. OdometerValueMidnightRecordArray

2.116. OverspeedNumber

2.117. PlaceRecord

2.118. PreviousVehicleInfo

2.119. PublicKey

2.120. RecordType

2.121. RegionAlpha

2.122. RegionNumeric

2.123. RemoteCommunicationModuleSerialNumber

2.124. RSAKeyModulus

2.125. RSAKeyPrivateExponent

2.126. RSAKeyPublicExponent

2.127. RtmData

2.128. SealDataCard

▼B

2.129. SealDataVu

2.130. SealRecord

2.131. SensorApprovalNumber

2.132. SensorExternalGNSSApprovalNumber

2.133. SensorExternalGNSSCoupledRecord

2.134. SensorExternalGNSSIdentification

2.135. SensorExternalGNSSInstallation

2.136. SensorExternalGNSSOSIdentifier

2.137. SensorExternalGNSSSCIdentifier

2.138. SensorGNSSCouplingDate

2.139. SensorGNSSSerialNumber

2.140. SensorIdentification

2.141. SensorInstallation

2.142. SensorInstallationSecData

2.143. SensorOSIdentifier

2.144. SensorPaired

2.145. SensorPairedRecord

2.146. SensorPairingDate

2.147. SensorSCIdentifier

2.148. SensorSerialNumber

2.149. Signature

2.150. SignatureRecordArray

2.151. SimilarEventsNumber

2.152. SpecificConditionRecord

2.153. SpecificConditions

2.154. SpecificConditionType

2.155. Greitis

2.156. SpeedAuthorised

2.157. SpeedAverage

2.158. SpeedMax

2.159. TachographPayload

2.160. TachographPayloadEncrypted

▼B

2.161. TDesSessionKey

2.162. TimeReal

2.163. TyreSize

2.164. VehicleIdentificationNumber

2.165. VehicleIdentificationNumberRecordArray

2.166. VehicleRegistrationIdentification

2.167. VehicleRegistrationNumber

2.168. VehicleRegistrationNumberRecordArray

2.169. VuAbility

2.170. VuActivityDailyData

2.171. VuActivityDailyRecordArray

2.172. VuApprovalNumber

2.173. VuCalibrationData

2.174. VuCalibrationRecord

2.175. VuCalibrationRecordArray

2.176. VuCardIWData

2.177. VuCardIWRecord

2.178. VuCardIWRecordArray

2.179. VuCardRecord

2.180. VuCardRecordArray

2.181. VuCertificate

2.182. VuCertificateRecordArray

2.183. VuCompanyLocksData

2.184. VuCompanyLocksRecord

2.185. VuCompanyLocksRecordArray

2.186. VuControlActivityData

2.187. VuControlActivityRecord

2.188. VuControlActivityRecordArray

▼B

2.189. VuDataBlockCounter

2.190. VuDetailedSpeedBlock

2.191. VuDetailedSpeedBlockRecordArray

2.192. VuDetailedSpeedData

2.193. VuDownloadablePeriod

2.194. VuDownloadablePeriodRecordArray

2.195. VuDownloadActivityData

2.196. VuDownloadActivityDataRecordArray

2.197. VuEventData

2.198. VuEventRecord

2.199. VuEventRecordArray

2.200. VuFaultData

2.201. VuFaultRecord

2.202. VuFaultRecordArray

2.203. VuGNSSCDRecord

2.204. VuGNSSCDRecordArray

2.205. VuIdentification

2.206. VuIdentificationRecordArray

2.207. VuITSConsentRecord

2.208. VuITSConsentRecordArray

2.209. VuManufacturerAddress

2.210. VuManufacturerName

2.211. VuManufacturingDate

2.212. VuOverSpeedingControlData

2.213. VuOverSpeedingControlDataRecordArray

2.214. VuOverSpeedingEventData

▼B

2.215. VuOverSpeedingEventRecord

2.216. VuOverSpeedingEventRecordArray

2.217. VuPartNumber

2.218. VuPlaceDailyWorkPeriodData

2.219. VuPlaceDailyWorkPeriodRecord

2.220. VuPlaceDailyWorkPeriodRecordArray

2.221. VuPrivateKey

2.222. VuPublicKey

2.223. VuSerialNumber

2.224. VuSoftInstallationDate

2.225. VuSoftwareIdentification

2.226. VuSoftwareVersion

2.227. VuSpecificConditionData

2.228. VuSpecificConditionRecordArray

2.229. VuTimeAdjustmentData

2.230. VuTimeAdjustmentGNSSRecord

2.231. VuTimeAdjustmentGNSSRecordArray

2.232. VuTimeAdjustmentRecord

2.233. VuTimeAdjustmentRecordArray

2.234. WorkshopCardApplicationIdentification

2.235. WorkshopCardCalibrationData

2.236. WorkshopCardCalibrationRecord

2.237. WorkshopCardHolderIdentification

2.238. WorkshopCardPIN

2.239. W-VehicleCharacteristicConstant

2.240. VuPowerSupplyInterruptionRecord

▼B

2.241. VuPowerSupplyInterruptionRecordArray

2.242. VuSensorExternalGNSSCoupledRecordArray

2.243. VuSensorPairedRecordArray

3. VERČIŲ IR DYDŽIŲ RIBOS

4. ŽENKLŲ RINKINYS

5. KODUOTĖ

6. OBJEKTO IDENTIFIKATORIAI IR PROGRAMOS IDENTIFIKATORIAI

6.1. Objekto identifikatoriai

6.2. Programos identifikatoriai

1. ĮVADAS

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

1.1. **Duomenų tipų apibrėžčių metodas**

Šiame priedėlyje duomenų tipai apibrėžiami abstrakčiosios sintaksės kalba ASN.1. Ji leidžia paprastus ir struktūriškus 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 sudarytas iš kitų duomenų tipų, duomenų tipo pavadinimas yra viena raidžių seka, prasidedanti didžiąja raide, o kitos didžiosios raidės pavadinime naudojamos atskiriems žodžiams išskirti,

— duomenų tipų pavadinimai apskritai susiję su duomenų tipų, iš kurių jie sudaryti, įrangos, kurioje duomenys laikomi, ir su duomenimis susijusios funkcijos pavadinimais.

Jei ASN.1 tipas 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 identifikatoriais. Verčių diapazono identifikatoriai nurodyti 3 skyriuje ir 2 priedėlyje.

1.2. **Nuorodos**

Šiame priedėlyje naudoti šaltiniai:

ISO 639 Kalbų pavadinimų kodai. Pirmasis leidimas, 1988 m.

▼B

ISO 3166	Šalių ir jų regionų pavadinimų kodai. 1 dalis. Šalių pavadinimų kodai, 2013 m.
ISO 3779	Kelių transporto priemonės. Transporto priemonės identifikavimo numeris (VIN). Turinys ir sandara, 2009 m.
ISO/IEC 7816-5	Atpažinimo kortelės. Lustinės kortelės. 5 dalis. Taikmenų teikėjų registravimas. Antrasis leidimas. 2004.
ISO/IEC 7816-6	Atpažinimo kortelės. Lustinės kortelės. 6 dalis. Tarpsektoriniai duomenų mainų elementai, 2004 m. + Techninių klaidų ištaisymas 1: 2006.
ISO/IEC 8824-1	Informacijos technologija. Pirmos abstrakčios sintaksės specifikacija. Pagrindinės žymėjimo sistemos specifikacija. 2008 + Techninių klaidų ištaisymas 1: 2012 ir Techninių klaidų ištaisymas 2: 2014.
ISO/IEC 8825-2	Informacijos technologija. ASN.1 kodavimo taisyklės. Pakuojamojo kodavimo taisyklių aprašas. 2008.
ISO/IEC 8859-1	Informacijos technologija. 8 bitais koduotų ženklų rinkiniai. 1 dalis. Lotynų 1-oji abėcėlė. Pirmoji laida. 1998.
ISO/IEC 8859-7	Informacijos technologija. 8 bitais koduotų ženklų rinkiniai. 7 dalis. Lotynų/graikų abėcėlė. 2003.
ISO 16844-3	Kelių transporto priemonės. Tachografų sistemos. Judesio jutiklių sąsaja. 2004 + Techninių klaidų ištaisymas 1: 2006.
TR-03110-3	BSI / ANSSI techninės gairės TR-03110-3, Pažangūs saugos mechanizmai mašininio skaitymo kelionės dokumentams ir prieigos raktas eIDAS. 3 dalis. Bendrosios specifikacijos, red. 2.20, 2015 m. vasario 3 d.

2. DUOMENŲ TIPŲ APIBRĖŽTYS

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

Jei nenurodyta kitaip, visi duomenų tipai naudojami 1-osios kartos ir 2-osios kartos sistemose.

2.1. **ActivityChangeInfo**

Šiuo duomenų tipu dviejų baitų ilgio žodžiu užkoduojama vairuotojo arba vairuotojo porininko kortelės lizdo 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 1C priedo 105, 266, 291, 320, 321, 343 ir 344 reikalavimais.

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

Priskiriamos vertės. Sinchronizavimas pagal oktetą ‘scpaatttttttttt’B (16 bitų)

Įrašams duomenų atmintyje (arba kortelės lizdo būsena)

‘s’B	Kortelės lizdas: ‘0’B: VAIRUOTOJAS, ‘1’B: VAIRUOTOJAS PORININKAS,

▼B

‘c’B	Važiavimo būsena:
	‘0’B: VIENAS VAIRUOTOJAS,
	‘1’B: ĮGULA,
‘p’B	Vairuotojo (arba dirbtuvių) kortelės būsena atitinkamame kortelės lizde:
	‘0’B: ĮSTATYTA, kortelė įstatyta,
	‘1’B: NEĮSTATYTA, kortelė neįstatyta (arba išimta),
‘aa’B	Veikla:
	‘00’B: PERTRAUKA/POILSIS,
	‘01’B: PASIRENGĘS DIRBTI,
	‘10’B: DARBAS,
	‘11’B: VAIRAVIMAS,
‘ttttttttttt’B	Pokyčio laikas: minučių skaičius nuo tos dienos 00:00 val.

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

‘s’B	Kortelės lizdas (netaikytina, kai „p“ = 1, išskyrus kaip nurodyta pastaboje):
	‘0’B: VAIRUOTOJAS,
	‘1’B: VAIRUOTOJAS PORININKAS,
‘c’B	Važiavimo būsena (kai „p“ = 0) arba
	Kita veiklos būsena (kai „p“ = 1):
	‘0’B: VIENAS VAIRUOTOJAS,
	‘0’B: NEŽINOMA
	‘1’B: ĮGULA,
	‘1’B: ŽINOMA (= įvesta rankomis)
‘p’B	Kortelės būsena:
	‘0’B: ĮSTATYTA, kortelė įstatyta į tachografą,
	‘1’B: NEĮSTATYTA, kortelė neįstatyta (arba išimta),
‘aa’B	Veikla (netaikytina, kai „p“ = 1 ir „c“ = 0, išskyrus kaip nurodyta pastaboje):
	‘00’B: PERTRAUKA/POILSIS,
	‘01’B: PASIRENGĘS DIRBTI,
	‘10’B: DARBAS,
	‘11’B: VAIRAVIMAS,
‘ttttttttttt’B	Pokyčio laikas: minučių skaičius nuo tos dienos 00:00 val.

▼B

Pastaba atvejui „Kortelės išėmimas“

Kai kortelė išimama:

— „s“ taikytina ir nurodo kortelės lizdą, iš kurio kortelė buvo išimta,

— „c“ vertė turi būti 0,

— „p“ vertė turi būti 1,

— „aa“ turi koduoti tuo metu pasirinktą veiklą.

Įvedant rankomis žodžio dalys „c“ ir „aa“ (laikomos kortelės atmintyje) vėliau gali būti perrašytos, kad matytųsi, kas buvo įvesta.

2.2. **Adresas**

Adresas.

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

codePage nurodo rašmenų rinkinį, apibrėžtą 4 skyriuje,

address yra adresas, užkoduotas naudojant nurodytą rašmenų rinkinį.

2.3. **AESKey**

2-oji karta.

128, 192 arba 256 ilgio raktas AES.

```
AESKey ::= CHOICE {
   aes128Key                         AES128Key,
   aes192Key                         AES192Key,
   aes256Key                         AES256Key
}
```

Priskiriamos vertės: tiksliau nenustatyta.

2.4. **AES128Key**

2-oji karta.

Raktas AES128.

```
AES128Key ::= SEQUENCE {
   length                            INTEGER(0..255),
   aes128Key                         OCTET STRING (SIZE(16))
}
```

length reiškia rakto AES128 ilgį oktetais.

aes128Key yra 128 bitų raktas AES.

Priskiriamos vertės:

Ilgio vertė turi būti 16.

▼B

2.5. **AES192Key**

2-oji karta.

Raktas AES192.

```
AES192Key ::= SEQUENCE {
   length                                INTEGER(0..255),
   aes192Key                             OCTET STRING (SIZE(24))
}
```

length reiškia rakto AES192 ilgį oktetais.

aes192Key yra 192 bitų raktas AES.

Priskiriamos vertės:

Ilgio vertė turi būti 24.

2.6. **AES256Key**

2-oji karta.

Raktas AES256.

```
AES256Key ::= SEQUENCE {
   length                                INTEGER(0..255),
   aes256Key                             OCTET STRING (SIZE(32))
}
```

length reiškia rakto AES256 ilgį oktetais.

aes256Key yra 256 bitų raktas AES.

Priskiriamos vertės:

Ilgio vertė turi būti 32.

2.7. **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 reikšmingiausias okteto pusinis oktetas. Jei reikia, daugiau oktetų sudaroma nuo paties kairiausio pusinio okteto pozicijos pirmajame oktete įterpiant pusinius oktetus, kurie baigiasi nuliu.

Leidžiami šie skaitmenys: 0, 1, … 9.

2.8. **CalibrationPurpose**

Šis kodas paaiškina, kodėl buvo įrašytas kalibravimo parametrų rinkinys. Šis duomenų tipas susijęs su 1B priedo 097 ir 098 reikalavimais ir 1C priedo 119 reikalavimu.

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

▼B

Priskiriamos vertės:

1-oji karta.

‘00’H	rezervuotoji vertė,
‘01’H	aktyvinimas: žinomų kalibravimo parametrų įrašymas aktyvinant transporto priemonės bloką,
‘02’H	pirmasis įrengimas: pirmasis transporto priemonės bloko kalibravimas atlikus jo aktyvinimą,
‘03’H	įrengimas: pirmasis transporto priemonės bloko kalibravimas esamoje transporto priemonėje,
‘04’H	periodinė patikra.

2-oji karta.

Be 1-osios kartos verčių, vartojamos šios vertės:

‘05’H	įmonė įrašė transporto priemonės registracijos numerį,
‘06’H	laiko koregavimas be kalibravimo,
‘07’H – ‘7F’H	rezervuota panaudoti vėliau;
‘80’H – ‘FF’H	nustato gamintojas.

2.9. **CardActivityDailyRecord**

Kortelės atmintyje laikoma informacija, susijusi su vairuotojo veikla konkrečią kalendorinę dieną. Šis duomenų tipas susijęs su 1C priedo 266, 291, 320 ir 343 reikalavimais.

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

activityPreviousRecordLength yra ankstesnio dienos įrašo bendras ilgis baitais. Didžiausią galimą vertę apibrėžia OKTETO EILUTĖS, kurioje yra tie įrašai, ilgis (žr. 2 priedėlio 4 dalį, CardActivityLengthRange). Kai šis įrašas tampa seniausiu dienos įrašu, activityPreviousRecordLength vertė turi būti 0.

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

activityRecordDate yra įrašo data.

▼B

activityDailyPresenceCounter yra kortelės buvimo tą dieną skaitiklis.

activityDayDistance yra bendras tą dieną nuvažiuotas atstumas.

activityChangeInfo yra duomenų ActivityChangeInfo 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.

2.10. **CardActivityLengthRange**

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

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

Priskiriamos vertės: žr. 2 priedėlį.

2.11. **CardApprovalNumber**

Kortelės tipo patvirtinimo numeris.

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

Priskiriamos vertės:

Turi būti pateikiamas toks patvirtinimo numeris, koks paskelbtas atitinkamoje Europos Komisijos interneto svetainėje, pvz., su brūkšneliais, jei yra. Patvirtinimo numeris turi būti lygiuojamas kairėje.

2.12. **CardCertificate**

1-oji karta.

Kortelės viešojo rakto pažymėjimas.

```
CardCertificate ::= Certificate
```

2.13. **CardChipIdentification**

Kortelės atmintyje laikoma informacija apie kortelės lusto identifikaciją (1C priedo 249 reikalavimas). icSerialNumber ir icManufacturingReferences yra kortelės mikroschemos unikalios identifikacijos priemonės. Kortelės mikroschemos unikaliai identifikacijai vien tik icSerialNumber neužtenka.

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

icSerialNumber yra lusto serijos numeris.

icManufacturingReferences yra lusto gamintojo identifikatorius.

2.14. **CardConsecutiveIndex**

Kortelės numeracijos indeksas (h apibrėžtis).

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

Priskiriamos vertės: (žr. 1C priedo 7 skyrių)

Didėjimo tvarka: ‘0, …, 9, A, …, Z, a, …, z’

▼B

2.15. **CardControlActivityDataRecord**

Vairuotojo arba dirbtuvių kortelės atmintyje laikoma informacija apie paskutinę vairuotojo kontrolę (1C priedo 274, 299, 327 ir 350 reikalavimai).

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

controlType yra kontrolės rūšis.

controlTime yra kontrolės data ir laikas.

controlCardNumber yra kontrolės pareigūno FullCardNumber.

controlVehicleRegistration yra transporto priemonės, kurioje atlikta kontrolė, registracijos numeris ir tą transporto priemonę užregistravusi valstybė narė.

controlDownloadPeriodBegin ir **controlDownloadPeriodEnd** žymi laikotarpio, kurio duomenys perkelti, pradžią ir pabaigą (jei duomenys buvo parsisiųsti).

2.16. **CardCurrentUse**

Informacija apie tikrąjį kortelės naudojimą (1C priedo 273, 298, 326 ir 349 reikalavimai).

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

sessionOpenTime yra laikas, kada kortelė įstatyta dabartiniam naudojimui. Išimant kortelę nustatoma nulinė vertė.

sessionOpenVehicle yra tuo metu naudojamos transporto priemonės identifikacija, nustatyta įstačius kortelę. Išimant kortelę nustatoma nulinė vertė.

2.17. **CardDriverActivity**

Vairuotojo arba dirbtuvių kortelės atmintyje laikoma informacija apie vairuotojo veiklą (1C priedo 267, 268, 292, 293, 321 ir 344 reikalavimai).

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

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

▼B

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

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

Priskiriamos vertės: į šią okteto eilutę ciklišk ai įrašomi CardActivityDailyRecord įrašai. Pirmą kartą pradedama rašyti nuo pirmojo eilutės baito. Visi nauji įrašai prirašomi prie ankstesniųjų pabaigos. Kai eilutė užpildoma, vėl pradedama rašyti nuo pirmojo jos baito, 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, ir atstatyta šio (naujo) seniausio užbaigto dienos įrašo parametro activityPreviousRecord-Length vertė 0.

2.18. **CardDrivingLicenceInformation**

Vairuotojo kortelės atmintyje laikoma informacija, susijusi su kortelės turėtojo vairuotojo pažymėjimo duomenimis (1C priedo 259 ir 284 reikalavimas).

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

drivingLicenceIssuingAuthority yra už vairuotojo pažymėjimo išdavimą atsakinga institucija.

drivingLicenceIssuingNation yra vairuotojo pažymėjimą išdavusios institucijos valstybė.

drivingLicenceNumber yra vairuotojo pažymėjimo numeris.

2.19. **CardEventData**

Vairuotojo arba dirbtuvių kortelės atmintyje laikoma informacija apie įvykius, susijusius su kortelės turėtoju (1C priedo 260, 285, 318 ir 341 reikalavimai).

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

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

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

▼B

2.20. **CardEventRecord**

Vairuotojo arba dirbtuvių kortelės atmintyje laikoma informacija apie įvykį, susijusį su kortelės turėtoju (1C priedo 261, 286, 318 ir 341 reikalavimai).

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

eventType yra įvykio rūšis.

eventBeginTime yra įvykio pradžios data ir laikas.

eventEndTime yra įvykio pabaigos data ir laikas.

eventVehicleRegistration yra transporto priemonės, kurioje įvykis įvyko, registracijos numeris ir tą transporto priemonę užregistravusi valstybė narė.

2.21. **CardFaultData**

Vairuotojo arba dirbtuvių kortelės atmintyje laikoma informacija apie triktis, susijusias su kortelės turėtoju (1C priedo 263, 288, 318 ir 341 reikalavimai).

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

CardFaultData yra įrašų apie tachografo triktis seka ir po jos einanti įrašų apie kortelės triktis seka.

cardFaultRecords yra įrašų apie tam tikros rūšies (tachografo arba kortelės) triktis rinkinys.

2.22. **CardFaultRecord**

Vairuotojo arba dirbtuvių kortelės atmintyje laikoma informacija apie triktį, susijusią su kortelės turėtoju (1C priedo 264, 289, 318 ir 341 reikalavimai).

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

faultType yra trikties rūšis.

faultBeginTime yra trikties pradžios data ir laikas.

faultEndTime yra trikties pabaigos data ir laikas.

faultVehicleRegistration yra transporto priemonės, kurioje įvyko triktis, registracijos numeris ir tą transporto priemonę užregistravusi valstybė narė.

▼B

2.23. **CardIccIdentification**

Kortelės atmintyje laikoma lustinės kortelės identifikacijos informacija (1C priedo 248 reikalavimus).

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

clockStop yra 2 priedėlyje nustatytas režimas Clockstop.

cardExtendedSerialNumber yra unikalus lustinės kortelės serijos numeris, kuris konkrečiau apibūdinamas duomenų tipu ExtendedSerial-Number.

cardApprovalNumber yra kortelės tipo patvirtinimo numeris.

cardPersonaliserID yra kortelės individualizuotojo identifikatorius, užkoduojamas duomenų elementu ManufacturerCode.

embedderIcAssemblerId pateikiama informacija apie įmontuotoją (lusto surinkėją).

icIdentifier yra kortelės lusto ir lusto gamintojo identifikatorius, kaip nurodyta ISO/IEC 7816-6.

2.24. **CardIdentification**

Kortelės atmintyje laikoma informacija apie kortelės identifikaciją (1C priedo 255, 280, 310, 333, 359, 365, 371 ir 377 reikalavimai).

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

cardIssuingMemberState yra kortelę išdavusios valstybės narės kodas.

cardNumber yra kortelės numeris.

cardIssuingAuthorityName yra kortelę išdavusios institucijos pavadinimas.

cardIssueDate yra kortelės išdavimo dabartiniam turėtojui data.

cardValidityBegin yra kortelės galiojimo pradžios data.

cardExpiryDate yra kortelės galiojimo pabaigos data.

▼B

2.25. **CardMACertificate**

2-oji karta.

Kortelės viešojo rakto pažymėjimas abipusiam autentiškumo tikrinimui su transporto priemonės bloku. Šio pažymėjimo struktūra apibūdinta 11 priedėlyje.

```
CardMACertificate ::= Certificate
```

2.26. **CardNumber**

Kortelės numeris pagal g apibrėžtį.

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

driverIdentification yra unikali vairuotojo identifikacija valstybėje narėje.

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

cardConsecutiveIndex yra kortelės numeracijos indeksas.

cardReplacementIndex yra kortelės pakeitimo indeksas.

cardRenewalIndex yra kortelės atnaujinimo indeksas.

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

2.27. **CardPlaceDailyWorkPeriod**

Vairuotojo arba dirbtuvių kortelės atmintyje laikoma informacija apie vietas, kuriose prasideda ir (arba) baigiasi dienos darbo laikotarpiai (1C priedo 272, 297, 325 ir 348 reikalavimai).

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

placePointerNewestRecord yra paskutinio atnaujinto įrašo apie vietą indeksas.

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

placeRecords yra įrašų rinkinys, kuriame kaupiama informacija apie įvestas vietas.

▼B

2.28. **CardPrivateKey**

1-oji karta.

Kortelės privatusis raktas.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.29. **CardPublicKey**

Kortelės viešasis raktas.

```
CardPublicKey ::= PublicKey
```

2.30. **CardRenewalIndex**

Kortelės atnaujinimo indeksas (i apibrėžtis).

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

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

‘0’ Pirmasis išdavimas.

Didėjimo tvarka: ‘0, …, 9, A, …, Z’

2.31. **CardReplacementIndex**

Kortelės pakeitimo indeksas (j apibrėžtis).

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

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

‘0’ Pirmoji kortelė.

Didėjimo tvarka: ‘0, …, 9, A, …, Z’

2.32. **CardSignCertificate**

2-oji karta.

Kortelės viešojo rakto pažymėjimas parašui. Šio pažymėjimo struktūra apibūdinta 11 priedėlyje.

```
CardSignCertificate ::= Certificate
```

2.33. **CardSlotNumber**

Kodas, kuriuo atskiriami du transporto priemonės bloko kortelės lizdai.

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

Priskiriamos vertės: tiksliau nenustatyta.

2.34. **CardSlotsStatus**

Kodas, kuriuo nurodoma, kokių rūšių kortelės įstatytos į du transporto priemonės bloko kortelių lizdus.

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

▼B

Priskiriamos vertės. Sinchronizavimas pagal oktetą ‘ccccdddd’B

‘cccc’B — į vairuotojo porininko kortelės lizdą įstatytos kortelės rūšies identifikacija;

‘dddd’B — į vairuotojo kortelės lizdą įstatytos kortelės rūšies identifikacija;

tokiais identifikacijos kodais:

‘0000’B — neįstatyta jokia kortelė;

‘0001’B — įstatyta vairuotojo kortelė;

‘0010’B — įstatyta dirbtuvių kortelė;

‘0011’B — įstatyta kontrolės kortelė;

‘0100’B — įstatyta įmonės kortelė.

2.35. **CardSlotsStatusRecordArray**

2-oji karta.

CardSlotsStatus ir duomenų parsisiuntimo protokole naudojami metaduomenys.

```
CardSlotsStatusRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CardSlotsStatus
}
```

recordType žymi įrašo rūšį (CardSlotsStatus). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento CardSlotsStatus dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra duomenų elemento CardSlotsStatus įrašų rinkinys.

2.36. **CardStructureVersion**

Kodas, kuriuo nurodoma tachografo kortelėje įgyvendintos struktūros versija.

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

Priskiriamos vertės: ‘aabb’H:

‘aa’H — Struktūros pakeitimų indeksas.

‘00’H skirta 1-osios kartos sistemoms

‘01’H skirta 2-osios kartos sistemoms

‘bb’H — Aukštesniuoju baitu nurodytai struktūrai nustatytų duomenų elementų naudojimo pakeitimų indeksas.

‘00’H skirta šios versijos 1-osios kartos sistemoms

‘00’H skirta šios versijos 2-osios kartos sistemoms

▼B

2.37. **CardVehicleRecord**

Vairuotojo arba dirbtuvių kortelės atmintyje laikoma informacija apie transporto priemonės naudojimo laikotarpį kalendorinę dieną (1C priedo 269, 294, 322 ir 345 reikalavimai).

1-oji karta.

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

vehicleOdometerBegin yra transporto priemonės odometro rodmens vertė transporto priemonės naudojimo laikotarpio pradžioje.

vehicleOdometerEnd yra transporto priemonės odometro rodmens vertė transporto priemonės naudojimo laikotarpio pabaigoje.

vehicleFirstUse yra transporto priemonės naudojimo laikotarpio pradžios data ir laikas.

vehicleLastUse yra transporto priemonės naudojimo laikotarpio pabaigos data ir laikas.

vehicleRegistration yra transporto priemonės registracijos numeris ir tą transporto priemonę užregistravusi valstybė narė.

vuDataBlockCounter yra duomenų elemento VuDataBlockCounter vertė tada, kai paimtas paskutinis transporto priemonės naudojimo laikotarpio išrašas.

2-oji karta.

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

Be 1-osios kartos verčių, naudojamas šis duomenų elementas:

VehicleIdentificationNumber yra visą transporto priemonę žymintis transporto priemonės identifikavimo numeris.

2.38. **CardVehiclesUsed**

Vairuotojo arba dirbtuvių kortelės atmintyje laikoma informacija apie transporto priemones, kurias naudoja kortelės turėtojas (1C priedo 270, 295, 323 ir 346 reikalavimai).

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

vehiclePointerNewestRecord yra paskutinio atnaujinto transporto priemonės įrašo indeksas.

▼B

Priskiriamos vertės: skaičius, atitinkantis transporto priemonės įrašo (trupmenos) skaitiklio vertę; pirmojo transporto priemonės įrašo struktūroje vertė yra 0.

cardVehicleRecords yra įrašų rinkinys, kuriame kaupiama informacija apie naudojamas transporto priemones.

2.39. **CardVehicleUnitRecord**

2-oji karta.

Vairuotojo arba dirbtuvių kortelės atmintyje laikoma informacija apie naudojamą transporto priemonės bloką (1C priedo 303 ir 351 reikalavimai).

```
CardVehicleUnitRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   manufacturerCode                       ManufacturerCode,
   deviceID                               INTEGER(0..255),
   vuSoftwareVersion                      VuSoftwareVersion
}
```

timeStamp yra transporto priemonės bloko naudojimo laikotarpio pradžia (t. y. pirmas per laikotarpį kortelės įstatymas į transporto priemonės bloką).

manufacturerCode identifikuoja transporto priemonės bloko gamintoją.

deviceID identifikuoja gamintojo priskirtą transporto priemonės bloko tipą. Ši vertė yra būdinga tik tam gamintojui.

vuSoftwareVersion yra transporto priemonės bloko programinės įrangos versijos numeris.

2.40. **CardVehicleUnitsUsed**

2-oji karta.

Vairuotojo arba dirbtuvių kortelės atmintyje laikoma informacija apie kortelės turėtojo naudotus transporto priemonės blokus (1C priedo 306 ir 352 reikalavimai).

```
CardVehicleUnitsUsed := SEQUENCE {
   vehicleUnitPointerNewestRecord       INTEGER(0..NoOfCardVehicleUnitRecords-1),
   cardVehicleUnitRecords               SET SIZE(NoOfCardVehicleUnitRecords) OF
                                        CardVehicleUnitRecord
}
```

vehicleUnitPointerNewestRecord yra paskutinio atnaujinto transporto priemonės bloko įrašo indeksas.

Priskiriamos vertės: skaičius, atitinkantis transporto priemonės bloko įrašo (trupmenos) skaitiklio vertę; pirmojo transporto priemonės bloko įrašo struktūroje vertė yra 0.

cardVehicleUnitRecords yra įrašų rinkinys, kuriame kaupiama informacija apie naudojamus transporto priemonės blokus.

2.41. **Certificate**

Pažymėjimų išdavimo institucijos išduodamas viešojo rakto pažymėjimas.

1-oji karta.

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

▼B

Priskiriamos vertės: skaitmeninis parašas su daliniu duomenų elemento CertificateContent atkūrimu pagal 11 priedėlį „Bendrieji apsaugos mechanizmai“ Parašas (128 baitai) || Viešojo rakto liekana (58 baitai) || Pažymėjimų išdavimo institucijos žymuo (8 baitai).

2-oji karta.

```
Certificate ::= OCTET STRING (SIZE(204..341))
```

Priskiriamos vertės: Žr. 11 priedėlį.

2.42. **CertificateContent**

1-oji karta.

Viešojo 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 yra atitinkamo pažymėjimo versija.

Priskiriamos vertės: ‘01h’ (šios versijos).

certificationAuthorityReference žymi pažymėjimą išdavusią pažymėjimų išdavimo instituciją. Jis taip pat žymi šios pažymėjimų išdavimo institucijos viešąjį raktą.

certificateHolderAuthorisation žymi pažymėjimo turėtojo teises.

certificateEndOfValidity yra pažymėjimo administracinio galiojimo pabaigos data.

certificateHolderReference žymi pažymėjimo turėtoją. Taip pat žymi viešąjį raktą.

publicKey yra viešasis raktas, kuris patvirtinamas šiuo pažymėjimu.

2.43. **CertificateHolderAuthorisation**

Pažymėjimo turėtojo teisių identifikacija.

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

1-oji karta.

tachographApplicationID yra tachografo programos identifikatorius.

Priskiriamos vertės: ‘FFh’ ‘54h’ ‘41h’ ‘43h’ ‘48h’ ‘4Fh’. AID yra patentuotas neregistruotos programos identifikatorius 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**.

▼B

2-oji karta.

tachographApplicationID žymi 2-osios kartos tachografų kortelių programos identifikatoriaus (AID) 6 reikšmingiausius baitus. Tachografų kortelių taikomosios programos AID apibūdinta 6.2 skyriuje.

Priskiriamos vertės: ‘FF 53 4D 52 44 54’.

equipmentType yra 2-osios kartos tachografams nustatytos įrangos, kuriai skirtas pažymėjimas, rūšies identifikacija.

Priskiriamos vertės: pagal duomenų tipą EquipmentType.

2.44. **CertificateRequestID**

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

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

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

requestMonthYear yra pažymėjimo prašymo metų ir mėnesio identifikacija.

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

crIdentifier yra identifikatorius, kuriuo pažymėjimo prašymas atskiriamas nuo pailginto serijos numerio.

Priskiriamos vertės: ‘FFh’.

manufacturerCode yra gamintojo, kuris prašo pažymėjimo, skaitinis kodas.

2.45. **CertificationAuthorityKID**

Pažymėjimų išdavimo institucijos (valstybė narė arba Europos pažymėjimų išdavimo institucija) viešojo rakto identifikatorius.

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

nationNumeric yra pažymėjimų išdavimo institucijos raidinis skaitinis valstybės kodas.

nationAlpha yra pažymėjimų išdavimo institucijos raidinis skaitinis valstybės kodas.

▼B

keySerialNumber yra serijos numeris skirtingiems pažymėjimų išdavimo institucijos raktams atskirti, jei jie būtų keičiami.

additionalInfo yra dviejų baitų ilgio sritis papildomam kodui (skirta pažymėjimų išdavimo institucijai).

caIdentifier yra identifikatorius, kuriuo pažymėjimų išdavimo institucijos rakto identifikatorius atskiriamas nuo kitų raktų identifikatorių.

Priskiriamos vertės: ‘01h’.

2.46. **CompanyActivityData**

Įmonės kortelės atmintyje laikoma informacija apie veiklą, vykdytą su kortele (1C priedo 373 ir 379 reikalavimai).

```
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 yra paskutinio atnaujinto įrašo companyActivityRecord indeksas.

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

companyActivityRecords yra visų įrašų apie įmonės veiklą rinkinys.

companyActivityRecord yra informacijos apie vieną įmonės veiklą seka.

companyActivityType yra įmonės veiklos rūšis.

companyActivityTime yra įmonės veiklos data ir laikas.

cardNumberInformation yra kortelės, iš kurios buvo perkelti duomenys, numeris ir ją išdavusi valstybė narė (jei duomenys buvo perkelti iš kortelės).

vehicleRegistrationInformation yra transporto priemonės, iš kurios buvo parsisiųsti, užrakinti arba atrakinti duomenys, registracijos numeris ir tą transporto priemonę užregistravusi valstybė narė.

downloadPeriodBegin ir **downloadPeriodEnd** žymi laikotarpio, kurio duomenys buvo parsisiųsti iš transporto priemonės bloko, pradžią ir pabaigą (jei duomenys buvo parsisiųsti).

2.47. **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)
}
```

▼B

2.48. **CompanyCardApplicationIdentification**

Įmonės kortelės atmintyje laikomi įmonės kortelės naudojimo identifikacijos duomenys (1C priedo 369 ir 375 reikalavimai).

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

typeOfTachographCardId rodo naudojamos kortelės rūšį.

cardStructureVersion rodo kortelės struktūros versiją.

noOfCompanyActivityRecords rodo, kiek įrašų apie įmonės veiklą telpa kortelės atmintyje.

2.49. **CompanyCardHolderIdentification**

Įmonės kortelės atmintyje laikomi kortelės turėtojo identifikacijos duomenys (1C priedo 372 ir 378 reikalavimai).

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

companyName yra įmonės turėtojos pavadinimas.

companyAddress yra įmonės turėtojos adresas.

cardHolderPreferredLanguage yra kortelės turėtojo pageidaujama kalba.

2.50. **ControlCardApplicationIdentification**

Kontrolės kortelės atmintyje laikomi kortelės naudojimo identifikacijos duomenys (1C priedo 357 ir 363 reikalavimai).

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

typeOfTachographCardId rodo naudojamos kortelės rūšį.

cardStructureVersion žymi kortelės struktūros versiją.

noOfControlActivityRecords rodo, kiek įrašų apie kontrolės veiklą telpa kortelės atmintyje.

▼B

2.51. **ControlCardControlActivityData**

Kontrolės kortelės atmintyje laikoma informacija apie kontrolę, vykdytą su kortele (1C priedo 361 ir 367 reikalavimai).

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

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

controlActivityRecords yra visų įrašų apie kontrolės veiklą rinkinys.

controlActivityRecord yra informacijos apie vieną kontrolės veiklą seka.

controlType yra kontrolės rūšis.

controlTime yra kontrolės data ir laikas.

controlledCardNumber yra kontroliuojamos kortelės numeris ir ją išdavusi valstybė narė.

controlledVehicleRegistration yra transporto priemonės, kurioje atlikta kontrolė, registracijos numeris ir tą transporto priemonę užregistravusi valstybė narė.

controlDownloadPeriodBegin ir **controlDownloadPeriodEnd** žymi laikotarpio, kurio duomenys parsisiųsti, pradžią ir pabaigą (jei duomenys buvo parsisiųsti).

2.52. **ControlCardHolderIdentification**

Kontrolės kortelės atmintyje laikomi kortelės turėtojo identifikacijos duomenys (1C priedo 360 ir 366 reikalavimai).

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

controlBodyName yra kortelės turėtojo kontrolės institucija.

controlBodyAddress yra kortelės turėtojo kontrolės institucijos adresas.

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

▼B

cardHolderPreferredLanguage yra kortelės turėtojo pageidaujama kalba.

2.53. **ControlType**

Per kontrolę vykdytos veiklos kodas. Šis duomenų tipas susijęs su 1C priedo 126, 274, 299, 327 ir 350 reikalavimais.

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

1-oji karta.

Priskiriamos vertės. Sinchronizavimas pagal oktetą ‘cvpdxxxx’B (8 bitai)

‘c’B	duomenų perkėlimas iš kortelės:
	‘0’B: šios kontrolės metu duomenys iš kortelės nebuvo parsisiųsti;
	‘1’B: šios kontrolės metu duomenys buvo perkelti iš kortelės;
‘v’B	duomenų perkėlimas iš transporto priemonės bloko:
	‘0’B: šios kontrolės metu duomenys iš transporto priemonės bloko nebuvo parsisiųsti;
	‘1’B: šios kontrolės metu duomenys iš transporto priemonės bloko buvo parsisiųsti;
‘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 naudojamasi;
	‘1’B: šios kontrolės metu ekranu buvo naudojamasi;
‘xxxx’B	Nenaudojama.

2-oji karta.

Priskiriamos vertės. Sinchronizavimas pagal oktetą ‘cvpdexxx’B (8 bitai)

‘c’B	duomenų perkėlimas iš kortelės:
	‘0’B: šios kontrolės metu duomenys iš kortelės nebuvo parsisiųsti;
	‘1’B: šios kontrolės metu duomenys buvo perkelti iš kortelės;
‘v’B	duomenų perkėlimas iš transporto priemonės bloko:
	‘0’B: šios kontrolės metu duomenys iš transporto priemonės bloko nebuvo parsisiųsti;
	‘1’B: šios kontrolės metu duomenys iš transporto priemonės bloko buvo parsisiųsti;
‘p’B	spausdinimas:
	‘0’B: šios kontrolės metu nebuvo spausdinama;
	‘1’B: šios kontrolės metu buvo spausdinama;

▼B

‘d’B	rodymas ekrane:
	‘0’B: šios kontrolės metu ekranu nebuvo naudojamasi;
	‘1’B: šios kontrolės metu ekranu buvo naudojamasi;
‘e’B	kalibravimo tikrinimas kelyje:
	‘0’B: šios kontrolės metu kalibravimo parametrai netikrinti;
	‘1’B: šios kontrolės metu kalibravimo parametrai patikrinti;
‘xxx’B	rezervuota panaudoti vėliau.

2.54. **CurrentDateTime**

Esama data ir laikas, rodomi tachografe.

```
CurrentDateTime ::= TimeReal
```

Priskiriamos vertės: tiksliau nenustatyta.

2.55. **CurrentDateTimeRecordArray**

2-oji karta.

Esama data ir laikas, taip pat duomenų parsisiuntimo protokole naudojami metaduomenys.

```
CurrentDateTimeRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CurrentDateTime
}
```

recordType žymi įrašo rūšį (CurrentDateTime). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento CurrentDateTime dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra esamos datos ir laiko įrašų rinkinys.

2.56. **DailyPresenceCounter**

Vairuotojo arba dirbtuvių kortelės atmintyje laikomas skaitiklis, kurio vertė didinama kiekvieną kalendorinę dieną, kurią kortelė buvo įstatyta į transporto priemonės bloką. Šis duomenų tipas susijęs su 1C priedo 266, 299, 320 ir 343 reikalavimais.

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

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

▼B

2.57. **Datef**

Data, išreikšta lengvai spausdinamu skaitiniu 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.

2.58. **DateOfDayDownloaded**

2-oji karta.

Parsisiuntimo data ir laikas.

```
DateOfDayDownloaded ::= TimeReal
```

Priskiriamos vertės: tiksliau nenustatyta.

2.59. **DateOfDayDownloadedRecordArray**

2-oji karta.

Parsiuntimo data ir laikas, taip pat duomenų parsisiuntimo protokole naudojami metaduomenys.

```
DateofDayDownloadedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       DateOfDayDownloaded
}
```

recordType žymi įrašo rūšį (DateOfDayDownloaded). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento CurrentDateTime dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra parsisiųstų įrašų datos ir laiko rinkinys.

2.60. **Distance**

Nuvažiuotas atstumas (dviejų transporto priemonės odometro rodmens verčių skirtumas kilometrais).

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

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

2.61. **DriverCardApplicationIdentification**

Vairuotojo kortelės atmintyje laikomi kortelės naudojimo identifikacijos duomenys (1C priedo 253 ir 278 reikalavimai).

▼B

1-oji karta.

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

typeOfTachographCardId rodo naudojamos kortelės rūšį.

cardStructureVersion rodo kortelės struktūros versiją.

noOfEventsPerType rodo, kiek vienos rūšies įvykių galima užregistruoti kortelės atmintyje.

noOfFaultsPerType rodo, kiek vienos rūšies trikčių galima užregistruoti kortelės atmintyje.

activityStructureLength rodo laisvų baitų skaičių įrašams apie veiklą.

noOfCardVehicleRecords rodo, kiek įrašų apie transporto priemonę telpa kortelės atmintyje.

noOfCardPlaceRecords rodo, kiek įrašų apie vietas telpa kortelės atmintyje.

2-oji karta.

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

Be 1-osios kartos verčių, naudojami šie duomenų elementai:

noOfGNSSCDRecords rodo, kiek GNSS įrašų apie nepertraukiamą vairavimą telpa kortelės atmintyje.

noOfSpecificConditionRecords rodo, kiek įrašų apie ypatingą būseną telpa kortelės atmintyje.

2.62. **DriverCardHolderIdentification**

Vairuotojo kortelės atmintyje laikomi kortelės turėtojo identifikacijos duomenys (1C priedo 256 ir 281 reikalavimai).

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

▼B

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

cardHolderBirthDate yra vairuotojo kortelės turėtojo gimimo data.

cardHolderPreferredLanguage yra kortelės turėtojo pageidaujama kalba.

2.63. **DSRCSecurityData**

2-oji karta.

Paprastu tekstu pateikiama informacija ir tinklo plokštės adresas (MAC), kurie iš tachografo skirtuoju trumpojo nuotolio ryšiu (DSRC) perduodami į nuotolinį apklausiklį, daugiau žr. 11 priedėlio B dalies 13 skyriuje.

```
DSRCSecurityData ::= SEQUENCE {
   tagLenthPlainText                    OCTET STRING(SIZE(2)),
   currentDateTime                      CurrentDateTime,
   counter                              INTEGER(0..2^24-1),
   vuSerialNumber                       VuSerialNumber,
   dSRCMKVersionNumber                  INTEGER(SIZE(1)),
   tagLengthMac                         OCTET STRING(SIZE(2)),
   mac                                  MAC
}
```

tagLength yra DER-TLV kodavimo dalis, kurios vertė yra ‘81 10’ (žr. 11 priedėlio B dalies 13 skyriuje).

currentDateTime yra transporto priemonės bloko esama data ir laikas.

counter numeruoja RTM pranešimus.

vuSerialNumber yra transporto priemonės bloko serijos numeris.

dSRCMKVersionNumber yra DSRC pagrindinio rakto, iš kurio gaunami transporto priemonės bloko DSRC raktai, versijos numeris.

tagLengthMac yra DER-TLV kodavime naudojamo duomenų objekto MAC žymė ir ilgis. Žymės vertė turi būti ‘8E’, ilgiu užkoduojamas MAC ilgis oktetais (žr, 11 priedėlio B dalies 13 skyrių).

mac yra MAC, apskaičiuotas iš RTM pranešimo (žr. 11 priedėlio B dalies 13 skyrių).

2.64. **EGFCertificate**

2-oji karta.

Išorinio GNSS įrenginio viešojo rakto pažymėjimas abipusiam autentiškumo tikrinimui su transporto priemonės bloku. Šio pažymėjimo struktūra apibūdinta 11 priedėlyje.

```
EGFCertificate ::= Certificate
```

▼B

2.65. **EmbedderIcAssemblerId**

Pateikiama informacija apie lusto įmontuotoją.

```
EmbedderIcAssemblerId ::= SEQUENCE{
   countryCode                          IA5String(SIZE(2)),
   moduleEmbedder                       BCDString(SIZE(2)),
   manufacturerInformation              OCTET STRING(SIZE(1))
}
```

countryCode yra modulio įmontuotojo valstybės 2 raidžių kodas pagal ISO 3166.

moduleEmbedder rodo modulio įmontuoją.

manufacturerInformation skirta gamintojo vidaus naudojimui.

2.66. **EntryTypeDailyWorkPeriod**

Kodas, kuriuo atskiriama įrašo apie dienos darbo laikotarpio vietą pradžia, pabaiga ir įrašo būsena.

1-oji karta.

```
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-oji karta.

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5),
   Begin,  related time based on GNSS data                             (6),
   End     related time based on GNSS data                             (7)
}
```

Priskiriamos vertės: pagal ISO/IEC 8824-1.

2.67. **EquipmentType**

Kodas, kuriuo atskiriama įvairių rūšių įranga, reikalinga tachografo programai.

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

▼B

1-oji karta.

```
 --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-oji karta.

Naudojamos tokios pačios kaip 1-osios kartos vertės su šiais papildymais:

```
--GNSS Facility                         (8),
--Remote Communication Module           (9),
--ITS interface module                  (10),
--Plaque                                (11), -- may be used in SealRecord
--M1/N1 Adapter                         (12), -- may be used in SealRecord
--European Root CA (ERCA)               (13),
--Member State CA (MSCA)                (14),
--External GNSS connection              (15), -- may be used in SealRecord
--Unused                                (16), -- used in SealDataVu
--RFU                                   (17..255)
```

Pastaba. 2-osios kartos plokštelės, adapterio ir GNSS išorinės jungties vertės, taip pat 1-osios kartos transporto priemonės bloko ir judesio jutiklio vertės gali būti naudojamos duomenyse, kurių tipas SealRecord, t. y., jei taikoma.

2.68. **EuropeanPublicKey**

1-oji karta.

Europos viešasis raktas.

```
EuropeanPublicKey ::= PublicKey
```

2.69. **EventFaultRecordPurpose**

Kodas, kuriuo paaiškinama, kodėl įvykis arba triktis buvo užregistruoti.

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

Priskiriamos vertės:

'00'H	vienas iš 10 pastarųjų (arba paskutinių) įvykių arba trikčių;
'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	svarbiausias įvykis per pastarąsias 10 dienų;
'05'H	vienas iš 5 svarbiausių įvykių per pastarąsias 365 dienas;
'06'H	pirmasis įvykis arba triktis po paskutinio kalibravimo;
'07'H	vykstantis (esamas) įvykis arba triktis;
'08'H to '7F'H	rezervuota panaudoti vėliau
'80'H to 'FF'H	nustato gamintojas

▼B

2.70. **EventFaultType**

Įvykio arba trikties apibūdinimo kodas.

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

Priskiriamos vertės:

1-oji karta.

‘0x’H	bendrieji įvykiai;
‘00’H	jokios papildomos informacijos;
‘01’H	įstatyta negaliojanti kortelė;
‘02’H	kortelių nesuderinamumas;
‘03’H	dalinis laiko sutapimas;
‘04’H	važiavimas be reikiamos kortelės;
‘05’H	kortelė įstatyta važiuojant;
‘06’H	netinkamai užbaigtas paskutinis kortelės naudojimo seansas;
‘07’H	greičio viršijimas;
‘08’H	maitinimo nutrūkimas;
‘09’H	duomenų apie judėjimą klaida;
‘0A’H	transporto priemonės judėjimo nesuderinamumas;
‘0B’ to ‘0F’H	rezervuota panaudoti vėliau;
‘1x’H	su transporto priemonės bloku susiję bandymo pažeisti apsaugą įvykiai;
‘10’H	jokios papildomos informacijos;
‘11’H	judesio jutiklio autentiškumo tikrinimo nesėkmė;
‘12’H	tachografo kortelės autentiškumo tikrinimo nesėkmė;
‘13’H	neleistinas judesio jutiklio pakeitimas;
‘14’H	duomenų įvedimo į kortelę nepažeistumo klaida;
‘15’H	laikomų naudotojo duomenų nepažeistumo klaida;
‘16’H	vidinio duomenų perdavimo klaida;
‘17’H	neleistinas korpuso atidarymas;
‘18’H	kenkimas techninei įrangai;
‘19’H to ‘1F’H	rezervuota panaudoti vėliau;
‘2x’H	su jutikliu susiję bandymo pažeisti apsaugą įvykiai;
‘20’H	jokios papildomos informacijos;
‘21’H	autentiškumo tikrinimo nesėkmė;
‘22’H	laikomų duomenų nepažeistumo klaida;
‘23’H	vidinio duomenų perdavimo klaida;
‘24’H	neleistinas korpuso atidarymas;
‘25’H	kenkimas techninei įrangai;
‘26’H to ‘2F’H	rezervuota panaudoti vėliau;
‘3x’H	tachografo triktys;
‘30’H	jokios papildomos informacijos;
‘31’H	transporto priemonės bloko vidinė triktis;
‘32’H	spausdintuvo triktis;
‘33’H	ekrano triktis;
‘34’H	duomenų perkėlimo triktis;
‘35’H	jutiklio triktis;
‘36’H to ‘3F’H	rezervuota panaudoti vėliau;
‘4x’H	kortelės triktys;
‘40’H	jokios papildomos informacijos;
‘41’H to ‘4F’H	rezervuota panaudoti vėliau;
‘50’H to ‘7F’H	rezervuota panaudoti vėliau;
‘80’H to ‘FF’H	nustato gamintojas.

▼B

2-oji karta.

Naudojamos tokios pačios kaip 1-osios kartos vertės su šiais papildymais:

‘0B’H	nesuderintas laikas (transporto priemonės bloko vidaus laikrodis, palyginti su GNSS)
‘0C’ to ‘0F’H	rezervuota panaudoti vėliau;
‘5x’H	su GNSS susijusios triktys;
‘50’H	jokios papildomos informacijos;
‘51’H	GNSS vidinio imtuvo triktis;
‘52’H	GNSS išorinio imtuvo triktis;
‘53’H	GNSS išorinio ryšio triktis;
‘54’H	nėra buvimo vietos nustatymo duomenų iš GNSS;
‘55’H	aptiktas piktavališkas GNSS duomenų keitimas;
‘56’H	baigėsi išorinio GNSS įrenginio pažymėjimo galiojimas;
‘57’H to ‘5F’H	rezervuota panaudoti vėliau;
‘6x’H	su nuotolinio ryšio moduliu susijusios triktys;
‘60’H	jokios papildomos informacijos;
‘61’H	nuotolinio ryšio modulio triktis;
‘62’H	nuotolinio ryšio modulio ryšio triktis;
‘63’H to ‘6F’H	rezervuota panaudoti vėliau;
‘7x’H	sąsajos ITS triktys;
‘70’H	jokios papildomos informacijos;
‘71’H to ‘7F’H	rezervuota panaudoti vėliau.

2.71. **ExtendedSealIdentifier**

2-oji karta.

Pailgintas unikalus plombos identifikatorius (1C priedo 401 reikalavimas)

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                    OCTET STRING (SIZE(2)),
   sealIdentifier                      OCTET STRING (SIZE(6))
}
```

manufacturerCode yra plombos gamintojo kodas.

sealIdentifier yra plombos identifikatorius, skirtingas kiekvienam gamintojui.

2.72. **ExtendedSerialNumber**

Unikali įrangos identifikacija. Ją galima naudoti ir kaip įrangos viešojo rakto identifikatorių.

1-oji karta.

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

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

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

▼B

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

type yra įrangos rūšies identifikatorius.

Priskiriamos vertės: nustato gamintojas, rezervuota vertė ‘FFh’.

manufacturerCode: patvirtintos rūšies įrangos gamintojo identifikavimo skaitinis kodas.

2-oji karta.

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

serialNumber žr. prie 1-osios kartos.

monthYear žr. prie 1-osios kartos.

type žymi įrangos rūšį.

manufacturerCode: žr. prie 1-osios kartos.

2.73. **FullCardNumber**

Tachografo kortelę visiškai identifikuojantis kodas.

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

cardType yra tachografo kortelės rūšis.

cardIssuingMemberState yra kortelę išdavusios valstybės narės kodas.

cardNumber yra kortelės numeris.

2.74. **FullCardNumberAndGeneration**

2-oji karta.

Tachografo kortelę ir jos kartą visiškai identifikuojantis kodas.

```
FullCardNumberAndGeneration ::= SEQUENCE {
   fullCardNumber                        FullCardNumber,
   generation                            Generation
}
```

fullcardNumber žymi tachografo kortelę.

generation žymi naudojamos tachografo kortelės kartą.

▼B

2.75. **Generation**

2-oji karta.

Žymi naudojamos tachografo kortelės kartą.

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

Priskiriamos vertės:

‘00’H	rezervuota panaudoti vėliau
‘01’H	1-oji karta.
‘02’H	2-oji karta.
‘03’H … ‘FF’H	rezervuota panaudoti vėliau

2.76. **GeoCoordinates**

2-oji karta.

Sveikaisiais skaičiais užkoduotos geografinės koordinatės. Šie sveikieji skaičiai yra platumos koduotės ± DDMM.M ir ilgumos koduotės ± DDDMM.M kartotiniai. Čia ± DD ir atitinkamai ± DDD reiškia laipsnius, o MM.M reiškia minutes.

```
GeoCoordinates ::= SEQUENCE {
   latitude                                INTEGER(-90000..90001),
   longitude                               INTEGER(-180000..180001)
}
```

latitude yra kartotiniu (daugiklis 10) užkoduota išraiška ± DDMM.M

longitude yra kartotiniu (daugiklis 10) užkoduota išraiška ± DDDMM.M

2.77. **GNSSAccuracy**

2-oji karta.

Buvimo vietos nustatymo duomenų, gautų iš GNSS, tikslumas (eee apibrėžtis). Tikslumas užkoduojamas sveikuoju skaičiumi ir yra vertės X.Y, gautos iš jūrinės įrangos ryšių protokolo (NMEA) sakinio GSA, kartotinis (daugiklis 10).

```
GNSSAccuracy ::= INTEGER(1..100)
```

2.78. **GNSSContinuousDriving**

2-oji karta.

Vairuotojo arba dirbtuvių kortelėje saugoma informacija, susijusi su transporto priemonės buvimo vietos duomenimis, gautais iš GNSS, kai vairuotojo nepertraukiamo vairavimo trukmė pasiekia trijų valandų kartotinį (1C priedo 306 ir 354 reikalavimai).

```
GNSSContinuousDriving := SEQUENCE {
   gnssCDPointerNewestRecord               INTEGER(0..NoOfGNSSCDRecords -1),
   gnssContinuousDrivingRecords            SET SIZE(NoOfGNSSCDRecords) OF
                                           GNSSContinuousDrivingRecord
}
```

gnssCDPointerNewestRecord yra nepertraukiamo vairavimo įrašo paskutinio atnaujinimo pagal GNSS duomenis indeksas.

▼B

Priskiriamos vertės: skaičius, atitinkantis nepertraukiamo vairavimo įrašo, gauto pagal GNSS duomenis, (trupmenos) skaitiklio vertę; nepertraukiamo vairavimo pirmojo įrašo, gauto pagal GNSS duomenis, struktūroje vertė yra 0.

gnssContinuousDrivingRecords yra įrašų rinkinys, kuriame saugoma data ir laikas, kada nepertraukiamo vairavimo trukmė pasiekia trijų valandų kartotinį, ir informacija apie transporto priemonės buvimo vietą.

2.79. **GNSSContinuousDrivingRecord**

2-oji karta.

Vairuotojo arba dirbtuvių kortelėje saugoma informacija, susijusi su transporto priemonės buvimo vietos duomenimis, gautais iš GNSS, kai vairuotojo nepertraukiamo vairavimo trukmė pasiekia trijų valandų kartotinį (1C priedo 305 ir 353 reikalavimai).

```
GNSSContinuousDrivingRecord ::= SEQUENCE {
   timeStamp                                TimeReal,
   gnssPlaceRecord                          GNSSPlaceRecord
}
```

timeStamp žymi datą ir laiką, kada kortelės turėtojo nepertraukiamo vairavimo trukmė pasiekia trijų valandų kartotinį.

gnssPlaceRecord laikoma informacija apie transporto priemonės buvimo vietą.

2.80. **GNSSPlaceRecord**

2-oji karta.

Informacija apie transporto priemonės buvimo vietą, gauta iš GNSS (1C priedo 108, 109, 110, 296, 305, 347 ir 353 reikalavimai).

```
GNSSPlaceRecord ::= SEQUENCE {
   timeStamp                                TimeReal,
   gnssAccuracy                             GNSSAccuracy,
   geoCoordinates                           GeoCoordinates
}
```

timeStamp žymi transporto priemonės buvimo vietos nustatymo pagal GNSS duomenis datą ir laiką.

gnssAccuracy iš GNSS gautų buvimo vietos duomenų tikslumas.

geoCoordinates žymi vietą, užregistruotą pagal duomenis, gautus iš GNSS.

2.81. **HighResOdometer**

Transporto priemonės odometro rodmens vertė: visas transporto priemonės naudojimo metu nuvažiuotas atstumas.

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

▼B

Priskiriamos vertės: dvejetainis be ženklo. Vertė 1/200 km iš skalės nuo 0 iki 21 055 406 km.

2.82. **HighResTripDistance**

Per visą kelionę arba jos dalį nuvažiuotas atstumas.

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

Priskiriamos vertės: dvejetainis be ženklo. Vertė 1/200 km iš skalės nuo 0 iki 21 055 406 km.

2.83. **HolderName**

Kortelės turėtojo pavardė ir vardas (-ai).

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

holderSurname yra turėtojo pavardė. Pavardė turi būti be kreipinio.

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

holderFirstNames yra turėtojo vardas (-ai) ir inicialai.

2.84. **InternalGNSSReceiver**

2-oji karta.

Informacija apie tai, ar GNSS imtuvas yra transporto priemonės bloko viduje ar išorėje. Vertė *True* reiškia, kad GNSS imtuvas yra transporto priemonės bloko viduje. Vertė *False* reiškia, kad GNSS imtuvas yra transporto priemonės bloko išorėje.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.85. **K-ConstantOfRecordingEquipment**

Tachografo konstanta (m apibrėžtis)

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

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

2.86. **KeyIdentifier**

Viešojo rakto unikalus identifikatorius, naudojamas raktui nurodyti ir pasirinkti. Jis taip pat identifikuoja rakto turėtoją.

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

▼B

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

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

Trečiasis pasirinkimas tinka valstybės narės viešajam raktui nurodyti.

2.87. **KMWCKey**

2-oji karta.

Raktas AES ir jo rakto versija, naudojama transporto priemonės bloke (judesio jutiklių susiejimas) Daugiau žr. 11 priedėlyje

```
KMWCKey ::= SEQUENCE {
   kMWCKey                                 AESKey,
   keyVersion                              INTEGER (SIZE(1))
}
```

kMWCKey yra rakto AES, sujungto su transporto priemonės bloke naudojamu raktu, ilgis (judesio jutiklių susiejimas).

keyVersion žymi rakto AES rakto versiją.

2.88. **Language**

Kalbos identifikavimo kodas.

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

Priskiriamos vertės: dviejų mažųjų raidžių kodas pagal ISO 639.

2.89. **LastCardDownload**

Vairuotojo kortelės atmintyje laikomų duomenų paskutinio perkėlimo (ne kontrolei) iš kortelės data ir laikas (1C priedo 257 ir 282 reikalavimai). Data gali būti keičiama transporto priemonės bloke arba bet kokiu kortelės nuskaitymo įrenginiu.

```
LastCardDownload ::= TimeReal
```

Priskiriamos vertės: tiksliau nenustatyta.

2.90. **LinkCertificate**

2-oji karta.

Europos vyriausiosios pažymėjimų įstaigos raktų porų susiejimo sertifikatas

```
LinkCertificate ::= Certificate
```

2.91. **L-TyreCircumference**

Ratų padangų efektyvusis apskritimo ilgis (u apibrėžtis).

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

▼B

Priskiriamos vertės: Dvejetainis be ženklo. Vertė 1/8 mm iš skalės nuo 0 iki 8 031 mm.

2.92. **MAC**

2-oji karta.

8, 12 arba 16 baitų ilgio kriptografinė kontrolinė suma, atitinkanti 11 priedėlyje nustatytus šifrų rinkinius.

```
MAC ::= CHOICE {
   mac8                                    OCTET STRING (SIZE(8)),
   mac12                                   OCTET STRING (SIZE(12)),
   mac16                                   OCTET STRING (SIZE(12))
}
```

2.93. **ManualInputFlag**

Kodas, kuriuo žymima, ar tuo metu, kai kortelė buvo įstatyta, kortelės turėtojas rankomis įvedė informaciją apie vairuotojo veiklą, ar ne (1B priedo 081 reikalavimas ir 1C priedo 102 reikalavimas).

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

Priskiriamos vertės: tiksliau nenustatyta.

2.94. **ManufacturerCode**

Patvirtinto tipo įrangos gamintoją identifikuojantis kodas.

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

Laboratorija, kompetentinga atlikti sąveikumo bandymus, rengia gamintojų kodų sąrašą ir skelbia jį savo interneto svetainėje (1C priedo 454 reikalavimas).

Gamintojų kodai (ManufacturerCodes) laikinai skiriami tachografų įrangos kūrėjams pagal paraišką kompetentingai sąveikumo bandymų laboratorijai.

2.95. **ManufacturerSpecificEventFaultData**

2-oji karta.

Gamintojo parengti klaidų kodai, padedantys lengviau nagrinėti klaidas ir techniškai prižiūrėti transporto priemonės blokus.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
   manufacturerCode                        ManufacturerCode,
   manufacturerSpecificErrorCode           OCTET STRING(SIZE(3))
}
```

manufacturerCode žymi transporto priemonės bloko gamintoją.

manufacturerSpecificErrorCode yra specialus gamintojo sukurtas klaidos kodas.

▼B

2.96. **MemberStateCertificate**

Europos pažymėjimų išdavimo institucijos išduotas valstybės narės viešojo rakto pažymėjimas.

```
MemberStateCertificate ::= Certificate
```

2.97. **MemberStateCertificateRecordArray**

2-oji karta.

Valstybės narės pažymėjimas ir duomenų parsisiuntimo protokole naudojami metaduomenys.

```
MemberStateCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       MemberStateCertificate
}
```

recordType žymi įrašo rūšį (MemberStateCertificate). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento MemberStateCertificate dydis baitais.

noOfRecords yra rinkinio įrašų skaičius. Vertė turi būti 1, nes pažymėjimai gali būti skirtingo ilgio.

records yra valstybių narių pažymėjimų rinkinys.

2.98. **MemberStatePublicKey**

1-oji karta.

Valstybės narės viešasis raktas.

```
MemberStatePublicKey ::= PublicKey
```

2.99. **Name**

Pavadinimas

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

codePage nurodo rašmenų rinkinį, apibrėžtą 4 skyriuje,

name yra pavadinimas, užkoduotas naudojant nurodytą rašmenų rinkinį.

2.100. **NationAlpha**

Raidinis šalies žymuo pagal skiriamuosius ženklus, naudojamus ant tarptautiniam eismui naudojamų transporto priemonių (1968 m. Jungtinių Tautų Vienos kelių eismo konvencija).

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

Raidinis šalies žymuo ir skaitiniai kodai išvardijami sąraše, kuris pateikiamas laboratorijos, kompetentingos atlikti sąveikumo bandymus, interneto svetainėje, kaip nustatyta 1C priedo 440 reikalavime.

▼B

2.101. **NationNumeric**

Skaitinis šalies žymuo.

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

Priskiriamos vertės: žr. duomenų tipą 2.100 punkte (NationAlpha)

Bet koks raidinio šalies žymens (NationAlpha) ar skaitinės specifikacijos, aprašytos pirmesnėje pastraipoje, pakeitimas ar atnaujinimas atliekamas tik po to, kai paskirta laboratorija sužino patvirtinto tipo skaitmeninio ir išmaniojo tachografo transporto priemonės bloko gamintojų nuomonę.

2.102. **NoOfCalibrationRecords**

Dirbtuvių kortelės atmintyje telpančių įrašų apie kalibravimą skaičius.

1-oji karta.

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

Priskiriamos vertės: žr. 2 priedėlį.

2-oji karta.

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

Priskiriamos vertės: žr. 2 priedėlį.

2.103. **NoOfCalibrationsSinceDownload**

Skaitiklis, rodantis, kiek kalibravimų atlikta su dirbtuvių kortele nuo paskutinio duomenų parsisiuntimo iš jos (1C priedo 317 ir 340 reikalavimai).

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

Priskiriamos vertės: tiksliau nenustatyta.

2.104. **NoOfCardPlaceRecords**

Vairuotojo arba dirbtuvių kortelės atmintyje telpančių įrašų apie vietas skaičius.

1-oji karta.

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

Priskiriamos vertės: žr. 2 priedėlį.

2-oji karta.

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

Priskiriamos vertės: žr. 2 priedėlį.

▼B

2.105. **NoOfCardVehicleRecords**

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

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

Priskiriamos vertės: žr. 2 priedėlį.

2.106. **NoOfCardVehicleUnitRecords**

2-oji karta.

Vairuotojo arba dirbtuvių kortelės atmintyje telpančių įrašų apie naudotus transporto priemonės blokus skaičius.

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

Priskiriamos vertės: žr. 2 priedėlį.

2.107. **NoOfCompanyActivityRecords**

Įmonės kortelės atmintyje telpančių įrašų apie įmonės veiklą skaičius.

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

Priskiriamos vertės: žr. 2 priedėlį.

2.108. **NoOfControlActivityRecords**

Kontrolės kortelės atmintyje telpančių įrašų apie kontrolės veiklą skaičius.

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

Priskiriamos vertės: žr. 2 priedėlį.

2.109. **NoOfEventsPerType**

Kortelės atmintyje telpančių įrašų apie tam tikros rūšies įvykius skaičius.

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

Priskiriamos vertės: žr. 2 priedėlį.

2.110. **NoOfFaultsPerType**

Kortelės atmintyje telpančių įrašų apie tam tikros rūšies triktis skaičius.

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

Priskiriamos vertės: žr. 2 priedėlį.

▼B

2.111. **NoOfGNSSCDRecords**

2-oji karta.

Skaičius, kiek GNSS įrašų apie nepertraukiamą vairavimą telpa kortelės atmintyje.

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

Priskiriamos vertės: žr. 2 priedėlį.

2.112. **NoOfSpecificConditionRecords**

2-oji karta.

Skaičius, kiek įrašų apie ypatingą būseną telpa kortelės atmintyje.

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

Priskiriamos vertės: žr. 2 priedėlį.

2.113. **OdometerShort**

Transporto priemonės odometro rodmens vertė trumpąja forma.

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

Priskiriamos vertės: dvejetainis be ženklo. Vertė kilometrais iš skalės nuo 0 iki 9 999 999 km.

2.114. **OdometerValueMidnight**

Transporto priemonės odometro rodmens vertė tam tikros dienos vidurnaktį (1B priedo 090 reikalavimas ir 1C priedo 113 reikalavimas).

```
OdometerValueMidnight ::= OdometerShort
```

Priskiriamos vertės: tiksliau nenustatyta.

2.115. **OdometerValueMidnightRecordArray**

2-oji karta.

OdometerValueMidnight ir duomenų parsisiuntimo protokole naudojami metaduomenys.

```
OdometerValueMidnightRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       OdometerValueMidnight
}
```

recordType žymi įrašo rūšį (OdometerValueMidnight). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento OdometerValueMidnight dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra duomenų elemento OdometerValueMidnight įrašų rinkinys.

▼B

2.116. **OverspeedNumber**

Greičio viršijimo įvykių skaičius nuo paskutinės greičio kontrolės.

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

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

2.117. **PlaceRecord**

Informacija apie vietą, kurioje prasideda arba baigiasi dienos darbo laikotarpis (1C priedo 108, 271, 296, 324 ir 347 reikalavimai).

1-oji karta.

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

entryTime yra įrašo data ir laikas.

entryTypeDailyWorkPeriod yra įrašo rūšis.

dailyWorkPeriodCountry yra nurodyta šalis.

dailyWorkPeriodRegion yra nurodytas regionas.

vehicleOdometerValue yra odometro rodmens vertė įrašo apie vietą sukūrimo momentu.

2-oji karta.

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

Be 1-osios kartos verčių, naudojamas šis komponentas:

entryGNSSPlaceRecord yra nurodyta vieta ir laikas.

▼B

2.118. **PreviousVehicleInfo**

Informacija apie vairuotojo, savo kortelę įstatančio į transporto priemonės bloką, pirmiau naudotas transporto priemones (1B priedo 081 reikalavimas ir 1C priedo 102 reikalavimas).

1-oji karta.

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

vehicleRegistrationIdentification yra transporto priemonės registracijos numeris ir tą transporto priemonę užregistravusi valstybė narė.

cardWithdrawalTime yra kortelės išėmimo data ir laikas.

2-oji karta.

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

Be 1-osios kartos verčių, naudojamas šis duomenų elementas:

vuGeneration žymi transporto priemonės bloko kartą.

2.119. **PublicKey**

1-oji karta.

Atvirasis raktas RSA.

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

rsaKeyModulus yra raktų poros modulis.

rsaKeyPublicExponent yra raktų poros viešoji eksponentė.

2.120. **RecordType**

2-oji karta.

Nuoroda į įrašo tipą. Šis duomenų tipas naudojamas RecordArrays.

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

▼B

Priskiriamos vertės:

‘01’H	ActivityChangeInfo,
‘02’H	CardSlotsStatus,
‘03’H	CurrentDateTime,
‘04’H	MemberStateCertificate,
‘05’H	OdometerValueMidnight,
‘06’H	DateOfDayDownloaded,
‘07’H	SensorPaired,
‘08’H	Signature,
‘09’H	SpecificConditionRecord,
‘0A’H	VehicleIdentificationNumber,
‘0B’H	VehicleRegistrationNumber,
‘0C’H	VuCalibrationRecord,
‘0D’H	VuCardIWRecord,
‘0E’H	VuCardRecord,
‘0F’H	VuCertificate,
‘10’H	VuCompanyLocksRecord,
‘11’H	VuControlActivityRecord,
‘12’H	VuDetailedSpeedBlock,
‘13’H	VuDownloadablePeriod,
‘14’H	VuDownloadActivityData,
‘15’H	VuEventRecord,
‘16’H	VuGNSSCDRecord,
‘17’H	VuITSConsentRecord,
‘18’H	VuFaultRecord,
‘19’H	VuIdentification,
‘1A’H	VuOverSpeedingControlData,
‘1B’H	VuOverSpeedingEventRecord,
‘1C’H	VuPlaceDailyWorkPeriodRecord,
‘1D’H	VuTimeAdjustmentGNSSRecord,
‘1E’H	VuTimeAdjustmentRecord,
‘1F’H	VuPowerSupplyInterruptionRecord,
‘20’H	SensorPairedRecord,
‘21’H	SensorExternalGNSSCoupledRecord,
‘22’H to ‘7F’H	rezervuota panaudoti vėliau;
‘80’H to ‘FF’H	nustato gamintojas.

2.121. **RegionAlpha**

Tam tikros šalies regiono raidinis žymuo.

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

1-oji karta.

Priskiriamos vertės:

‘ ’	No information available,
Spain:	
‘AN’	Andalucía,
‘AR’	Aragón,
‘AST’	Asturias,
‘C ’	Cantabria,
‘CAT’	Cataluña,
‘CL’	Castilla-León,
‘CM’	Castilla-La-Mancha,
‘CV’	Valencia,
‘EXT’	Extremadura,
‘G ’	Galicia,
‘IB’	Baleares,
‘IC’	Canarias,
‘LR’	La Rioja,
‘M ’	Madrid,
‘MU’	Murcia,
‘NA’	Navarra,
‘PV’	País Vasco

▼B

2-oji karta.

Kodai RegionAlpha išvardijami sąraše, kuris pateikiamas laboratorijos, kompetentingos atlikti sąveikumo bandymus, interneto svetainėje.

2.122. **RegionNumeric**

Tam tikros šalies regiono skaitinis žymuo.

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

1-oji karta.

Priskiriamos vertės:

```
'00'H        No information available,
Spain:
'01'H        Andalucía,
'02'H        Aragón,
'03'H        Asturias,
'04'H        Cantabria,
'05'H        Cataluña,
'06'H        Castilla-León,
'07'H        Castilla-La-Mancha,
'08'H        Valencia,
'09'H        Extremadura,
'0A'H        Galicia,
'0B'H        Baleares,
'0C'H        Canarias,
'0D'H        La Rioja,
'0E'H        Madrid,
'0F'H        Murcia,
'10'H        Navarra,
'11'H        País Vasco
```

2-oji karta.

Kodai RegionNumeric išvardijami sąraše, kuris pateikiamas laboratorijos, kompetentingos atlikti sąveikumo bandymus, interneto svetainėje.

2.123. **RemoteCommunicationModuleSerialNumber**

2-oji karta.

Nuotolinio ryšio modulio serijos numeris.

```
RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber
```

2.124. **RSAKeyModulus**

1-oji karta.

RSA raktų poros modulis.

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

Priskiriamos vertės: nenustatytos.

2.125. **RSAKeyPrivateExponent**

1-oji karta.

RSA raktų poros privačioji eksponentė.

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

Priskiriamos vertės: nenustatytos.

▼B

2.126. **RSAKeyPublicExponent**

1-oji karta.

Rakto RSA poros viešoji eksponentė.

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

Priskiriamos vertės: nenustatytos.

2.127. **RtmData**

2-oji karta.

Duomenų tipo apibrėžtį žr. 14 priedėlyje.

2.128. **SealDataCard**

2-oji karta.

Šio tipo duomenyse, kurie skirti įrašyti į kortelę, laikoma informacija apie plombas, pritvirtintas prie įvairių transporto priemonės komponentų. Šis duomenų tipas susijęs su 1C priedo 337 reikalavimu.

```
SealDataCard ::= SEQUENCE {
   noOfSealRecords                    INTEGER(1..5),
   sealRecords                        SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords yra rinkinio sealRecords įrašų skaičius.

sealRecords yra įrašų apie plombas rinkinys.

2.129. **SealDataVu**

2-oji karta.

Šio tipo duomenyse, kurie skirti įrašyti į transporto priemonės bloką, laikoma informacija apie plombas, pritvirtintas prie įvairių transporto priemonės komponentų.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
   sealRecords                        SealRecord
}
```

sealRecords yra įrašų apie plombas rinkinys. Jei yra mažiau kaip 5 plombos, visų nepanaudotų sealRecords vertė EquipmentType turi būti 16, kuri reiškia „nenaudojama“.

2.130. **SealRecord**

2-oji karta.

Šio tipo duomenyse saugoma informacija apie plombą, pritvirtintą prie komponento. Šis duomenų tipas susijęs su 1C priedo 337 reikalavimu.

```
SealRecord ::= SEQUENCE {
   equipmentType                      EquipmentType,
   extendedSealIdentifier             ExtendedSealIdentifier
}
```

equipmentType žymi įrangos, prie kurios pritvirtinta plomba, tipą.

extendedSealIdentifier yra prie įrangos pritvirtintos plombos identifikatorius.

▼B

2.131. **SensorApprovalNumber**

Jutiklio tipo patvirtinimo numerius.

1-oji karta.

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

Priskiriamos vertės: nenustatytos.

2-oji karta.

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

Priskiriamos vertės:

Turi būti pateikiamas toks patvirtinimo numeris, koks paskelbtas atitinkamoje Europos Komisijos interneto svetainėje, pvz., su brūkšneliais, jei yra. Patvirtinimo numeris turi būti lygiuojamas kairėje.

2.132. **SensorExternalGNSSApprovalNumber**

2-oji karta.

Išorinio GNSS įrenginio tipo patvirtinimo numeris.

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

Priskiriamos vertės:

Turi būti pateikiamas toks patvirtinimo numeris, koks paskelbtas atitinkamoje Europos Komisijos interneto svetainėje, pvz., su brūkšneliais, jei yra. Patvirtinimo numeris turi būti lygiuojamas kairėje.

2.133. **SensorExternalGNSSCoupledRecord**

2-oji karta.

Transporto priemonės bloko atmintyje laikomi išorinio GNSS įrenginio, sujungto su transporto priemonės bloku, identifikacijos duomenys (1C priedo 100 reikalavimas).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorCouplingDate                  SensorGNSSCouplingDate
}
```

sensorSerialNumber yra išorinio GNSS įrenginio, sujungto su transporto priemonės bloku, serijos numeris.

sensorApprovalNumber yra šio išorinio GNSS įrenginio tipo patvirtinimo numeris.

sensorCouplingDate yra išorinio GNSS įrenginio sujungimo su transporto priemonės bloku data.

2.134. **SensorExternalGNSSIdentification**

2-oji karta.

Išorinio GNSS įrenginio identifikacijos informacija (1C priedo 98 reikalavimus).

▼B

```
SensorExternalGNSSIdentification ::= SEQUENCE {
   sensorSerialNumber                    SensorGNSSSerialNumber,
   sensorApprovalNumber                  SensorExternalGNSSApprovalNumber,
   sensorSCIdentifier                    SensorExternalGNSSSCIdentifier,
   sensorOSIdentifier                    SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber yra išorinio GNSS įrenginio pailgintas serijos numeris.

sensorApprovalNumber yra išorinio GNSS įrenginio tipo patvirtinimo numeris.

sensorSCIdentifier yra išorinio GNSS įrenginio apsaugos komponento identifikatorius.

sensorOSIdentifier yra išorinio GNSS įrenginio operacinės sistemos identifikatorius.

2.135. **SensorExternalGNSSInstallation**

2-oji karta.

Išoriniame GNSS įrenginyje laikoma informacija apie išorinio GNSS įrenginio jutiklio įrengimą (1C priedo 123 reikalavimas).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
   sensorCouplingDateFirst               SensorGNSSCouplingDate,
   firstVuApprovalNumber                 VuApprovalNumber,
   firstVuSerialNumber                   VuSerialNumber,
   sensorCouplingDateCurrent             SensorGNSSCouplingDate,
   currentVuApprovalNumber               VuApprovalNumber,
   currentVUSerialNumber                 VuSerialNumber
}
```

sensorCouplingDateFirst yra išorinio GNSS įrenginio pirmojo sujungimo su transporto priemonės bloku data.

firstVuApprovalNumber yra pirmojo transporto priemonės bloko, sujungto su išoriniu GNSS įrenginiu, patvirtinimo numeris.

firstVuSerialNumber yra pirmojo transporto priemonės bloko, susieto su išoriniu GNSS įrenginiu, serijos numeris.

sensorCouplingDateCurrent yra išorinio GNSS įrenginio dabartinio sujungimo su transporto priemonės bloku data.

currentVuApprovalNumber yra transporto priemonės bloko, dabar susieto su išoriniu GNSS įrenginiu, patvirtinimo numeris.

currentVUSerialNumber yra transporto priemonės bloko, dabar susieto su išoriniu GNSS įrenginiu, serijos numeris.

▼B

2.136. **SensorExternalGNSSOSIdentifier**

2-oji karta.

Išorinio GNSS įrenginio operacinės sistemos identifikatorius.

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

Priskiriamos vertės: nustato gamintojas.

2.137. **SensorExternalGNSSSCIdentifier**

2-oji karta.

Šis tipas naudojamas, pavyzdžiui, išorinio GNSS įrenginio kriptografiniam moduliui identifikuoti.

Išorinio GNSS įrenginio apsaugos komponento identifikatorius.

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

Priskiriamos vertės: nustato komponento gamintojas.

2.138. **SensorGNSSCouplingDate**

2-oji karta.

Išorinio GNSS įrenginio sujungimo su transporto priemonės bloku data.

```
SensorGNSSCouplingDate ::= TimeReal
```

Priskiriamos vertės: nenustatytos.

2.139. **SensorGNSSSerialNumber**

2-oji karta.

Šio tipo duomenyse laikomas GNSS imtuvo – ir kai jis yra transporto priemonės bloko viduje, ir kai jis yra transporto priemonės bloko išorėje – serijos numeris.

GNSS imtuvo serijos numeris.

```
SensorGNSSSerialNumber ::= ExtendedSerialNumber
```

2.140. **SensorIdentification**

Judesio jutiklio atmintyje laikomi jo identifikacijos duomenys (1B priedo 077 reikalavimas ir 1C priedo 95 reikalavimas).

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

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

sensorApprovalNumber yra judesio jutiklio patvirtinimo numeris.

sensorSCIdentifier yra judesio jutiklio apsaugos komponento identifikatorius.

▼B

sensorOSIdentifier yra judesio jutiklio operacinės sistemos identifikatorius.

2.141. **SensorInstallation**

Judesio jutiklio atmintyje laikomi jo įrengimo duomenys (1B priedo 099 reikalavimas ir 1C priedo 122 reikalavimas).

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

sensorPairingDateFirst yra judesio jutiklio pirmojo susiejimo su transporto priemonės bloku data.

firstVuApprovalNumber yra su judesio jutikliu susieto pirmojo transporto priemonės bloko patvirtinimo numeris.

firstVuSerialNumber yra su judesio jutikliu susieto pirmojo transporto priemonės bloko serijos numeris.

sensorPairingDateCurrent yra judesio jutiklio esamo susiejimo su transporto priemonės bloku data.

currentVuApprovalNumber yra su judesio jutikliu dabar susieto transporto priemonės bloko patvirtinimo numeris.

currentVUSerialNumber yra su judesio jutikliu dabar susieto transporto priemonės bloko serijos numeris.

2.142. **SensorInstallationSecData**

Dirbtuvių kortelės atmintyje laikoma informacija apie apsaugos duomenis, reikalingus judesio jutikliams susieti su transporto priemonės blokais (1C priedo 308 ir 331 reikalavimai).

1-oji karta.

```
SensorInstallationSecData ::= TdesSessionKey
```

Priskiriamos vertės: pagal ISO 16844-3.

2-oji karta.

Pagal 11 priedėlio aprašą dirbtuvių kortelėje turi būti vietos iki trijų raktų, naudojamų transporto priemonės bloko judesio jutikliui susieti. Šių raktų versijos yra skirtingos.

```
SensorInstallationSecData ::= SEQUENCE {
   kMWCKey1                              KMWCKey,
   kMWCKey2                              KMWCKey OPTIONAL,
   kMWCKey3                              KMWCKey OPTIONAL
}
```

▼B

2.143. **SensorOSIdentifier**

Judesio jutiklio operacinės sistemos identifikatorius.

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

Priskiriamos vertės: nustato gamintojas.

2.144. **SensorPaired**

1-oji karta.

Transporto priemonės bloko atmintyje laikomi su juo susieto judesio jutiklio identifikacijos duomenys (1B priedo 079 reikalavimas).

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

sensorSerialNumber yra su transporto priemonės bloku dabar susieto judesio jutiklio serijos numeris.

sensorApprovalNumber yra su transporto priemonės bloku dabar susieto judesio jutiklio patvirtinimo numeris.

sensorPairingDateFirst yra su transporto priemonės bloku dabar susieto judesio jutiklio pirmojo susiejimo su transporto priemonės bloku data.

2.145. **SensorPairedRecord**

2-oji karta.

Transporto priemonės bloko atmintyje laikomi su juo susieto judesio jutiklio identifikacijos duomenys (1C priedo 97 reikalavimas).

```
SensorPairedRecord ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorPairingDate                     SensorPairingDate
}
```

sensorSerialNumber yra su transporto priemonės bloku susieto judesio jutiklio serijos numeris.

sensorApprovalNumber yra šio judesio jutiklio patvirtinimo numeris.

sensorPairingDate yra judesio jutiklio esamo susiejimo su transporto priemonės bloku data.

2.146. **SensorPairingDate**

Judesio jutiklio susiejimo su transporto priemonės bloku data.

```
SensorPairingDate ::= TimeReal
```

Priskiriamos vertės: nenustatytos.

▼B

2.147. **SensorSCIdentifier**

Judesio jutiklio apsaugos komponento identifikatorius.

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

Priskiriamos vertės: nustato komponento gamintojas.

2.148. **SensorSerialNumber**

Judesio jutiklio serijos numeris.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.149. **Signature**

Skaitmeninis parašas.

1-oji karta.

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

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

2-oji karta.

```
Signature ::= OCTET STRING (SIZE(64..132))
```

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

2.150. **SignatureRecordArray**

2-oji karta.

Parašų rinkinys ir duomenų parsisiuntimo protokole naudojami metaduomenys.

```
SignatureRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF Signature
}
```

recordType žymi įrašo rūšį (Signature). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento Signature dydis baitais.

noOfRecords yra rinkinio įrašų skaičius. Vertė turi būti 1, nes parašai gali būti skirtingo ilgio.

records yra parašų rinkinys.

2.151. **SimilarEventsNumber**

Panašių įvykių tam tikrą vieną dieną skaičius (1B priedo 094 reikalavimas ir 1C priedo 117 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 arba daugiau tos rūšies įvykių.

▼B

2.152. **SpecificConditionRecord**

Vairuotojo, dirbtuvių kortelės arba transporto priemonės bloko atmintyje laikoma informacija apie ypatingą būseną (1C priedo 130, 276, 301, 328 ir 355 reikalavimai).

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

entryTime yra įrašo data ir laikas.

specificConditionType yra ypatingos būsenos identifikavimo kodas.

2.153. **SpecificConditions**

Vairuotojo, dirbtuvių kortelės arba transporto priemonės bloko atmintyje laikoma informacija apie ypatingą būseną (1C priedo 131, 277, 302, 329 ir 356 reikalavimai).

2-oji karta.

```
SpecificConditions := SEQUENCE {
   conditionPointerNewestRecord         INTEGER(0..NoOfSpecificConditionRecords-1),
   specificConditionRecords             SET SIZE(NoOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

conditionPointerNewestRecord yra paskutinio atnaujinto įrašo apie ypatingą būseną indeksas.

Priskiriamos vertės: skaičius, atitinkantis ypatingos būsenos įrašo (trupmenos) skaitiklio vertę; pirmojo ypatingos būsenos įrašo struktūroje vertė yra 0.

specificConditionRecords yra įrašų rinkinys, kuriame kaupiama informacija apie užregistruotą ypatingą būseną.

2.154. **SpecificConditionType**

Ypatingos būsenos identifikavimo kodas (1B priedo 050b, 105a, 212a ir 230a reikalavimai ir 1C priedo 62 reikalavimas).

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

1-oji karta.

Priskiriamos vertės:

‘00’H	rezervuota panaudoti vėliau
‘01’H	nekontroliuojamo laikotarpio pradžia;
‘02’H	nekontroliuojamo laikotarpio pabaiga;
‘03’H	kėlimas keltu / vežimas traukiniu;
‘04’H .. ‘FF’H	rezervuota panaudoti vėliau

2-oji karta.

Priskiriamos vertės:

‘00’H	rezervuota panaudoti vėliau
‘01’H	nekontroliuojamo laikotarpio pradžia;
‘02’H	nekontroliuojamo laikotarpio pabaiga;
‘03’H	kėlimo keltu / vežimo traukiniu pradžia;
‘04’H	kėlimo keltu / vežimo traukiniu pabaiga;
‘05’H .. ‘FF’H	rezervuota panaudoti vėliau

▼B

2.155. **Greitis**

Transporto priemonės greitis (km/h).

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

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

2.156. **SpeedAuthorised**

Didžiausias leidžiamasis transporto priemonės greitis (hh apibrėžtis).

```
SpeedAuthorised ::= Speed
```

2.157. **SpeedAverage**

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

```
SpeedAverage ::= Speed
```

2.158. **SpeedMax**

Didžiausias greitis, išmatuotas per anksčiau nustatytą laikotarpį.

```
SpeedMax ::= Speed
```

2.159. **TachographPayload**

2-oji karta.

Duomenų tipo apibrėžtį žr. 14 priedėlyje.

2.160. **TachographPayloadEncrypted**

2-oji karta.

Pagal taisykles DER-TLV užšifruotas informacinis tachografo turinys, t. y. duomenys, kurie siunčiami užšifruotu RTM pranešimu. Daugiau apie šifravimą žr. 11 priedėlio B dalies 13 skyriuje.

```
TachographPayloadEncrypted ::= SEQUENCE {
   tag                                  OCTET STRING(SIZE(1)),
   length                               OCTET STRING(SIZE(1..2)),
   paddingContentIndicatorByte          OCTET STRING(SIZE(1)),
   encryptedData                        OCTET STRING(SIZE(16..192))
}
```

tag yra DER-TLV kodavimo dalis, kurios vertė yra ‘87’ (žr. 11 priedėlio B dalies 13 skyriuje).

length yra DER-TLV kodavimo dalis, kurioje užkoduojamas duomenų elementas paddingContentIndicatorByte ir encryptedData ilgis.

paddingContentIndicatorByte vertė turi būti ‘00’.

encryptedData yra užšifruotas duomenų elementas tachographPayload, kaip nurodyta 11 priedėlio B dalies 13 skyriuje. Šių duomenų ilgis oktetais turi visada būti 16 kartotinis.

2.161. **TDesSessionKey**

1-oji karta.

Trigubo DES seanso raktas.

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

Priskiriamos vertės: tiksliau nenustatyta.

▼B

2.162. **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. Grinvičo laiku.

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

Priskiriamos vertės. Sinchronizavimas pagal oktetą: sekundžių skaičius po 1970 m. sausio 1 d. vidurnakčio Grinvičo laiku.

Didžiausioji galima data/laikas yra 2106 m.

2.163. **TyreSize**

Padangų matmenų žymuo.

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

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

2.164. **VehicleIdentificationNumber**

Visą transporto priemonę žymintis Transporto priemonės identifikavimo numeris yra paprastai važiuoklės serijos numeris arba rėmo numeris.

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

Priskiriamos vertės: kaip nustatyta ISO 3779.

2.165. **VehicleIdentificationNumberRecordArray**

2-oji karta.

Transporto priemonės identifikavimo numeris ir duomenų parsisiuntimo protokole naudojami metaduomenys.

```
VehicleIdentificationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleIdentificationNumber
}
```

recordType žymi įrašo rūšį (VehicleIdentificationNumber). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento VehicleIdentificationNumber dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra transporto priemonės identifikavimo numerių rinkinys.

2.166. **VehicleRegistrationIdentification**

Transporto priemonės unikali europinė identifikacija (transporto priemonės registracijos numeris ir valstybė narė).

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

vehicleRegistrationNation žymi valstybę, kurioje užregistruota transporto priemonė.

▼B

vehicleRegistrationNumber yra transporto priemonės registracijos numeris.

2.167. **VehicleRegistrationNumber**

Transporto priemonės registracijos numeris. Registracijos numerį suteikia transporto priemonių licencijavimo institucija.

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

codePage nurodo rašmenų rinkinį, apibrėžtą 4 skyriuje,

vehicleRegNumber yra transporto priemonės registracijos numeris, užkoduotas naudojant nurodytą rašmenų rinkinį.

Priskiriamos vertės: nustato šalis.

2.168. **VehicleRegistrationNumberRecordArray**

2-oji karta.

Transporto priemonės registracijos numeris ir duomenų parsisiuntimo protokole naudojami metaduomenys.

```
VehicleRegistrationNumberRecordArray ::= SEQUENCE {
   recordType                        RecordType,
   recordSize                        INTEGER(1..65535),
   noOfRecords                       INTEGER(0..65535),
   records                           SET SIZE(noOfRecords) OF
                                     VehicleRegistrationNumber
}
```

recordType žymi įrašo rūšį (VehicleRegistrationNumber). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento VehicleRegistrationNumber dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra transporto priemonės registracijos numerių rinkinys.

2.169. **VuAbility**

2-oji karta.

Transporto priemonės bloke saugoma informacija, ar tame bloke galima (negalima) naudoti 1-osios kartos tachografo korteles (-ių) (1C priedo 121 reikalavimas).

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

Priskiriamos vertės. Sinchronizavimas pagal oktetą ‘xxxxxxxa’B (8 bitai)

1-osios kartos tachografo kortelių naudojimo galimybė:

‘a’B	1-osios kartos tachografo kortelių naudojimo galimybė: ‘0’ B reiškia, kad 1-osios kartos tachografo korteles galima naudoti, ‘1’ B reiškia, kad 1-osios kartos tachografo kortelių negalima naudoti,
‘xxxxxxx’B	rezervuota panaudoti vėliau

▼B

2.170. **VuActivityDailyData**

1-oji karta.

Transporto priemonės bloke laikoma informacija apie veiklos ir (arba) važiavimo būsenos ir (arba) kortelės būsenos pasikeitimus tam tikrą kalendorinę dieną (1B priedo 084 reikalavimas ir 1C priedo 105, 106, 107 reikalavimai) ir kortelių lizdų būseną tos dienos 00:00 val.

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

noOfActivityChanges yra ActivityChangeInfo žodžių skaičius rinkinyje activityChangeInfos.

activityChangeInfos yra transporto priemonės bloke laikomų tos dienos ActivityChangeInfo žodžių rinkinys. Jame visada yra du ActivityChangeInfo žodžiai, kuriais apibūdinama dviejų kortelės lizdų būsena tos dienos 00:00 val.

2.171. **VuActivityDailyRecordArray**

2-oji karta.

Transporto priemonės bloke laikoma informacija apie veiklos ir (arba) važiavimo būsenos ir (arba) kortelės būsenos pasikeitimus tam tikrą kalendorinę dieną (1C priedo 105, 106, 107 reikalavimai) ir kortelės lizdų būseną tos dienos 00:00 val.

```
VuActivityDailyRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF ActivityChangeInfo
}
```

recordType žymi įrašo rūšį (ActivityChangeInfo). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento ActivityChangeInfo dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra transporto priemonės bloke laikomų tos dienos ActivityChangeInfo žodžių rinkinys. Jame visada yra du ActivityChangeInfo žodžiai, kuriais apibūdinama dviejų kortelės lizdų būsena tos dienos 00:00 val.

2.172. **VuApprovalNumber**

Transporto priemonės bloko tipo patvirtinimo numeris.

1-oji karta.

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

Priskiriamos vertės: nenustatytos.

2-oji karta.

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

▼B

Priskiriamos vertės:

Turi būti pateikiamas toks patvirtinimo numeris, koks paskelbtas atitinkamoje Europos Komisijos interneto svetainėje, pvz., su brūkšneliais, jei yra. Patvirtinimo numeris turi būti lygiuojamas kairėje.

2.173. **VuCalibrationData**

1-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie tachografo kalibravimą (1B priedo 098 reikalavimas).

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

noOfVuCalibrationRecords yra rinkinyje vuCalibrationRecords esančių įrašų skaičius.

vuCalibrationRecords yra įrašų apie kalibravimą rinkinys.

2.174. **VuCalibrationRecord**

Transporto priemonės bloke laikoma informacija apie tachografo kalibravimą (1B priedo 098 reikalavimas ir 1C priedo 119 ir 120 reikalavimai).

1-oji karta.

```
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 yra kalibravimo tikslas.

workshopName, workshopAddress yra dirbtuvių pavadinimas ir adresas.

workshopCardNumber nurodo kalibruojant naudotą dirbtuvių kortelę.

workshopCardExpiryDate yra kortelės galiojimo pabaigos data.

vehicleIdentificationNumber yra transporto priemonės identifikavimo numeris.

▼B

vehicleRegistrationIdentification yra transporto priemonės registracijos numeris ir tą transporto priemonę užregistravusi valstybė narė.

wVehicleCharacteristicConstant yra transporto priemonės būdingasis koeficientas.

kConstantOfRecordingEquipment yra tachografo konstanta.

lTyreCircumference yra ratų padangų efektyvusis apskritimo ilgis.

tyreSize yra transporto priemonėje sumontuotų padangų matmens žymuo.

authorisedSpeed yra leidžiamasis transporto priemonės greitis.

oldOdometerValue, newOdometerValue yra senoji ir naujoji odometro rodmens vertės.

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

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

2-oji karta.

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber,
   workshopCardExpiryDate                TimeReal,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistrationIdentification     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal,
   sealDataVu                            SealDataVu
}
```

Be 1-osios kartos verčių, naudojamas šis duomenų elementas:

sealDataVu laikoma informacija apie plombas, pritvirtintas prie įvairių transporto priemonės komponentų.

2.175. **VuCalibrationRecordArray**

2-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie tachografo kalibravimą (1C priedo 119 ir 120 reikalavimai).

▼B

```
VuCalibrationRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuCalibrationRecord
}
```

recordType žymi įrašo rūšį (VuCalibrationRecord). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento VuCalibrationRecord dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra įrašų apie kalibravimą rinkinys.

2.176. **VuCardIWData**

1-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie vairuotojo arba dirbtuvių kortelių įstatymo ir išėmimo ciklus transporto priemonės bloke (1B priedo 081 reikalavimas ir 1C priedo 103 reikalavimas).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                           INTEGER(0..2^16-1),
   vuCardIWRecords                         SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

noOfIWRecords yra įrašų rinkinyje vuCardIWRecords skaičius.

vuCardIWRecords yra įrašų apie kortelių įstatymo ir išėmimo ciklus rinkinys.

2.177. **VuCardIWRecord**

Transporto priemonės bloko atmintyje laikoma informacija apie vairuotojo arba dirbtuvių kortelės įstatymo ir išėmimo ciklą transporto priemonės bloke (1B priedo 081 reikalavimas ir 1C priedo 102 reikalavimas).

1-oji karta.

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

cardHolderName yra vairuotojo arba dirbtuvių kortelės atmintyje laikoma jos turėtojo pavardė ir vardas (-ai).

fullCardNumber yra kortelės rūšis, ją išdavusi valstybė narė ir kortelės atmintyje laikomas kortelės numeris.

▼B

cardExpiryDate yra kortelės atmintyje laikoma jos galiojimo pabaigos data.

cardInsertionTime yra kortelės įstatymo data ir laikas.

vehicleOdometerValueAtInsertion yra transporto priemonės odometro rodmens vertė kortelės įstatymo metu.

cardSlotNumber yra lizdas, į kurį įstatyta kortelė.

cardWithdrawalTime yra išėmimo data ir laikas.

vehicleOdometerValueAtWithdrawal yra transporto priemonės odometro rodmens vertė kortelės išėmimo metu.

previousVehicleInfo yra kortelės atmintyje laikoma informacija apie anksčiau vairuotojo naudotą transporto priemonę.

manualInputFlag yra ženklas, kuriuo nurodoma, ar įstatęs kortelę jos turėtojas rankomis įvedė informaciją apie savo veiklos rūšis, ar ne.

2-oji karta.

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

Vietoje duomenų elemento fullCardNumber 2-osios kartos duomenų struktūroje naudojamas šis duomenų elementas:

fullCardNumberAndGeneration yra kortelės atmintyje laikomi kortelės rūšies, ją išdavusios valstybės narės, kortelės numerio ir kartos duomenys.

2.178. **VuCardIWRecordArray**

2-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie vairuotojo arba dirbtuvių kortelių įstatymo ir išėmimo ciklus transporto priemonės bloke (1C priedo 103 reikalavimas).

```
VuCardIWRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCardIWRecord
}
```

recordType žymi įrašo rūšį (VuCardIWRecord). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento VuCardIWRecord dydis baitais.

▼B

noOfRecords yra rinkinio įrašų skaičius.

records yra įrašų apie kortelių įstatymo ir išėmimo ciklus rinkinys.

2.179. **VuCardRecord**

2-oji karta.

Transporto priemonės bloke laikoma informacija apie naudojamą tachografo kortelę (1C priedo 132 reikalavimas).

```
VuCardRecord ::= SEQUENCE {
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardPersonaliserID                  OCTET STRING(SIZE(1)),
   typeofTachographCardID              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   cardNumber                          CardNumber
}
```

cardExtendedSerialNumber perskaityta iš rinkmenos EF_ICC pagrindinėje kortelės rinkmenoje.

cardPersonaliserID perskaityta iš rinkmenos EF_ICC pagrindinėje kortelės rinkmenoje.

typeOfTachographCardId perskaityta iš rinkmenos EF_Application_Identification, esančios DF_Tachograph_G2

cardStructureVersion perskaityta iš rinkmenos EF_Application_Identification rinkmenose DF_Tachograph_G2

cardNumber perskaityta iš rinkmenos EF_Identification, esančios DF_Tachograph_G2.

2.180. **VuCardRecordArray**

2-oji karta.

Transporto priemonės bloke laikoma informacija apie tachografo korteles, naudojamas su šiuo bloku. Ši informacija skirta transporto priemonės bloko (kortelių problemų) analizei (1C priedas 132 reikalavimas)

```
VuCardRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCardRecord
}
```

recordType žymi įrašo rūšį (VuCardRecord). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento VuCardRecord dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra įrašų apie tachografo korteles, naudojamas su transporto priemonės bloku, rinkinys.

▼B

2.181. **VuCertificate**

Transporto priemonės bloko viešojo rakto pažymėjimas.

```
VuCertificate ::= Certificate
```

2.182. **VuCertificateRecordArray**

2-oji karta.

Transporto priemonės bloko pažymėjimas ir duomenų parsisiuntimo protokole naudojami metaduomenys.

```
VuCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCertificate
}
```

recordType žymi įrašo rūšį (VuCertificate). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento VuCertificate dydis baitais.

noOfRecords yra rinkinio įrašų skaičius. Vertė turi būti 1, nes pažymėjimai gali būti skirtingo ilgio.

records yra transporto priemonės bloko pažymėjimų rinkinys.

2.183. **VuCompanyLocksData**

1-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie įmonės užraktus (1B priedo 104 reikalavimas).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                           INTEGER(0..255),
   vuCompanyLocksRecords               SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks yra duomenų elemente vuCompanyLocksRecords išvardytų užraktų skaičius.

vuCompanyLocksRecords yra įrašų apie įmonės užraktus rinkinys.

2.184. **VuCompanyLocksRecord**

Transporto priemonės bloko atmintyje laikoma informacija apie vieną įmonės užraktą (1B priedo 104 reikalavimas, 1C priedo 128 reikalavimas).

1-oji karta.

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

▼B

lockInTime, lockOutTime yra užrakinimo ir atrakinimo data ir laikas.

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

companyCardNumber žymi kortelę, naudotą užrakinant.

2-oji karta.

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                          TimeReal,
   lockOutTime                         TimeReal,
   companyName                         Name,
   companyAddress                      Address,
   companyCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

Vietoje duomenų elemento companyCardNumber 2-osios kartos duomenų struktūroje naudojamas šis duomenų elementas.

companyCardNumberAndGeneration žymi užrakinimui naudotą kortelę ir tos kortelės kartą.

2.185. **VuCompanyLocksRecordArray**

2-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie įmonės užraktus (1C priedo 128 reikalavimas).

```
VuCompanyLocksRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCompanyLocksRecord
}
```

recordType žymi įrašo rūšį (VuCompanyLocksRecord). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento VuCompanyLocksRecord dydis baitais.

noOfRecords yra rinkinio įrašų skaičius. Vertė 0..255.

records yra įrašų apie įmonės užraktus rinkinys.

2.186. **VuControlActivityData**

1-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie naudojant jį atliktas kontroles (1B priedo 102 reikalavimas).

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

▼B

noOfControls yra duomenų elemente vuControlActivityRecords išvardytų kontrolių skaičius.

vuControlActivityRecords yra įrašų apie kontrolės veiklą rinkinys.

2.187. **VuControlActivityRecord**

Transporto priemonės bloko atmintyje laikoma informacija apie kontrolę, atliktą naudojant šį transporto priemonės bloką (1B priedo 102 reikalavimas, 1C priedo 126 reikalavimas).

1-oji karta.

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

controlType yra kontrolės rūšis.

controlTime yra kontrolės data ir laikas.

ControlCardNumber žymi kontrolės kortelę, su kuria buvo atlikta kontrolė.

downloadPeriodBeginTime yra perkeltų duomenų laikotarpio pradžia (jei duomenys parsisiųsti).

downloadPeriodEndTime yra perkeltų duomenų laikotarpio pabaiga (jei duomenys parsisiųsti).

2-oji karta.

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumberAndGeneration       FullCardNumberAndGeneration,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

Vietoje duomenų elemento controlCardNumber 2-osios kartos duomenų struktūroje naudojamas šis duomenų elementas.

controlCardNumberAndGeneration žymi kontrolei naudotą kontrolės kortelę ir tos kortelės kartą.

2.188. **VuControlActivityRecordArray**

2-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie naudojant jį atliktas kontroles (1C priedo 126 reikalavimas).

▼B

```
VuControlActivityRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuControlActivityRecord
}
```

recordType žymi įrašo rūšį (VuControlActivityRecord). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento VuControlActivityRecord dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra įrašų apie transporto priemonės bloko kontrolės veiklą rinkinys.

2.189. **VuDataBlockCounter**

Kortelės atmintyje laikomas skaitiklis, kuriuo identifikuojama kortelės įstatymo ir išėmimo ciklų transporto priemonės bloke seka.

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

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

2.190. **VuDetailedSpeedBlock**

Transporto priemonės bloko atmintyje laikoma informacija apie tikslų transporto priemonės greitį tą minutę, kai transporto priemonė važiavo (1B priedo 093 reikalavimas ir 1C priedo 116 reikalavimas).

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

speedBlockBeginDate yra pirmosios greičio vertės bloke data ir laikas.

speedsPerSecond yra kiekvieną tos minutės sekundę išmatuoto greičio verčių chronologinė seka pradedant imtinai nuo momento speedBlock-BeginDate.

2.191. **VuDetailedSpeedBlockRecordArray**

2-oji karta.

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

```
VuDetailedSpeedBlockRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuDetailedSpeedBlock
}
```

recordType žymi įrašo rūšį (VuDetailedSpeedBlock). **Priskiriamos vertės**: žr. RecordType

▼B

recordSize yra duomenų elemento VuDetailedSpeedBlock dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra tikslaus greičio blokų rinkinys.

2.192. **VuDetailedSpeedData**

1-oji karta.

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

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                    INTEGER(0..2^16-1),
   vuDetailedSpeedBlocks              SET SIZE(noOfSpeedBlocks) OF
                                      VuDetailedSpeedBlock
}
```

noOfSpeedBlocks yra greičio blokų skaičius rinkinyje vuDetailedSpeed-Blocks.

vuDetailedSpeedBlocks yra tikslaus greičio blokų rinkinys.

2.193. **VuDownloadablePeriod**

Seniausia ir naujausia datos, kurių duomenys apie vairuotojo veiklą laikomi transporto priemonės bloko atmintyje (1B priedo 081, 084 arba 087 reikalavimai ir 1C priedo 102, 105, 108 reikalavimai).

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

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

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

2.194. **VuDownloadablePeriodRecordArray**

2-oji karta.

Duomenų elementas VUDownloadablePeriod ir duomenų parsisiuntimo protokole naudojami metaduomenys.

```
VuDownloadablePeriodRecordArray ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF
                                      VuDownloadablePeriod
}
```

recordType žymi įrašo rūšį (VuDownloadablePeriod). **Priskiriamos vertės**: žr. RecordType

▼B

recordSize yra duomenų elemento VuDownloadablePeriod dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra duomenų elemento VuDownloadablePeriod įrašų rinkinys.

2.195. **VuDownloadActivityData**

Transporto priemonės bloko atmintyje laikoma informacija apie paskutinį informacijos parsisiuntimą (1B priedo 105 reikalavimas, 1C priedo 129 reikalavimas).

1-oji karta.

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

downloadingTime yra duomenų perkėlimo data ir laikas.

fullCardNumber nurodo kortelę, kuria duodamas leidimas perkelti duomenis.

companyOrWorkshopName yra įmonės arba dirbtuvių pavadinimas.

2-oji karta.

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                      TimeReal,
   fullCardNumberAndGeneration          FullCardNumberAndGeneration,
   companyOrWorkshopName                Name
}
```

Vietoje duomenų elemento fullCardNumber 2-osios kartos duomenų struktūroje naudojamas šis duomenų elementas:

fullCardNumberAndGeneration žymi kortelę, kuria duodamas leidimas parsisiųsti duomenis, ir tos kortelės kartą.

2.196. **VuDownloadActivityDataRecordArray**

2-oji karta.

Informacija apie paskutinį parsisiuntimą iš transporto priemonės bloko (1C priedo 129 reikalavimus).

```
VuDownloadActivityDataRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF VuDownloadActivityData
}
```

recordType žymi įrašo rūšį (VuDownloadActivityData). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento VuDownloadActivityData dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

▼B

records yra įrašų apie veiklos duomenų parsisiuntimą rinkinys.

2.197. **VuEventData**

1-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie įvykius (1B priedo 094 reikalavimas, išskyrus greičio viršijimo įvykius).

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

noOfVuEvents yra duomenų elemente vuEventRecords išvardytų įvykių skaičius.

vuEventRecords yra įrašų apie įvykius rinkinys.

2.198. **VuEventRecord**

Transporto priemonės bloko atmintyje laikoma informacija apie įvykį (1B priedo 094 reikalavimas ir 1C priedo 117 reikalavimas, išskyrus greičio viršijimo įvykį).

1-oji karta.

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

eventType yra įvykio rūšis.

eventRecordPurpose yra įvykio užregistravimo tikslas.

eventBeginTime yra įvykio pradžios data ir laikas.

eventEndTime yra įvykio pabaigos data ir laikas.

cardNumberDriverSlotBegin žymi kortelę, kuri buvo vairuotojo kortelės lizde, kai prasidėjo įvykis.

cardNumberCodriverSlotBegin žymi kortelę, kuri buvo vairuotojo porininko kortelės lizde, kai prasidėjo įvykis.

cardNumberDriverSlotEnd žymi kortelę, kuri buvo vairuotojo kortelės lizde, kai įvykis baigėsi.

cardNumberCodriverSlotEnd žymi kortelę, kuri buvo vairuotojo porininko kortelės lizde, kai įvykis baigėsi.

similarEventsNumber yra panašių įvykių skaičius tą dieną.

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

▼B

2-oji karta.

```
VuEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   similarEventsNumber                    SimilarEventsNumber,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Be 1-osios kartos verčių, naudojami šie duomenų elementai:

manufacturerSpecificEventFaultData yra papildoma gamintojo nustatyta informacija apie įvykį.

Vietoje duomenų elementų cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd, ir cardNumberCodriverSlotEnd 2-osios kartos duomenų struktūroje naudojami šie duomenų elementai:

cardNumberAndGenDriverSlotBegin žymi kortelę (įskaitant jos kartą), kuri įvykio pradžioje yra įstatyta į vairuotojo kortelės lizdą.

cardNumberAndGenCodriverSlotBegin žymi kortelę (įskaitant jos kartą), kuri įvykio pradžioje yra įstatyta į vairuotojo porininko kortelės lizdą.

cardNumberAndGenDriverSlotEnd žymi kortelę (įskaitant jos kartą), kuri įvykio pabaigoje yra įstatyta į vairuotojo kortelės lizdą.

cardNumberAndGenCodriverSlotEnd žymi kortelę (įskaitant jos kartą), kuri įvykio pabaigoje yra įstatyta į vairuotojo porininko kortelės lizdą.

Jei įvykis yra laiko nesuderinimas, duomenų elementai eventBeginTime ir eventEndTime suprantami taip:

eventBeginTime yra tachografo data ir laikas,

eventEndTime yra GNSS data ir laikas.

2.199. **VuEventRecordArray**

2-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie įvykius (1C priedo 117 reikalavimas, išskyrus greičio viršijimo įvykius).

```
VuEventRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuEventRecord
}
```

recordType žymi įrašo rūšį (VuEventRecord). **Priskiriamos vertės**: žr. RecordType

▼B

recordSize yra duomenų elemento VuEventRecord dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra įrašų apie įvykius rinkinys.

2.200. **VuFaultData**

1-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie triktis (1B priedo 096 reikalavimas).

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

noOfVuFaults yra rinkinyje vuFaultRecords išvardytų trikčių skaičius.

vuFaultRecords yra įrašų apie triktis rinkinys.

2.201. **VuFaultRecord**

Transporto priemonės bloko atmintyje laikoma informacija apie triktį (1B priedo 096 reikalavimas, 1C priedo 118 reikalavimas).

1-oji karta.

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

faultType yra tachografo trikties rūšis.

faultRecordPurpose yra trikties užregistravimo tikslas.

faultBeginTime yra trikties pradžios data ir laikas.

faultEndTime yra trikties pabaigos data ir laikas.

cardNumberDriverSlotBegin žymi kortelę, kuri buvo vairuotojo kortelės lizde, kai prasidėjo triktis.

cardNumberCodriverSlotBegin žymi kortelę, kuri buvo vairuotojo porininko kortelės lizde, kai prasidėjo triktis.

cardNumberDriverSlotEnd žymi kortelę, kuri buvo vairuotojo kortelės lizde, kai triktis baigėsi.

cardNumberCodriverSlotEnd žymi kortelę, kuri buvo vairuotojo porininko kortelės lizde, kai triktis baigėsi.

▼B

2-oji karta.

```
VuFaultRecord ::= SEQUENCE {
   faultType                              EventFaultType,
   faultRecordPurpose                     EventFaultRecordPurpose,
   faultBeginTime                         TimeReal,
   faultEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Be 1-osios kartos verčių, naudojamas šis duomenų elementas:

manufacturerSpecificEventFaultData yra papildoma gamintojo nustatyta informacija apie triktį.

Vietoje duomenų elementų cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd, ir cardNumberCodriverSlotEnd 2-osios kartos duomenų struktūroje naudojami šie duomenų elementai:

cardNumberAndGenDriverSlotBegin žymi kortelę (įskaitant jos kartą), kuri trikties pradžioje yra įstatyta į vairuotojo kortelės lizdą.

cardNumberAndGenCodriverSlotBegin žymi kortelę (įskaitant jos kartą), kuri trikties pradžioje yra įstatyta į vairuotojo porininko kortelės lizdą.

cardNumberAndGenDriverSlotEnd žymi kortelę (įskaitant jos kartą), kuri trikties pabaigoje yra įstatyta į vairuotojo kortelės lizdą.

cardNumberAndGenCodriverSlotEnd žymi kortelę (įskaitant jos kartą), kuri trikties pabaigoje yra įstatyta į vairuotojo porininko kortelės lizdą.

2.202. **VuFaultRecordArray**

2-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie triktis (1C priedo 118 reikalavimas).

```
VuFaultRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuFaultRecord
}
```

recordType žymi įrašo rūšį (VuFaultRecord). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento VuFaultRecord dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra įrašų apie triktis rinkinys.

▼B

2.203. **VuGNSSCDRecord**

2-oji karta.

Transporto priemonės bloke saugoma informacija, susijusi su transporto priemonės buvimo vietos duomenimis, gautais iš GNSS, kai vairuotojo nepertraukiamo vairavimo trukmė pasiekia trijų valandų kartotinį (1C priedo 108, 110 reikalavimai).

```
VuGNSSCDRecord ::= SEQUENCE {
   timeStamp                          TimeReal,
   cardNumberAndGenDriverSlot         FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot       FullCardNumberAndGeneration,
   gnssPlaceRecord                    GNSSPlaceRecord
}
```

timeStamp žymi datą ir laiką, kada kortelės turėtojo nepertraukiamo vairavimo trukmė pasiekia trijų valandų kartotinį.

cardNumberAndGenDriverSlot žymi kortelę (įskaitant jos kartą), kuri yra įstatyta į vairuotojo kortelės lizdą.

cardNumberAndGenCodriverSlot žymi kortelę (įskaitant jos kartą), kuri yra įstatyta į vairuotojo porininko kortelės lizdą.

gnssPlaceRecord laikoma informacija apie transporto priemonės buvimo vietą.

2.204. **VuGNSSCDRecordArray**

2-oji karta.

Transporto priemonės bloke saugoma informacija, susijusi su transporto priemonės buvimo vietos duomenimis, gautais iš GNSS, kai vairuotojo nepertraukiamo vairavimo trukmė pasiekia trijų valandų kartotinį (1C priedo 108 ir 110 reikalavimai).

```
VuGNSSCDRecordArray  ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF VuGNSSCDRecord
}
```

recordType žymi įrašo rūšį (VuGNSSCDRecord). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento VuGNSSCDRecord dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra iš GNSS gautų įrašų apie nepertraukiamą vairavimą rinkinys.

2.205. **VuIdentification**

Transporto priemonės bloke laikoma informacija apie transporto priemonės bloko identifikaciją (1B priedo 075 reikalavimas ir 1C priedo 93 ir 121 reikalavimai).

▼B

1-oji karta.

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

vuManufacturerName yra transporto priemonės bloko gamintojo pavadinimas.

vuManufacturerAddress yra transporto priemonės bloko gamintojo adresas.

vuPartNumber yra transporto priemonės bloko komponento šifras.

vuSerialNumber yra transporto priemonės bloko serijos numeris.

vuSoftwareIdentification žymi transporto priemonės bloke įdiegtą programinę įrangą.

vuManufacturingDate yra transporto priemonės bloko pagaminimo data.

vuApprovalNumber yra transporto priemonės bloko tipo patvirtinimo numeris.

2-oji karta.

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

Be 1-osios kartos verčių, naudojami šie duomenų elementai:

vuGeneration žymi transporto priemonės bloko kartą.

vuAbility rodo, ar transporto priemonės blokui tinka 1-osios kartos tachografo kortelės, ar ne.

2.206. **VuIdentificationRecordArray**

2-oji karta.

Duomenų elementas VuIdentification ir duomenų parsisiuntimo protokole naudojami metaduomenys.

▼B

```
VuIdentificationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuIdentification
}
```

recordType žymi įrašo rūšį (VuIdentification). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento VuIdentification dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra įrašų VuIdentification rinkinys.

2.207. **VuITSConsentRecord**

2-oji karta.

Transporto priemonės bloke saugoma informacija apie vairuotojo sutikimą naudoti intelektines transporto sistemas.

```
VuITSConsentRecord ::= SEQUENCE {
   cardNumberAndGen                    FullCardNumberAndGeneration,
   consent                             BOOLEAN
}
```

cardNumberAndGen žymi kortelę ir tos kortelės kartą. Tai turi būti vairuotojo kortelė arba dirbtuvių kortelė.

consent yra ženklas, ar vairuotojas sutiko naudoti intelektinę transporto sistemą šioje transporto priemonėje / transporto priemonės bloke.

Priskiriamos vertės:

TRUE	rodo, kad vairuotojas sutinka naudoti intelektinę transporto sistemą.
FALSE	rodo, kad vairuotojas nesutinka naudoti intelektinės transporto sistemos.

2.208. **VuITSConsentRecordArray**

2-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie vairuotojo sutikimą naudoti intelektinę transporto sistemą (1C priedo 200 reikalavimas).

```
VuITSConsentRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuITSConsentRecord
}
```

recordType žymi įrašo rūšį (VuITSConsentRecord). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento VuITSConsentRecord dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra įrašų apie sutikimą naudoti intelektinę transporto sistemą rinkinys.

▼B

2.209. **VuManufacturerAddress**

Transporto priemonės bloko gamintojo adresas.

```
VuManufacturerAddress ::= Address
```

Priskiriamos vertės: nenustatytos.

2.210. **VuManufacturerName**

Transporto priemonės bloko gamintojo pavadinimas.

```
VuManufacturerName ::= Name
```

Priskiriamos vertės: nenustatytos.

2.211. **VuManufacturingDate**

Transporto priemonės bloko pagaminimo data.

```
VuManufacturingDate ::= TimeReal
```

Priskiriamos vertės: nenustatytos.

2.212. **VuOverSpeedingControlData**

Transporto priemonės bloko atmintyje laikoma informacija apie greičio viršijimo įvykius nuo paskutinės greičio kontrolės (1B priedo 095 reikalavimas ir 1C priedo 117 reikalavimas).

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

lastOverspeedControlTime yra paskutinės greičio viršijimo kontrolės data ir laikas.

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

numberOfOverspeedSince yra greičio viršijimo įvykių skaičius nuo paskutinės greičio kontrolės.

2.213. **VuOverSpeedingControlDataRecordArray**

2-oji karta.

Duomenų elementas VuOverSpeedingControlData ir duomenų parsisiuntimo protokole naudojami metaduomenys.

```
VuOverSpeedingControlDataRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuOverSpeedingControlData
}
```

▼B

recordType žymi įrašo rūšį (VuOverSpeedingControlData). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento VuOverSpeedingControlData dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra įrašų apie greičio viršijimo kontrolės įvykius rinkinys.

2.214. **VuOverSpeedingEventData**

1-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie greičio viršijimo įvykius (1B priedo 094 reikalavimas).

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

noOfVuOverSpeedingEvents yra rinkinyje vuOverSpeedingEventRecords išvardytų įvykių skaičius.

vuOverSpeedingEventRecords yra įrašų apie greičio viršijimo įvykius rinkinys.

2.215. **VuOverSpeedingEventRecord**

1-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie greičio viršijimo įvykius (1B priedo 094 reikalavimas, 1C priedo 117 reikalavimas).

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

eventType yra įvykio rūšis.

eventRecordPurpose yra įvykio užregistravimo tikslas.

eventBeginTime yra įvykio pradžios data ir laikas.

eventEndTime yra įvykio pabaigos data ir laikas.

maxSpeedValue yra didžiausias įvykio metu išmatuotas greitis.

averageSpeedValue yra per įvykį išmatuoto greičio aritmetinis vidurkis.

▼B

cardNumberDriverSlotBegin žymi kortelę, kuri buvo vairuotojo kortelės lizde, kai prasidėjo įvykis.

similarEventsNumber yra panašių įvykių skaičius tą dieną.

2-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie greičio viršijimo įvykius (1B priedo 094 reikalavimas, 1C priedo 117 reikalavimas).

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

Vietoje duomenų elemento cardNumberDriverSlotBegin 2-osios kartos duomenų struktūroje naudojamas šis duomenų elementas:

cardNumberAndGenDriverSlotBegin žymi kortelę (įskaitant jos kartą), kuri įvykio pradžioje yra įstatyta į vairuotojo kortelės lizdą.

2.216. **VuOverSpeedingEventRecordArray**

2-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie greičio viršijimo įvykius (1C priedo 117 reikalavimas).

```
VuOverSpeedingEventRecordArray ::= SEQUENCE {
   recordType                             RecordType,
   recordSize                             INTEGER(1..65535),
   noOfRecords                            INTEGER(0..65535),
   records                                SET SIZE(noOfRecords) OF
                                          VuOverSpeedingEventRecord
}
```

recordType žymi įrašo rūšį (VuOverSpeedingEventRecord). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento VuOverSpeedingEventRecord dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra įrašų apie greičio viršijimo įvykius rinkinys.

2.217. **VuPartNumber**

Transporto priemonės bloko komponento šifras.

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

Priskiriamos vertės: nustato transporto priemonės bloko gamintojas.

▼B

2.218. **VuPlaceDailyWorkPeriodData**

1-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie vietas, kuriose vairuotojai pradeda arba baigia dienos darbo laikotarpį (1B priedo 087 reikalavimas ir 1C priedo 108 ir 110 reikalavimai).

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

noOfPlaceRecords yra rinkinyje vuPlaceDailyWorkPeriodRecords išvardytų įrašų skaičius.

vuPlaceDailyWorkPeriodRecords yra įrašų apie vietas rinkinys.

2.219. **VuPlaceDailyWorkPeriodRecord**

1-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie vietą, kurioje vairuotojas pradeda arba baigia dienos darbo laikotarpį (1B priedo 087 reikalavimas ir 1C priedo 108 ir 110 reikalavimai).

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

fullCardNumber yra vairuotojo kortelės rūšis, kortelę išdavusi valstybė narė ir kortelės numeris.

placeRecord yra informacija apie nurodytą vietą.

2-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie vietą, kurioje vairuotojas pradeda arba baigia dienos darbo laikotarpį (1B priedo 087 reikalavimas ir 1C priedo 108 ir 110 reikalavimai).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   placeRecord                         PlaceRecord
}
```

Vietoje duomenų elemento fullCardNumber 2-osios kartos duomenų struktūroje naudojamas šis duomenų elementas:

fullCardNumberAndGeneration yra kortelės rūšis, ją išdavusi valstybė narė, kortelės atmintyje laikomas kortelės numeris ir karta.

▼B

2.220. **VuPlaceDailyWorkPeriodRecordArray**

2-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie vietas, kuriose vairuotojai pradeda arba baigia dienos darbo laikotarpį (1C priedo 108 ir 110 reikalavimai).

```
VuPlaceDailyWorkPeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

recordType žymi įrašo rūšį (VuPlaceDailyWorkPeriodRecord). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento VuPlaceDailyWorkPeriodRecord dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra įrašų apie vietas rinkinys.

2.221. **VuPrivateKey**

1-oji karta.

Transporto priemonės bloko privatusis raktas.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.222. **VuPublicKey**

1-oji karta.

Transporto priemonės bloko viešasis raktas.

```
VuPublicKey ::= PublicKey
```

2.223. **VuSerialNumber**

Transporto priemonės bloko serijos numeris (1B priedo 075 reikalavimas, 1C priedo 93 reikalavimas).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.224. **VuSoftInstallationDate**

Transporto priemonės bloko programinės įrangos versijos įdiegimo data.

```
VuSoftInstallationDate ::= TimeReal
```

Priskiriamos vertės: nenustatytos.

▼B

2.225. **VuSoftwareIdentification**

Transporto priemonės bloko atmintyje laikomi duomenys apie įdiegtą programinę įrangą.

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

vuSoftwareVersion yra transporto priemonės bloko programinės įrangos versijos numeris.

vuSoftInstallationDate yra programinės įrangos versijos įdiegimo data.

2.226. **VuSoftwareVersion**

Transporto priemonės bloko programinės įrangos versijos numeris.

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

Priskiriamos vertės: nenustatytos.

2.227. **VuSpecificConditionData**

1-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie ypatingas būsenas.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords         INTEGER(0..2^16-1)
   specificConditionRecords             SET SIZE (noOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

noOfSpecificConditionRecords yra rinkinyje specificConditionRecords išvardytų įrašų skaičius.

specificConditionRecords yra įrašų apie ypatingas būsenas rinkinys.

2.228. **VuSpecificConditionRecordArray**

2-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie ypatingas būsenas (1C priedo 130 reikalavimas).

```
VuSpecificConditionRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        SpecificConditionRecord
}
```

recordType žymi įrašo rūšį (SpecificConditionRecord). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento SpecificConditionRecord dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra įrašų apie ypatingas būsenas rinkinys.

▼B

2.229. **VuTimeAdjustmentData**

1-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie laiko koregavimą, atliktą ne įprasto kalibravimo metu (1B priedo 101 reikalavimas).

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

noOfVuTimeAdjRecords yra įrašų rinkinyje vuTimeAdjustmentRecords skaičius.

vuTimeAdjustmentRecords yra įrašų apie laiko koregavimą rinkinys.

2.230. **VuTimeAdjustmentGNSSRecord**

2-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie laiko koregavimą pagal laiko duomenis, gautus iš GNSS (1C priedo 124 ir 125 reikalavimai).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal
}
```

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

2.231. **VuTimeAdjustmentGNSSRecordArray**

2-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie laiko koregavimą pagal laiko duomenis, gautus iš GNSS (1C priedo 124 ir 125 reikalavimai).

```
VuTimeAdjustmentGNSSRecordArray ::= SEQUENCE {
   recordType                            RecordType,
   recordSize                            INTEGER(1..65535),
   noOfRecords                           INTEGER(0..65535),
   records                               SET SIZE(noOfRecords) OF
                                         VuTimeAdjustmentGNSSRecord
}
```

recordType žymi įrašo rūšį (VuTimeAdjustmentGNSSRecord). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento VuTimeAdjustmentGNSSRecord dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra iš GNSS gautų įrašų apie laiko koregavimą rinkinys.

▼B

2.232. **VuTimeAdjustmentRecord**

Transporto priemonės bloko atmintyje laikoma informacija apie laiko koregavimą, atliktą ne įprasto kalibravimo metu (1B priedo 101 reikalavimas ir 1C priedo 124 ir 125 reikalavimai).

1-oji karta.

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

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

workshopName, workshopAddress yra dirbtuvių pavadinimas ir adresas.

workshopCardNumber žymi laikui koreguoti naudotą dirbtuvių kortelę.

2-oji karta.

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

Vietoje duomenų elemento workshopCardNumber 2-osios kartos duomenų struktūroje naudojamas šis duomenų elementas:

workshopCardNumberAndGeneration žymi laikui koreguoti naudotą dirbtuvių kortelę, įskaitant jos kartą.

2.233. **VuTimeAdjustmentRecordArray**

2-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie laiko koregavimą, atliktą ne įprasto kalibravimo metu (1C priedo 124 ir 125 reikalavimai).

```
VuTimeAdjustmentRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuTimeAdjustmentRecord
}
```

recordType žymi įrašo rūšį (VuTimeAdjustmentRecord). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento VuTimeAdjustmentRecord dydis baitais.

▼B

noOfRecords yra rinkinio įrašų skaičius.

records yra įrašų apie laiko koregavimą rinkinys.

2.234. **WorkshopCardApplicationIdentification**

Dirbtuvių kortelės atmintyje laikomi kortelės naudojimo identifikacijos duomenys (1C priedo 307 ir 330 reikalavimai).

1-oji karta.

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

typeOfTachographCardId rodo naudojamos kortelės rūšį.

cardStructureVersion rodo kortelės struktūros versiją.

noOfEventsPerType rodo, kiek vienos rūšies įvykių galima užregistruoti kortelės atmintyje.

noOfFaultsPerType rodo, kiek vienos rūšies trikčių galima užregistruoti kortelės atmintyje.

activityStructureLength rodo laisvų baitų skaičių įrašams apie veiklą.

noOfCardVehicleRecords rodo, kiek įrašų apie transporto priemonę telpa kortelės atmintyje.

noOfCardPlaceRecords rodo, kiek įrašų apie vietas telpa kortelės atmintyje.

noOfCalibrationRecords rodo, kiek įrašų apie kalibravimą telpa kortelės atmintyje.

2-oji karta.

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

Be 1-osios kartos verčių, naudojami šie duomenų elementai:

noOfGNSSCDRecords rodo, kiek GNSS įrašų apie nepertraukiamą vairavimą telpa kortelės atmintyje.

▼B

noOfSpecificConditionRecords rodo, kiek įrašų apie ypatingą būseną telpa kortelės atmintyje.

2.235. **WorkshopCardCalibrationData**

Dirbtuvių kortelėje laikoma informacija apie dirbtuvių veiklą, atliktą su kortele (1C priedo 314, 316, 337 ir 339 reikalavimai).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber               INTEGER(0 .. 2^16-1),
   calibrationPointerNewestRecord       INTEGER(0 .. NoOfCalibrationRecords-1),
   calibrationRecords                   SET SIZE(NoOfCalibrationRecords) OF
                                        WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber yra bendras su kortele atliktų kalibravimų skaičius.

calibrationPointerNewestRecord yra paskutinio atnaujinto įrašo apie kalibravimą indeksas.

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

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

2.236. **WorkshopCardCalibrationRecord**

Dirbtuvių kortelės atmintyje laikoma informacija apie kalibravimą, atliktą su kortele (1C priedo 314 ir 337 reikalavimai).

1-oji karta.

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                   CalibrationPurpose,
   vehicleIdentificationNumber          VehicleIdentificationNumber,
   vehicleRegistration                  VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant       W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment        K-ConstantOfRecordingEquipment,
   lTyreCircumference                   L-TyreCircumference,
   tyreSize                             TyreSize,
   authorisedSpeed                      SpeedAuthorised,
   oldOdometerValue                     OdometerShort,
   newOdometerValue                     OdometerShort,
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   nextCalibrationDate                  TimeReal,
   vuPartNumber                         VuPartNumber,
   vuSerialNumber                       VuSerialNumber,
   sensorSerialNumber                   SensorSerialNumber
}
```

calibrationPurpose yra kalibravimo tikslas.

vehicleIdentificationNumber yra transporto priemonės identifikavimo numeris.

vehicleRegistration yra transporto priemonės registracijos numeris ir tą transporto priemonę užregistravusi valstybė narė.

wVehicleCharacteristicConstant yra transporto priemonės būdingasis koeficientas.

▼B

kConstantOfRecordingEquipment yra tachografo konstanta.

lTyreCircumference yra ratų padangų efektyvusis apskritimo ilgis.

tyreSize yra transporto priemonėje sumontuotų padangų matmenų žymuo.

authorisedSpeed yra didžiausias leidžiamasis transporto priemonės greitis.

oldOdometerValue, newOdometerValue yra senoji ir naujoji odometro rodmens vertės.

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

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

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

2-oji karta.

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistration                   VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal,
   vuPartNumber                          VuPartNumber,
   vuSerialNumber                        VuSerialNumber,
   sensorSerialNumber                    SensorSerialNumber,
   sensorGNSSSerialNumber                SensorGNSSSerialNumber,
   rcmSerialNumber                       RemoteCommunicationModuleSerialNumber,
   sealDataCard                          SealDataCard
}
```

Be 1-osios kartos verčių, naudojami šie duomenų elementai:

sensorGNSSSerialNumber žymi išorinį GNSS įrenginį.

rcmSerialNumber žymi nuotolinio ryšio modulį.

sealDataCard laikoma informacija apie plombas, pritvirtintas prie įvairių transporto priemonės komponentų.

▼B

2.237. **WorkshopCardHolderIdentification**

Dirbtuvių kortelės atmintyje laikomi kortelės turėtojo identifikacijos duomenys (1C priedo 311 ir 334 reikalavimai).

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

workshopName yra kortelės turėtojo dirbtuvių pavadinimas.

workshopAddress yra kortelės turėtojo dirbtuvių adresas.

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

cardHolderPreferredLanguage yra kortelės turėtojo pageidaujama kalba.

2.238. **WorkshopCardPIN**

Dirbtuvių kortelės asmeninis identifikavimo numeris (1C priedo 309 ir 332 reikalavimai).

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

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

2.239. **W-VehicleCharacteristicConstant**

Transporto priemonės būdingasis koeficientas (k apibrėžtis).

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

Priskiriamos vertės: Impulsai per kilometrą iš skalės nuo 0 iki 64 255 imp./km.

2.240. **VuPowerSupplyInterruptionRecord**

2-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie maitinimo nutrūkimo įvykius (1C priedo 117 reikalavimas).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   cardNumberAndGenDriverSlotBegin       FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd         FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin     FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd       FullCardNumberAndGeneration,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType yra įvykio rūšis.

eventRecordPurpose yra įvykio užregistravimo tikslas.

eventBeginTime yra įvykio pradžios data ir laikas.

▼B

eventEndTime yra įvykio pabaigos data ir laikas.

cardNumberAndGenDriverSlotBegin žymi kortelę (įskaitant jos kartą), kuri buvo vairuotojo kortelės lizde įvykio pradžioje.

cardNumberAndGenDriverSlotEnd žymi kortelę (įskaitant jos kartą), kuri buvo vairuotojo kortelės lizde įvykio pabaigoje.

cardNumberAndGenCodriverSlotBegin žymi kortelę (įskaitant jos kartą), kuri buvo vairuotojo porininko kortelės lizde įvykio pradžioje.

cardNumberAndGenCodriverSlotEnd žymi kortelę, (įskaitant jos kartą), kuri buvo vairuotojo porininko kortelės lizde įvykio pabaigoje.

similarEventsNumber yra panašių įvykių skaičius tą dieną.

2.241. **VuPowerSupplyInterruptionRecordArray**

2-oji karta.

Transporto priemonės bloko atmintyje laikoma informacija apie maitinimo nutrūkimo įvykius (1C priedo 117 reikalavimas).

```
VuPowerSupplyInterruptionRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPowerSupplyInterruptionRecord
}
```

recordType žymi įrašo rūšį (VuPowerSupplyInterruptionRecord).
Priskiriamos vertės: žr. RecordType

recordSize yra duomenų elemento VuPowerSupplyInterruptionRecord dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra įrašų apie maitinimo nutrūkimo įvykius rinkinys.

2.242. **VuSensorExternalGNSSCoupledRecordArray**

2-oji karta.

Rinkinys SensorExternalGNSSCoupledRecord ir duomenų parsisiuntimo protokole naudojami metaduomenys.

```
VuSensorExternalGNSSCoupledRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       SensorExternalGNSSCoupledRecord
}
```

recordType žymi įrašo rūšį (SensorExternalGNSSCoupledRecord).
Priskiriamos vertės: žr. RecordType

▼B

recordSize yra duomenų elemento SensorExternalGNSSCoupledRecord dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra įrašų SensorExternalGNSSCoupled rinkinys.

2.243. **VuSensorPairedRecordArray**

2-oji karta.

Rinkinys SensorPairedRecord ir duomenų parsisiuntimo protokole naudojami metaduomenys.

```
VuSensorPairedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF SensorPairedRecord
}
```

recordType žymi įrašo rūšį (SensorPairedRecord). **Priskiriamos vertės**: žr. RecordType

recordSize yra duomenų elemento SensorPairedRecord dydis baitais.

noOfRecords yra rinkinio įrašų skaičius.

records yra įrašų apie susietus jutiklius rinkinys.

3. VERČIŲ IR DYDŽIŲ RIBOS

2 dalies apibrėžtyse naudojamų kintamųjų verčių ribos.

```
TimeRealRange ::= 2^32-1
```

4. ŽENKLŲ RINKINYS

Eilutėse IA5Strings naudojami ISO/IEC 8824-1 nustatyti ASCII rašmenys. Kad būtų aiškiau, jie pateikti toliau. Atsiradus neatitikimų viršenybę 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 161 iki 255 kodais koduojami dešimtainiai simboliai 8 bitų formatu iš standartinių ženklų rinkinių, nurodytų pagal kodų lentelės numerį: Standartinis ženklų rinkinys	Kodų lentelė (dešimtainis)
ISO/IEC 8859-1 Latin-1 Western European	1
ISO/IEC 8859-2 Latin-2 Central European	2
ISO/IEC 8859-3 Latin-3 South European	3
ISO/IEC 8859-5 Latin / Cyrillic	5
ISO/IEC 8859-7 Latin / Greek	7
ISO/IEC 8859-9 Latin-5 Turkish	9

▼B

Kitose rašmenų eilutėse (Address, Name, VehicleRegistrationNumber) papildomai naudojami nuo 161 iki 255 kodais koduojami dešimtainiai simboliai 8 bitų formatu iš standartinių ženklų rinkinių, nurodytų pagal kodų lentelės numerį: Standartinis ženklų rinkinys	Kodų lentelė (dešimtainis)
ISO/IEC 8859-13 Latin-7 Baltic Rim	13
ISO/IEC 8859-15 Latin-9	15
ISO/IEC 8859-16 Latin-10 South Eastern European	16
KOI8-R Latin / Cyrillic	80
KOI8-U Latin / Cyrillic	85

5. KODUOTĖ

Koduojant pagal ASN.1 kodavimo taisykles, visi nustatyti duomenų tipai koduojami pagal ISO/IEC 8825–2 nurodytą sulygiuotąjį variantą.

6. OBJEKTO IDENTIFIKATORIAI IR PROGRAMOS IDENTIFIKATORIAI

6.1. **Objekto identifikatoriai**

Šiame skyriuje išvardyti objekto identifikatoriai yra aktualūs tik 2-ajai kartai. Šie objekto identifikatoriai apibūdinti techninėse gairėse TR-03110-3, o čia jie pakartoti dėl baigtumo. Šie objekto identifikatoriai yra bsi-de atšakoje:

```
bsi-de OBJECT IDENTIFIER ::= {
   itu-t(0) identified-organization(4) etsi(0)
   reserved(127) etsi-identified-organization(0) 7
}
```

Transporto priemonės bloko autentiškumo tikrinimo protokolo identifikatoriai

```
id-TA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 2}

id-TA-ECDSA                OBJECT IDENTIFIER ::= {id-TA 2}

id-TA-ECDSA-SHA-256 OBJECT IDENTIFIER ::= {id-TA-ECDSA 3}

id-TA-ECDSA-SHA-384 OBJECT IDENTIFIER ::= {id-TA-ECDSA 4}

id-TA-ECDSA-SHA-512 OBJECT IDENTIFIER ::= {id-TA-ECDSA 5}
```

Pavyzdys. Jei transporto priemonės bloko autentiškumo tikrinimui naudojamas algoritmas SHA-384, tuomet reikia naudoti objekto identifikatorių `bsi-de protocols(2) smartcard(2) 2 2 4` (abstrakčiosios sintaksės kalba ASN.1). Šio objekto identifikatoriaus vertė yra taškais atskirti skaitmenys `0.4.0.127.0.7.2.2.2.2.4`.

	Taškinis atskyrimas	Baitinis atskyrimas
id-TA-ECDSA-SHA-256	0.4.0.127.0.7.2.2.2.2.3	‘04 00 7F 00 07 02 02 02 02 03’
id-TA-ECDSA-SHA-384	0.4.0.127.0.7.2.2.2.2.4	‘04 00 7F 00 07 02 02 02 02 04’
id-TA-ECDSA-SHA-512	0.4.0.127.0.7.2.2.2.2.5	‘04 00 7F 00 07 02 02 02 02 05’

▼B

Lusto autentiškumo tikrinimas protokolo identifikatoriai

```
id-CA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 3}

id-CA-ECDH                        OBJECT IDENTIFIER ::= {id-CA 2}

id-CA-ECDH-AES-CBC-CMAC-128       OBJECT IDENTIFIER ::= {id-CA-ECDH 2}

id-CA-ECDH-AES-CBC-CMAC-192       OBJECT IDENTIFIER ::= {id-CA-ECDH 3}

id-CA-ECDH-AES-CBC-CMAC-256       OBJECT IDENTIFIER ::= {id-CA-ECDH 4}
```

Pavyzdys. Jei lusto autentiškumo tikrinimui naudojamas algoritmas ECDH, o gauto seanso rakto AES ilgis yra 128 bitai. Šis seanso raktas paskui naudojamas veikimo režimu CBC, siekiant užtikrinti duomenų slaptumą, ir su algoritmu CMAC, kad būtų užtikrintas duomenų autentiškumas. Todėl reikia naudoti objekto identifikatorių `bsi-de protocols(2) smartcard(2) 3 2 2` (abstrakčiosios sintaksės kalba ASN.1). Šio objekto identifikatoriaus vertė yra taškais atskirti skaitmenys `0.4.0.127.0.7.2.2.3.2.2`.

	Taškinis atskyrimas	Baitinis atskyrimas
id-CA-ECDH-AES-CBC-CMAC-128	0.4.0.127.0.7.2.2.3.2.2	‘04 00 7F 00 07 02 02 03 02 0’
id-CA-ECDH-AES-CBC-CMAC-192	0.4.0.127.0.7.2.2.3.2.3	‘04 00 7F 00 07 02 02 03 02 03’
id-CA-ECDH-AES-CBC-CMAC-256	0.4.0.127.0.7.2.2.3.2.4	‘04 00 7F 00 07 02 02 03 02 04’

6.2. **Programos identifikatoriai**

2-oji karta.

Išorinio GNSS įrenginio (2-osios kartos) programos identifikatorius (AID) žymimas ‘FF 44 54 45 47 4D’. Šis AID patentuotas pagal ISO/IEC 7816-4.

Pastaba. Paskutiniais penkiais baitais koduojamas išmaniojo tachografo išorinio GNSS įrenginio DTEGM.

Programos identifikatorius, skirtas 2-osios kartos tachografo kortelės programai, žymimas ‘FF 53 4D 52 44 54’. Šis AID patentuotas pagal ISO/IEC 7816-4.

▼B

2 priedėlis

TACHOGRAFO KORTELIŲ SPECIFIKACIJA

TURINYS

1. ĮVADAS

1.1. Santrumpos

1.2. Nuorodos

2. ELEKTRINĖS IR FIZINĖS SAVYBĖS

2.1. Maitinimo įtampa ir srovės naudojimas

2.2. Programavimo įtampa V_{pp}

2.3. Laikrodžio signalo generavimas ir dažnis

2.4. Įvesties ir išvesties (I/O) kontaktas

2.5. Kortelės būsenos

3. TECHNINĖ ĮRANGA IR INFORMACIJOS PERDAVIMAS

3.1. Įvadas

3.2. Siuntimo protokolas

3.2.1 Protokolai

3.2.2 ATR

3.2.3 PTS

3.3. Prieigos taisyklės

3.4. Komandų ir klaidų kodų apžvalga

3.5. Komandų aprašymai

3.5.1 SELECT

3.5.2 READ BINARY

3.5.3 UPDATE_BINARY

3.5.4 GET_CHALLENGE

3.5.5 VERIFY

3.5.6 GET_RESPONSE

3.5.7 PSO: VERIFY_CERTIFICATE

3.5.8 INTERNAL_AUTHENTICATE

3.5.9 EXTERNAL_AUTHENTICATE

3.5.10 GENERAL AUTHENTICATE

3.5.11 MANAGE SECURITY ENVIRONMENT

3.5.12 PSO: HASH

▼B

3.5.13 PERFORM HASH of FILE

3.5.14 PSO: COMPUTE DIGITAL SIGNATURE

3.5.15 PSO: VERIFY_DIGITAL_SIGNATURE

3.5.16 PROCESS DSRC MESSAGE

4. TACHOGRAFO KORTELIŲ STRUKTŪRA

4.1. Pagrindinė rinkmena MF

4.2. Vairuotojo kortelės programos

4.2.1 Vairuotojo kortelės 1-osios kartos programa

4.2.2 Vairuotojo kortelės 2-osios kartos programa

4.3. Dirbtuvių kortelės programos

4.3.1 Dirbtuvių kortelės 1-osios kartos programa

4.3.2 Dirbtuvių kortelės 2-osios kartos programa

4.4. Kontrolės kortelės programos

4.4.1 Kontrolės kortelės 1-osios kartos programa

4.4.2 Kontrolės kortelės 2-osios kartos programa

4.5. Įmonės kortelės programos

4.5.1 Įmonės kortelės 1-osios kartos programa

4.5.2 Įmonės kortelės 2-osios kartos programa

1. ĮVADAS

1.1. **Santrumpos**

Šiame priedėlyje vartojamos santrumpos:

AC –	prieigos sąlygos
AES –	patobulintasis šifravimo standartas
AID –	programos identifikatorius
ALW	visada
APDU –	programos protokolo duomenų vienetas (komandos struktūra)
ATR –	atsakas į atstatos komandą
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	komandos APDU klasės baitas

▼B

DSRC –	skirtasis trumpojo nuotolio ryšys
DF	specialioji rinkmena. Specialiojoje rinkmenoje gali būti kitų rinkmenų (EF arba DF)
ECC –	elipsinių kreivių kriptografija
EF	elementarioji rinkmena
etu –	elementarusis laiko vienetas
G1 –	1-oji karta
G2 –	2-oji karta
IC	lustas
ICC	lustinė kortelė
ID –	identifikatorius
IFD –	sąsajos įtaisas
IFS –	informacijos lauko dydis
IFSC –	informacijos lauko dydis kortelei
IFSD –	informacijos lauko dydis įtaisui (terminalui)
INS	komandos APDU komandos baitas
Lc	komandos APDU pradinių duomenų ilgis
Le	laukiamų duomenų dydis (komandos išvesties duomenys)
MF	pagrindinė rinkmena (esminė specialioji rinkmena (DF))
NAD –	protokole T=1 naudojamas mazginių taškų adresas
NEV	niekada
P1-P2 –	parametrų baitai
PIN –	asmeninis identifikavimo numeris
PRO SM –	apsaugota saugiu keitimusi pranešimais
PTS –	protokolo siuntimo pasirinkimas
RFU –	rezervuota panaudoti vėliau
RST –	(kortelės) pradinės būsenos atkūrimas
SFID –	trumpas elementariosios rinkmenos identifikatorius
SM –	saugusis keitimasis pranešimais
SW1-SW2 –	būsenos baitai
TS –	pirmasis ATR rašmuo
VPP –	programavimo įtampa
VU –	transporto priemonės blokas
XXh –	vertė XX šešioliktainėje skaičių sistemoje
‘XXh’	vertė XX šešioliktainėje skaičių sistemoje
||	sujungimo ženklas 03||04=0304

▼B

1.2. **Nuorodos**

Šiame priedėlyje naudoti šaltiniai:

ISO/IEC 7816-2 Atpažinimo kortelės. Lustinės kortelės su kontaktais. 2 dalis. Kontaktų matmenys ir vieta ISO/IEC 7816-2:2007.

ISO/IEC 7816-3 Atpažinimo kortelės. Lustinės kortelės. 3 dalis. Elektrinis sietuvas ir siuntimo protokolai ISO/IEC 7816-3:2006.

ISO/IEC 7816-4 Atpažinimo kortelės. Lustinės kortelės. 4 dalis. Organizavimas, saugumas ir mainų komandos ISO/IEC 7816-4:2013 + 2014 m. 1 pataisa.

ISO/IEC 7816-6 Atpažinimo kortelės. Lustinės kortelės. 6 dalis. Tarpsektoriniai duomenų mainų elementai ISO/IEC 7816-6:2004 + 2006 m. pataisa Nr. 1.

ISO/IEC 7816-8 Atpažinimo kortelės. Lustinės kortelės su kontaktais. 8 dalis. Su saugumu susijusios tarpsektorinės komandos ISO/IEC 7816-8:2004.

ISO/IEC 9797-2 Informacijos technologija. Saugumo metodai. Pranešimų tapatumo nustatymo kodai. 2 dalis. Mechanizmai, pagrįsti specialiąja maišos funkcija ISO/IEC 9797-2:2011

2. ELEKTRINĖS IR FIZINĖS SAVYBĖS

TCS_01 Jei nenurodyta kitaip, visi elektroniniai signalai turi atitikti ISO/IEC 7816-3.

TCS_02 Kortelės kontaktų vieta ir matmenys turi atitikti ISO/IEC 7816-2.

2.1. **Maitinimo įtampa ir srovės naudojimas**

TCS_03 Kortelė turi veikti pagal specifikacijas neviršydama ISO/IEC 7816-3 nurodytų naudojimo ribų.

TCS_04 Kortelė turi veikti su Vcc = 3V (± 0,3V) arba Vcc = 5V (± 0,5V).

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

2.2. **Programavimo įtampa V_{pp}**

TCS_05 Kortelei neturi reikėti programavimo įtampos 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 turi būti ignoruojama.

2.3. **Laikrodžio signalo generavimas ir dažnis**

TCS_06 Kortelė turi veikti 1–5 MHz dažnių diapazone ir gali būti tinkama aukštesniam dažniui. Vieno kortelės naudojimo seanso metu laikrodžio dažnis negali keistis daugiau kaip ± 2 %. Laikrodžio dažnį generuoja transporto priemonės blokas, o ne pati kortelė. Darbinis ciklas gali trukti nuo 40 iki 60 %.

TCS_07 Pagal kortelės rinkmenoje EF ICC esančias sąlygas išorinį laikrodį galima sustabdyti. Pirmasis rinkmenos EFICC baitas koduoja laikrodžio sustabdymo režimo sąlygas:

▼B

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_08 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_09 Esant maitinimo įtampai kortelė veikia dviem būsenomis:

darbine būsena, kai vykdo komandas arba sąveikauja su skaitmeniniu bloku;

budėjimo būsena visais kitais atvejais; esant šiai būsenai kortelė turi išlaikyti visus duomenis.

3. TECHNINĖ ĮRANGA IR INFORMACIJOS PERDAVIMAS

3.1. **Įvadas**

Šiame poskyryje aprašytos būtiniausios tachografo kortelių ir transporto priemonės bloko funkcinės savybės, reikalingos, kad jie tinkamai veiktų ir būtų funkciškai suderinami tarpusavyje.

Tachografo kortelės turi kuo labiau atitikti taikomų ISO/IEC standartų (ypač ISO/IEC 7816) reikalavimus. Tačiau komandos ir protokolai yra išsamiai aprašyti, nurodant tam tikrus naudojimo apribojimus ar galimus skirtumus. Nurodytos komandos visiškai atitinka minėtus standartus (jei nenurodyta kitaip).

3.2. **Siuntimo protokolas**

TCS_10 Siuntimo protokolai T = 0 ir T = 1 turi atitikti ISO/IEC 7816-3. Pažymėtina, kad transporto priemonės blokas turi atpažinti kortelės siunčiamus laukimo laiko plėtinius.

3.2.1 *Protokolai*

TCS_11 Kortelė turi naudoti tiek protokolą **T=0**, tiek protokolą **T=1**. Be to, kortelė gali būti tinkama kitiems kontaktinio ryšio protokolams.

TCS_12 **T=0** yra numatytasis protokolas, todėl norint jį pakeisti į protokolą **T=1**, reikia **PTS** komandos.

▼B

TCS_13 Įtaisai turi gebėti taikyti **tiesioginį susitarimą** abiem protokolais: taigi tiesioginio susitarimo funkcija yra privaloma kortelei.

TCS_14 **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_15 **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 baitų duomenims priimti negalima naudoti komandos GET-RESPONSE.

TCS_16 **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 dydį įtaisui (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.

▼B

3.2.2 *ATR*

TCS_17 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 (bent F0h)	Informacijos lauko dydis kortelei (IFSC)
TH1–TH5	‘XXh’	Istoriniai rašmenys
TCK	‘XXh’	Kontrolinis rašmuo (išskyrus OR)

TCS_18 Po atsakymo į perkrovimą (ATR), besąlygiškai parenkama pagrindinė rinkmena (MF), kuri tampa esamuoju katalogu.

3.2.3 *PTS*

TCS_19 Numatytasis protokolas yra T=0. Protokolui T=1 nustatyti, įtaisas turi nusiųsti į kortelę PTS (dar žinomą PPS pavadinimu).

TCS_20 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)).

Didesnis perdavimo greitis kortelei nėra privalomas.

TCS_21 Jei galima naudoti tik numatytąjį perdavimo greitį (arba jei pasirinktas greitis netinkamas), kortelė turi tinkamai atsakyti į PTS pagal ISO/IEC 7816-3, praleisdama baitą PPS1.

Bazinio PTS pavyzdžiai protokolui pasirinkti:

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

▼B

3.3. **Prieigos taisyklės**

TCS_22 Prieigos taisykle nustatomos prieigos režimo, t. y. komandos, atitinkamos saugumo sąlygos. Jei šios saugumo sąlygos įvykdytos, atitinkama komanda apdorojama.

TCS_23 Tachografo kortelei taikomos šios saugumo sąlygos:

Santrumpa	Reikšmė
ALW	veiksmas visuomet galimas ir jį galima atlikti be jokių apribojimų. Komandos ir atsakymo APDU siunčiami kaip paprastas tekstas, t. y. be saugiojo keitimosi pranešimais.
NEV	veiksmas niekada negalimas.
PLAIN-C	Komandos APDU siunčiami atvirai, t. y. be saugiojo keitimosi pranešimais.
PWD	Veiksmą galima atlikti tik jei dirbtuvių kortelės PIN patikrinimo rezultatas teigiamas, t. y. jei nustatyta kortelės vidinė apsaugos būsena „PIN_Verified“. Komanda turi būti siunčiama be saugiojo keitimosi pranešimais.
EXT-AUT-G1	Veiksmą galima atlikti tik jei 1-osios kartos autentiškumo tikrinimo komanda External Authenticate (taip pat žr. A dalies 11 priedėlį) įvykdyta sėkmingai.
SM-MAC-G1	Su 1-osios kartos saugiuoju keitimusi pranešimais vien autentiškumo tikrinimo režimu turi būti naudojami (komandos ir atsakymo) APDU (žr. A dalies 11 priedėlį).
SM-C-MAC-G1	Su 1-osios kartos saugiuoju keitimusi pranešimais vien autentiškumo tikrinimo režimu turi būti naudojami komandos APDU (žr. A dalies 11 priedėlį).
SM-R-ENC-G1	Su 1-osios kartos saugiuoju keitimusi pranešimais šifravimo režimu turi būti naudojami atsakymo APDU (žr. A dalies 11 priedėlį), t. y. negaunama jokio pranešimo autentiškumo tikrinimo kodo.
SM-R-ENC-MAC-G1	Su 1-osios kartos saugiuoju keitimusi pranešimais vien šifravimo–autentiškumo tikrinimo režimu turi būti naudojami atsakymo APDU (žr. A dalies 11 priedėlį).
SM-MAC-G2	Su 2-osios kartos saugiuoju keitimusi pranešimais vien autentiškumo tikrinimo režimu turi būti naudojami (komandos ir atsakymo) APDU (žr. B dalies 11 priedėlį).
SM-C-MAC-G2	Su 2-osios kartos saugiuoju keitimusi pranešimais vien autentiškumo tikrinimo režimu turi būti naudojami komandos APDU (žr. B dalies 11 priedėlį).
SM-R-ENC-MAC-G2	Su 2-osios kartos saugiuoju keitimusi pranešimais vien šifravimo–autentiškumo tikrinimo režimu turi būti naudojami atsakymo APDU (žr. B dalies 11 priedėlį).

TCS_24 Šios saugumo sąlygos gali būti jungiamos taip:

AND – turi būti įvykdytos visos saugumo sąlygos

OR – turi būti įvykdyta bent viena sąlyga

Rinkmenų sistemos prieigos taisyklės, t. y. komanda SELECT, READ BINARY ir UPDATE BINARY, nustatytos 4 skyriuje. Kitų komandų prieigos taisyklės nustatytos toliau pateikiamose lentelėse.

▼B

TCS_25 Kai naudojama rinkmena DF Tachograph G1, taikomos šios prieigos taisyklės:

Komanda	Vairuotojo kortelė	Dirbtuvių kortelė	Kontrolės kortelė	Įmonės kortelė
External Authenticate				
— 1-osios kartos autentiškumo tikrinimas	ALW	ALW	ALW	ALW
— 2-osios kartos autentiškumo tikrinimas	ALW	PWD	ALW	ALW
Internal Authenticate	ALW	PWD	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Netaikoma	Netaikoma	Netaikoma	Netaikoma
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Netaikoma	Netaikoma
PSO: Hash	Netaikoma	Netaikoma	ALW	Netaikoma
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Netaikoma	Netaikoma
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Netaikoma	Netaikoma	ALW	Netaikoma
Tikrinti	Netaikoma	ALW	Netaikoma	Netaikoma

TCS_26 Kai naudojama rinkmena DF Tachograph_G2, taikomos šios prieigos taisyklės:

Komanda	Vairuotojo kortelė	Dirbtuvių kortelė	Kontrolės kortelė	Įmonės kortelė
External Authenticate				
— 1-osios kartos autentiškumo tikrinimas	Netaikoma	Netaikoma	Netaikoma	Netaikoma
— 2-osios kartos autentiškumo tikrinimas	ALW	PWD	ALW	ALW
Internal Authenticate	Netaikoma	Netaikoma	Netaikoma	Netaikoma

▼B

Komanda	Vairuotojo kortelė	Dirbtuvių kortelė	Kontrolės kortelė	Įmonės kortelė
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Netaikoma	ALW	ALW	Netaikoma
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Netaikoma	Netaikoma
PSO: Hash	Netaikoma	Netaikoma	ALW	Netaikoma
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Netaikoma	Netaikoma
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Netaikoma	Netaikoma	ALW	Netaikoma
VERIFY [patikrinti]	Netaikoma	ALW	Netaikoma	Netaikoma

TCS_27 Pagrindinėje rinkmenoje (MF) taikomos šios prieigos taisyklės:

Komanda	Vairuotojo kortelė	Dirbtuvių kortelė	Kontrolės kortelė	Įmonės kortelė
External Authenticate				
— 1-osios kartos autentiškumo tikrinimas	Netaikoma	Netaikoma	Netaikoma	Netaikoma
— 2-osios kartos autentiškumo tikrinimas	ALW	PWD	ALW	ALW
Internal Authenticate	Netaikoma	Netaikoma	Netaikoma	Netaikoma
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Netaikoma	Netaikoma	Netaikoma	Netaikoma

▼B

Komanda	Vairuotojo kortelė	Dirbtuvių kortelė	Kontrolės kortelė	Įmonės kortelė
PSO: Compute Digital Signature	Netaikoma	Netaikoma	Netaikoma	Netaikoma
PSO: Hash	Netaikoma	Netaikoma	Netaikoma	Netaikoma
PSO: Hash of File	Netaikoma	Netaikoma	Netaikoma	Netaikoma
PSO: Verify Certificate	ALW	ALW	ALW	ALW
VERIFY [patikrinti]	Netaikoma	ALW	Netaikoma	Netaikoma

TCS_28 Tachografo kortelė gali priimti didesnio saugumo lygio, nei nurodytasis nustatytose saugumo sąlygose, komandą arba gali jos nepriimti. T. y., jei saugumo sąlyga yra ALW (arba PLAIN-C), kortelė gali priimti komandą su saugiuoju keitimusi pranešimais (šifravimo ir (arba) autentiškumo tikrinimo režimas). Jei pagal saugumo sąlygą būtinas saugusis keitimasis pranešimais ir autentiškumo tikrinimo režimas, tachografo kortelė gali priimti komandą su saugiuoju keitimusi pranešimais, kurio autentiškumo tikrinimo ir šifravimo režimas yra tos pačios kartos.

Pastaba. Komandų aprašymuose pateikiama daugiau informacijos apie tai, kokioms komandoms tinkamos įvairių rūšių kortelės ir įvairios rinkmenos DF.

3.4. **Komandų ir klaidų kodų apžvalga**

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

Šiame poskyryje aprašytos tokios APDU komandų ir atsakymų poros. 1-ajai ir 2-ajai kartai tinkami komandos variantai nustatyti atitinkamuose komandų aprašymuose.

Komanda	INS
SELECT	‘A4h’
READ BINARY	‘B0h’, ‘B1h’
UPDATE_BINARY	‘D6h’, ‘D7h’
GET_CHALLENGE	‘84h’
VERIFY	‘20h’
GET_RESPONSE	‘C0h’
PERFORM SECURITY OPERATION	‘2Ah’

▼B

Komanda	INS
— VERIFY_CERTIFICATE	
— COMPUTE DIGITAL SIGNATURE	
— VERIFY_DIGITAL_SIGNATURE	
— HASH	
— PERFORM_HASH_OF_FILE	
— PROCESS DSRC MESSAGE	
INTERNAL_AUTHENTICATE	‘88h’
EXTERNAL_AUTHENTICATE	‘82h’
MANAGE SECURITY ENVIRONMENT	‘22h’
— SET DIGITAL SIGNATURE TEMPLATE	
— SET AUTHENTICATION TEMPLATE	
GENERAL AUTHENTICATE	‘86h’

TCS_29 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	Perspėjamasis apdorojimas. Dalis grąžinamų duomenų gali būti sugadinti.
63	00	Autentiškumas nepatikrintas (Įspėjimas)
63	CX	Neteisingas CHV (PIN). Likusių bandymų skaitiklio vertė pateikiama kaip X.
64	00	Vykdymo klaida. Ilgalaikės atminties būsena nepakitusi. Nepažeistumo klaida.
65	00	Vykdymo klaida. Ilgalaikės atminties būsena pakitusi.
65	81	Vykdymo klaida. Ilgalaikės atminties būsena pakitusi. Atminties sutrikimas.
66	88	Apsaugos klaida: neteisinga kriptografinė kontrolinė suma (vykstant saugiajam keitimuisi pranešimais) arba neteisingas pažymėjimas (tikrinant pažymėjimą); neteisinga kriptograma (išoriškai tikrinant autentiškumą); neteisingas parašas (tikrinant parašą).
67	00	Neteisingas ilgis (neteisingas Lc arba Le).

▼B

SW1	SW2	Reikšmė
68	82	Nepritaikyta saugiajam keitimuisi pranešimais.
68	83	Laukiama sekos paskutinės komandos.
69	00	Uždrausta komanda (kai T=0, atsakymas negalimas).
69	82	Neįvykdyti apsaugos būsenos reikalavimai.
69	83	Autentiškumo tikrinimo būdas užblokuotas.
69	85	Neįvykdytos naudojimo sąlygos.
69	86	Komanda neleidžiama (nėra esamojo EF).
69	87	Nėra lauktų saugaus keitimosi pranešimais duomenų objektų.
69	88	Neteisingi saugaus keitimosi pranešimais duomenų objektai.
6 A	80	Neteisingi duomenų laukelio parametrai.
6 A	82	Rinkmena nerasta.
6 A	86	Neteisingi parametrai P1-P2.
6 A	88	Nurodytų duomenų nerasta.
6 B	00	Neteisingi parametrai (nuokrypis už rinkmenos EF ribų).
6C	XX	Neteisingas ilgis; teisingą ilgį rodo SW2. Duomenų laukelis atsakyme negrąžinamas.
6D	00	Instrukcijos kodas netinkamas arba neteisingas.
6E	00	Klasė netinkama.
6F	00	Kitos tikrinimo klaidos.

TCS_30 Jei komanda APDU atitinka daugiau nei vieną klaidos sąlygą, kortelės atsakyme gali būti bet kurie atitinkami būsenos žodžiai.

3.5. **Komandų aprašymai**

Šiame poskyryje aprašytos tachografo kortelių privalomosios komandos.

Papildoma išsamesnė informacija apie naudojamas kriptografines operacijas pateikta 11 priedėlyje „1-osios ir 2-osios kartos tachografų 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_31 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. 3.5.6 punktą) su P3=Le.

TCS_32 Jei reikalaujami abu ilgio baitai ir Le=0 (saugus keitimasis pranešimais):

▼B

— 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.

TCS_33 Pasirinktinai kortelė gali būti tinkama didesnio ilgio laukeliams pagal ISO/IEC 7816-4. Jei tachografo kortelė tinkama didesnio ilgio laukeliams:

— jos tinkamumas didesnio ilgio laukeliams nurodomas ATR;

— tinkamas buferio dydis nurodomas rinkmenos EF ATR/INFO išplėstinėje informacijoje, žr. TCS_146;

— nurodoma, ar ji tinkama išplėstinės rinkmenos EF didesnio ilgio laukeliams T = 1 ir (arba) T = 0, žr. TCS_147;

— ji yra tinkama 1-osios ir 2-osios kartos tachografo programos didesnio ilgio laukeliams.

Pastabos.

Visos komandos nustatytos nedidelio ilgio laukeliams. Didesnio ilgio APDU naudojimas paaiškintas ISO/IEC 7816-4.

Komandos paprastai nustatomos paprastajam režimui, t. y. be saugiojo keitimosi pranešimais, nes saugiojo keitimosi pranešimais lygmuo nustatytas 11 priedėlyje. Iš komandos prieigos taisyklių aišku, ar komanda tinkama saugiajam keitimuisi pranešimais ir ar ji tinkama 1-osios ir (arba) 2-osios kartos saugiajam keitimuisi pranešimais. Kai kurie komandos variantai aprašomi su saugiuoju keitimusi pranešimais, taip siekiama paaiškinti saugiojo keitimosi pranešimais naudojimą.

TCS_34 Transporto priemonės bloke įvykdomas visas seanso 2-osios kartos transporto priemonės bloko ir kortelės abipusio autentiškumo tikrinimo protokolas, įkaitant pažymėjimo tikrinimą (jei reikia) rinkmenose DF Tachograph, DF Tachograph_G2 arba MF.

3.5.1 *SELECT*

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

Komanda SELECT naudojama:

— taikomosios programos DF pasirinkti (reikia naudoti pasirinkimą pagal pavadinimą),

— pateiktos rinkmenos ID atitinkančiai elementariajai rinkmenai pasirinkti.

3.5.1.1 Pasirinkimas pagal pavadinimą (AID).

Ši komanda leidžia pasirinkti kortelėje taikomosios programos DF.

TCS_35 Šią komandą galima atlikti iš bet kurios rinkmenos struktūros vietos (po ATR ar bet kada).

▼B

TCS_36 Pasirinkus pritaikymą, esama apsaugos aplinka perkraunama. Pasirinkus pritaikymą, neparinktas joks esamas viešasis raktas. Taip pat prarandama prieigos sąlyga EXT-AUT-G1. Jei komanda įvykdyta be saugiojo keitimosi pranešimais, buvusių saugiojo keitimosi pranešimais seanso raktų nebegalima naudoti.

TCS_37 **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: 1-osios kartos tachografo programa – ‘FF 54 41 43 48 4F’ AID: 2-osios kartos tachografo programa – ‘FF 53 4D 52 44 54’

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

TCS_38 **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 būsena ‘**6A82**’.

— Protokole T=1, jei yra baitas Le, gauta būsena – **‘6700’**.

— Protokole T=0, jei po komandos SELECT yra atsakymo prašymas, gauta būsena – **‘6900’**.

— Jei pasirinkta programa laikoma sugadinta (rinkmenos atributuose randama nepažeistumo klaida), atsakyme nurodoma apdorojimo būsena ‘**6400**’ arba ‘**6581**’.

3.5.1.2 Elementariosios rinkmenos pasirinkimas naudojantis jos identifikatoriumi

TCS_39 **Komandos pranešimas**

TCS_40 Kad veiktų šis komandos variantas, tachografo kortelė turi būti tinkama 2-osios kartos saugiajam keitimuisi pranešimais, nustatytam 11 priedėlio B dalyje.

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘00h’	
INS	1	‘A4h’	
P1	1	‘02h’	EF pasirinkimas pagal esamą DF.

▼B

Baitas	Ilgis	Vertė	Aprašymas
P2	1	‘0Ch’	Atsakymo nelaukiama.
Lc	1	‘02h’	Į kortelę nusiųstų baitų skaičius.
#6-#7	2	‘XXXXh’	Rinkmenos identifikatorius.

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

TCS_41 **Atsakymo pranešimas (atsakyti neprašoma)**

Baitas	Ilgis	Vertė	Aprašymas
SW	2	‘XXXXh’	Būsenos žodžiai (SW1, SW2)

— Jei komanda sėkmingai įvykdoma, kortelė atsako ‘**9000**’.

— Jei rinkmenos, atitinkančio rinkmenos identifikatorių, nerandama, atsakyme nurodoma apdorojimo būsena ‘**6A82**’.

— Protokole T=1, jei yra baitas Le, gauta būsena – **‘6700’**.

— Protokole T=0, jei po komandos SELECT yra atsakymo prašymas, gauta būsena – **‘6900’**.

— Jei pasirinkta rinkmena laikoma sugadinta (rinkmenos atributuose randama nepažeistumo klaida), atsakyme nurodoma apdorojimo būsena ‘**6400**’ arba ‘**6581**’.

3.5.2 *READ BINARY*

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 pranešimais struktūrą.

3.5.2.1 Komanda su P1-P2 poslinkiu

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

Pastaba. Ši komanda be saugiojo keitimosi pranešimais gali būti naudojama tik skaityti rinkmenai, kuri palaiko skaitymo prieigos režimo saugumo sąlygą ALW.

TCS_42 **Komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘00h’	
INS	1	‘B0h’	Nuskaityti dvejetainį
P1	1	‘XXh’	Poslinkis baitais nuo rinkmenos pradžios: reikšmingiausias baitas.

▼B

Baitas	Ilgis	Vertė	Aprašymas
P2	1	‘XXh’	Poslinkis baitais nuo rinkmenos pradžios: mažiausiai reikšmingas baitas.
Le	1	‘XXh’	Laukiamas duomenų ilgis. Nuskaitytinų baitų skaičius.

Pastaba. P1 8 bitas turi būti 0.

TCS_43 **Atsakymo pranešimas**

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 nepasirinkta jokia EF, atsakyme nurodoma apdorojimo būsena **‘6986’**.

— Jei pasirinktos rinkmenos saugumo sąlygos neįvykdytos, nurodoma komandos vykdymo nutraukimo būsena ‘**6982**’.

— Jei poslinkis neatitinka rinkmenos EF dydžio (poslinkis > EF dydis), atsakyme nurodoma apdorojimo būsena **‘6B00’**.

— Jei nuskaitytinų duomenų dydis neatitinka rinkmenos EF dydžio (poslinkis + Le > EF dydis), atsakyme nurodoma apdorojimo būsena ‘**6700**’ arba ‘**6Cxx**’ (čia ‘xx’ nurodo tikslų ilgį).

— Jei rinkmenos atributuose randama nepažeistumo klaida, kortelė turi laikyti rinkmeną sugadinta ir neatkuriama, o atsakyme nurodoma apdorojimo būsena **‘6400’** arba ‘**6581**’.

— Jei atmintyje laikomuose duomenyse randama nepažeistumo klaida, kortelė turi grąžinti pareikalautus duomenis, o atsakyme nurodoma apdorojimo būsena **‘6281’**.

3.5.2.1.1 Komanda su saugiuoju keitimusi pranešimais (pavyzdžiai)

Ši komanda leidžia IFD nuskaityti duomenis iš tuo metu pasirinktos rinkmenos EF naudojant saugiojo keitimosi pranešimais būdą, kad būtų patikrintas gautų duomenų nepažeistumas ir apsaugotas duomenų konfidencialumas, jei taikoma saugumo sąlyga SM-R-ENC-MAC-G1 (1-osios kartos) arba SM-R-ENC-MAC-G2 (2-osios kartos).

TCS_44 **Komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘0Ch’	Prašoma saugaus keitimosi pranešimais.
INS	1	‘B0h’	Nuskaityti dvejetainį
P1	1	‘XXh’	P1 (poslinkis baitais nuo rinkmenos pradžios): reikšmingiausias baitas.
P2	1	‘XXh’	P2 (poslinkis baitais nuo rinkmenos pradžios): mažiausiai reikšmingas baitas.

▼B

Baitas	Ilgis	Vertė	Aprašymas
Lc	1	‘XXh’	Saugaus keitimosi pranešimais pradinių 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.
#9	1	‘8Eh’	T_{CC}: kriptografinės kontrolinės sumos žymena.
#10	1	‘XXh’	L_{CC}: kitos iš eilės kriptografinės kontrolinės sumos ilgis. ‘04h’ – 1-osios kartos saugiajam keitimuisi pranešimais (žr. 11 priedėlio A dalį) ‘08h’, ‘0Ch’ arba ‘10h’ (priklauso nuo rakto AES ilgio) 2-osios kartos saugiajam keitimuisi pranešimais (žr. 11 priedėlio B dalį)
#11-#(10+L)	L	‘XX..XXh’	Kriptografinė kontrolinė suma.
Le	1	‘00h’	Kaip nurodyta ISO/IEC 7816-4.

TCS_45 **Atsakymo pranešimas, jei sąlyga SM-R-ENC-MAC-G1 (1-osios kartos) / SM-R-ENC-MAC-G2 (2-osios kartos) nebūtina ir jei saugiojo keitimosi pranešimais įvesties formatas yra tinkamas**

Baitas	Ilgis	Vertė	Aprašymas
#1	1	‘99h’	Apdorojimo būsenos žymena (SW1-SW2) – 1-osios kartos saugiajam keitimuisi pranešimais nebūtina
#2	1	‘02h’	Apdorojimo būsenos ilgis
#3 – #4	2	‘XX XXh’	Neapsaugotojo atsakymo APDU apdorojimo būsena
#5	1	‘81h’	T_{PV}: paprastųjų verčių duomenų žymena.
#6	L	‘NNh’ arba ‘81 NNh’	L_{PV}: grąžinamų duomenų ilgis (= pradiniam Le). Jei L_{PV}> 127 baitai, L yra 2 baitai.
#(6+L)-#(5+L+NN)	NN	‘XX..XXh’	Paprastųjų verčių duomenys.
#(6+L+NN)	1	‘8Eh’	T_{CC}: kriptografinės kontrolinės sumos žymena.
#(7+L+NN)	1	‘XXh’	L_{CC}: kitos iš eilės kriptografinės kontrolinės sumos ilgis. ‘04h’ – 1-osios kartos saugiajam keitimuisi pranešimais (žr. 11 priedėlio A dalį) ‘08h’, ‘0Ch’ arba ‘10h’ (priklauso nuo rakto AES ilgio) 2-osios kartos saugiajam keitimuisi pranešimais (žr. 11 priedėlio B dalį)
#(8+L+NN)-#(7+M+L+NN)	M	‘XX..XXh’	Kriptografinė kontrolinė suma.
SW	2	‘XXXXh’	Būsenos žodžiai (SW1, SW2)

▼B

TCS_46 **Atsakymo pranešimas, jei sąlyga SM-R-ENC-MAC-G1 (1-osios kartos) / SM-R-ENC-MAC-G2 (2-osios kartos) būtina ir jei saugiojo keitimosi pranešimais įvesties formatas yra tinkamas**

Baitas	Ilgis	Vertė	Aprašymas
#1	1	‘87h’	$T_{PI\ CG}$: užšifruotųjų duomenų (kriptogramos) žymena.
#2	L	‘MMh’ arba ‘81 MMh’	$L_{PI\ CG}$: grąžinamų užšifruotųjų 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’	Užšifruotieji duomenys: išplėtimo indikatorius ir kriptograma.
#(2+L+MM)	1	‘99h’	Apdorojimo būsenos žymena (SW1-SW2) – 1-osios kartos saugiajam keitimuisi pranešimais nebūtina
#(3+L+MM)	1	‘02h’	Apdorojimo būsenos ilgis
#(4+L+MM) – #(5+L+MM)	2	‘XX XXh’	Neapsaugotojo atsakymo APDU apdorojimo būsena
#(6+L+MM)	1	‘8Eh’	T_{CC}: kriptografinės kontrolinės sumos žymena.
#(7+L+MM)	1	‘XXh’	L_{CC}: kitos iš eilės kriptografinės kontrolinės sumos ilgis. ‘04h’ – 1-osios kartos saugiajam keitimuisi pranešimais (žr. 11 priedėlio A dalį) ‘08h’, ‘0Ch’ arba ‘10h’ (priklauso nuo rakto AES ilgio) 2-osios kartos saugiajam keitimuisi pranešimais (žr. 11 priedėlio B dalį)
#(8+L+MM)-#(7+N+L+MM)	N	‘XX..XXh’	Kriptografinė kontrolinė suma.
SW	2	‘XXXXh’	Būsenos žodžiai (SW1, SW2)

Komandos READ BINARY atsakyme gali būti įrašytos įprastinės apdorojimo būsenos, išvardytos TCS_43 su žymena ‘99h’, kaip aprašyta TCS_59 naudojant saugiojo keitimosi pranešimais atsakymo struktūrą.

Be to, gali įvykti tam tikrų su saugiu keitimusi pranešimais susijusių klaidų. Tokiais atvejais apdorojimo būsenos nuoroda paprasčiausiai grąžinama nenaudojant saugiojo keitimosi pranešimais struktūros.

TCS_47 **Atsakymo pranešimas, jei saugaus keitimosi pranešimais įvesties formatas netinkamas:**

Baitas	Ilgis	Vertė	Aprašymas
SW	2	‘XXXXh’	Būsenos žodžiai (SW1, SW2)

— Jei nėra jokio esamo seanso rakto, atsakyme nurodoma apdorojimo būsena **‘6A88’**. Taip atsitinka, jei seanso raktas dar nesugeneruotas arba baigėsi jo galiojimo laikas (šiuo atveju IFD turi pakartoti abipusio autentiškumo tikrinimo procesą naujam seanso raktui nustatyti).

▼B

— 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’**.

3.5.2.2 Komanda su trumpuoju EF (elementariosios rinkmenos) identifikatoriumi

Pasinaudojus šiuo komandos variantu ir nurodžius trumpąjį EF identifikatorių, IFD gali išrinkti tam tikrą rinkmeną EF ir perskaityti duomenis iš jos.

TCS_48 Tachografo kortelė turi būti tinkama šiam komandos variantui ir visoms elementariosioms rinkmenoms su nustatytu trumpuoju EF identifikatoriumi. Šie trumpieji EF identifikatoriai nustatyti 4 skyriuje.

TCS_49 **Komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘00h’	
INS	1	‘B0h’	Nuskaityti dvejetainį
P1	1	‘XXh’	8 bito vertė yra 1 7 ir 6 bitų vertė yra 00 5–1 bitais užkoduojamas atitinkamos rinkmenos EF trumpasis EF identifikatorius
P2	1	‘XXh’	Užkoduojamas 0–255 bitų poslinkis rinkmenoje EF, į kurią daroma nuoroda parametre P1
Le	1	‘XXh’	Laukiamas duomenų ilgis. Nuskaitytinų baitų skaičius.

Pastaba. 2-osios kartos tachografo programoje naudojami trumpieji rinkmenos EF identifikatoriai nustatyti 4 skyriuje.

Jei parametre P1 užkoduotas trumpasis EF identifikatorius ir komanda įvykdyta gerai, identifikatorius EF tampa tuo metu pasirinkta rinkmena EF (esamąja rinkmena EF).

TCS_50 **Atsakymo pranešimas**

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

— Jei komanda sėkmingai įvykdoma, kortelė atsako ‘**9000**’.

— Jei rinkmenos, atitinkančios trumpąjį EF identifikatorių, nerandama, atsakyme nurodoma apdorojimo būsena ‘**6A82**’.

— Jei pasirinktos rinkmenos saugumo sąlygos neįvykdytos, nurodoma komandos vykdymo nutraukimo būsena ‘**6982**’.

▼B

— Jei poslinkis neatitinka rinkmenos EF dydžio (poslinkis > EF dydis), atsakyme nurodoma apdorojimo būsena **‘6B00’**.

— Jei nuskaitytinų duomenų dydis neatitinka rinkmenos EF dydžio (poslinkis + Le > EF dydis), atsakyme nurodoma apdorojimo būsena ‘**6700**’ arba ‘**6Cxx**’ (čia ‘xx’ nurodo tikslų ilgį).

— Jei rinkmenos atributuose randama nepažeistumo klaida, kortelė turi laikyti rinkmeną sugadinta ir neatkuriama, o atsakyme nurodoma apdorojimo būsena ‘**6400**’ arba ‘**6581**’.

— Jei atmintyje laikomuose duomenyse randama nepažeistumo klaida, kortelė turi grąžinti pareikalautus duomenis, o atsakyme nurodoma apdorojimo būsena **‘6281’**.

3.5.2.3 Komanda su nelyginiu komandos baitu

Pasinaudojus šiuo komandos variantu, IDF gali perskaityti duomenis iš tam tikros rinkmenos EF su ne mažiau kaip 32 768 baitais.

TCS_51 Jei tachografo kortelė yra tinkama rinkmenoms EF su ne mažiau kaip 32 768 baitų, ji turi būti tinkama ir šiam komandos variantui, naudojamam su tokiomis rinkmenomis EF. Tachografo kortelė gali būti arba nebūti tinkama šiam komandos variantui kitų rinkmenų EF atžvilgiu, išskyrus rinkmeną EF Sensor_Installation_Data, žr. TCS_156 ir TCS_160.

TCS_52 **Komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘00h’	
INS	1	‘B1h’	Nuskaityti dvejetainį
P1	1	‘00h’	Esamoji rinkmena EF
P2	1	‘00h’	
Lc	1	‘NNh’	Lc Paslinktųjų duomenų objekto ilgis
#6-#(5+NN)	NN	‘XX..XXh’	Paslinktųjų duomenų objektas: žymena ‘54h’ ilgis ‘01h’ arba ‘02h’ vertė offset
Le	1	‘XXh’	Nuskaitytinų baitų skaičius.

IFD užkoduoja paslinktųjų duomenų objekto ilgį mažiausiu įmanomu oktetų skaičiumi, t. y. naudojant ilgio baitą ‘01h’ IFD užkoduoja poslinkį nuo 0 iki 255 baitų, o naudojant ilgio baitą ‘02h’ – poslinkį nuo 256 iki 65 535 baitų.

TCS_53 **Atsakymo pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
#1-#L	L	‘XX..XXh’	Nuskaityti duomenys sutelkti diskrečiųjų duomenų objekte, kurio žymena ‘53h’.
SW	2	‘XXXXh’	Būsenos žodžiai (SW1, SW2)

▼B

— Jei komanda sėkmingai įvykdoma, kortelė atsako ‘**9000**’.

— Jei nepasirinkta jokia rinkmena EF, atsakyme nurodoma apdorojimo būsena ‘**6986**’.

— Jei pasirinktos rinkmenos saugumo sąlygos neįvykdytos, nurodoma komandos vykdymo nutraukimo būsena ‘**6982**’.

— Jei poslinkis neatitinka rinkmenos EF dydžio (poslinkis > EF dydis), atsakyme nurodoma apdorojimo būsena ‘**6B00**’.

— Jei nuskaitytinų duomenų dydis neatitinka rinkmenos EF dydžio (poslinkis + Le > EF dydis), atsakyme nurodoma apdorojimo būsena ‘**6700**’ arba ‘**6Cxx**’ (čia ‘xx’ nurodo tikslų ilgį).

— Jei rinkmenos atributuose randama nepažeistumo klaida, kortelė turi laikyti rinkmeną sugadinta ir neatkuriama, o atsakyme nurodoma apdorojimo būsena ‘**6400**’ arba ‘**6581**’.

— Jei atmintyje laikomuose duomenyse randama nepažeistumo klaida, kortelė turi grąžinti pareikalautus duomenis, o atsakyme nurodoma apdorojimo būsena ‘**6281**’.

3.5.2.3.1 Komanda su saugiuoju keitimusi pranešimais (pavyzdys)

Šiame pavyzdyje paaiškinta, kaip naudojamas saugusis keitimasis pranešimais, jei taikoma saugumo sąlyga SM-MAC-G2.

TCS_54 Komandos pranešimas

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘0Ch’	Prašoma saugaus keitimosi pranešimais.
INS	1	‘B1h’	Nuskaityti dvejetainį
P1	1	‘00h’	Esamoji rinkmena EF
P2	1	‘00h’	
Lc	1	‘XXh’	Apsaugotų duomenų laukelio ilgis.
#6	1	‘B3h’	Paprastųjų verčių duomenų, užkoduotų objekte BER-TLV, žymena.
#7	1	‘NNh’	L_{PV}: perduodamų duomenų ilgis.
#(8)-#(7+NN)	NN	‘XX..XXh’	Paprastieji duomenys, užkoduoti BER-TLV, t. y. paslinktųjų duomenų objektas su žymena ‘54h’ ‖
#(8+NN)	1	‘97h’	T_{LE}: laukiamo ilgio specifikacijos žymena.
#(9+NN)	1	‘01h’	L_{LE}: laukiamas ilgis.
#(10+NN)	1	‘XXh’	Laukiamo ilgio specifikacija (pradinis Le): nuskaitytinų baitų skaičius.
#(11+NN)	1	‘8Eh’	T_{CC}: kriptografinės kontrolinės sumos žymena.
#(12+NN)	1	‘XXh’	L_{CC}: kitos iš eilės kriptografinės kontrolinės sumos ilgis. ‘08h’, ‘0Ch’ arba ‘10h’ (priklauso nuo rakto AES ilgio) 2-osios kartos saugiajam keitimuisi pranešimais (žr. 11 priedėlio B dalį)
#(13+NN)-#(12+M+NN)	M	‘XX..XXh’	Kriptografinė kontrolinė suma.
Le	1	‘00h’	Kaip nurodyta ISO/IEC 7816-4.

▼B

TCS_55 Atsakymo pranešimas, jei komanda įvykdyta sėkmingai

Baitas	Ilgis	Vertė	Aprašymas
#1	1	‘B3h’	Paprastieji duomenys, užkoduoti BER-TLV
#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’	Nuskaityti duomenys, užkoduoti BER-TLV, t. y. nuskaityti duomenys sutelkti diskrečiųjų duomenų objekte, kurio žymena ‘53h’.
#(2+L+NN)	1	‘99h’	Neapsaugotojo atsakymo APDU apdorojimo būsena
#(3+L+NN)	1	‘02h’	Apdorojimo būsenos ilgis
#(4+L+NN) – #(5+L+NN)	2	‘XX XXh’	Neapsaugotojo atsakymo APDU apdorojimo būsena
#(6+L+NN)	1	‘8Eh’	T_{CC}: kriptografinės kontrolinės sumos žymena.
#(7+L+NN)	1	‘XXh’	L_{CC}: kitos iš eilės kriptografinės kontrolinės sumos ilgis. ‘08h’, ‘0Ch’ arba ‘10h’ (priklauso nuo rakto AES ilgio) 2-osios kartos saugiajam keitimuisi pranešimais (žr. 11 priedėlio B dalį)
#(8+L+NN)-#(7+M+L+NN)	M	‘XX..XXh’	Kriptografinė kontrolinė suma.
SW	2	‘XXXXh’	Būsenos žodžiai (SW1, SW2)

3.5.3 *UPDATE_BINARY*

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.

3.5.3.1 Komanda su P1-P2 poslinkiu

Ši komanda leidžia IFD rašyti duomenis į tuo metu pasirinktą EF, kortelei netikrinant gautų duomenų nepažeistumo.

Pastaba. Ši komanda be saugiojo keitimosi pranešimais gali būti naudojama tik rinkmenai, kuri palaiko atnaujinimo prieigos režimo saugumo sąlygą ALW, atnaujinti.

TCS_56 **Komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘00h’	
INS	1	‘D6h’	Atnaujinti dvejetainį
P1	1	‘XXh’	Poslinkis baitais nuo rinkmenos pradžios: reikšmingiausias baitas.
P2	1	‘XXh’	Poslinkis baitais nuo rinkmenos pradžios: mažiausiai reikšmingas baitas.

▼B

Baitas	Ilgis	Vertė	Aprašymas
Lc	1	‘NNh’	Atnaujintinų duomenų Lc ilgis. Rašytinų baitų skaičius.
#6-#(5+NN)	NN	‘XX..XXh’	Rašytini duomenys.

Pastaba. P1 8 bitas turi būti 0.

TCS_57 **Atsakymo pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
SW	2	‘XXXXh’	Būsenos žodžiai (SW1, SW2)

— Jei komanda sėkmingai įvykdoma, kortelė atsako ‘**9000**’.

— Jei nepasirinkta jokia EF, atsakyme nurodoma apdorojimo būsena **‘6986’**.

— Jei pasirinktos rinkmenos saugumo sąlygos neįvykdytos, nurodoma komandos vykdymo nutraukimo būsena ‘**6982**’.

— Jei poslinkis neatitinka rinkmenos EF dydžio (poslinkis > EF dydis), atsakyme nurodoma apdorojimo būsena **‘6B00’**.

— Jei rašytinų duomenų dydis neatitinka EF dydžio (poslinkis + Lc > EF dydis), atsakyme nurodoma apdorojimo būsena **‘6700’**.

— Jei rinkmenos atributuose randama nepažeistumo klaida, kortelė turi laikyti rinkmeną sugadinta ir neatkuriama, o atsakyme nurodoma apdorojimo būsena ‘**6400**’ arba ‘**6500**’.

— Jei rašyti nepavyksta, atsakyme nurodoma apdorojimo būsena **‘6581’**.

3.5.3.1.1 Komanda su saugiuoju keitimusi pranešimais (pavyzdžiai)

Ši komanda leidžia IFD rašyti duomenis į tuo metu pasirinktą EF, kortelei tikrinant gautų duomenų nepažeistumą. Kadangi konfidencialumo nereikalaujama, duomenys nešifruoti.

TCS_58 **Komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘0Ch’	Prašoma saugaus keitimosi pranešimais.
INS	1	‘D6h’	Atnaujinti dvejetainį
P1	1	‘XXh’	Poslinkis baitais nuo rinkmenos pradžios: reikšmingiausias baitas.
P2	1	‘XXh’	Poslinkis baitais nuo rinkmenos pradžios: mažiausiai reikšmingas baitas.
Lc	1	‘XXh’	Apsaugotų duomenų laukelio ilgis.
#6	1	‘81h’	T_{PV}: paprastųjų verčių duomenų žymena.
#7	L	‘NNh’ arba ‘81 NNh’	L_{PV}: perduodamų duomenų ilgis. Jei L_{PV}> 127 baitai, L yra 2 baitai.

▼B

Baitas	Ilgis	Vertė	Aprašymas
#(7+L)-#(6+L+NN)	NN	‘XX..XXh’	Paprastųjų duomenų vertė (rašytini duomenys).
#(7+L+NN)	1	‘8Eh’	T_{CC}: kriptografinės kontrolinės sumos žymena.
#(8+L+NN)	1	‘XXh’	L_{CC}: Kriptografinės kontrolinės sumos ‘04h’ ilgis 1-osios kartos saugiajam keitimuisi pranešimais (žr. 11 priedėlio A dalį) ‘08h’, ‘0Ch’ arba ‘10h’ (priklauso nuo rakto AES ilgio) 2-osios kartos saugiajam keitimuisi pranešimais (žr. 11 priedėlio B dalį)
#(9+L+NN)-#(8+M+L+NN)	M	‘XX..XXh’	Kriptografinė kontrolinė suma.
Le	1	‘00h’	Kaip nurodyta ISO/IEC 7816-4.

TCS_59 **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’	Neapsaugotojo atsakymo APDU apdorojimo būsena
#5	1	‘8Eh’	T_{CC}: kriptografinės kontrolinės sumos žymena.
#6	1	‘XXh’	L_{CC}: kitos iš eilės kriptografinės kontrolinės sumos ilgis. ‘04h’ – 1-osios kartos saugiajam keitimuisi pranešimais (žr. 11 priedėlio A dalį) ‘08h’, ‘0Ch’ arba ‘10h’ (priklauso nuo rakto AES ilgio) 2-osios kartos saugiajam keitimuisi pranešimais (žr. 11 priedėlio B dalį)
#7-#(6+L)	L	‘XX..XXh’	Kriptografinė kontrolinė suma.
SW	2	‘XXXXh’	Būsenos žodžiai (SW1, SW2)

Aprašytos komandos UPDATE BINARY „įprastos“ apdorojimo būsenos, nenaudojant saugaus keitimosi pranešimais (žr. 3.5.3.1 punktą), atsakyme gali būti nurodytos naudojant pirmiau aprašytą atsakymo pranešimų struktūrą.

Be to, gali įvykti tam tikrų su saugiu keitimusi pranešimais susijusių klaidų. Tokiais atvejais apdorojimo būsenos nuoroda paprasčiausiai grąžinama nenaudojant saugiojo keitimosi pranešimais struktūros.

TCS_60 **Atsakymo pranešimas, jei saugaus keitimosi pranešimais įvesties formatas netinkamas:**

Baitas	Ilgis	Vertė	Aprašymas
SW	2	‘XXXXh’	Būsenos žodžiai (SW1, SW2)

▼B

— Jei nėra jokio esamo seanso rakto, atsakyme nurodoma apdorojimo būsena **‘6A88’**.

— 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’**.

3.5.3.2 Komanda su trumpuoju rinkmenos EF identifikatoriumi

Pasinaudojus šiuo komandos variantu ir nurodžius trumpąjį EF identifikatorių, IFD gali išrinkti tam tikrą rinkmeną EF ir įrašyti duomenis iš jos.

TCS_61 Tachografo kortelė turi būti tinkama šiam komandos variantui ir visoms elementariosioms rinkmenoms su nustatytu trumpuoju EF identifikatoriumi. Šie trumpieji rinkmenos EF identifikatoriai nustatyti 4 skyriuje.

TCS_62 **Komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘00h’	
INS	1	‘D6h’	Atnaujinti dvejetainį
P1	1	‘XXh’	8 bito vertė yra 1 7 ir 6 bitų vertė yra 00 5–1 bitais užkoduojamas atitinkamos rinkmenos EF trumpasis EF identifikatorius
P2	1	‘XXh’	Užkoduojamas 0–255 bitų poslinkis rinkmenoje EF, į kurią daroma nuoroda parametre P1
Lc	1	‘NNh’	Atnaujintinų duomenų Lc ilgis. Rašytinų baitų skaičius.
#6-#(5+NN)	NN	‘XX..XXh’	Rašytini duomenys.

TCS_63 **Atsakymo pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
SW	2	‘XXXXh’	Būsenos žodžiai (SW1, SW2)

Pastaba. 2-osios kartos tachografo programoje naudojami trumpieji EF identifikatoriai nustatyti 4 skyriuje.

Jei parametre P1 užkoduotas trumpasis EF identifikatorius ir komanda įvykdyta gerai, identifikatorius EF tampa tuo metu pasirinkta rinkmena EF (esamąja rinkmena EF).

▼B

— Jei komanda sėkmingai įvykdoma, kortelė atsako ‘**9000**’.

— Jei rinkmenos, atitinkančios trumpąjį EF identifikatorių, nerandama, atsakyme nurodoma apdorojimo būsena ‘**6A82**’.

— Jei pasirinktos rinkmenos saugumo sąlygos neįvykdytos, nurodoma komandos vykdymo nutraukimo būsena ‘**6982**’.

— Jei poslinkis neatitinka rinkmenos EF dydžio (poslinkis > EF dydis), atsakyme nurodoma apdorojimo būsena **‘6B00’**.

— Jei rašytinų duomenų dydis neatitinka EF dydžio (poslinkis + Lc > EF dydis), atsakyme nurodoma apdorojimo būsena **‘6700’**.

— Jei rinkmenos atributuose randama nepažeistumo klaida, kortelė turi laikyti rinkmeną sugadinta ir neatkuriama, o atsakyme nurodoma apdorojimo būsena ‘**6400**’ arba ‘**6581**’.

— Jei rašyti nepavyksta, atsakyme nurodoma apdorojimo būsena **‘6581’**.

3.5.3.3 Komanda su nelyginiu komandos baitu

Pasinaudojus šiuo komandos variantu, IDF gali įrašyti duomenis į tam tikrą rinkmeną EF su ne mažiau kaip 32 768 baitais.

TCS_64 Jei tachografo kortelė yra tinkama rinkmenoms EF su ne mažiau kaip 32 768 baitų, ji turi būti tinkama ir šiam komandos variantui, naudojamam su tokiomis rinkmenomis EF. Kitų rinkmenų EF atžvilgiu tachografo kortelė gali būti arba nebūti tinkama šiam komandos variantui.

TCS_65 **Komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘00h’	
INS	1	‘D7h’	Atnaujinti dvejetainį
P1	1	‘00h’	Esamoji rinkmena EF
P2	1	‘00h’	
Lc	1	‘NNh’	Lc Duomenų ilgis komandos duomenų laukelyje
#6-#(5+NN)	NN	‘XX..XXh’	Paslinktųjų duomenų objektas, kurio žymena ‘54h’ || diskrečiųjų duomenų objektas, kurio žymena ‘53h’ ir kuriame yra rašytini duomenys

IFD užkoduoja paslinktųjų duomenų objekto ir diskrečiųjų duomenų objekto ilgį mažiausiu įmanomu oktetų skaičiumi, t. y. naudojant ilgio baitą ‘01h’ IFD užkoduoja poslinkį / ilgį nuo 0 iki 255 baitų, o naudojant ilgio baitą ‘02h’ – poslinkį / ilgį nuo 256 iki 65 535 baitų.

TCS_66 **Atsakymo pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
SW	2	‘XXXXh’	Būsenos žodžiai (SW1, SW2)

▼B

— Jei komanda sėkmingai įvykdoma, kortelė atsako ‘**9000**’.

— Jei nepasirinkta jokia EF, atsakyme nurodoma apdorojimo būsena **‘6986’**.

— Jei pasirinktos rinkmenos saugumo sąlygos neįvykdytos, nurodoma komandos vykdymo nutraukimo būsena ‘**6982**’.

— Jei poslinkis neatitinka rinkmenos EF dydžio (poslinkis > EF dydis), atsakyme nurodoma apdorojimo būsena **‘6B00’**.

— Jei rašytinų duomenų dydis neatitinka EF dydžio (poslinkis + Lc > EF dydis), atsakyme nurodoma apdorojimo būsena **‘6700’**.

— Jei rinkmenos atributuose randama nepažeistumo klaida, kortelė turi laikyti rinkmeną sugadinta ir neatkuriama, o atsakyme nurodoma apdorojimo būsena ‘**6400**’ arba ‘**6500**’.

— Jei rašyti nepavyksta, atsakyme nurodoma apdorojimo būsena **‘6581’**.

3.5.3.3.1 Komanda su saugiuoju keitimusi pranešimais (pavyzdys)

Šiame pavyzdyje paaiškinta, kaip naudojamas saugusis keitimasis pranešimais, jei taikoma saugumo sąlyga SM-MAC-G2.

TCS_67 Komandos pranešimas

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘0Ch’	Prašoma saugaus keitimosi pranešimais.
INS	1	‘D7h’	Atnaujinti dvejetainį
P1	1	‘00h’	Esamoji rinkmena EF
P2	1	‘00h’	
Lc	1	‘XXh’	Apsaugotų duomenų laukelio ilgis.
#6	1	‘B3h’	Paprastųjų verčių duomenų, užkoduotų objekte BER-TLV, žymena.
#7	L	‘NNh’ arba ‘81 NNh’	L_{PV}: perduodamų duomenų ilgis. Jei L_{PV}> 127 baitai, L yra 2 baitai.
#(7+L)-#(6+L+NN)	NN	‘XX..XXh’	Paprastieji duomenys, užkoduoti objekte BER-TLV, t. y. paslinktųjų duomenų objektas su žymena ‘54h’ || diskrečiųjų duomenų objektas, kurio žymena ‘53h’ ir kuriame yra rašytini duomenys
#(7+L+NN)	1	‘8Eh’	T_{CC}: kriptografinės kontrolinės sumos žymena.
#(8+L+NN)	1	‘XXh’	L_{CC}: kitos iš eilės kriptografinės kontrolinės sumos ilgis. ‘08h’, ‘0Ch’ arba ‘10h’ (priklauso nuo rakto AES ilgio) 2-osios kartos saugiajam keitimuisi pranešimais (žr. 11 priedėlio B dalį)
#(9+L+NN)-#(8+M+L+NN)	M	‘XX..XXh’	Kriptografinė kontrolinė suma.
Le	1	‘00h’	Kaip nurodyta ISO/IEC 7816-4.

▼B

TCS_68 Atsakymo pranešimas, jei komanda įvykdyta sėkmingai

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’	Neapsaugotojo atsakymo APDU apdorojimo būsena
#5	1	‘8Eh’	T_{CC}: kriptografinės kontrolinės sumos žymena.
#6	1	‘XXh’	L_{CC}: kitos iš eilės kriptografinės kontrolinės sumos ilgis. ‘08h’, ‘0Ch’ arba ‘10h’ (priklauso nuo rakto AES ilgio) 2-osios kartos saugiajam keitimuisi pranešimais (žr. 11 priedėlio B dalį)
#7-#(6+L)	L	‘XX..XXh’	Kriptografinė kontrolinė suma.
SW	2	‘XXXXh’	Būsenos žodžiai (SW1, SW2)

3.5.4 *GET_CHALLENGE*

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_69 Kortelės duodamas slaptažodis galioja tik kitai į kortelę siunčiamai komandai, kuri tą slaptažodį panaudoja.

TCS_70 **Komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘00h’	
INS	1	‘84h’	INS
P1	1	‘00h’	P1
P2	1	‘00h’	P2
Le	1	‘08h’	Le (laukiamas slaptažodžio ilgis).

TCS_71 **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 būsena yra **‘6700’**.

— Jei parametrai P1-P2 neteisingi, apdorojimo būsena yra **‘6A86’**.

▼B

3.5.5 *VERIFY*

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

Tik dirbtuvių kortelė turi būti tinkama šiai komandai.

Kitų rūšių tachografo kortelėms ši komanda gali būti arba nebūti įdiegta, tačiau šioms kortelėms nepritaikomas joks standartinis CHV. Todėl tokios kortelės negali įvykdyti šios komandos. Kitų rūšių nei dirbtuvių tachografo kortelių reagavimas, t. y. klaidos kodas atsakyme, nėra šios specifikacijos dalykas, jei tokia komanda siunčiama.

Komanda VERIFY nurodo kortelėje sulyginti atsiųstus CHV (PIN) duomenis su kortelės atmintyje laikomu standartiniu CHV.

TCS_72 Naudotojo įvestą ASCI koduotės PIN sąsajos įtaisas turi papildyti dešinėje prirašydamas iki 8 ‘FFh’ baitų; taip pat žr. 1 priedėlyje duomenų tipą WorkshopCardPIN.

TCS_73 1-osios ir 2-osios kartos tachografo programos naudoja tokį patį CHV.

TCS_74 Tachografo kortelė tikrina, ar komanda užkoduota teisingai. Jei komanda užkoduota neteisingai, kortelė nelygina CHV verčių, nesumažina likusių CHV mėginimų skaitiklio rodmens ir neatstato apsaugos būsenos PIN_Verified, o nutraukia komandos vykdymą. Komanda užkoduota teisingai, jei baitai CLA, INS, P1, P2, Lc turi vertes, kokios nustatytos, Le nėra, o komandos duomenų laukelis yra teisingo ilgio.

TCS_75 Jei komanda yra sėkmingai įvykdoma, likusių CHV mėginimų skaitiklis paleidžiamas iš naujo. Likusių CHV mėginimų skaitiklio pradinė vertė yra 5. Jei komanda sėkmingai įvykdoma, kortelė nustato vidinės apsaugos būseną PIN_Verified. Kortelė atkuria pradinę apsaugos būseną, jei atkuriama kortelės pradinė būsena arba jei kodas CHV, kurį perdavė komanda, nesutampa su laikomu standartiniu kodu CHV.

Pastaba. Kai naudojamas tas pats standartinis kodas CHV ir taikoma bendroji apsaugos būsena, dirbtuvių darbininkui po kitos tachografo programos rinkmenos DF pasirinkimo nereikia dar kartą įvesti PIN kodo.

TCS_76 Jei sulyginimas nepavyksta, jis registruojamas kortelėje, t. y. likusių kodo CHV mėginimų skaitiklio vertė sumažėja vienetu, kad būtų apribotas papildomų mėginimų panaudoti standartinį kodą CHV skaičius.

TCS_77 **Komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘00h’	
INS	1	‘20h’	INS
P1	1	‘00h’	P1

▼B

Baitas	Ilgis	Vertė	Aprašymas
P2	1	‘00h’	P2 (patikrintas kodas CHV žinomas netiesiogiai)
Lc	1	‘08h’	Persiųsto CHV kodo ilgis.
#6-#13	8	‘XX..XXh’	CHV –

TCS_78 **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 būsena **‘6A88’**.

— Jei CHV užblokuotas (likusių mėginimų skaitiklio vertė lygi nuliui), atsakyme nurodoma apdorojimo būsena **‘6983’**. Esant šiai būsenai CHV daugiau nebegalima pateikti.

— Jei sulyginimas nepavyksta, likusių mėginimų skaitiklio vertė sumažėja, o atsakyme nurodoma būsena **‘63CX’** (X > 0, o X reiškia likusių CHV mėginimų skaitiklio vertę.

— Jei standartinis CHV laikomas sugadintu, atsakyme nurodoma apdorojimo būsena **‘6400’** arba **‘6581’**.

— Jei Lc yra ne ‘08h’, apdorojimo būsena yra **‘6700’**.

3.5.6 *GET_RESPONSE*

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 (atvejis, kai komandoje yra tiek Lc, tiek Le).

Komanda GET RESPONSE turi būti duodama iškart po duomenis paruošiančios komandos, priešingu atveju duomenys prarandami. Įvykdžius komandą GET RESPONSE (išskyrus atvejus, kai įvyksta klaida ‘**61xx**’ arba ‘**6Cxx**’, žr. toliau), pirmiau paruošti duomenys tampa nebeprieinami.

TCS_79 **Komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘00h’	
INS	1	‘C0h’	
P1	1	‘00h’	
P2	1	‘00h’	
Le	1	‘XXh’	Laukiamas baitų skaičius.

▼B

TCS_80 **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 būsena **‘6900’** arba **‘6F00’**.

— Jei Le viršija galimų baitų skaičių arba lygus nuliui, atsakyme nurodoma apdorojimo būsena **‘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 būsena **‘61xx’** (čia xx nurodo dar galimų panaudoti su kita komanda GET RESPONSE baitų skaičių).

— Jei komanda netinkama (protokolas T=1), kortelė atsako **‘6D00’**.

3.5.7 *PSO: VERIFY_CERTIFICATE*

Ši komanda atitinka ISO/IEC 7816-8, tačiau jos naudojimas, palyginti su standarte nustatyta komanda, yra labiau apribotas.

Komandą VERIFY_CERTIFICATE kortelė naudoja viešajam raktui iš išorės gauti ir jo galiojimui patikrinti.

3.5.7.1 1-osios kartos komanda. Atsakymo į komandą pora

TCS_81 Tik pirmosios kartos tachografo programa yra tinkama šiam komandos variantui.

TCS_82 Kai komanda VERIFY_CERTIFICATE yra sėkmingai įvykdoma, viešasis raktas įrašomas į atmintį būsimam panaudojimui apsaugos aplinkoje. Šis raktas, naudojant jo rakto identifikatorių, komanda MSE (žr. 3.5.11punktą) turi būti aiškiai nustatytas naudoti su apsaugos komandomis (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE arba VERIFY CERTIFICATE).

TCS_83 Bet kuriuo atveju pažymėjimui atidaryti komanda VERIFY_CERTIFICATE naudoja viešąjį raktą, kurį anksčiau parinko komanda MSE. Šis viešasis raktas turi būti valstybės narės arba Europos.

TCS_84 **Komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘00h’	
INS	1	‘2Ah’	Atlikti apsaugos operaciją.
P1	1	‘00h’	P1

▼B

Baitas	Ilgis	Vertė	Aprašymas
P2	1	‘AEh’	P2: ne pagal BER-TLV užkoduoti duomenys (duomenų elementų junginys).
Lc	1	‘C2h’	Lc: pažymėjimo ilgis, 194 baitai.
#6-#199	194	‘XX..XXh’	Pažymėjimas: duomenų elementų junginys (kaip aprašyta 11 priedėlyje).

TCS_85 **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 būsena **‘6688’**. 1-osios ir 2-osios kartos pažymėjimo tikrinimo ir išnagrinėjimo procesas aprašytas 11 priedėlyje.

— Jei apsaugos aplinkoje nėra viešojo rakto, atsakyme nurodoma apdorojimo būsena **‘6A88’**.

— Jei pasirinktas viešasis raktas (naudotas pažymėjimui išnagrinėti) laikomas sugadintu, atsakyme nurodoma apdorojimo būsena **‘6400’** arba **‘6581’**.

— Tik 1-ajai kartai. Jei pasirinkto viešojo rakto (naudoto pažymėjimui išnagrinėti) CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) yra ne ‘00’ (t. y. jis yra ne valstybės narės ir ne europinis), atsakyme nurodoma apdorojimo būsena **‘6985’**.

3.5.7.2 2-osios kartos komanda. Atsakymo į komandą pora

Priklausomai nuo ECC kreivės dydžio pažymėjimai gali būti tokio ilgio, kad jų neįmanoma perduoti vienu APDU. Tokiu atveju pagal ISO/IEC 7816-4 turi būti sudaromos komandų grandinės, o pažymėjimas perduodamas dviem PSO: Verify Certificate APDU iš eilės.

Pažymėjimo struktūra ir srities parametrai apibrėžti 11 priedėlyje.

TCS_86 Komandą galima įvykdyti rinkmenose MF, DF Tachograph ir DF Tachograph_G2, taip pat žr. TCS_33.

TCS_87 **Komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘X0h’	CLA baitas, kuriuo žymimas komandos jungimas: ‘00h’ – vienintelė arba paskutinė sekos komanda, ‘10h’ – nepaskutinė sekos komanda
INS	1	‘2Ah’	Atlikti apsaugos operaciją.
P1	1	‘00h’	
P2	1	‘BEh’	Patikrinti save apibūdinantįjį pažymėjimą

▼B

Baitas	Ilgis	Vertė	Aprašymas
Lc	1	‘XXh’	Komandos duomenų laukelio ilgis, žr. TCS_88 ir TCS_89.
#6-#5+L	L	‘XX..XXh’	Pagal DER-TLV užkoduoti duomenys: pirmas duomenų objektas ECC Certificate Body, sujungtas su antru duomenų objektu ECC Certificate Signature, arba šio junginio dalis. Žymena ‘7F21’ ir atitinkamas ilgis neperduodami. Šių duomenų objektų eilės tvarka pastovi.

TCS_88 Jei APDU trumpieji, taikomos šios sąlygos: IFD naudoja mažiausią APDU kiekį, būtiną komandos turiniui perduoti, ir perduoda maksimalų baitų kiekį pirmosios komandos APDU pagal Information Field Size Card Byte vertę (žr. TCS_14). Jei IFD veikia kitaip, kortelės veikimas nenagrinėjamas.

TCS_89 Jei APDU didesnio ilgio, taikomos šios sąlygos: jei pažymėjimas netelpa viename APDU, kortelė turi būti tinkama komandų jungimui. IFD naudoja mažiausią APDU kiekį, būtiną komandos turiniui perduoti, ir perduoda maksimalų baitų skaičių pirmosios komandos APDU. Jei IFD veikia kitaip, kortelės veikimas nenagrinėjamas.

Pastaba. Pagal 11 priedėlį kortelėje laikomas pažymėjimas arba atitinkamas pažymėjimo turinys ir atnaujinamas jos currentAuthenticatedTime.

Atsakymo pranešimo struktūra ir būsenos žodžiai tokie, kokie nustatyti TCS_85.

TCS_90 Be TCS_85 išvardytų klaidos kodų, kortelės atsakyme gali būti šie klaidos kodai:

— Jei pasirinkto viešojo rakto (naudoto pažymėjimui išnagrinėti) CHA.LSB (CertificateHolderAuthorisation.equipmentType) netinkamas pažymėjimo tikrinimui pagal 11 priedėlį, atsakyme nurodoma apdorojimo būsena ‘**6985**’.

— Jei kortelės currentAuthenticatedTime vėlesnis už Certificate Expiration Date, atsakyme nurodoma apdorojimo būsena ‘**6985**’

— Jei laukiama sekos paskutinės komandos, kortelė atsako ‘**6883**’.

— Jei komandos duomenų laukelyje išsiunčiami neteisingi parametrai, kortelės atsakyme nurodoma ‘**6A80**’ (tas pats kodas naudojamas, kai duomenų objektai siunčiami ne nustatyta eilės tvarka).

▼B

3.5.8 *INTERNAL_AUTHENTICATE*

Ši komanda atitinka ISO/IEC 7816-4.

TCS_91 Visos tachografo kortelės turi būti tinkamos šiai komandai rinkmenoje DF Tachograph generation 1. Komanda gali būti arba nebūti prieinama rinkmenoje MF ir (arba) rinkmenoje DF Tachograph_G2. Jei komanda prieinama, jos vykdymas baigiamas atitinkamu klaidos kodu, nes kortelės privatusis raktas (Card.SK), skirtas 1-osios kartos autentiškumo tikrinimo protokolui, prieinamas tik rinkmenoje DF_Tachograph generation 1.

Naudodamasis komanda INTERNAL_AUTHENTICATE sąsajos įtaisas gali patikrinti kortelės autentiškumą. Autentiškumo tikrinimo procesas aprašytas 11 priedėlyje. Jį sudaro tokios instrukcijos:

TCS_92 Autentiškumo tikrinimo duomenims, įskaitant K1 (pirmasis seanso rakto sutarties elementas) ir RND1, pasirašyti komanda INTERNAL_AUTHENTICATE naudoja kortelės privatųjį raktą (netiesiogiai pasirinktą), o parašui šifruoti ir autentiškumo tikrinimo leksemai suformuoti – esamu metu pasirinktą viešąjį raktą (naudodamasi komanda MSE) (išsamiau aprašyta 11 priedėlyje).

TCS_93 **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’	Į 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_94 **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 viešojo rakto, atsakyme nurodoma apdorojimo būsena **‘6A88’**.

— Jei apsaugos aplinkoje nėra privačiojo rakto, atsakyme nurodoma apdorojimo būsena **‘6A88’**.

— Jei VU.CHR neatitinka esamo viešojo rakto identifikatoriaus, atsakyme nurodoma apdorojimo būsena **‘6A88’**.

▼B

— Jei pasirinktas privatusis raktas laikomas sugadintu, atsakyme nurodoma apdorojimo būsena **‘6400’** arba **‘6581’**.

TCS_95 Jei komanda INTERNAL AUTHENTICATE yra sėkmingai įvykdoma, esamas seanso raktas (jei yra) yra ištrinamas ir daugiau nenaudojamas. Tam, kad galima būtų gauti naują seanso raktą, reikia sėkmingai įvykdyti 1-osios kartos autentiškumo tikrinimo mechanizmo komandą EXTERNAL AUTHENTICATE.

3.5.9 *EXTERNAL_AUTHENTICATE*

Ši komanda atitinka ISO/IEC 7816-4.

Naudodamasi komanda EXTERNAL_AUTHENTICATE kortelė gali patikrinti IFD autentiškumą. 1-osios ir 2-osios kartos tachografų autentiškumo tikrinimo procesas aprašytas 11 priedėlyje („Transporto priemonės bloko autentiškumo tikrinimas“).

TCS_96 Tik 1-osios kartos tachografo programa yra tinkama 1-osios kartos abipusio autentiškumo tikrinimo mechanizmo komandos variantui.

TCS_97 2-osios kartos transporto priemonės bloko kortelės abipusio autentiškumo tikrinimo komandos variantą galima įvykdyti rinkmenose MF, DF Tachograph ir DF Tachograph_G2, taip pat žr. TCS_34.

TCS_98 **Komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘00h’	CLA
INS	1	‘82h’	INS
P1	1	‘00h’	Raktai ir algoritmai žinomi netiesiogiai.
P2	1	‘00h’	
Lc	1	‘XXh’	Lc (į kortelę nusiųstų duomenų ilgis).
#6-#(5+L)	L	‘XX..XXh’	1-osios kartos autentiškumo tikrinimas. Kriptograma (žr. 11 priedėlio A dalį). 2-osios kartos autentiškumo tikrinimas. IFD sugeneruotas parašas (žr. 11 priedėlio B dalį).

TCS_99 **Atsakymo pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
SW	2	‘XXXXh’	Būsenos žodžiai (SW1, SW2)

— Jei komanda sėkmingai įvykdoma, kortelė atsako ‘**9000**’.

— Jei esamo viešojo rakto CHA nėra tachografo programos AID ir transporto priemonės bloko įrangos tipo junginys, atsakyme nurodoma apdorojimo būsena **‘6F00’**.

— Jei prieš komandą nėra komandos GET CHALLENGE, atsakyme nurodoma apdorojimo būsena **‘6985’**.

▼B

1-osios kartos tachografo programos atsakymuose gali būti papildomų klaidos kodų.

— Jei apsaugos aplinkoje nėra viešojo rakto, atsakyme nurodoma apdorojimo būsena **‘6A88’**.

— Jei apsaugos aplinkoje nėra privačiojo rakto, atsakyme nurodoma apdorojimo būsena **‘6A88’**.

— Jei kriptogramos patikrinimas neteisingas, atsakyme nurodoma apdorojimo būsena **‘6688’**.

— Jei pasirinktas privatusis raktas laikomas sugadintu, atsakyme nurodoma apdorojimo būsena **‘6400’** arba **‘6581’**.

2-osios kartos autentiškumo tikrinimo komandos varianto atsakymuose gali būti šis papildomas klaidos kodas:

— jei parašo patikrinti nepavyko, kortelė atsako ‘**6300**’.

3.5.10 *GENERAL AUTHENTICATE*

Ši komanda naudojama 2-osios kartos lusto autentiškumo tikrinimo protokole, nustatytame 11 priedėlio B dalyje, ir atitinka standartą ISO/IEC 7816-4.

TCS_100 Komandos variantą galima įvykdyti rinkmenose MF, DF Tachograph ir DF Tachograph_G2, taip pat žr. TCS_34.

TCS_101 **Komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘00h’	
INS	1	‘86h’	
P1	1	‘00h’	Raktai ir protokolas žinomi netiesiogiai.
P2	1	‘00h’	
Lc	1	‘NNh’	Lc: kito duomenų laukelio ilgis.
#6-#(5+L)	L	‘7Ch’ + L_{7C} + ‘80h’ + L_{80} + ‘XX..XXh’	Pagal DER-TLV užkoduoto trumpalaikio viešojo rakto vertė (žr. 11 priedėlį) Transporto priemonės blokas turi siųsti duomenų objektus šia tvarka.

TCS_102 **Atsakymo pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
#1-#L	L	‘7Ch’ + L_{7C} + ‘81h’ + ‘08h’ + ‘XX..XXh’ + ‘82h’ + L_{82} + ‘XX..XXh’	Pagal DER-TLV užkoduoti dinaminio autentiškumo tikrinimo duomenys: laikinoji vertė ir autentiškumo tikrinimo leksema (žr. 11 priedėlį).
SW	2	‘XXXXh’	Būsenos žodžiai (SW1, SW2)

— Jei komanda sėkmingai įvykdoma, kortelė atsako ‘**9000**’.

— Kortelės atsakyme ‘**6A80**’ reiškia, kad parametrai duomenų laukelyje neteisingi.

▼B

— Kortelės atsakyme ‘**6982**’, jei komanda External Authenticate neįvykdyta sėkmingai.

Atsakymo Dynamic Authentication Data objektas ‘7Ch’

— turi būti pateiktas, jei veiksmo rezultatas teigiamas, t. y. būsenos žodžiai yra ‘**9000**’,

— turi būti nepateiktas, jei įvyko vykdymo arba tikrinimo klaida, t. y. jei būsenos žodžių intervalas ‘**6400**’ – ‘**6FFF**’, ir

— gali būti nepateiktas, jei duotas įspėjimas, t. y. jei būsenos žodžių intervalas ‘**6200**’ – ‘**63FF**’.

3.5.11 *MANAGE SECURITY ENVIRONMENT*

Ši komanda skirta autentiškumo tikrinimo viešajam raktui nustatyti.

3.5.11.1 1-osios kartos komanda. Atsakymo į komandą pora

Ši komanda atitinka ISO/IEC 7816-4. Šios komandos naudojimas apribotas pagal atitinkamą standartą.

TCS_103 Tik 1-osios kartos tachografo programa yra tinkama šiai komandai.

TCS_104 MSE duomenų laukelyje nurodytas raktas lieka esamuoju viešuoju raktu iki kitos teisingos MSE komandos, rinkmenos DF pasirinkimo arba kortelės pradinės būsenos atkūrimo.

TCS_105 Jei nurodyto rakto kortelėje (jau) nėra, apsaugos aplinka lieka nepakitusi.

TCS_106 **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 parašą).
Lc	1	‘0Ah’	Lc: kito duomenų laukelio ilgis.
#6	1	‘83h’	Viešojo rakto nurodymo žymena asimetriškais atvejais.
#7	1	‘08h’	Rakto nuorodos (rakto identifikatoriaus) ilgis.
#8-#15	8	‘XX..XXh’	Rakto identifikatorius (žr. 11 priedėlį).

TCS_107 **Atsakymo pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
SW	2	‘XXXXh’	Būsenos žodžiai (SW1, SW2)

▼B

— Jei komanda sėkmingai įvykdoma, kortelė atsako ‘**9000**’.

— Jei kortelėje nėra nurodyto rakto, atsakyme nurodoma apdorojimo būsena **‘6A88’**.

— Jei saugaus keitimosi pranešimais formatu nėra kai kurių lauktų duomenų objektų, atsakyme nurodoma apdorojimo būsena **‘6987’**. Taip gali įvykti, jei nėra žymenos ‘83h’.

— Jei kai kurie duomenų objektai yra neteisingi, atsakyme nurodoma apdorojimo būsena **‘6988’**. Taip gali įvykti, jei rakto identifikatoriaus ilgis yra ne ‘08h’.

— Jei pasirinktas atvirasis raktas laikomas sugadintu, atsakyme nurodoma apdorojimo būsena **‘6400’** arba **‘6581’**.

3.5.11.2 2-osios kartos komanda. Atsakymo į komandą poros

2-osios kartos autentiškumo tikrinimo tachografo kortelė yra tinkama šioms komandos MSE: Set versijoms, atitinkančioms standartą ISO/IEC 7816-4. Šios komandos versijos netinka 1-osios kartos autentiškumo tikrinimui.

3.5.11.2.1 MSE:SET AT lusto autentiškumo tikrinimui

Naudojantis šia komanda MSE:SET AT išrenkami lusto autentiškumo tikrinimo parametrai, o tikrinimas paskui atliekamas komanda General Authenticate.

TCS_108 Komandos variantą galima įvykdyti rinkmenose MF, DF Tachograph ir DF Tachograph_G2, taip pat žr. TCS_34.

TCS_109 **MSE:SET AT komandos pranešimas lusto autentiškumui tikrinti**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘41h’	Vidinio autentiškumo tikrinimo nustatymas
P2	1	‘A4h’	Autentiškumo tikrinimas
Lc	1	‘NNh’	Lc: kito duomenų laukelio ilgis.
#6-#(5+L)	L	‘80h’ + ‘0Ah’ + ‘XX..XXh’	Pagal DER-TLV užkoduota kriptografinio mechanizmo nuoroda: Chip Authentication objekto identifikatorius (tik vertė, žymena ‘06h’ praleidžiama). Objekto identifikatorių vertes žr. 1 priedėlyje; vartojama baitinė išraiška. Žr. 11 priedėlyje paaiškinimą, kaip pasirinkti vieną iš šių objekto identifikatorių.

3.5.11.2.2 MSE:SET AT transporto priemonės bloko autentiškumo tikrinimui

Naudojantis šia komanda MSE:SET AT išrenkami transporto priemonės bloko autentiškumo tikrinimo parametrai ir raktai, o tikrinimas paskui atliekamas komanda External Authenticate.

▼B

TCS_110 Komandos variantą galima įvykdyti rinkmenose MF, DF Tachograph ir DF Tachograph_G2, taip pat žr. TCS_34.

TCS_111 **MSE:SET AT komandos pranešimas transporto priemonės bloko autentiškumui tikrinti**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Išorinio autentiškumo tikrinimo nustatymas
P2	1	‘A4h’	Autentiškumo tikrinimas
Lc	1	‘NNh’	Lc: kito duomenų laukelio ilgis.
#6-#(5+L)	L	‘80h’ + ‘0Ah’ + ‘XX..XXh’	Pagal DER-TLV užkoduota kriptografinio mechanizmo nuoroda: VU Authentication objekto identifikatorius (tik vertė, žymena ‘06h’ praleidžiama). Objekto identifikatorių vertes žr. 1 priedėlyje; vartojama baitinė išraiška. Žr. 11 priedėlyje paaiškinimą, kaip pasirinkti vieną iš šių objekto identifikatorių.
		‘83h’ + ‘08h’ + ‘XX..XXh’	Pagal DER-TLV užkoduota nuoroda į transporto priemonės bloko viešąjį raktą per pažymėjimo turėtojo nuorodą, įrašytą pažymėjime.
		‘91h’ + L_{91} + ‘XX..XXh’	Pagal DER-TLV užkoduotas transporto priemonės bloko trumpalaikio viešojo rakto suglaudintas atvaizdis, kuris bus naudojamas lusto autentiškumo patikrinimui (žr. 11 priedą).

3.5.11.2.3 MSE:SET DST

Naudojantis šia komanda MSE:SET DST nustatomas viešasis raktas arba:

— tikrinamas parašas, kurį pateikia komanda PSO: Verify Digital Signature, arba

— tikrinamas parašas pažymėjime, kurį pateikia komanda PSO: Verify Certificate.

TCS_112 Komandą galima įvykdyti rinkmenose MF, DF Tachograph ir DF Tachograph_G2, taip pat žr. TCS_33.

TCS_113 **MSE:SET DST komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Tikrinimo nustatymas
P2	1	‘B6h’	Skaitmeninis parašas

▼B

Lc	1	‘NNh’	Lc: kito duomenų laukelio ilgis.
#6-#(5+L)	L	‘83h’ + ‘08h’ + ‘XX...XXh’	Pagal DER-TLV užkoduotas viešasis raktas, t. y. viešojo rakto pažymėjimo Certificate Holder Reference (žr. 11 priedėlį)

Visų komandos versijų atsakymo pranešimų struktūra ir būsenos žodžiai nurodomi taip:

TCS_114 **Atsakymo pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
SW	2	‘XXXXh’	Būsenos žodžiai (SW1, SW2)

— Jei komanda sėkmingai įvykdoma, kortelė atsako ‘**9000**’. Protokolas pasirinktas ir inicijuotas

— **‘6A80’** reiškia, kad parametrai komandos duomenų laukelyje neteisingi.

— **‘6A88’** reiškia, kad nurodytų duomenų (t. y. nurodyto rakto) nėra.

3.5.12 *PSO: HASH*

Ši komanda naudojama kai kurių duomenų maišos skaičiavimo rezultatams perkelti į kortelę. Ji naudojama skaitmeniniams parašams tikrinti. Maišos vertė saugoma laikinai kitai komandai PSO: Verify Digital Signature

Ši komanda atitinka ISO/IEC 7816-8. Šios komandos naudojimas apribotas pagal atitinkamą standartą.

Reikalaujama, kad tik kontrolės kortelė būtų tinkama šiai komandai rinkmenose DF Tachograph ir DF Tachograph_G2.

Kitų rūšių tachografo kortelėms ši komanda gali būti arba nebūti įdiegta. Komanda gali būti arba nebūti prieinama rinkmenoje MF.

Kontrolės kortelės 1-osios kartos programa tinkama tik algoritmui SHA-1.

TCS_115 Laikinai saugoma maišos vertė turi būti panaikinama, jei naudojantis komanda PSO: HASH apskaičiuojama nauja maišos vertė, jei pasirenkama rinkmena DF ir jei atkuriama tachografo kortelės pradinė būsena.

TCS_116 **Komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Atlikti apsaugos operaciją.
P1	1	‘90h’	Grąžinti maišos kodą.

▼B

Baitas	Ilgis	Vertė	Aprašymas
P2	1	‘A0h’	Žymena: duomenų laukelyje yra maišai reikalingi DO.
Lc	1	‘XXh’	Kito duomenų laukelio ilgis Lc.
#6	1	‘90h’	Maišos kodo žymena.
#7	1	‘XXh’	Maišos kodo ilgis L: ‘04h’ – 1-osios kartos programoje (žr. 11 priedėlio A dalį), ‘20h’, ‘30h’ arba ‘40h’ – 2-osios kartos programoje (žr. 11 priedėlio B dalį).
#8-#(7+L)	L	‘XX..XXh’	Maišos kodas.

TCS_117 **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 būsena **‘6987’**. Taip gali įvykti, jei nėra žymenos ‘90h’.

— Jei kai kurie duomenų objektai yra neteisingi, atsakyme nurodoma apdorojimo būsena **‘6988’**. Ši klaida įvyksta, jei būtina žymena yra, tačiau jos ilgis yra kitos nei ‘14h’ algoritmui SHA-1, ‘20h’ – SHA-256, ‘30h’ – SHA-384, ‘40h’ – SHA-512 (2-osios kartos programa).

3.5.13 *PERFORM HASH of FILE*

Ši komanda neatitinka ISO/IEC 7816-8. Taigi šios komandos baitas CLA rodo, kad PERFORM SECURITY OPERATION / HASH naudojimas yra nuosavybinis.

Reikalaujama, kad tik vairuotojo ir dirbtuvių kortelės būtų tinkamos šiai komandai rinkmenose DF Tachograph ir DF Tachograph_G2.

Kitų rūšių tachografo kortelėms ši komanda gali būti arba nebūti įdiegta. Jei įmonės arba kontrolės kortelei įdiegta ši komanda, komanda turi būti vykdoma, kaip nustatyta šiame skyriuje.

Komanda gali būti arba nebūti prieinama rinkmenoje MF. Jei komanda įdiegta, ji turi būti įdiegta, kaip nustatyta šiame skyriuje, t. y. ja negalima apskaičiuoti maišos vertės, o jos vykdymas baigiamas atitinkamu klaidos kodu.

TCS_118 Komanda PERFORM HASH of FILE naudojama esamu metu pasirinktos rinkmenos EF duomenų srities maišai atlikti.

TCS_119 Tachografo kortelė tinkama šiai komandai tik su tomis rinkmenomis EF, kurios išvardytos 4 skyriaus DF_Tachograph ir DF_Tachograph_G2; taip pat daroma ši išimtis: Tachografo kortelė netinkama komandai su rinkmena EF Sensor_Installation_Data of DF Tachograph_G2.

▼B

TCS_120 Maišos operacijos rezultatas laikinai įrašomas į kortelės atmintį. Tuomet jį galima panaudoti rinkmenos skaitmeniniam parašui gauti naudojant komandą PSO: COMPUTE DIGITAL SIGNATURE.

TCS_121 Laikinai saugoma rinkmenos maišos vertė turi būti panaikinama, jei naudojantis komanda PSO: Hash of File apskaičiuojama nauja rinkmenos maišos vertė, jei pasirenkama rinkmena DF ir jei atkuriama tachografo kortelės pradinė būsena.

TCS_122 1-osios kartos tachografo programa tinkama algoritmui SHA-1.

TCS_123 2-osios kartos tachografo programa tinkama algoritmams SHA-1 ir SHA-2 (256, 384 ir 512 bitų).

TCS_124 **Komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	80h	CLA
INS	1	‘2Ah’	Atlikti apsaugos operaciją.
P1	1	‘90h’	Žymena: Hash
P2	1	‘XXh’	P2: rodo, kurį algoritmą naudoti esamu metu pasirinktos atvirosios rinkmenos duomenų maišai: ‘00h’ – SHA-1 ‘01h’ – SHA-256 ‘02h’ – SHA-384 ‘03h’ – SHA-512

TCS_125 **Atsakymo pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
SW	2	‘XXXXh’	Būsenos žodžiai (SW1, SW2)

— Jei komanda sėkmingai įvykdoma, kortelė atsako ‘**9000**’.

— Jei dabartinėje rinkmenoje EF negalima įvykdyti komandos (EF Sensor_Installation_Data rinkmenoje DF Tachograph_G2), atsakyme nurodoma apdorojimo būsena **‘6985’**.

— Jei pasirinkta EF laikoma sugadinta (yra rinkmenos atributų arba laikomų duomenų nepažeistumo klaidų), atsakyme nurodoma apdorojimo būsena ‘**6400**’ arba **‘6581’**.

— Jei pasirinkta rinkmena nėra atviroji arba jei dabartinės rinkmenos EF nėra, atsakyme nurodoma apdorojimo būsena ‘**6986**’.

3.5.14 *PSO: COMPUTE DIGITAL SIGNATURE*

Ši komanda naudojama anksčiau apskaičiuoto maišos kodo (žr. 3.5.13 punktą PERFORM HASH of FILE) skaitmeniniam parašui apskaičiuoti.

Reikalaujama, kad tik vairuotojo ir dirbtuvių kortelės būtų tinkamos šiai komandai rinkmenose DF Tachograph ir DF Tachograph_G2.

▼B

Kitų rūšių tachografo kortelėms ši komanda gali būti arba nebūti įdiegta, tačiau jos neturi turėti parašo rakto. Todėl su šiomis kortelėmis neįmanoma įvykdyti komandos, o jos vykdymas baigiasi tinkamu klaidos kodu.

Komanda gali būti arba nebūti prieinama rinkmenoje MF. Jei ji prieinama, jos vykdymas baigiasi tinkamu klaidos kodu.

Ši komanda atitinka ISO/IEC 7816-8. Šios komandos naudojimas apribotas pagal atitinkamą standartą.

TCS_126 Ši komanda neapskaičiuoja maišos kodo, anksčiau apskaičiuoto naudojant komandą PSO: HASH command, skaitmeninio parašo.

TCS_127 Kortelės privatusis raktas naudojamas skaitmeniniam parašui apskaičiuoti ir yra netiesiogiai žinomas kortelei.

TCS_128 1-osios kartos tachografo programa sudaro skaitmeninį parašą naudodama išplėtimo metodą, kuris atitinka PKCS1 (išsamiau skaitykite 11 priedėlyje).

TCS_129 2-osios kartos tachografo programa apskaičiuoja elipsine kreive grindžiamą skaitmeninį parašą (daugiau žr. 11 priedėlyje).

TCS_130 **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	‘NNh’	Laukiamo parašo ilgis.

TCS_131 **Atsakymo pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
#1-#L	L	‘XX..XXh’	Anksčiau apskaičiuotos maišos parašas.
SW	2	‘XXXXh’	Būsenos žodžiai (SW1, SW2)

— Jei komanda sėkmingai įvykdoma, kortelė atsako ‘**9000**’.

— Jei netiesiogiai pasirinktas privatusis raktas laikomas sugadintu, atsakyme nurodoma apdorojimo būsena ‘**6400**’ arba ‘**6581**’.

— Jei maišos, gautos įvykdžius ankstesnę komandą Perform Hash of File, nėra, atsakyme nurodoma apdorojimo būsena **‘6985’**.

▼B

3.5.15 *PSO: VERIFY_DIGITAL_SIGNATURE*

Ši komanda naudojama skaitmeniniam parašui, pateikiamam kaip įvestis, kurio maiša kortelei yra žinoma, patikrinti. Parašo algoritmas kortelei žinomas netiesiogiai.

Ši komanda atitinka ISO/IEC 7816-8. Šios komandos naudojimas apribotas pagal atitinkamą standartą.

Reikalaujama, kad tik kontrolės kortelė būtų tinkama šiai komandai rinkmenose DF Tachograph ir DF Tachograph_G2.

Kitų rūšių tachografo kortelėms ši komanda gali būti arba nebūti įdiegta. Komanda gali būti arba nebūti prieinama rinkmenoje MF.

TCS_132 Komanda VERIFY DIGITAL SIGNATURE visuomet naudoja viešąjį raktą, kurį pasirinko ankstesnė komanda Manage Security Environment MSE: Set DST, ir ankstesnį maišos kodą, kurį įvedė komanda PSO: HASH.

TCS_133 **Komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Atlikti apsaugos operaciją.
P1	1	‘00h’	
P2	1	‘A8h’	Žymena: duomenų laukelyje yra tikrinimui reikalingi DO.
Lc	1	‘83h’	Kito duomenų laukelio ilgis Lc.
6	1	‘9Eh’	Skaitmeninio parašo žymena.
#7-#8	2	‘81 XXh’	Skaitmeninio parašo ilgis: 1-osios kartos tachografo programai – 128 baitai užkoduoti pagal 11 priedėlio A dalį, 2-osios kartos tachografo programai – priklausomai nuo pasirinktos kreivės (žr. 11 priedėlio B dalį).
#9-#(8+L)	L	‘XX..XXh’	Skaitmeninio parašo turinys.

TCS_134 **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 būsena **‘6688’**. Tikrinimo procesas aprašytas 11 priedėlyje.

— Jei nepasirinktas joks viešasis raktas, atsakyme nurodoma apdorojimo būsena **‘6A88’**.

— Jei nėra kai kurių lauktų duomenų objektų (kaip nurodyta pirmiau), atsakyme nurodoma apdorojimo būsena **‘6987’**. Taip gali įvykti, jei nėra vienos iš reikalingų žymenų.

▼B

— Jei komandai apdoroti nėra maišos kodo (dėl ankstesnės komandos PSO: Hash), atsakyme nurodoma apdorojimo būsena **‘6985’**.

— Jei kai kurie duomenų objektai yra neteisingi, atsakyme nurodoma apdorojimo būsena **‘6988’**. Ši klaida įvyksta, jei vieno iš reikiamų duomenų objektų ilgis yra neteisingas.

— Jei pasirinktas viešasis raktas laikomas sugadintu, atsakyme nurodoma apdorojimo būsena **‘6400’** arba **‘6581’**.

3.5.16 *PROCESS DSRC MESSAGE*

Naudojantis šia komanda tikrinamas DSRC pranešimo nepažeistumas ir autentiškumas, taip pat iššifruojami duomenys, kurie kontrolės institucijai arba dirbtuvėms perduodami DSRC saitu. Kortelė šifravimo raktą ir raktą MAC, kuriuo apsaugomas DSRC pranešimas, gauna taip, kaip nustatyta 11 priedėlio B dalies 13 skyriuje.

Reikalaujama, kad tik kontrolės kortelė ir dirbtuvių kortelė būtų tinkamos šiai komandai rinkmenose DF Tachograph ir DF Tachograph_G2.

Kitų rūšių tachografo kortelėms ši komanda gali būti arba nebūti įdiegta, tačiau jos neturi turėti DSRC pagrindinio rakto. Todėl su šiomis kortelėmis neįmanoma įvykdyti komandos, o jos vykdymas baigiasi tinkamu klaidos kodu.

Komanda gali būti arba nebūti prieinama rinkmenoje MF ir (arba) rinkmenoje DF Tachograph. Jei ji prieinama, jos vykdymas baigiasi tinkamu klaidos kodu.

TCS_135 DSRC pagrindinis raktas prieinamas tik rinkmenoje DF Tachograph_G2, t. y. kontrolės ir dirbtuvių kortelė tinkama šiai komandai vykdyti tik rinkmenoje DF Tachograph_G2.

TCS_136 Komanda turi tik iššifruoti DSRC duomenis ir patikrinti kriptografinę kontrolinę sumą, tačiau neinterpretuoti pradinių duomenų.

TCS_137 Duomenų objektų eilės tvarka komandos duomenų laukelyje nustatyta šia specifikacija.

TCS_138 **Komandos pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	80h	Patentuotas CLA
INS	1	‘2Ah’	Atlikti apsaugos operaciją.
P1	1	80h	Atsakymo duomenys: paprastoji vertė
P2	1	‘B0h’	Komandos duomenys: paprastoji vertė, kuri užkoduota BER-TLV ir į kurią įtraukti SM DO.
Lc	1	‘NNh’	Kito duomenų laukelio ilgis Lc.

▼B

Baitas	Ilgis	Vertė	Aprašymas
#6-#(5+L)	L	‘87h’ + L_{87} + ‘XX..XXh’	Pagal DER-TLV užkoduotas išplėtimo turinio žymėjimo baitas, po kurio seka užšifruotas informacinis tachografo turinys. Išplėtimo turinio žymėjimo baitui turi būti naudojama vertė ‘00h’ (jokio papildomo žymėjimo pagal ISO/IEC 7816-4:2013 52 lentelę). Daugiau apie šifravimo mechanizmą žr. 11 priedėlio B dalies 13 skyriuje. Leidžiamosios ilgio L_{87} vertės yra AES bloko ilgio kartotiniai plius 1 išplėtimo turinio žymėjimo baitui, t. y. nuo 17 baitų iki 193 baitų imtinai. *Pastaba.* Daugiau apie duomenų objektą SM, kurio žymena ‘87h’, žr. standarto ISO/IEC 7816-4:2013 49 lentelėje.
		‘81h’ + ‘10h’	Pagal DER-TLV užkoduotas šablonas Control Reference Template for Confidentiality, kuriuo užtikrinamas šių duomenų elementų jungimas (žr. 1 priedėlyje DSRCSecurityData ir 11 priedėlio B dalies 13 skyrių). — 4 baitų laiko antspaudas — 3 baitų skaitiklis — 8 baitų transporto priemonės bloko serijos numeris — 1 baito DSRC pagrindinio rakto versija *Pastaba.* Daugiau apie duomenų objektą SM, kurio žymena ‘81h’, žr. standarto ISO/IEC 7816-4:2013 49 lentelėje.
		‘8Eh’ + L_{8E} + ‘XX..XXh’	Pagal DER-TLV užkoduotas MAC per DSRC pranešimą. Daugiau apie MAC algoritmą ir apskaičiavimą žr. 11 priedėlio B dalies 13 skyriuje. *Pastaba.* Daugiau apie duomenų objektą SM, kurio žymena ‘8Eh’, žr. standarto ISO/IEC 7816-4:2013 49 lentelėje.

TCS_139 **Atsakymo pranešimas**

Baitas	Ilgis	Vertė	Aprašymas
#1-#L	L	‘XX..XXh’	Nėra (jei įvyko klaida) arba iššifruoti duomenys (išplėtimas pašalintas)
SW	2	‘XXXXh’	Būsenos žodžiai (SW1, SW2)

— Jei komanda sėkmingai įvykdoma, kortelė atsako ‘**9000**’.

— **‘6A80’** reiškia, kad parametrai komandos duomenų laukelyje neteisingi (taip pat naudojamas, jei duomenų objektai nesiunčiami nustatyta eilės tvarka).

— **‘6A88’** reiškia, kad nurodytų duomenų nėra (t. y. nurodyto DSRC pagrindinio rakto nėra).

— **‘6900’** reiškia, kad kriptografinės kontrolinės sumos patikrinimas arba duomenų iššifravimas neįvyko.

4. TACHOGRAFO KORTELIŲ STRUKTŪRA

Šiame skyriuje nurodyta tachografo kortelių rinkmenų struktūra, skirta prieinamiems duomenims laikyti.

▼B

Čia nenustatoma nei nuo kortelės gamintojo priklausančios vidinės struktūros, pvz., rinkmenų antraščių, nei vien tik vidaus naudojimui reikalingų duomenų elementų, pvz., `EuropeanPublicKey`, `CardPrivateKey`,`TdesSessionKey` or `WorkshopCardPin`, laikymo ir tvarkymo.

TCS_140 2-osios kartos tachografo kortelėje laikoma pagrindinė rinkmena MF ir 1-osios ir 2-osios kartos tachografo to paties tipo programa (pvz., vairuotojo kortelės programos).

TCS_141 Tachografo kortelė turi būti tinkama bent minimaliam atitinkamai programai nustatytam įrašų skaičiui ir neturi būti tinkama įrašų skaičiui, kuris būtų didesnis už maksimalų atitinkamai programai nustatytų įrašų skaičių.

Minimalus ir maksimalus įrašų skaičius šiame skyriuje nustatytas įvairioms programoms.

Kokios šiame visame skyriuje naudojamos prieigos taisyklių saugumo sąlygos, žr. 3.3 skyriuje. Paprastai prieigos režimas „skaityti“ reiškia komandą READ BINARY su lyginiu ir, jei palaikomas, nelyginiu baitu INS, išskyrus dirbtuvių kortelės rinkmeną EF Sensor_Installation_Data, žr. TCS_156 ir TCS_160. Prieigos režimas „atnaujinti“ reiškia komandą Update Binary su lyginiu ir, jei palaikomas, nelyginiu baitu INS ir prieigos režimą „pasirinkti“ komandai SELECT.

4.1. **Pagrindinė rinkmena MF**

TCS_142 Individualizuotos pagrindinės rinkmenos MF nuolatinė rinkmenos struktūra ir prieigos taisyklės turi būti tokios:

Pastaba. Trumpasis rinkmenos EF identifikatorius nurodomas dešimtainiu skaičiumi, pvz., 30 atitinka dvejetainį 11110.

			Prieigos taisyklės	
Rinkmena	**Rinkmenos ID**	**SFID**	**Skaityti / Pasirinkti**	**Atnaujinti**
MF	‘3F00h’			
├─ EF ICC	‘0002h’		ALW	NEV
├─ EF IC	‘0005h’		ALW	NEV
├─ EF DIR	‘2F00h’	30	ALW	NEV
├─ EF ATR/INFO (conditional)	‘2F01h’	29	ALW	NEV
├─ EF Extended_Length (conditional)	‘0006h’	28	ALW	NEV
├─ DF Tachograph	‘0500h’		SC1	
└─ DF Tachograph_G2			SC1	

Lentelėje vartojamos šios saugumo sąlygų santrumpos:

SC1 ALW OR SM-MAC-G2

TCS_143 Visa rinkmenos EF struktūra turi būti atvira.

TCS_144 Pagrindinės rinkmenos struktūra turi būti tokia:

▼B

Rinkmenos / duomenų elementas	Įrašų skaičius	Dydis (baitais) Min.	Maks.	Numatytosios vertės
MF		*63*	*184*	
EF ICC		*25*	*25*	
CardIccIdentification		*25*	*25*	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		*8*	*8*	
CardChipIdentification		*8*	*8*	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
EF DIR		*20*	*20*	
See TCS_145		*20*	*20*	{00..00}
EF ATR/INFO		*7*	*128*	
See TCS_146		*7*	*128*	{00..00}
EF EXTENDED_LENGTH		*3*	*3*	
See TCS_147		*3*	*3*	{00..00}
DF Tachograph				
DF Tachograph_G2				

TCS_145 Elementariojoje rinkmenoje EF DIR turi būti laikomi šie programos duomenys, susiję su duomenų objektais: ‘61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54’

TCS_146 Turi būti elementarioji rinkmena EF ATR/INFO, jei tachografo kortelės ATR nurodyta, kad ji tinkama didesnio ilgio laukeliams. Tokiu atveju rinkmenoje EF ATR/INFO turi būti išplėstinės informacijos duomenų objektas (DO‘7F66’), kaip nustatyta standarto ISO/IEC 7816-4:2013 12.7.1 punkte.

TCS_147 Turi būti elementarioji rinkmena EF Extended_Length, jei tachografo kortelės ATR nurodyta, kad ji tinkama didesnio ilgio laukeliams. Tokiu atveju rinkmenoje EF turi būti šie duomenų objektai: ‘02 01 xx’, kur ‘xx’ rodo didesnio ilgio laukeliai tinkami protokolams T = 1 ir (arba) T = 0.

Vertė ‘01’ rodo, kad didesnio ilgio laukelis tinkamas protokolui T = 1.

Vertė ‘10’ rodo, kad didesnio ilgio laukelis tinkamas protokolui T = 0.

Vertė ‘11’ rodo, kad didesnio ilgio laukelis tinkamas protokolams T = 1 ir T = 0.

4.2. Vairuotojo kortelės programos

4.2.1 *Vairuotojo kortelės 1-osios kartos programa*

TCS_148 Individualizuotos vairuotojo kortelės 1-osios kartos programos nuolatinė rinkmenų struktūra ir prieigos taisyklės turi būti tokios:

Rinkmena	Rinkmenos ID	Prieigos taisyklės Skaityti	Pasirinkti	Atnaujinti
DF Tachograph	‘0500h’		SC1	
EF Application_Identification	‘0501h’	SC2	SC1	NEV
EF Card_Certificate	‘C100h’	SC2	SC1	NEV
EF CA_Certificate	‘C108h’	SC2	SC1	NEV
EF Identification	‘0520h’	SC2	SC1	NEV
EF Card_Download	‘050Eh’	SC2	SC1	SC1
EF Driving_Licence_Info	‘0521h’	SC2	SC1	NEV
EF Events_Data	‘0502h’	SC2	SC1	SC3
EF Faults_Data	‘0503h’	SC2	SC1	SC3
EF Driver_Activity_Data	‘0504h’	SC2	SC1	SC3
EF Vehicles_Used	‘0505h’	SC2	SC1	SC3
EF Places	‘0506h’	SC2	SC1	SC3
EF Current_Usage	‘0507h’	SC2	SC1	SC3
EF Control_Activity_Data	‘0508h’	SC2	SC1	SC3
EF Specific_Conditions	‘0522h’	SC2	SC1	SC3

▼B

Lentelėje vartojamos šios saugumo sąlygų santrumpos:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

TCS_149 Visa rinkmenos EF struktūra turi būti atvira.

TCS_150 Vairuotojo kortelės 1-osios kartos programos duomenų struktūra turi būti tokia:

Rinkmenos / duomenų elementas	Įrašų skaičius	Dydis (baitais) Min.	Maks.	Numatytosios vertės
DF Tachograph		*11378*	*24926*	
EF Application_Identification		*10*	*10*	
DriverCardApplicationIdentification		*10*	*10*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*864*	*1728*	
CardEventData		*864*	*1728*	
cardEventRecords	6	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				

▼B

vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
CardDriverActivity		*5548*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*2606*	*6202*	
CardVehiclesUsed		*2606*	*6202*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*2604*	*6200*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
CardPlaceDailyWorkPeriod		*841*	*1121*	
placePointerNewestRecord		1	1	{00}
placeRecords		*840*	*1120*	
PlaceRecord	n_4	*10*	*10*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*280*	*280*	
SpecificConditionRecord	56	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

▼B

TCS_151 Vairuotojo kortelės 1-osios kartos programos duomenų struktūroje turi būti naudojamos tokios didžiausios ir mažiausios įrašų skaičiaus vertės pirmiau esančioje lentelėje pateiktiems dydžiams nurodyti.

		Min.	Maks.
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 baitai (28 dienos * 93 veiklos rūšies pasikeitimai)	13 776 baitai (28 dienos * 240 veiklos rūšies pasikeitimų)

4.2.2 *Vairuotojo kortelės 2-osios kartos programa*

TCS_152 Individualizuotos vairuotojo kortelės 2-osios kartos programos nuolatinė rinkmenų struktūra ir prieigos taisyklės turi būti tokios:

Pastaba. Trumpasis rinkmenos EF identifikatorius nurodomas dešimtainiu skaičiumi, pvz., 30 atitinka dvejetainį 11110.

			Prieigos taisyklės	
Rinkmena	**Rinkmenos ID**	**SFID**	**Skaityti / Pasirinkti**	**Atnaujinti**
└─ DF Tachograph_G2			SC1	
├─ EF Application_Identification	‘0501h’	1	SC1	NEV
├─ EF CardMA_Certificate	‘C100h’	2	SC1	NEV
├─ EF CardSignCertificate	‘C101h’	3	SC1	NEV
├─ EF CA_Certificate	‘C108h’	4	SC1	NEV
├─ EF Link_Certificate	‘C109h’	5	SC1	NEV
├─ EF Identification	‘0520h’	6	SC1	NEV
├─ EF Card_Download	‘050Eh’	7	SC1	SC1
├─ EF Driving_Licence_Info	‘0521h’	10	SC1	NEV
├─ EF Events_Data	‘0502h’	12	SC1	SM-MAC-G2
├─ EF Faults_Data	‘0503h’	13	SC1	SM-MAC-G2
├─ EF Driver_Activity_Data	‘0504h’	14	SC1	SM-MAC-G2
├─ EF Vehicles_Used	‘0505h’	15	SC1	SM-MAC-G2
├─ EF Places	‘0506h’	16	SC1	SM-MAC-G2
├─ EF Current_Usage	‘0507h’	17	SC1	SM-MAC-G2
├─ EF Control_Activity_Data	‘0508h’	18	SC1	SM-MAC-G2
├─ EF Specific_Conditions	‘0522h’	19	SC1	SM-MAC-G2
├─ EF VehicleUnits_Used	‘0523h’	20	SC1	SM-MAC-G2
└─ EF GNSS_Places	‘0524h’	21	SC1	SM-MAC-G2

Lentelėje vartojamos šios saugumo sąlygų santrumpos:

SC1 ALW OR SM-MAC-G2

TCS_153 Visa rinkmenos EF struktūra turi būti atvira.

TCS_154 Vairuotojo kortelės 2-osios kartos programos duomenų struktūra turi būti tokia:

▼B

Rinkmenos / duomenų elementas	Įrašų skaičius	Dydis (baitais) Min.	Dydis (baitais) Maks.	Numatytosios vertės
DF Tachograph_G2		*19510*	*39306*	
EF Application_Identification		*15*	*15*	
DriverCardApplicationIdentification		*15*	*15*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*1584*	*3168*	
CardEventData		*1584*	*3168*	
cardEventRecords	11	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	

▼B

├─faultType		1	1	{00}
├─faultBeginTime		4	4	{00..00}
├─faultEndTime		4	4	{00..00}
└─faultVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
└CardDriverActivity		*5548*	*13780*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*4034*	*9602*	
└CardVehiclesUsed		*4034*	*9602*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*4032*	*9600*	
└─CardVehicleRecord	n_3	*48*	*48*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─vuDataBlockCounter		2	2	{00 00}
└─vehicleIdentificationNumber		17	17	{20..20}
EF Places		*1766*	*2354*	
└CardPlaceDailyWorkPeriod		*1766*	*2354*	
├─placePointerNewestRecord		2	2	{00 00}
└─placeRecords		*1764*	*2352*	
└─PlaceRecord	n_4	*21*	*21*	
├─entryTime		4	4	{00..00}
├─entryTypeDailyWorkPeriod		1	1	{00}
├─dailyWorkPeriodCountry		1	1	{00}
├─dailyWorkPeriodRegion		1	1	{00}
├─vehicleOdometerValue		3	3	{00..00}
└─entryGNSSPlaceRecord		11	11	
├─timeStamp		4	4	{00..00}
├─gnssAccuracy		1	1	{00}
└─geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├─sessionOpenTime		4	4	{00..00}
└─sessionOpenVehicle				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlCardNumber				
├─cardType		1	1	{00}
├─cardIssuingMemberState		1	1	{00}
└─cardNumber		16	16	{20..20}
├─controlVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}

▼B

EF Specific_Conditions		*282*	*562*	
SpecificConditions		*282*	*562*	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		*280*	*560*	
SpecificConditionRecord	n_9	*5*	*5*	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}
EF VehicleUnits_Used		*842*	*2002*	
CardVehicleUnitsUsed		*842*	*2002*	
vehicleUnitPointerNewestRecord		2	2	{00 00}
cardVehicleUnitRecords		*840*	*2000*	
CardVehicleUnitRecord	n_7	*10*	*10*	
timeStamp		4	4	{00..00}
manufacturerCode		1	1	{00}
deviceID		1	1	{00}
vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*3782*	*5042*	
GNSSContinuousDriving		*3782*	*5042*	
gnssCDPointerNewestRecord		2	2	{00 00}
gnssContinuousDrivingRecords		3780	5040	{00}
GNSSContinuousDrivingRecord	n_8	*15*	*15*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}

TCS_155 Vairuotojo kortelės 2-osios kartos programos duomenų struktūroje turi būti naudojamos tokios didžiausios ir mažiausios įrašų skaičiaus vertės pirmiau esančioje lentelėje pateiktiems dydžiams nurodyti.

		Min.	Maks.
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 baitai (28 dienos * 93 veiklos rūšies pasikeitimai)	13 776 baitai (28 dienos * 240 veiklos rūšies pasikeitimai)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3. **Dirbtuvių kortelės programos**

4.3.1 *Dirbtuvių kortelės 1-osios kartos programa*

TCS_156 Individualizuotos dirbtuvių kortelės 1-osios kartos programos nuolatinė rinkmenų struktūra ir prieigos taisyklės turi būti tokios:

▼B

		Prieigos taisyklės		
Rinkmena	**Rinkmenos ID**	**Skaityti**	**Pasirinkti**	**Atnaujinti**
└DF Tachograph	‘0500h’		SC1	
├EF Application_Identification	‘0501h’	SC2	SC1	NEV
├EF Card_Certificate	‘C100h’	SC2	SC1	NEV
├EF CA_Certificate	‘C108h’	SC2	SC1	NEV
├EF Identification	‘0520h’	SC2	SC1	NEV
├EF Card_Download	‘0509h’	SC2	SC1	**SC1**
├EF Calibration	‘050Ah’	SC2	SC1	SC3
├EF Sensor_Installation_Data	‘050Bh’	**SC4**	SC1	NEV
├EF Events_Data	‘0502h’	SC2	SC1	SC3
├EF Faults_Data	‘0503h’	SC2	SC1	SC3
├EF Driver_Activity_Data	‘0504h’	SC2	SC1	SC3
├EF Vehicles_Used	‘0505h’	SC2	SC1	SC3
├EF Places	‘0506h’	SC2	SC1	SC3
├EF Current_Usage	‘0507h’	SC2	SC1	SC3
├EF Control_Activity_Data	‘0508h’	SC2	SC1	SC3
└EF Specific_Conditions	‘0522h’	SC2	SC1	SC3

Lentelėje vartojamos šios saugumo sąlygų santrumpos:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC4 Komanda READ BINARY su lyginiu baitu INS:

(PLAIN-C AND SM-R-ENC-G1) OR (SM-C-MAC-G1 AND SM-R-ENC-MAC-G1) OR

(SM-C-MAC-G2 AND SM-R-ENC-MAC-G2)

Komanda READ BINARY su nelyginiu baitu INS (jei palaikoma): NEV

TCS_157 Visa rinkmenos EF struktūra turi būti atvira.

TCS_158 Dirbtuvių kortelės 1-osios kartos programos duomenų struktūra turi būti tokia:

▼B

Rinkmenos / duomenų elementas	Įrašų skaičius	Dydis (baitais) Min.	Maks.	Numatytosios vertės
DF Tachograph		*11055*	*29028*	
EF Application_Identification		*11*	*11*	
WorkshopCardApplicationIdentification		*11*	*11*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
noOfCalibrationRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*9243*	*26778*	
WorkshopCardCalibrationData		*9243*	*26778*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		*9240*	*26775*	
WorkshopCardCalibrationRecord	n_5	*105*	*105*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}

▼B

EF Sensor_Installation_Data		*16*	*16*	
SensorInstallationSecData		16	16	{00..00}
EF Events_Data		*432*	*432*	
CardEventData		*432*	*432*	
cardEventRecords	6	*72*	*72*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
CardFaultData		*288*	*288*	
cardFaultRecords	2	*144*	*144*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
CardDriverActivity		*202*	*496*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*126*	*250*	
CardVehiclesUsed		*126*	*250*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*124*	*248*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		*61*	*81*	
CardPlaceDailyWorkPeriod		*61*	*81*	
placePointerNewestRecord		1	1	{00}
placeRecords		*60*	*80*	
PlaceRecord	n_4	*10*	*10*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}

▼B

EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*10*	*10*	
SpecificConditionRecord	2	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_159 Dirbtuvių kortelės 1-osios kartos programos duomenų struktūroje turi būti naudojamos tokios didžiausios ir mažiausios įrašų skaičiaus vertės pirmiau esančioje lentelėje pateiktiems dydžiams nurodyti.

		Min.	Maks.
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 baitai (1 diena * 93 veiklos rūšies pasikeitimai)	492 baitai (1 diena * 240 veiklos rūšies pasikeitimų)

4.3.2 *Dirbtuvių kortelės 2-osios kartos programa*

TCS_160 Individualizuotos dirbtuvių kortelės 2-osios kartos programos nuolatinė rinkmenų struktūra ir prieigos taisyklės turi būti tokios:

Pastaba. Trumpasis rinkmenos EF identifikatorius nurodomas dešimtainiu skaičiumi, pvz., 30 atitinka dvejetainį 11110.

			Prieigos taisyklės		
Rinkmena	**Rinkmenos ID**	**SFID**	**Skaityti**	**Pasirinkti**	**Atnaujinti**
DF Tachograph_G2			SC1	SC1	
EF Application_Identification	'0501h'	1	SC1	SC1	NEV
EF CardMA_Certificate	'C100h'	2	SC1	SC1	NEV
EF CardSignCertificate	'C101h'	3	SC1	SC1	NEV
EF CA_Certificate	'C108h'	4	SC1	SC1	NEV
EF Link_Certificate	'C109h'	5	SC1	SC1	NEV
EF Identification	'0520h'	6	SC1	SC1	NEV
EF Card_Download	'0509h'	7	SC1	SC1	SC1
EF Calibration	'050Ah'	10	SC1	SC1	SM-MAC-G2
EF Sensor_Installation_Data	'050Bh'	11	**SC5**	SM-MAC-G2	NEV
EF Events_Data	'0502h'	12	SC1	SC1	SM-MAC-G2
EF Faults_Data	'0503h'	13	SC1	SC1	SM-MAC-G2
EF Driver_Activity_Data	'0504h'	14	SC1	SC1	SM-MAC-G2
EF Vehicles_Used	'0505h'	15	SC1	SC1	SM-MAC-G2
EF Places	'0506h'	16	SC1	SC1	SM-MAC-G2
EF Current_Usage	'0507h'	17	SC1	SC1	SM-MAC-G2
EF Control_Activity_Data	'0508h'	18	SC1	SC1	SM-MAC-G2
EF Specific_Conditions	'0522h'	19	SC1	SC1	SM-MAC-G2
EF VehicleUnits_Used	'0523h'	20	SC1	SC1	SM-MAC-G2
EF GNSS_Places	'0524h'	21	SC1	SC1	SM-MAC-G2

▼B

Lentelėje vartojamos šios saugumo sąlygų santrumpos:

SC1 ALW OR SM-MAC-G2

SC5 Komanda READ BINARY su lyginiu baitu INS: SM-C-MAC-G2 AND SM-R-ENC-MAC-G2

Komanda READ BINARY su nelyginiu baitu INS (jei palaikoma): NEV

TCS_161 Visa EF struktūra turi būti atvira.

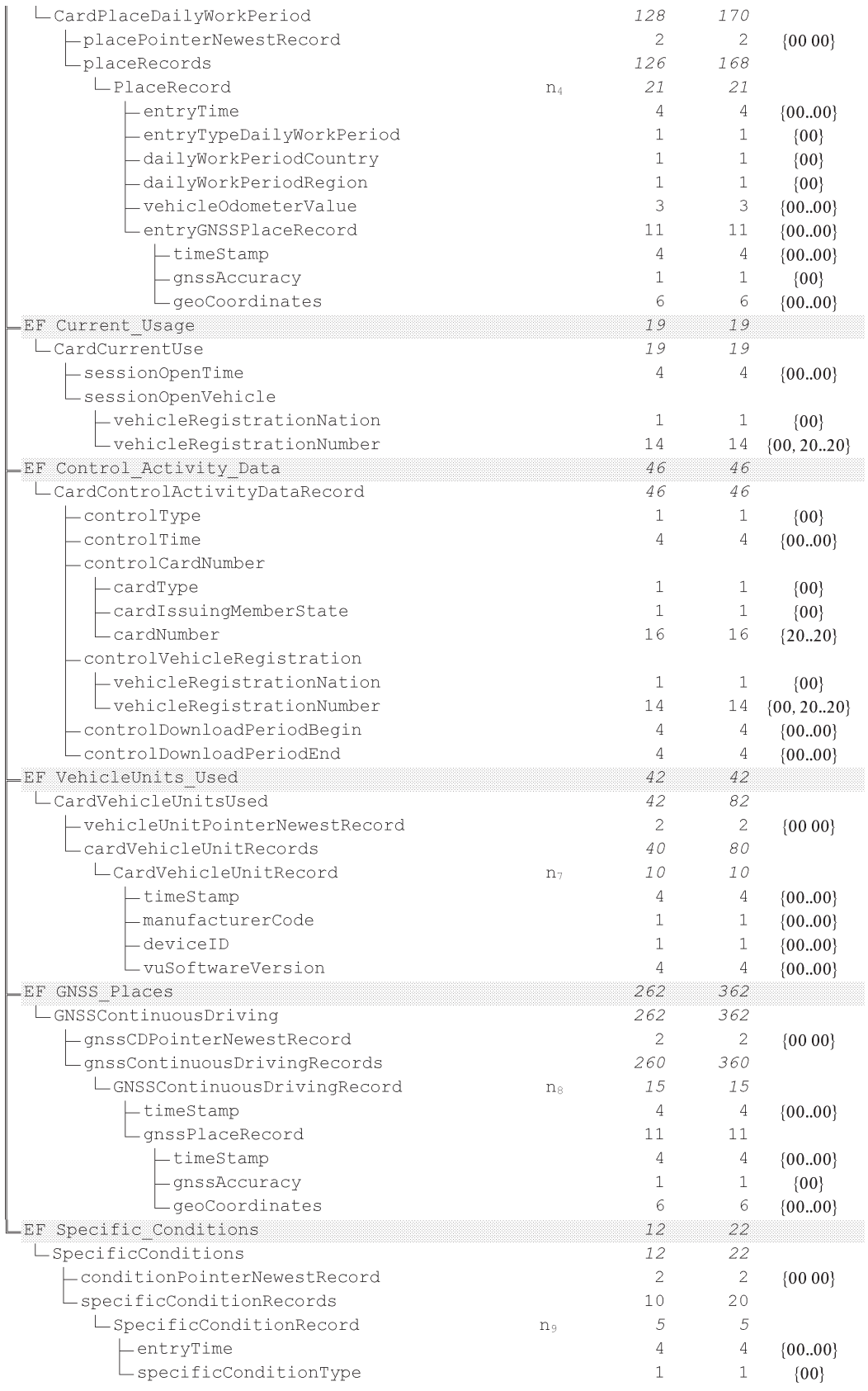
TCS_162 Dirbtuvių kortelės 2-osios kartos programos duomenų struktūra turi būti tokia:

Rinkmenos / duomenų elementas	Įrašų skaičius	Dydis (baitais) Min.	Maks.	Numatytosios vertės
DF Tachograph_G2		*17837*	*47163*	
EF Application_Identification		*17*	*17*	
WorkshopCardApplicationIdentification		*17*	*17*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfCalibrationRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00..00}
noOfSpecificConditionRecords		2	2	{00..00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*14788*	*42844*	
WorkshopCardCalibrationData		*14788*	*42844*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*14784*	*42840*	
WorkshopCardCalibrationRecord	n_5	*168*	*168*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}

▼B

├─oldTimeValue		4	4	{00..00}
├─newTimeValue		4	4	{00..00}
├─nextCalibrationDate		4	4	{00..00}
├─vuPartNumber		16	16	{20..20}
├─vuSerialNumber		8	8	{00..00}
├─sensorSerialNumber		8	8	{00..00}
├─sensorGNSSSerialNumber		8	8	{00..00}
├─rcmSerialNumber		8	8	{00..00}
├─vuAbility		1	1	{00}
└─sealDataCard		46	46	
├─noOfSealRecords		1	1	{00}
└─SealRecords		45	45	
└─SealRecord	5	9	9	
├─equipmentType		1	1	{00}
└─extendedSealIdentifier		8	8	{00..00}
EF Sensor_Installation_Data		*18*	*102*	
└─SensorInstallationSecData		18	102	{00..00}
EF Events_Data		*792*	*792*	
└─CardEventData		*792*	*792*	
└─cardEventRecords	11	*72*	*72*	
└─CardEventRecord	n_1	*24*	*24*	
├─eventType		1	1	{00}
├─eventBeginTime		4	4	{00..00}
├─eventEndTime		4	4	{00..00}
└─eventVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
└─CardFaultData		*288*	*288*	
└─cardFaultRecords	2	*144*	*144*	
└─CardFaultRecord	n_2	*24*	*24*	
├─faultType		1	1	{00}
├─faultBeginTime		4	4	{00..00}
├─faultEndTime		4	4	{00..00}
└─faultVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
└─CardDriverActivity		*202*	*496*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*194*	*386*	
└─CardVehiclesUsed		*194*	*386*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*192*	*384*	
└─CardVehicleRecord	n_3	*48*	*48*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─vuDataBlockCounter		2	2	{00 00}
└─vehicleIdentificationNumber		*17*	17	{20..20}
EF Places		*128*	*170*	

▼B



└CardPlaceDailyWorkPeriod		*128*	*170*	
├placePointerNewestRecord		2	2	{00 00}
└placeRecords		*126*	*168*	
└PlaceRecord	n_4	*21*	*21*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
├vehicleOdometerValue		3	3	{00..00}
└entryGNSSPlaceRecord		11	11	{00..00}
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlCardNumber				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}
EF VehicleUnits_Used		*42*	*42*	
└CardVehicleUnitsUsed		*42*	*82*	
├vehicleUnitPointerNewestRecord		2	2	{00 00}
└cardVehicleUnitRecords		*40*	*80*	
└CardVehicleUnitRecord	n_7	*10*	*10*	
├timeStamp		4	4	{00..00}
├manufacturerCode		1	1	{00..00}
├deviceID		1	1	{00..00}
└vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*262*	*362*	
└GNSSContinuousDriving		*262*	*362*	
├gnssCDPointerNewestRecord		2	2	{00 00}
└gnssContinuousDrivingRecords		*260*	*360*	
└GNSSContinuousDrivingRecord	n_8	*15*	*15*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		11	11	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Specific_Conditions		*12*	*22*	
└SpecificConditions		*12*	*22*	
├conditionPointerNewestRecord		2	2	{00 00}
└specificConditionRecords		10	20	
└SpecificConditionRecord	n_9	*5*	*5*	
├entryTime		4	4	{00..00}
└specificConditionType		1	1	{00}

▼B

TCS_163 Dirbtuvių kortelės 2-osios kartos programos duomenų struktūroje turi būti naudojamos tokios didžiausios ir mažiausios įrašų skaičiaus vertės pirmiau esančioje lentelėje pateiktiems dydžiams nurodyti.

		Min.	Maks.
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 baitai (1 diena * 93 veiklos rūšies pasikeitimai)	492 baitai (1 diena * 240 veiklos rūšies pasikeitimų)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4. Kontrolės kortelės programos

4.4.1 *Kontrolės kortelės 1-osios kartos programa*

TCS_164 Individualizuotos kontrolės kortelės 1-osios kartos programos nuolatinė rinkmenų struktūra ir prieigos taisyklės turi būti tokios:

		Prieigos taisyklės		
Rinkmena	**Rinkmenos ID**	**Skaityti**	**Pasirinkti**	**Atnaujinti**
└─DF Tachograph	‘0500h’			
├─EF Application_Identification	‘0501h’	SC2	SC1	NEV
├─EF Card_Certificate	‘C100h’	SC2	SC1	NEV
├─EF CA_Certificate	‘C108h’	SC2	SC1	NEV
├─EF Identification	‘0520h’	**SC6**	SC1	NEV
└─EF Controller_Activity_Data	‘050Ch’	SC2	SC1	SC3

Lentelėje vartojamos šios saugumo sąlygų santrumpos:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC6 EXT-AUT-G1 OR SM-MAC-G1 OR SM-MAC-G2

TCS_165 Visa rinkmenos EF struktūra turi būti atvira.

TCS_166 Kontrolės kortelės 1-osios kartos programos duomenų struktūra turi būti tokia:

▼B

Rinkmenos / duomenų elementas	Įrašų skaičius	Dydis (baitais) Min.	Maks.	
DF Tachograph		*11186*	*24526*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_167 Kontrolės kortelės 1-osios kartos programos duomenų struktūroje turi būti naudojamos tokios didžiausios ir mažiausios įrašų skaičiaus vertės pirmiau esančioje lentelėje pateiktiems dydžiams nurodyti.

		Min.	Maks.
n_7	NoOfControlActivityRecords	230	520

4.4.2 *Kontrolės kortelės 2-osios kartos programa*

TCS_168 Individualizuotos kontrolės kortelės 2-osios kartos programos nuolatinė rinkmenų struktūra ir prieigos taisyklės turi būti tokios:

Pastaba. Trumpasis rinkmenos EF identifikatorius nurodomas dešimtainiu skaičiumi, pvz., 30 atitinka dvejetainį 11110.

▼B

Rinkmena	Rinkmenos ID	SFID	Prieigos taisyklės: Skaityti / Pasirinkti	Prieigos taisyklės: Atnaujinti
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
└─EF Controller_Activity_Data	'050Ch'	14	SC1	SM-MAC-G2

Lentelėje vartojamos šios saugumo sąlygų santrumpos:

SC1 ALW OR SM-MAC-G2

TCS_169 Visa rinkmenos EF struktūra turi būti atvira.

TCS_170 Kontrolės kortelės 2-osios kartos programos duomenų struktūra turi būti tokia:

Rinkmenos / duomenų elementas	Įrašų skaičius	Dydis (baitais) Min.	Maks.	
└─DF Tachograph_G2		*11410*	*25161*	
├─EF Application_Identification		*5*	*5*	
│ └─ControlCardApplicationIdentification		*5*	*5*	
│ ├─typeOfTachographCardId		1	1	{00}
│ ├─cardStructureVersion		2	2	{00 00}
│ └─noOfControlActivityRecords		2	2	{00 00}
├─EF CardMA_Certificate		*204*	*341*	
│ └─CardMACertificate		204	341	{00..00}
├─EF CA_Certificate		*204*	*341*	
│ └─MemberStateCertificate		204	341	{00..00}
├─EF Link_Certificate		*204*	*341*	
│ └─LinkCertificate		204	341	{00..00}
├─EF Identification		*211*	*211*	
│ ├─CardIdentification		*65*	*65*	
│ │ ├─cardIssuingMemberState		1	1	{00}
│ │ ├─cardNumber		16	16	{20..20}
│ │ ├─cardIssuingAuthorityName		36	36	{00, 20..20}
│ │ ├─cardIssueDate		4	4	{00..00}
│ │ ├─cardValidityBegin		4	4	{00..00}
│ │ └─cardExpiryDate		4	4	{00..00}
│ └─ControlCardHolderIdentification		*146*	*146*	
│ ├─controlBodyName		36	36	{00, 20..20}
│ ├─controlBodyAddress		36	36	{00, 20..20}
│ ├─cardHolderName				
│ │ ├─holderSurname		36	36	{00, 20..20}
│ │ └─holderFirstNames		36	36	{00, 20..20}
│ └─cardHolderPreferredLanguage		2	2	{20 20}
└─EF Controller_Activity_Data		*10582*	*23922*	
└─ControlCardControlActivityData		*10582*	*23922*	
├─controlPointerNewestRecord		2	2	{00 00}
└─controlActivityRecords		*10580*	*23920*	
└─controlActivityRecord	n_7	*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlledCardNumber				
│ ├─cardType		1	1	{00}
│ ├─cardIssuingMemberState		1	1	{00}
│ └─cardNumber		16	16	{20..20}
├─controlledVehicleRegistration				
│ ├─vehicleRegistrationNation		1	1	{00}
│ └─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}

TCS_171 Kontrolės kortelės 2-osios kartos programos duomenų struktūroje turi būti naudojamos tokios didžiausios ir mažiausios įrašų skaičiaus vertės pirmiau esančioje lentelėje pateiktiems dydžiams nurodyti.

▼B

		Min.	Maks.
n_7	NoOfControlActivityRecords	230	520

4.5. **Įmonės kortelės programos**

4.5.1 *Įmonės kortelės 1-osios kartos programa*

TCS_172 Individualizuotos įmonės kortelės 1-osios kartos programos nuolatinė rinkmenų struktūra ir prieigos taisyklės turi būti tokios:

		Prieigos taisyklės		
Rinkmena	**Rinkmenos ID**	**Skaityti**	**Pasirinkti**	**Atnaujinti**
└DF Tachograph	'0500h'		SC1	
├EF Application_Identification	'0501h'	SC2	SC1	NEV
├EF Card_Certificate	'C100h'	SC2	SC1	NEV
├EF CA_Certificate	'C108h'	SC2	SC1	NEV
├EF Identification	'0520h'	**SC6**	SC1	NEV
└EF Company_Activity_Data	'050Dh'	SC2	SC1	SC3

Lentelėje vartojamos šios saugumo sąlygų santrumpos:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC6 EXT-AUT-G1 OR SM-MAC-G1 OR SM-MAC-G2

TCS_173 Visa rinkmenos EF struktūra turi būti atvira.

TCS_174 Įmonės kortelės 1-osios kartos programos duomenų struktūra turi būti tokia:

Rinkmenos / duomenų elementas	Įrašų skaičius	Dydis (baitais) Min	Maks	Numatytosios vertės
└DF Tachograph		*11114*	*24454*	
├EF Application_Identification		*5*	*5*	
│└CompanyCardApplicationIdentification		*5*	*5*	
│├typeOfTachographCardId		1	1	{00}
│├cardStructureVersion		2	2	{00 00}
│└noOfCompanyActivityRecords		2	2	{00 00}
├EF Card_Certificate		*194*	*194*	
│└CardCertificate		194	194	{00..00}
├EF CA_Certificate		*194*	*194*	
│└MemberStateCertificate		194	194	{00..00}
├EF Identification		*139*	*139*	
│├CardIdentification		*65*	*65*	
││├cardIssuingMemberState		1	1	{00}
││├cardNumber		16	16	{20..20}
││├cardIssuingAuthorityName		36	36	{00, 20..20}
││├cardIssueDate		4	4	{00..00}
││├cardValidityBegin		4	4	{00..00}
││└cardExpiryDate		4	4	{00..00}
│└CompanyCardHolderIdentification		*74*	*74*	
│├companyName		36	36	{00, 20..20}
│├companyAddress		36	36	{00, 20..20}
│└cardHolderPreferredLanguage		2	2	{20 20}
└EF Company_Activity_Data		*10582*	*23922*	
└CompanyActivityData		*10582*	*23922*	
├companyPointerNewestRecord		2	2	{00 00}
└companyActivityRecords		*10580*	*23920*	
└companyActivityRecord	n_8	*46*	*46*	
├companyActivityType		1	1	{00}
├companyActivityTime		4	4	{00..00}
├cardNumberInformation				
│├cardType		1	1	{00}
│├cardIssuingMemberState		1	1	{00}
│└cardNumber		16	16	{20..20}
├vehicleRegistrationInformation				
│├vehicleRegistrationNation		1	1	{00}
│└vehicleRegistrationNumber		14	14	{00, 20..20}
├downloadPeriodBegin		4	4	{00..00}
└downloadPeriodEnd		4	4	{00..00}

▼B

TCS_175 Įmonės kortelės 1-osios kartos programos duomenų struktūroje turi būti naudojamos tokios didžiausios ir mažiausios įrašų skaičiaus vertės pirmiau esančioje lentelėje pateiktiems dydžiams nurodyti.

		Min	Maks
n_8	NoOfCompanyActivityRecords	230	520

4.5.2 *Įmonės kortelės 2-osios kartos programa*

TCS_176 Individualizuotos įmonės kortelės 2-osios kartos programos nuolatinė rinkmenų struktūra ir prieigos taisyklės turi būti tokios:

Pastaba. Trumpasis rinkmenos EF identifikatorius nurodomas dešimtainiu skaičiumi, pvz., 30 atitinka dvejetainį 11110.

			Prieigos taisyklės	
Rinkmena	**Rinkmenos ID**	**SFID**	**Skaityti / Pasirinkti**	**Atnaujinti**
└DF Tachograph_G2			SC1	
├EF Application_Identification	'0501h'	1	SC1	NEV
├EF CardMA_Certificate	'C100h'	2	SC1	NEV
├EF CA_Certificate	'C108h'	4	SC1	NEV
├EF Link_Certificate	'C109h'	5	SC1	NEV
├EF Identification	'0520h'	6	SC1	NEV
└EF Company_Activity_Data	'050Dh'	14	SC1	SM-MAC-G2

Lentelėje vartojamos šios saugumo sąlygų santrumpos:

SC1 ALW OR SM-MAC-G2

TCS_177 Visa rinkmenos EF struktūra turi būti atvira.

TCS_178 Įmonės kortelės 2-osios kartos programos duomenų struktūra turi būti tokia:

Rinkmenos / duomenų elementas	Įrašų skaičius	Dydis (baitais) Min	Maks	Numatytosios vertės
└DF Tachograph_G2		*11338*	*25089*	
├EF Application_Identification		*5*	*5*	
└CompanyCardApplicationIdentification		*5*	*5*	
├typeOfTachographCardId		1	1	{00}
├cardStructureVersion		2	2	{00 00}
└noOfCompanyActivityRecords		2	2	{00 00}
├EF CardMA_Certificate		*204*	*341*	
└CardMACertificate		204	341	{00..00}
├EF CA_Certificate		*204*	*341*	
└MemberStateCertificate		204	341	{00..00}
├EF Link_Certificate		*204*	*341*	
└LinkCertificate		204	341	{00..00}
├EF Identification		*139*	*139*	
├CardIdentification		*65*	*65*	
├cardIssuingMemberState		1	1	{00}
├cardNumber		16	16	{20..20}
├cardIssuingAuthorityName		36	36	{00, 20..20}
├cardIssueDate		4	4	{00..00}
├cardValidityBegin		4	4	{00..00}
└cardExpiryDate		4	4	{00..00}
└CompanyCardHolderIdentification		*74*	*74*	
├companyName		36	36	{00, 20..20}
├companyAddress		36	36	{00, 20..20}
└cardHolderPreferredLanguage		2	2	{20 20}
├EF Company_Activity_Data		*10582*	*23922*	
└CompanyActivityData		*10582*	*23922*	
├companyPointerNewestRecord		2	2	{00 00}
└companyActivityRecords		*10580*	*23920*	
└companyActivityRecord	n_8	*46*	*46*	
├companyActivityType		1	1	{00}
├companyActivityTime		4	4	{00..00}
├cardNumberInformation				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├vehicleRegistrationInformation				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├downloadPeriodBegin		4	4	{00..00}
└downloadPeriodEnd		4	4	{00..00}

▼B

TCS_179 Įmonės kortelės 2-osios kartos programos duomenų struktūroje turi būti naudojamos tokios didžiausios ir mažiausios įrašų skaičiaus vertės pirmiau esančioje lentelėje pateiktiems dydžiams nurodyti.

		Min	Maks
n_8	NoOfCompanyActivityRecords	230	520

▼B

3 priedėlis

PIKTOGRAMOS

PIC_001 Tachografe gali būti naudojamos šios piktogramas ir jų deriniai (arba pakankamai panašios piktogramos ir jų deriniai, kad jas būtų galima aiškiai atpažinti)

1. PAGRINDINĖS PIKTOGRAMOS

	Žmonės	**Veiksmai**	**Veikimo režimai**
	Įmonė		Įmonės režimas
	Kontrolierius	Kontrolė	Kontrolės režimas
	Vairuotojas	Vairuoja	Naudojimo režimas
	Dirbtuvė (tikrinimo stotis)	Patikra/kalibravimas	Kalibravimo režimas
	Gamintojas		

	Veikla	**Trukmė**
	Pasirengęs dirbti	Esamas buvimo pasirengus dirbti laikotarpis
	Vairavimas	Nepertraukiamo vairavimo trukmė
	Poilsis	Esamas poilsio laikotarpis
	Kiti darbai	Esamas darbo laikotarpis
	Pertrauka	Bendroji poilsio trukmė
	Nežinoma	

	Įranga	**Funkcijos**
	Vairuotojo kortelės lizdas	
	Vairuotojo porininko kortelės lizdas	
	Kortelė	
	Laikrodis	
	Ekranas	Rodymas ekrane
	Išorinė laikmena	Duomenų perkėlimas
	Maitinimas	
	Spausdintuvas/spaudinys	Spausdinimas
	Jutiklis	
	Padangų dydis	
	Transporto priemonė/transporto priemonės blokas	
	GNSS įrenginys	
	Nuotolinio aptikimo įrenginys	
	ITS sąsaja	

▼B

	Ypatingos būsenos
OUT	Nekontroliuojama
	Kėlimasis keltu / vežimas traukiniu

	Kita		
!	Įvykiai		Triktys
	Dienos darbo laikotarpio pradžia		Dienos darbo laikotarpio pabaiga
	Vieta		
M	Rankomis įvesta informacija apie vairuotojo veiklą		
	Saugumas		
	Greitis		
	Laikas		
Σ	Iš viso / suvestinė		

	Kvalifikatoriai
24h	Kasdien
I	Kas savaitę
II	Dvi savaitės
+	Nuo arba iki

2. PIKTOGRAMŲ DERINIAI

	Kita		
+	Kontrolės vieta		
+	Dienos darbo laikotarpio pradžios vieta	+	Dienos darbo laikotarpio pabaigos vieta
+	Nuo kada	+	Iki kada
+	Iš transporto priemonės		
OUT+	Nekontroliuojamo laikotarpio pradžia	+OUT	Nekontroliuojamo laikotarpio pabaiga

	Kortelės
	Vairuotojo kortelė
	Įmonės kortelė
	Kontrolės kortelė
	Dirbtuvių kortelė
– – –	Kortelės nėra

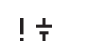
	Vairavimas
	Įgula
I	Vienos savaitės vairavimo trukmė
II	Dviejų savaičių vairavimo trukmė

▼B

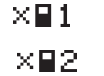
Spaudiniai

	Vairuotojo veiklos kasdienis spaudinys iš kortelės
	Vairuotojo veiklos kasdienis spaudinys iš transporto priemonės bloko
	Įvykių ir trikčių spaudinys iš kortelės
	Įvykių ir trikčių spaudinys iš transporto priemonės bloko
	Techninių duomenų spaudinys
	Greičio viršijimo spaudinys

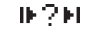
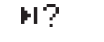
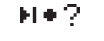
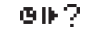
Įvykiai

	Įstatyta negaliojanti kortelė
	Kortelių nesuderinamumas
	Dalinis laiko sutapimas
	Važiavimas be reikiamos kortelės
	Kortelė įstatyta važiuojant
	Netinkamai užbaigtas paskutinis kortelės naudojimo seansas
	Greičio viršijimas
	Maitinimo nutrūkimas
	Duomenų apie judėjimą klaida
	Transporto priemonės judėjimo nesuderinamumas
	Apsaugos pažeidimas
	Laiko koregavimas (dirbtuvėse)
	Greičio viršijimo kontrolė

Triktys

	Kortelės triktis (vairuotojo kortelės lizdas)
	Kortelės triktis (vairuotojo porininko kortelės lizdas)
	Ekrano triktis
	Duomenų perkėlimo triktis
	Spausdintuvo triktis
	Jutiklio triktis
	Transporto priemonės bloko vidinė triktis
	GNSS triktis
	Nuotolinio aptikimo triktis

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 blokus arba įrašų identifikatorius, nurodyti 4 priedėlyje.

▼B

4 priedėlis

SPAUDINIAI

TURINYS

1. BENDRA INFORMACIJA

2. DUOMENŲ BLOKŲ SPECIFIKACIJA

3. SPAUDINIO SPECIFIKACIJOS

3.1. Vairuotojo veiklos kasdienis spaudinys iš kortelės

3.2. Vairuotojo veiklos kasdienis spaudinys iš transporto priemonės bloko

3.3. Įvykių ir trikčių spaudinys iš kortelės

3.4. Įvykių ir trikčių spaudinys iš transporto priemonės bloko

3.5. Techninių duomenų spaudinys

3.6. Greičio viršijimo spaudinys

3.7. Įstatytų kortelių žurnalas

1. BENDRA INFORMACIJA

Kiekvienas spaudinys sudaromas susiejant įvairius duomenų blokus, kurie gali būti pažymėti bloko identifikatoriais.

Duomenų bloke yra vienas ar keli įrašai, kurie gali būti pažymėti įrašų identifikatoriais.

PRT_001 Kai prieš pat įrašo identifikatorių yra bloko identifikatorius, įrašo identifikatorius nespausdinamas.

PRT_002 Jeigu duomenų vienetas nėra žinomas arba neturi būti spausdinamas dėl priežasčių, susijusių su prieigos prie duomenų teisėmis, vietoj jo paliekama tuščia vieta.

PRT_003 Jei nežinomas visos eilutės turinys arba jo nereikia spausdinti, tuomet praleidžiama visa eilutė.

PRT_004 Skaitmeniniai duomenų laukeliai spausdinami sulygiuoti prie dešiniojo krašto, atskiriant tūkstančius bei milijonus tarpeliu ir nerašant priekyje nulių.

PRT_005 Sekų duomenų laukeliai spausdinami sulygiuoti prie kairiojo krašto ir papildomi tarpeliais iki duomenų vieneto ilgio arba (kai reikia) sutrumpinami iki duomenų vieneto ilgio (pavardės, pavadinimai ir adresai).

PRT_006 Jei ilgo teksto eilutė perkeliama, naujos eilutės pradžioje turėtų būti spausdinamas specialus ženklas (taškas ties eilutės aukščio viduriu, „•“).

2. DUOMENŲ BLOKŲ SPECIFIKACIJA

Šiame skyriuje naudotos tokios formato sąlyginio žymėjimo priemonės:

— **paryškintu šriftu** išspausdinti rašmenys reiškia spausdinamą paprastą tekstą (tekstas spausdinamas įprastu šriftu),

▼B

— įprastu šriftu išspausdinti rašmenys žymi kintamuosius (piktogramas arba duomenis), vietoj kurių spausdinamos jų vertės,

— greta kintamųjų pavadinimų esanti linija rodo galimą duomenų vieneto ilgį,

— datos pateikiamos formatu „dd/mm/yyyy“ (diena, mėnuo, metai). Galima naudoti ir formatą „dd.mm.yyyy“,

— terminas „kortelės identifikacija“ reiškia: kortelių piktogramų deriniu pavaizduotą kortelės rūšį, kortelę išdavusios valstybės narės kodą, įžambaus brūkšnio rašmenį ir kortelės numerį su pakeitimo indeksu bei atnaujinimo indeksu, tarp kurių yra tarpelis:

P	■	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Kortelės piktogramų deriniai		Kortelę išdavusios valstybės narės kodas				Pirmieji 14 kortelės numerio ženklų (gali būti su numeracijos indeksu)														Pakeitimo indeksas		Atnaujinimo indeksas

▼B

PRT_007 Spaudiniuose naudojami tokie duomenų blokai ir (arba) duomenų įrašai, kurių reikšmės ir formatai yra tokie:

Bloko arba įrašo numeris Reikšmė	Duomenų formatas
1 ***Dokumento spausdinimo data ir laikas***	▼ dd/mm/yyyy hh:mm **(UTC)**
2 ***Spaudinio rūšis*** Bloko identifikatorius Spaudinio piktogramų derinys (žr. 3 priedėlį), greičio ribotuvo nuostatis (tik greičio viršijimo spaudinyje)	----------▼---------- Picto xxx **km/h**
3 ***Kortelės turėtojo identifikacija*** Bloko identifikatorius. P = žmonių piktograma Kortelės turėtojo pavardė Kortelės turėtojo vardas (-ai) (jei yra) Kortelės identifikacija Kortelės galiojimo pabaigos data (jei yra) ir Kortelės kartos numeris (GEN 1 arba GEN 2) (*)	----------P---------- P Last_Name_____ First_Name_____ Card_Identification_____ dd/mm/yyyy - GEN 2

Jei kortelė yra neasmeninė ir joje neįrašyta kortelės turėtojo pavardė, vietoj jos spausdinamas įmonės, dirbtuvių arba kontrolės institucijos pavadinimas.

(*) Kortelės kartos numerį gali išspausdinti tik išmanusis tachografas.

4 ***Transporto priemonės identifikacija*** Bloko identifikatorius Transporto priemonės identifikavimo numeris Transporto priemonę užregistravusi valstybė narė ir transporto priemonės registracijos numeris	----------🚙---------- 🚙 VIN_____ Nat/VRN_____
5 ***Transporto priemonės bloko identifikacija*** Bloko identifikatorius Transporto priemonės bloko gamintojo pavadinimas Transporto priemonės bloko komponento šifras Transporto priemonės bloko kartos numeris (*)	----------⊟---------- ⊟ VU_Manufacturer_____ VU_Part_Number__ GEN 2

(*) Kortelės kartos numerį gali išspausdinti tik išmanusis tachografas.

6 ***Vėliausias tachografo kalibravimas*** Bloko identifikatorius Dirbtuvių pavadinimas Dirbtuvių kortelės identifikacija Kalibravimo data	----------T---------- T Last_Name_____ Card_Identification_____ T dd/mm/yyyy

▼B

7 ***Vėliausia kontrolė (atlikta kontrolės pareigūno)***

Bloko identifikatorius
Kontrolieriaus kortelės identifikacija
Kontrolės data, laikas ir rūšis

```
----------▫----------
Card_Identification_____
▫ dd/mm/yyyy hh:mm ppppp
```

Kontrolės rūšis: iki penkių piktogramų. Kontrolės rūšį gali nurodyti tokios piktogramos (jų deriniai):

▪: duomenų perkėlimas iš kortelės, ↧: duomenų perkėlimas iš transporto priemonės bloko, ▼: spausdinimas, ▫: rodymas ekrane, ⊺: Kalibravimo tikrinimas kelyje

8 ***Kortelės atmintyje laikoma informacija apie vairuotojo veiklą chronologine tvarka***

Bloko identifikatorius
Pareikalavimo data (kalendorinė diena, kurios duomenys spausdinami) + kortelės buvimo per dieną skaitiklis

```
----------⊡----------
    dd/mm/yyyy  xxx
```

8 a *Nekontroliuojamo laikotarpio būsena šios dienos pradžioje* (palikti tuščia, jei nepasirinkta nekontroliuojamo laikotarpio būsena)

```
----------OUT----------
```

8.1 *Laikotarpis, kuriuo kortelė nebuvo įstatyta*

8.1a Įrašo identifikatorius (laikotarpio pradžia)
8.1b *Nežinomas laikotarpis*. Pradžios laikas, trukmė
8.1c *Rankiniu būdu įvesti veiklos duomenys*.
Veiklos rūšies piktograma, pradžios laikas, trukmė

```
  --------------------
?       hh:mm hhhmm
A       hh:mm hhhmm
```

8.2 *Kortelės įstatymas į lizdą S*

Įrašo identifikatorius S = lizdo piktograma
Transporto priemonę užregistravusi valstybė narė ir transporto priemonės registracijos numeris.
Transporto priemonės odometro rodmens vertė įstatant kortelę

```
  ---------S---------
▲ Nat/VRN__________

  x xxx xxx km
```

8.3 *Veikla (kol kortelė buvo įstatyta)*

Veiklos rūšies piktograma, pradžios laikas, trukmė, įgulos būsena (jei ĮGULA – įgulos piktograma, jei VIENAS VAIRUOTOJAS – tuščia)

```
A       hh:mm hhhmm ⊡⊡
```

8.3 a *Ypatinga būsena* Įrašo laikas, ypatingos būsenos piktograma (arba jų derinys).

```
        hh:mm ---pppp---
```

8.4 *Kortelės išėmimas*

Transporto priemonės odometro rodmens vertė ir nuo paskutinio kortelės įstatymo, kurio metu žinoma odometro rodmens vertė, nuvažiuotas atstumas.

```
  x xxx xxx km; x xxx km
```

9 ***Transporto priemonės bloko atmintyje chronologine tvarka laikoma (kiekvieno lizdo) informacija apie vairuotojo veiklą***

Bloko identifikatorius
Pareikalavimo data (kalendorinė diena, kurios duomenys spausdinami)
Transporto priemonės odometro rodmens vertė 00.00 val. ir 24.00 val.)

```
----------⊡----------
       dd/mm/yyyy
x xxx xxx - x xxx xxx km
```

10 ***Kortelės lizde S užregistruota veikla***

Bloko identifikatorius

```
----------S----------
```

10 a *Nekontroliuojamo laikotarpio būsena šios dienos pradžioje* (palikti tuščia, jei nepasirinkta nekontroliuojamo laikotarpio būsena)

```
----------OUT----------
```

10.1 *Laikotarpis, kuriuo lizde S nebuvo jokios kortelės*

Įrašo identifikatorius.
Kortelė neįstatyta
Transporto priemonės odometro rodmens vertė laikotarpio pradžioje

```
  --------------------
⊡▪---
  x xxx xxx km
```

10.2 *Kortelės įstatymas*

Kortelės įstatymo įrašo identifikatorius
Vairuotojo pavardė

```
  --------------------
⊡ Last_Name_____________
```

▼B

	Vairuotojo vardas	First_Name_____
	Vairuotojo kortelės identifikacija	Card_Identification_____
	Kortelės galiojimo pabaigos data (jei yra) ir Kortelės kartos numeris (GEN 1 arba GEN 2) (*)	dd/mm/yyyy - GEN 2
	Anksčiau naudotą transporto priemonę užregistravusi valstybė narė valstybė narė ir tos transporto priemonės registracijos numeris	Nat/VRN_____
	Kortelės išėmimo iš ankstesnės transporto priemonės data ir laikas	dd/mm/yyyy hh:mm
	Tuščia eilutė	
	Transporto priemonės odometro rodmens vertė įstatant kortelę, rankomis įvestos informacijos apie vairuotojo veiklą žymuo (jei buvo įvesta – M, jei ne – tuščia). Jei vairuotojo kortelė nebuvo įstatyta tą dieną, kurios spaudinį reikia išspausdinti, tada 10.2 bloke naudojami paskutinio iki tos dienos kortelės įstatymo odometro rodmenys.	x xxx xxx **km** M
10.3	*Veikla*	
	Veiklos rūšies piktograma, pradžios laikas, trukmė, įgulos būsena (jei ĮGULA – įgulos piktograma, jei VIENAS VAIRUOTOJAS – tuščia)	A hh:mm hh**h**mm
10.3 a	*Ypatinga būsena* Įrašo laikas, ypatingos būsenos piktograma (arba jų derinys).	hh:mm ---pppp---
10.4	*Kortelės išėmimas arba laikotarpio „kortelė neįstatyta“ pabaiga*	
	Transporto priemonės odometro rodmens vertė išimant kortelę arba pasibaigus laikotarpiui „kortelė neįstatyta“ ir nuo kortelės įstatymo momento arba nuo laikotarpio „kortelė neįstatyta“ pradžios nuvažiuotas atstumas.	x xxx xxx **km**; x xxx **km**

(*) Kortelės kartos numerį gali išspausdinti tik išmanusis tachografas.

11	***Dienos suvestinė***	
	Bloko identifikatorius	----------Σ----------
11.1	***Laikotarpių, kai vairuotojo kortelės lizde nebuvo kortelės, transporto priemonės bloko suvestinė***	
	Bloko identifikatorius	1 ---
11.2	***Laikotarpių, kai vairuotojo porininko kortelės lizde nebuvo kortelės, transporto priemonės bloko suvestinė***	
	Bloko identifikatorius	2 ---
11.3	***Transporto priemonės bloko dienos suvestinė apie kiekvieną vairuotoją***	
	Įrašo identifikatorius	----------
	Vairuotojo pavardė	Last_Name_____
	Vairuotojo vardas (-ai)	First_Name_____
	Vairuotojo kortelės identifikacija	Card_Identification_____
11.4	*Įrašas apie vietą, kurioje prasideda ir (arba) baigiasi dienos darbo laikotarpis*	
	pi = pradžios (pabaigos) vietos piktograma, laikas, šalis, regionas	pihh:mm Cou Reg
	Odometro rodmens vertė	x xxx xxx **km**
11.5	*Įrašas apie vietą, kurioje prasideda ir (arba) baigiasi dienos darbo laikotarpis*	
	ir po 3 valandų nepertraukiamo vairavimo	hh:mm
	Odometro rodmens vertė	x xxx xxx **km**
11.6	*Veiklos suvestiniai duomenys (iš kortelės)*	
	Bendra vairavimo trukmė, nuvažiuotas atstumas	hh**h**mm x xxx **km**
	Bendra darbo ir parengties dirbti trukmė	hh**h**mm hh**h**mm
	Bendra poilsio ir nežinomų laikotarpių trukmė	hh**h**mm hh**h**mm
	Bendra įgulos veiklos trukmė	hh**h**mm
11.7	*Veiklos suvestiniai duomenys (laikotarpiai, kai vairuotojo kortelės lizde nebuvo kortelės)*	
	Bendra vairavimo trukmė, nuvažiuotas atstumas	hh**h**mm x xxx **km**
	Bendra darbo ir parengties dirbti trukmė	hh**h**mm hh**h**mm
	Bendra poilsio trukmė	hh**h**mm

▼B

11.8	*Veiklos suvestiniai duomenys (laikotarpiai, kai vairuotojo porininko kortelės lizde nebuvo kortelės)*	
	Bendra darbo ir parengties dirbti trukmė	* hhhmm ⧈ hhhmm
	Bendra poilsio trukmė	⊢ hhhmm
11.9	*Veiklos suvestiniai duomenys (vieno vairuotojo; abu kortelės lizdai)*	
	Bendra vairavimo trukmė, nuvažiuotas atstumas	⊙ hhhmm x xxx km
	Bendra darbo ir parengties dirbti trukmė	* hhhmm ⧈ hhhmm
	Bendra poilsio trukmė	⊢ hhhmm
	Bendra įgulos veiklos trukmė	⊙⊙ hhhmm

Kai reikia išspausdinti kasdienį spaudinį apie esamą dieną, suvestiniai duomenys apskaičiuojami pagal tuo metu turimą informaciją.

12	***Kortelės atmintyje laikoma informacija apie įvykius ir (arba) triktis***	
12.1	5 paskutinių „įvykių ir trikčių“ iš kortelės bloko identifikatorius	----------!×▪----------
12.2	Visų užregistruotų kortelėje „įvykių“ bloko identifikatorius	----------!▪----------
12.3	Visų užregistruotų kortelėje „trikčių“ bloko identifikatorius	----------×▪----------
12.4	*Įvykio ir (arba) trikties įrašas*	
	Įrašo identifikatorius	----------
	Įvykio (trikties) piktograma, įrašo tikslas, pradžios data ir laikas	Pic (p) dd/mm/yyyy hh:mm
	Papildomas įvykio (trikties) kodas (jei yra), trukmė	!xx hhhmm
	Transporto priemonę, kurioje įvyko įvykis arba triktis, užregistravusi valstybė narė ir transporto priemonės registracijos numeris	Nat/VRN_____

13	***Transporto priemonės bloko atmintyje laikoma informacija apie įvykius ir triktis arba jame vykstantys įvykiai ir triktys***	
13.1	Bloko identifikatorius paskutiniai 5 „įvykiai ir triktys“ iš transporto priemonės bloko	----------!×▟----------
13.2	Visų užregistruotų arba vykstančių transporto priemonės bloke „įvykių“ bloko identifikatorius	----------!▟----------
13.3	Visų užregistruotų arba vykstančių transporto priemonės bloke „trikčių“ bloko identifikatorius	----------×▟----------
13.4	*Įvyko ir (arba) trikties įrašas*	
	Įrašo identifikatorius	----------
	Įvykio (trikties) piktograma, įrašo tikslas, pradžios data ir laikas	Pic (p) dd/mm/yyyy hh:mm
	Papildomas įvykio (trikties) kodas (jei yra), panašių įvykių tą dieną skaičius, trukmė	!xx (xxx) hhhmm
	Įvykio arba trikties pradžios arba pabaigos momentu įstatytų kortelių identifikacija (iki 4 eilučių, dukart nekartojant vienos kortelės numerio)	Card_Identification_____ Card_Identification_____ Card_Identification_____ Card_Identification_____
	Atvejis, kai kortelė nebuvo įstatyta	▪---
	Gamintojo duomenys	< Literal><ErrorCode>

Įrašo paskirtis (p) – skaitinis kodas, kuriuo paaiškinama, kodėl įvykis arba triktis buvo užregistruoti. Koduojama pagal duomenų elementą `EventFaultRecordPurpose`.

`Literal` yra tachografo gamintojo literalas su ne daugiau kaip 12 ženklų.

`ErrorCode` yra tachografo gamintojo klaidos kodas su ne daugiau kaip 12 ženklų.

▼B

14	***Transporto priemonės bloko identifikacija***	
	Bloko identifikatorius	----------⊟----------
	Transporto priemonės bloko gamintojo pavadinimas	⊟ Name_____
	Transporto priemonės bloko gamintojo adresas	Address_____
	Transporto priemonės bloko komponento šifras	PartNumber_____
	Transporto priemonės bloko patvirtinimo numeris	Apprv_____
	Transporto priemonės bloko serijos numeris	S/N_____
	Transporto priemonės bloko pagaminimo metai	yyyy
	Transporto priemonės bloko programinės įrangos versija ir įdiegimo data	V xxxx dd/mm/yyyy
15	***Jutiklio identifikacija***	
	Bloko identifikatorius	----------⅄----------
15.1	*Siejimo įrašas*	
	Jutiklio serijos numeris	⅄ S/N_____
	Jutiklio patvirtinimo numeris	Apprv_____
	Jutiklio susiejimo data	dd/mm/yyyy hh:mm
16	***GNSS identifikacija***	
	Bloko identifikatorius	----------▚----------
16.1	*Sujungimo įrašas*	
	Išorinio GNSS įrenginio serijos numeris	▚ S/N_____
	Išorinio GNSS įrenginio patvirtinimo numeris	Apprv_____
	Išorinio GNSS įrenginio sujungimo data	dd/mm/yyyy hh:mm
17	***Kalibravimo duomenys***	
	Bloko identifikatorius	----------⊤----------
17.1	*Įrašas apie kalibravimą*	
	Įrašo identifikatorius	----------
	Kalibravimą atlikusios dirbtuvės	⊤ Workshop_name_____
	Dirbtuvių adresas	Workshop_address_____
	Dirbtuvių kortelės identifikacija	Card_Identification_____
	Dirbtuvių kortelės galiojimo pabaigos data	dd/mm/yyyy
	Tuščia eilutė	
	Kalibravimo data + kalibravimo tikslas	⊤ dd/mm/yyyy (p)
	Transporto priemonės identifikavimo numeris	⅄ VIN_____
	Transporto priemonę užregistravusi valstybė narė ir transporto priemonės registracijos numeris	Nat/VRN_____
	Transporto priemonės būdingasis koeficientas	w xx xxx Imp/km
	Tachografo konstanta	k xx xxx Imp/km
	Effective circumference of wheel tyres	l xx xxx mm
	Sumontuotų padangų dydis	● TyreSize_____
	Greičio ribotuvo nuostatis	› xxx km/h
	Senoji ir naujoji odometro rodmens vertės	x xxx xxx – x xxx xxx km

Kalibravimo paskirtis (p) – skaitinis kodas, kuriuo paaiškinama, kodėl užregistruoti šie kalibravimo parametrai. Koduojama pagal duomenų elementą `CalibrationPurpose`.

▼B

18	***Laiko koregavimas***	
	Bloko identifikatorius	----------◷----------
18.1	*Laiko koregavimo įrašas*	
	Įrašo identifikatorius	----------
	Senoji data ir laikas	!◷ dd/mm/yyyy hh:mm
	Naujoji data ir laikas	◷ dd/mm/yyyy hh:mm
	Laiko koregavimą atlikusios dirbtuvės	T Workshop_name_____
	Dirbtuvių adresas	Workshop_address_____
	Dirbtuvių kortelės identifikacija	Card_Identification_____
	Dirbtuvių kortelės galiojimo pabaigos data	dd/mm/yyyy

19	***Paskutinis transporto priemonės bloko atmintyje įrašytas įvykis ir triktis***	
	Bloko identifikatorius	----------!×Д----------
	Naujausio įvykio data ir laikas	! dd/mm/yyyy hh:mm
	Naujausios trikties data ir laikas	× dd/mm/yyyy hh:mm

20	***Greičio viršijimo kontrolės informacija***	
	Bloko identifikatorius	----------»»----------
	Paskutinės GREIČIO VIRŠIJIMO KONTROLĖS data ir laikas	»◘dd/mm/yyyy hh:mm
	Pirmojo greičio viršijimo data / laikas ir po jo buvusių greičio viršijimo įvykių skaičius	»»dd/mm/yyyy hh:mm (nnn)

21	***Greičio viršijimo įrašas***	
21.1	Bloko identifikatorius „Pirmasis greičio viršijimas po paskutinio kalibravimo“	--------»»T---------
21.2	Bloko identifikatorius „5 svarbiausi įvykiai per pastarąsias 365 dienas“	-------»»(365)------
21.3	Bloko identifikatorius „Svarbiausias įvykis per kiekvienas pastarąsias 10 dienų“	-------»»(10)-------
21.4	Įrašo identifikatorius	----------
	Data, taikas ir trukmė	»»dd/mm/yyyy hh:mm hhhmm
	Didžiausias ir vidutinis greitis, panašių įvykių skaičius šią dieną	xxx km/h xxx km/h(xxx)
	Vairuotojo pavardė	◙ Last_Name_____
	Vairuotojo vardas (-ai)	First_Name_____
	Vairuotojo kortelės identifikacija	Card_Identification_____
21.5	Jei bloke nėra greičio viršijimo įrašo	»»---

22	***Ranka įrašyta informacija***	
	Bloko identifikatorius	----------
22.1	Kontrolės vieta	◘• .....
22.2	Kontrolieriaus parašas	◘ .....
22.3	Nuo kada	◷+ .....
22.4	Iki kada	+◷ .....
22.5	Vairuotojo parašas	◙ .....

„Ranka įrašyta informacija“; Virš ranka įrašyto teksto palikti tiek tuščių eilučių, kad būtų iš tiesų įmanoma įrašyti būtiną tekstą arba liktų vietos parašui.

▼B

23 ***Naujausios į transporto priemonės bloką įstatytos kortelės***

Bloko identifikatorius

23.1 Įstatyta kortelė

Įrašo identifikatorius

Kortelės tipas, karta, versija, gamintojas (*)

Kortelės identifikacija

Kortelės serijos numeris

Naujausio kortelės įstatymo data ir laikas

```
-------- ▯▮◔ --------


----
↑ <gen> <version> <MC>
Card Identification
Card Serial Number
dd/mm/yyyy hh:mm
```

(*) (viskas vienoje eilutėje)

su

type of card piktograma, vienas ženklas + tarpelis

gen 1-oji ar 2-oji karta, 4 ženklai + tarpelis

version iki 10 ženklų

MC gamintojo kodas, 3 ženklai

3. SPAUDINIO SPECIFIKACIJOS

Šiame skyriuje naudojamas sutartinis žymėjimas:

N	Išspausdinti bloką arba įrašą N.
N	Išspausdinti bloką arba įrašą N tiek kartų, kiek reikia.
X/Y	Išspausdinti reikiamus blokus arba įrašus X ir (arba) Y tiek kartų, kiek reikia.

3.1. **Vairuotojo veiklos kasdienis spaudinys iš kortelės**

PRT_008 Vairuotojo veiklos kasdienis spaudinys iš kortelės turi būti tokio formato:

1	Dokumento spausdinimo data ir laikas
2	Spaudinio rūšis
3	Kontrolieriaus identifikacija (jei į transporto priemonės bloką įstatyta kontrolės kortelė)
3	Vairuotojo identifikacija (iš kortelės, iš kurios spausdinama, + karta)
4	Transporto priemonės identifikacija (transporto priemonė, iš kurios spausdinami duomenys)
5	Transporto priemonės bloko identifikacija (transporto priemonės blokas, iš kurio spausdinami duomenys, + karta)
6	Šio transporto priemonės bloko paskutinis kalibravimas
7	Paskutinė tikrinamo vairuotojo kontrolė
8	Vairuotojo veiklos skirtukas
8 a	Būsena nekontroliuojama šios dienos pradžioje
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Vairuotojo veikla chronologine tvarka
11	Dienos suvestinės skirtukas

▼B

11.4	Įvestos vietos chronologine tvarka
11.5	GNSS duomenys
11.6	Veiklos suvestinės
12.1	Įvykių arba trikčių iš kortelės skirtukas
12.4	Įvykių / trikčių įrašai (5 paskutiniai įvykiai arba triktys, laikomi kortelėje)
13.1	Įvykių arba trikčių iš transporto priemonės bloko skirtukas
13.4	Įvykių / trikčių įrašai (5 paskutiniai įvykiai arba triktys, laikomi arba vykstantys transporto priemonės bloke)
22.1	Kontrolės vieta
22.2	Kontrolieriaus parašas
22.5	Vairuotojo parašas

3.2. **Vairuotojo veiklos kasdienis spaudinys iš transporto priemonės bloko**

PRT_009 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 transporto priemonės bloką įstatytų kortelių + karta)
4	Transporto priemonės identifikacija (transporto priemonė, iš kurios spausdinami duomenys)
5	Transporto priemonės bloko identifikacija (transporto priemonės blokas, iš kurio spausdinami duomenys, + karta)
6	Šio transporto priemonės bloko paskutinis kalibravimas
7	Paskutinė šio tachografo kontrolė
9	Vairuotojo veiklos skirtukas
10	Vairuotojo kortelės lizdo skirtukas (1 lizdas)
10 a	Būsena nekontroliuojama šios dienos pradžioje
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Veikla chronologine tvarka (vairuotojo kortelės lizdas)
10	Vairuotojo porininko kortelės lizdo skirtukas (2 lizdas)
10 a	Būsena nekontroliuojama šios dienos pradžioje
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Veikla chronologine tvarka (vairuotojo porininko kortelės lizdas)
11	Dienos suvestinės skirtukas
11.1	Laikotarpių, kai vairuotojo kortelės lizde nebuvo kortelės, suvestinė
11.4	Įvestos vietos chronologine tvarka
11.5	GNSS duomenys

▼B

11.6	Veiklos suvestinės
11.2	Laikotarpių, kai vairuotojo porininko kortelės lizde nebuvo kortelės, suvestinė
11.4	Įvestos vietos chronologine tvarka
11.5	GNSS duomenys
11.7	Veiklos suvestinės
11.3	Vairuotojo veiklos pagal abu kortelės lizdus suvestinė
11.4	Vairuotojo įvestos vietos chronologine tvarka
11.5	GNSS duomenys
11.8	Vairuotojo veiklos suvestinė
13.1	Įvykių arba trikčių skirtukas
12.4	Įvykių / trikčių įrašai (5 paskutiniai įvykiai arba triktys, laikomi arba vykstantys transporto priemonės bloke)
13.1	Kontrolės vieta
22.2	Kontrolieriaus parašas
22.3	Nuo kada (vieta, kurioje kortelės neturintis vairuotojas gali nurodyti, kurie laikotarpiai yra susiję su juo)
22.4	Iki kada
22.5	Vairuotojo parašas

3.3. **Įvykių ir trikčių spaudinys iš kortelės**

PRT_010 Įvykių ir trikčių spaudinys iš kortelės turi būti tokio formato:

1	Dokumento spausdinimo data ir laikas
2	Spaudinio rūšis
3	Kontrolieriaus identifikacija (jei į transporto priemonės bloką įstatyta kontrolės kortelė + karta)
3	Vairuotojo identifikacija (iš spaudinio kortelės)
4	Transporto priemonės identifikacija (transporto priemonė, iš kurios spausdinami duomenys)
12.2	Įvykių skirtukas
12.4	Įvykių įrašai (visi kortelėje laikomi įvykiai)
12.3	Trikčių skirtukas
12.4	Trikčių įrašai (visos kortelėje laikomos triktys)
22.1	Kontrolės vieta
22.2	Kontrolieriaus parašas
22.5	Vairuotojo parašas

▼B

3.4. **Įvykių ir trikčių spaudinys iš transporto priemonės bloko**

PRT_011 Įvykių ir trikčių spaudinys iš transporto priemonės bloko turi būti tokio formato:

1	Dokumento spausdinimo data ir laikas
2	Spaudinio rūšis
3	Kortelės turėtojo identifikacija (visų į transporto priemonės bloką įstatytų kortelių + karta)
4	Transporto priemonės identifikacija (transporto priemonė, iš kurios spausdinami duomenys)
13.2	Įvykių skirtukas
13.4	Įvykių įrašai (visi transporto priemonės bloke laikomi arba vykstantys įvykiai)
13.3	Trikčių skirtukas
13.4	Trikčių įrašai (visos transporto priemonės bloke laikomos arba vykstančios triktys)
22.1	Kontrolės vieta
22.2	Kontrolieriaus parašas
22.5	Vairuotojo parašas

3.5. **Techninių duomenų spaudinys**

PRT_012 Techninių duomenų spaudinys turi būti tokio formato:

1	Dokumento spausdinimo data ir laikas
2	Spaudinio rūšis
3	Kortelės turėtojo identifikacija (visų į transporto priemonės bloką įstatytų kortelių + karta)
4	Transporto priemonės identifikacija (transporto priemonė, iš kurios spausdinami duomenys)
14	Transporto priemonės bloko identifikacija
15	Jutiklio identifikacija
15.1	Jutiklio susiejimo duomenys (visi turimi duomenys chronologine tvarka)
16	GNSS identifikacija
16.1	Išorinio GNSS įrenginio sujungimo duomenys (visi turimi duomenys chronologine tvarka)
17	Kalibravimo datos skirtukas
17.1	Įrašai apie kalibravimą (visi turimi įrašai chronologine tvarka)
18	Laiko koregavimo skirtukas
18.1	Laiko koregavimo įrašai (visi turimi įrašai iš duomenų apie laiko koregavimą ir kalibravimą)
19	Paskutinis transporto priemonės bloko atmintyje įrašytas įvykis ir triktis

▼B

3.6. **Greičio viršijimo spaudinys**

PRT_013 Greičio viršijimo spaudinys turi būti tokio formato:

1	Dokumento spausdinimo data ir laikas
2	Spaudinio rūšis
3	Kortelės turėtojo identifikacija (visų į transporto priemonės bloką įstatytų kortelių + karta)
4	Transporto priemonės identifikacija (transporto priemonė, iš kurios spausdinami duomenys)
20	Greičio viršijimo kontrolės informacija
21.1	Greičio viršijimo datos identifikatorius
21.4 / 21.5	Pirmasis greičio viršijimas po paskutinio kalibravimo
21.2	Greičio viršijimo datos identifikatorius
21.4 / 21.5	5 svarbiausi greičio viršijimai per pastarąsias 365 dienas
21.3	Greičio viršijimo datos identifikatorius
21.4 / 21.5	Svarbiausias greičio viršijimas kiekvieną iš paskutinių 10 dienų
22.1	Kontrolės vieta
22.2	Kontrolieriaus parašas
22.5	Vairuotojo parašas

3.7. **Įstatytų kortelių žurnalas**

PRT_014 Įstatytų kortelių žurnalo spaudinys turi būti tokio formato:

1	Dokumento spausdinimo data ir laikas
2	Spaudinio rūšis
3	Kortelės turėtojo identifikacija (visų į transporto priemonės bloką įstatytų kortelių)
23	Naujausia į transporto priemonės bloką įstatyta kortelė
23.1	Įstatytos kortelės (iki 88 įrašų)
12.3	Trikčių skirtukas

▼B

5 priedėlis

RODINYS

Šiame priedėlyje naudotos tokios formato sąlyginio žymėjimo priemonės:

— **paryškintu šriftu** išspausdinti rašmenys reiškia spausdinamą paprastą tekstą (rodomas tekstas spausdinamas įprastu šriftu),

— įprastu šriftu išspausdinti rašmenys žymi kintamuosius (piktogramas arba duomenis), vietoj kurių rodomos jų vertės:

  — dd mm yyyy: diena, mėnuo, metai,

  — hh: valandos,

  — mm: minutės,

  — D: trukmės piktograma,

  — EF: įvykių arba trikčių piktogramų derinys,

  — O: veikimo režimo piktograma.

DIS_001 Tachografas turi rodyti duomenis tokiais formatais:

Duomenys	Formatas
Numatytasis rodinys	
Vietos laikas	hh:mm
Veikimo režimas	O
Su vairuotoju susijusi informacija	1 Dhh**h**mm ▮▮hh**h**mm
Su vairuotojo porininku susijusi informacija	2 Dhh**h**mm
Prasidėjo nekontroliuojamo laikotarpio būsena	OUT
Įspėjamasis rodinys	
Viršyta nepertraukiamo vairavimo trukmė	1 ⊙ hh**h**mm ▮▮hh**h**mm
Įvykis arba triktis	EF
Kiti rodiniai	
UTC data laikas	UTC ⊙ dd/mm/yyyy arba UTC ⊙ dd.mm.yyyy hh:mm
Vairuotojo nepertraukiamo vairavimo trukmė ir bendroji poilsio trukmė	1 ⊙ hh**h**mm ▮▮hh**h**mm
Vairuotojo porininko nepertraukiamo vairavimo trukmė ir bendroji poilsio trukmė	2 ⊙ hh**h**mm ▮▮hh**h**mm
Ankstesnės ir esamos savaitės vairuotojo bendroji vairavimo trukmė	1 ⊙ ▮ hhh**h**mm
Ankstesnės ir esamos savaitės vairuotojo porininko bendroji vairavimo trukmė	2 ⊙ ▮ hhh**h**mm

▼B

6 priedėlis

PRIEKINĖ KALIBRAVIMO IR DUOMENŲ PERKĖLIMO JUNGTIS

TURINYS

1. TECHNINĖ ĮRANGA

1.1. Jungtis

1.2. Kontaktų paskirstymas

1.3. Schema

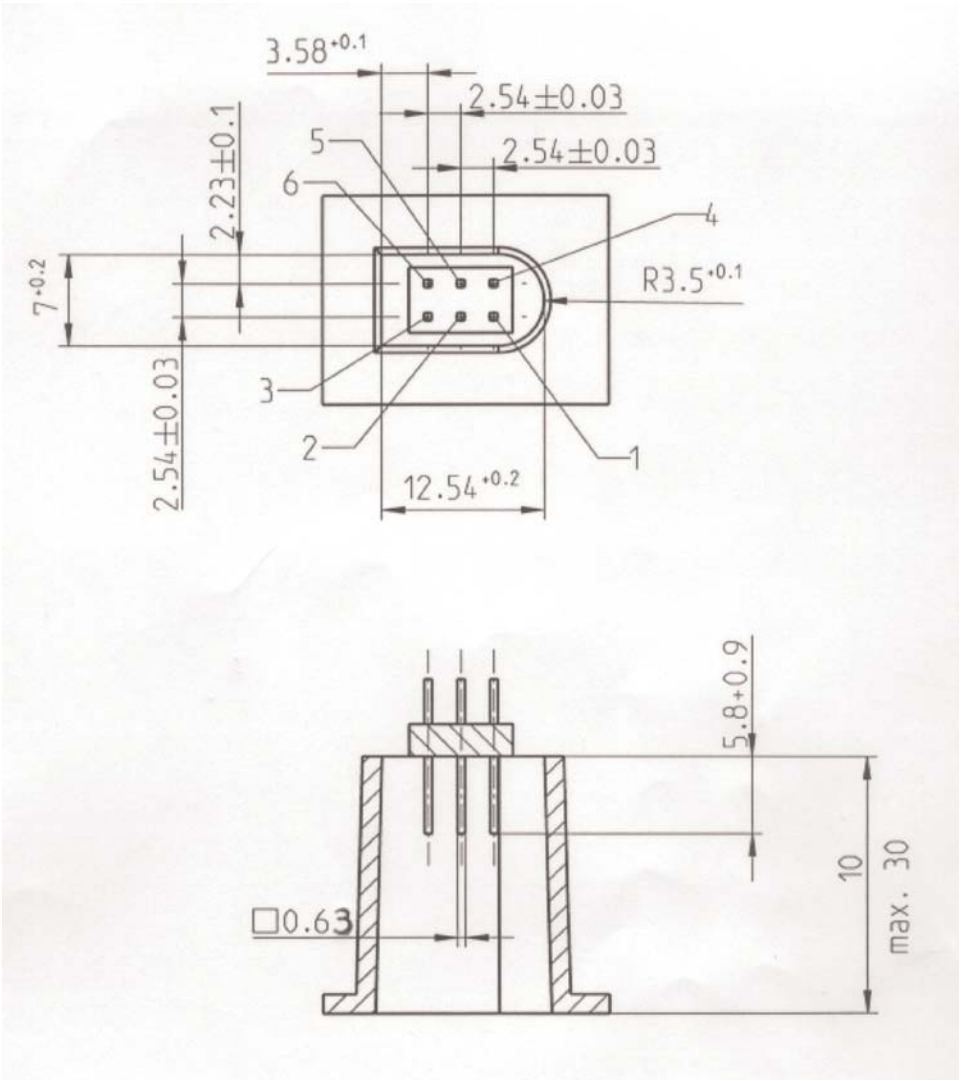
2. DUOMENŲ PERKĖLIMO SĄSAJA

3. KALIBRAVIMO SĄSAJA

1. TECHNINĖ ĮRANGA

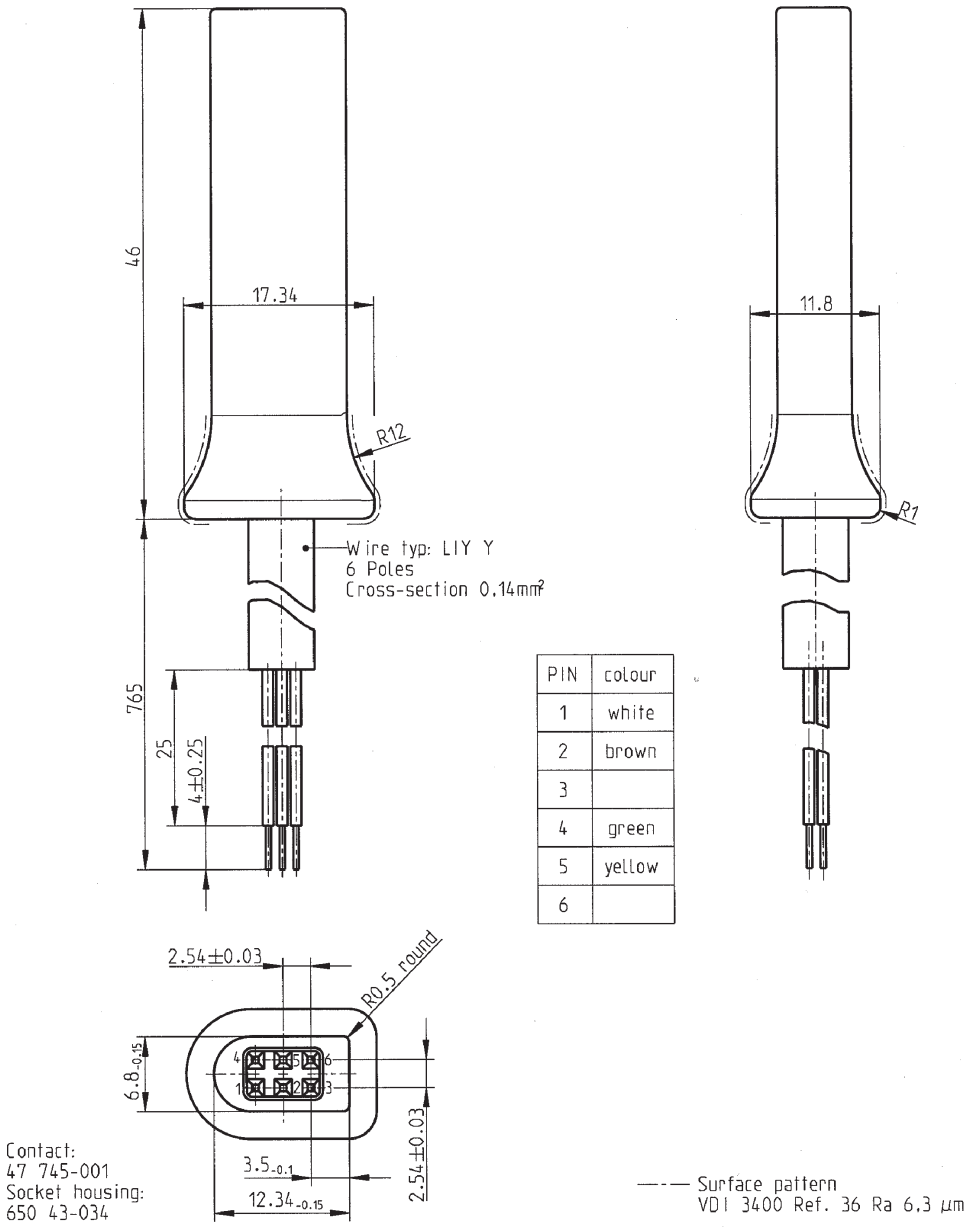
1.1. **Jungtis**

INT_001 Duomenų perkėlimo / kalibravimo jungtis turi būti 6 kontaktų, prieinama priekinėje plokštelėje neatjungiant nė vienos tachografo dalies ir atitinkanti toliau pateiktą brėžinį (visi matmenys nurodyti milimetrais):



▼B

Šiame brėžinyje pavaizduotas standartinis 6 kontaktų kištukas:



1.2. **Kontaktų paskirstymas**

INT_002 Kontaktai turi būti paskirstyti taip, kaip nurodyta lentelėje:

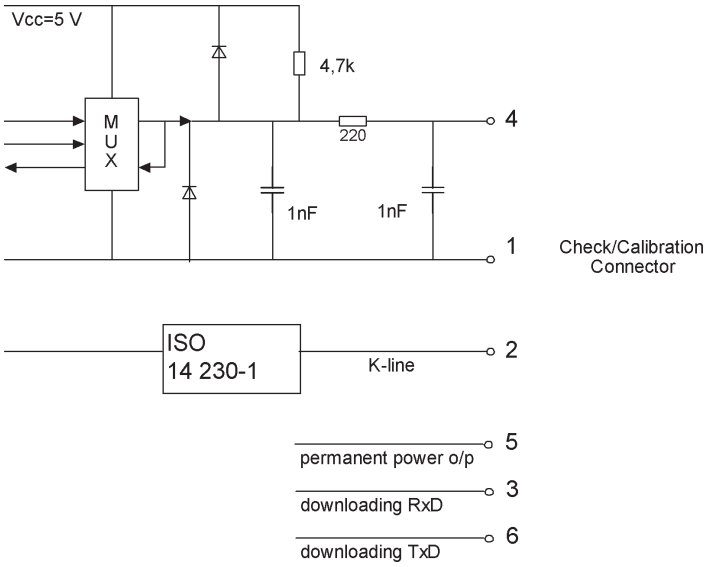
Kontaktas	Aprašymas	Pastaba
1	Akumuliatoriaus neigiamas polius	Sujungtas su transporto priemonės akumuliatoriaus neigiamu poliumi
2	Duomenų perdavimas	K linija (ISO 14230-1)
3	RxD – duomenų perkėlimas	Duomenų įvedimas į tachografą
4	Įvesties / išvesties signalas	Kalibravimas

▼B

Kontaktas	Aprašymas	Pastaba
5	Nuolatinio maitinimo išėjimas	Įtampa turi būti lygi transporto priemonės įtampai, sumažintai 3 V, įvertinant įtampos kritimą apsauginiame grandyne. Išėjimo srovė 40 mA
6	TxD – Duomenų perkėlimas	Tachografo išvesties duomenys

1.3. **Schema**

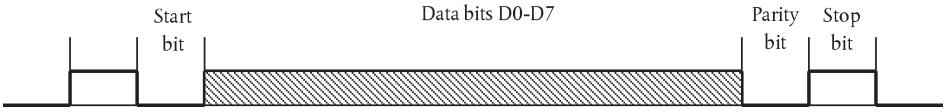
INT_003 Schema turi būti tokia:



2. DUOMENŲ PERKĖLIMO SĄSAJA

INT_004 Duomenų perkėlimo sąsaja turi atitikti specifikacijas 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: vienas loginio lygio 1 bitas.

Kai siunčiami skaitmeniniai duomenys, kuriuos sudaro daugiau kaip vienas baitas, reikšmingiausias baitas siunčiamas pirmiausia, o mažiausiai reikšmingas – paskiausia.

INT_006 Siuntimo spartą turi būti galima reguliuoti nuo 9 600 bps iki 115 200 bps. Turi būti siunčiama pačia didžiausia įmanoma sparta, o užmezgus ryšį nustatoma 9 600 bps pradinė sparta.

▼B

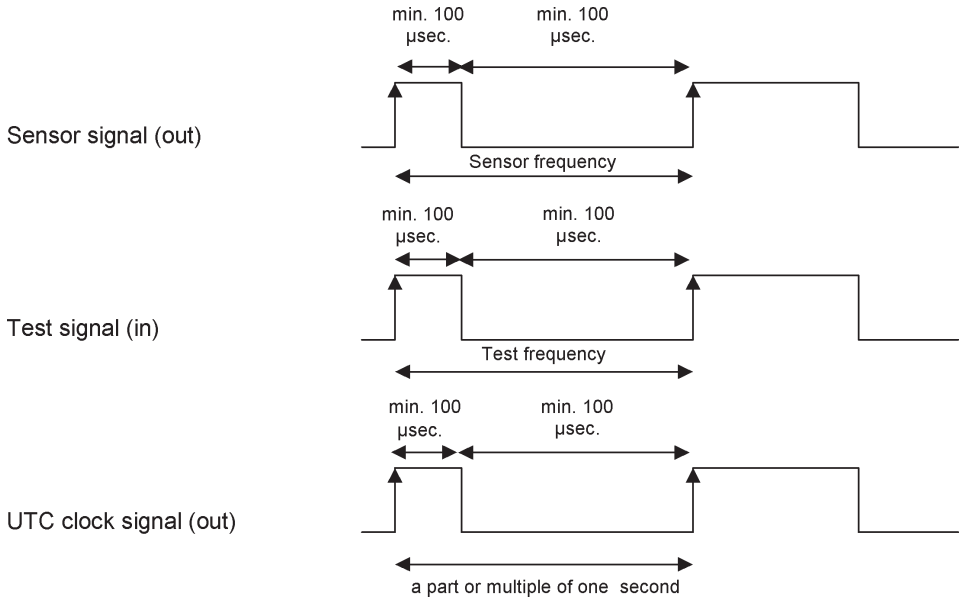
3. Kalibravimo sąsaja

INT_007 Duomenys turi būti perduodami pagal ISO 14 230-1 „Kelių transporto priemonės. Diagnostikos sistemos. Raktažodžių protokolas 2000. 1 dalis. Fizinis lygmuo“, 1999 m.

INT_008 Įvesties / išvesties signalas turi atitikti tokią elektrinę specifikaciją:

Parametras	Mažiausia vertė	Įprasta vertė	Didžiausia vertė	Pastaba
U_{low} (in)			1,0 V	I = 750 μA
U_{high} (in)	4 V			I = 200 μA
Dažnis			4 kHz	
U_{low} (out)			1,0 V	I = 1 mA
U_{high} (out)	4 V			I = 1 mA

INT_009 Įvesties ir išvesties signalas turi atitikti tokią laiko schemą:



▼B

7 priedėlis.

DUOMENŲ PERKĖLIMO PROTOKOLAI

TURINYS

1. ĮVADAS

1.1. Taikymo sritis

1.2. Santrumpos ir žymenys

2. DUOMENŲ PERKĖLIMAS IŠ TRANSPORTO PRIEMONĖS BLOKO

2.1. Duomenų perkėlimo procedūra

2.2. Duomenų perkėlimo protokolas

2.2.1 Pranešimų struktūra

2.2.2 Pranešimų rūšys

2.2.2.1 Start communication request (SID 81)

2.2.2.2 Positive response start communication (SID C1)

2.2.2.3 Start diagnostic session request (SID 10)

2.2.2.4 Positive response start diagnostic (SID 50)

2.2.2.5 Link control service (SID 87)

2.2.2.6 Link control positive response (SID C7)

2.2.2.7 Request upload (SID 35)

2.2.2.8 Positive response request upload (SID 75)

2.2.2.9 Transfer data request (SID 36)

2.2.2.10 Positive Response Transfer Data (SID 76)

2.2.2.11 Request Transfer Exit (SID 37)

2.2.2.12 Positive Response Request Transfer Exit (SID 77)

2.2.2.13 Stop Communication Request (SID 82)

2.2.2.14 Positive Response Stop Communication (SID C2)

2.2.2.15 Acknowledge Sub Message (SID 83)

2.2.2.16 Negative Response (SID 7F)

2.2.3 Pranešimų srautas

2.2.4 Sinchronizavimas

▼B

2.2.5 Klaidų valdymas

2.2.5.1 Ryšio pradžios etapas

2.2.5.2 Ryšio etapas

2.2.6 Atsakymo pranešimo turinys

2.2.6.1 Positive Response Transfer Data Overview

2.2.6.2 Positive Response Transfer Data Activities

2.2.6.3 Positive Response Transfer Data Events and Faults

2.2.6.4 Positive Response Transfer Data Detailed Speed

2.2.6.5 Positive Response Transfer Data Technical Data

2.3. ESM rinkmenų laikymas

3. DUOMENŲ PERKĖLIMO IŠ TACHOGRAFO KORTELIŲ PROTOKOLAS

3.1. Taikymo sritis

3.2. Apibrėžtys

3.3. Duomenų perkėlimas iš kortelės

3.3.1 Inicijavimo seka

3.3.2 Duomenų rinkmenų be parašo seka

3.3.3 Duomenų rinkmenų be parašo seka

3.3.4 Kalibravimo skaitiklio atstatos seka

3.4. Duomenų laikymo formatas

3.4.1 Įvadas

3.4.2 Rinkmenos formatas

4. DUOMENŲ PERKĖLIMAS IŠ TACHOGRAFO KORTELĖS PER TRANSPORTO PRIEMONĖS BLOKĄ

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 transporto priemonės bloku,

— iš tachografo kortelės – IDE, sujungta su kortelių sąsajos įtaisu (IFD),

▼B

— iš tachografo kortelės – per transporto priemonės bloką, IDE, sujungta su transporto priemonės bloku.

Tam, kad būtų galima patikrinti į ESM rašomų perkeltų duomenų autentiškumą ir nepažeistumą, duomenys perkeliami su pridėtu parašu laikantis 11 priedėlio „Bendrieji apsaugos mechanizmai“ nuostatų. Taip pat perkeliami šaltinio įrangos (transporto priemonės bloko arba kortelės) identifikacijos ir saugumo pažymėjimai (valstybės narės ir įrangos). Duomenų tikrintojas turi pats turėti patikimą Europos viešąjį raktą.

DDP_001 Vieno duomenų perkėlimo seanso metu perkelti duomenys turi būti laikomi vienoje pavienėje ESM rinkmenoje.

1.2. **Santrumpos ir žymenys**

Šiame priedėlyje vartojamos santrumpos:

AID – programos identifikatorius

ATR – atsakas į atstatos komandą

CS – kontrolinės sumos baitas

DF – specialioji rinkmena

DS_ – diagnostikos seansas

EF – elementarioji rinkmena

ESM – išorinė laikmena

FID – rinkmenos identifikatorius (rinkmenos ID)

FMT – formato baitas (pirmasis pranešimo antraštės baitas)

ICC – lustinė kortelė

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 parametrų pasirinkimas

PSO – atlikti apsaugos operaciją

SID – paslaugos identifikatorius

SRC – šaltinio baitas

TGT – tikslinis baitas

TLV – žymenos ilgio vertė

TREP – perdavimo atsakymo parametras

TRTP – perdavimo pareikalavimo parametras

VU – transporto priemonės blokas

▼B

2. DUOMENŲ PERKĖLIMAS IŠ TRANSPORTO PRIEMONĖS BLOKO

2.1. **Duomenų perkėlimo procedūra**

Kad perkeltų duomenis iš transporto priemonės bloko, operatorius turi atlikti tokius veiksmus:

— įstatyti savo tachografo kortelę į transporto priemonės bloko (*) kortelės lizdą,

— prijungti IDE prie transporto priemonės bloko duomenų perkėlimo jungties,

— užmegzti ryšį tarp IDE ir transporto priemonės bloko,

— IDE pasirinkti reikiamus perkelti duomenis ir nusiųsti pareikalavimą į transporto priemonės bloką,

— užbaigti duomenų perkėlimo seansą.

2.2. **Duomenų perkėlimo protokolas**

Protokolas sudarytas pagal pagrindinio–pavaldžiojo mazgų schemą, kai IDE atlieka pagrindinio, o transporto priemonės blokas – pavaldžiojo mazgo funkcijas.

Pranešimų struktūra, rūšys ir srautai iš daugiausia remiasi Raktažodžių protokolu 2000 (KWP) (ISO 14230-2 „Kelių transporto priemonės. Diagnostikos sistemos. Raktažodžių protokolas 2000“. 2 dalis. „Duomenų perdavimo kanalo lygmuo“).

Taikomasis lygmuo 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 Visų pranešimų, kuriais keičiasi IDE ir transporto priemonės blokas, struktūra iš trijų dalių:

— antraštė, kurią sudaro formato baitas (FMT), tikslinis baitas (TGT), šaltinio baitas (SRC) ir neprivalomas ilgio baitas (LEN),

— duomenų laukelis, kurį sudaro paslaugos identifikatoriaus 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	DATA	…	…	…	CS
4 baitai				Maks. 255 baitai					1 baitas

TGT ir SRC baitai žymi pranešimo gavėjo ir siuntėjo fizinį adresą. IDE vertės yra F0 Hex, o transporto priemonės bloko – 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.

(*) Įstačius kortelę, suaktyvinamos reikiamos teisės atlikti duomenų perkėlimą ir gauti prieigą prie jų. Vis dėlto turi būti įmanoma duomenis iš vairuotojo kortelės, įstatytos į vieną iš transporto priemonės bloko lizdų, perkelti net jei į kitą lizdą neįstatyta jokia kito tipo kortelė.

▼B

DDP_003 Jei pranešimu reikia persiųsti duomenis, kurių ilgis didesnis už duomenų laukeliui skirtą vietą, pranešimas siunčiamas keliomis dalimis. Kiekvienoje pranešimo dalyje yra antraštė, tas pats SID, TREP ir 2 baitų pranešimo dalių skaitiklis, nurodantis pranešimo dalies eilės numerį visame pranešime. Tam, kad galima būtų tikrinti, ar nėra klaidų ir nutraukti siuntimą, IDE patvirtina kiekvieną pranešimo dalį. IDE gali priimti pranešimo dalį, paprašyti ją pakartoti, pareikalauti, kad transporto priemonės blokas pradėtų ją siųsti iš naujo arba nutrauktų siuntimą.

DDP_004 Jei paskutinės pranešimo dalies duomenų laukelyje yra tiksliai 255 baitai, pranešimo pabaigai nurodyti turi būti išsiųsta galutinė pranešimo dalis su tuščiu duomenų laukeliu (išskyrus SID, TREP ir pranešimo dalių skaitiklį).

Pavyzdys.

Antraštė	SID	TREP	Pranešimas	CS
4 baitai	Daugiau kaip 255 baitai			

Siunčiama taip:

Antraštė	SID	TREP	00	01	1-oji pranešimo dalis	CS
4 baitai	255 baitai					

Antraštė	SID	TREP	00	02	2-oji pranešimo dalis	CS
4 baitai	255 baitai					

…

Antraštė	SID	TREP	xx	yy	n-oji pranešimo dalis	CS
4 baitai	Mažiau kaip 255 baitai					

arba

Antraštė	SID	TREP	00	01	1-oji pranešimo dalis	CS
4 baitai	255 baitai					

Antraštė	SID	TREP	00	02	2-oji pranešimo dalis	CS
4 baitai	255 baitai					

…

Antraštė	SID	TREP	xx	yy	n-oji pranešimo dalis	CS
4 baitai	255 baitai					

Antraštė	SID	TREP	xx	yy + 1	CS
4 baitai	4 baitai				

▼B

2.2.2 *Pranešimų rūšys*

Pagal duomenų perkėlimo iš transporto priemonės bloko ir IDE protokolą reikia naudoti 8 skirtingų rūšių pranešimus.

Šie pranešimai nurodyti toliau esančioje lentelėje.

Pranešimo struktūra	Maks. 4 baitai Antraštė				Maks. 255 baitai Duomenys			1 baitas Kontrolinė suma
IDE -> <- Transporto priemonės blokas	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		EA, 8F	9B
Pareikalavimo pradėti diagnostikos seansą pradžia	80	EE	F0	02	10	81		F1
Teigiamas atsakymas, diagnostikos pradžia	80	F0	EE	02	50	81		31
Ryšio kanalo valdymo paslauga								
Patikrinti perdavimo greitį (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	EE
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	80	EE	F0	04	87		01,01,05	F0
Teigiamas atsakymas, patikrinti perdavimo greitį	80	F0	EE	02	C7		01	28
Sandūros perdavimo greitis (2 etapas)	80	EE	F0	03	87		02,03	ED
Nusiuntimo pareikalavimas	80	EE	F0	0 A	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
Įvykis ir triktis	80	EE	F0	02	36	03		99
Tikslus greitis	80	EE	F0	02	36	04		9 A
Techniniai duomenys	80	EE	F0	02	36	05		9B
Duomenų perkėlimas iš kortelės	80	EE	F0	02	36	06	Kortelės lizdas	CS
Teigiamas atsakymas, persiųsti duomenis	80	F0	EE	Len	76	TREP	Duomenys	CS
Pareikalavimas nutraukti siuntimą	80	EE	F0	01	37			96
Teigiamas atsakymas, nutraukti siuntimą	80	F0	EE	01	77			D6

▼B

Pranešimo struktūra	Maks. 4 baitai Antraštė				Maks. 255 baitai Duomenys			1 baitas Kontrolinė suma
IDE -> <- Transporto priemonės blokas	FMT	TGT –	SRC	LEN	SID	DS_/TRTP	DATA	CS
Pareikalavimas nutraukti ryšį	80	EE	F0	01	82			E1
Teigiamas atsakymas, nutraukti ryšį	80	F0	EE	01	C2			21
Patvirtinti pranešimo dalį	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
Subfunkcija netinkama	80	F0	EE	03	7F	Sid Req	12	CS
Neteisingas 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 neatitinka srities	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.

— Tamsūs langeliai reiškia, kad niekas nesiunčiama.

— Žodis „nusiųsti“ [upload] (IDE atžvilgiu) vartojamas pagal ISO 14229. Jis reiškia tą patį, ką ir perkelti duomenis (transporto priemonės bloko atžvilgiu).

— Šioje lentelėje nepavaizduoti galimi 2 baitų ilgio pranešimo dalių skaitikliai.

— Lizdas yra lizdo numeris (1 – kortelė vairuotojo kortelės lizde arba 2 – kortelė vairuotojo porininko kortelės lizde).

— Jei lizdas nenurodytas, transporto priemonės blokas pasirenka lizdą Nr. 1, jei į jį įstatyta kortelė, o lizdą Nr. 2 pasirenka tik jei būtent jį renkasi naudotojas.

2.2.2.1 Start communication request (SID 81)

DDP_005 Šį pranešimą IDE siunčia norėdama užmegzti ryšį su transporto priemonės bloku. Iš pradžių visuomet bendraujama 9 600 bodų sparta (iki sparta pakeičiama naudojantis atitinkamomis ryšio kanalo valdymo paslaugomis).

▼B

2.2.2.2 Positive response start communication (SID C1)

DDP_006 Šį pranešimą transporto priemonės blokas siunčia kaip teigiamą atsakymą į pareikalavimą pradėti ryšį. Pranešime yra du raktiniai baitai 2 „EA“ ir „8F“, kurie nurodo, kad įrenginiui tinka protokolas su antrašte, kurioje yra informacija apie tikslą, šaltinį ir ilgį.

2.2.2.3 Start diagnostic session request (SID 10)

DDP_007 Pranešimą Start diagnostic session request IDE siunčia naujam diagnostikos seansui su transporto priemonės bloku pradėti. Subfunkcija „default session“ (81 Hex) nurodo, kad reikia pradėti standartinį diagnostikos seansą.

2.2.2.4 Positive response start diagnostic (SID 50)

DDP_008 Teigiamo atsakymo pranešimą Start diagnostic transporto priemonės blokas siunčia kaip teigiamą atsakymą į pareikalavimą pradėti diagnostikos seansą.

2.2.2.5 Link control service (SID 87)

DDP_052 Pranešimą Link control service IDE naudoja duomenų perdavimo greičiui pakeisti. Tai vyksta dviem etapais. Pirmu etapu IDE pasiūlo pakeisti greitį ir nurodo naują greitį. Jei atsakymas iš transporto priemonės bloko teigiamas, IDE siunčia į transporto priemonės bloką greičio pakeitimo patvirtinimą (antrasis etapas). Tuomet IDE pradeda laikytis naujo greičio. Gavęs patvirtinimą, transporto priemonės blokas taip pat pradeda laikytis naujo greičio.

2.2.2.6 Link control positive response (SID C7)

DDP_053 Pranešimą Link control positive response transporto priemonės blokas siunčia kaip teigiamą atsakymą į pareikalavimą suteikti ryšio kanalo valdymo paslaugą (pirmasis etapas). Atkreipkite dėmesį, kad į patvirtinimo pareikalavimą neatsakoma (antrasis etapas).

2.2.2.7 Request upload (SID 35)

DDP_009 Pranešimą Request upload IDE siunčia, kad transporto priemonės blokui praneštų, 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 nešifruojamas ir nearchyvuojamas, o atminties dydis nustatomas didžiausias.

2.2.2.8 Positive response request upload (SID 75)

DDP_010 Pranešimą Positive response request upload transporto priemonės blokas siunčia, kad praneštų IDE apie pasirengimą priimti duomenis. Laikantis ISO 14229 reikalavimų, šiame pranešime yra informacija, nurodanti IDE, kad kituose pranešimuose Positive Response Transfer Data bus ne daugiau kaip 00FF šešioliktainių baitų.

▼B

2.2.2.9 Transfer data request (SID 36)

DDP_011 Pranešimą Transfer data request IDE siunčia, kad transporto priemonės blokui nurodytų 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 triktys (TRTP 03),

— tikslus greitis (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), nes tik taip užtikrinama, kad į atsiųstą rinkmeną bus įrašyti transporto priemonės bloko pažymėjimai (ir galima bus patikrinti skaitmeninį parašą).

Antruoju atveju (TRTP 02) duomenų perdavimo pareikalavimo pranešime nurodoma kalendorinė diena (formatu `TimeReal`), kurios duomenys turi būti perkelti.

2.2.2.10 Positive Response Transfer Data (SID 76)

DDP_012 Pranešimą Positive response transfer data transporto priemonės blokas siunčia atsakydamas į duomenų perdavimo pareikalavimą. Pranešime yra pareikalauti duomenys ir pareikalavimo TRTP atitinkantis perdavimo atsakymo parametras (TREP).

DDP055 Pirmuoju atveju (TREP 01) transporto priemonės blokas siunčia duomenis, padėdamas IDE operatoriui pasirinkti, kokius dar duomenis jis nori perkelti. Šiame pranešime yra tokia informacija:

— saugumo pažymėjimai,

— transporto priemonės identifikacija,

— transporto priemonės bloko esama data ir laikas,

— anksčiausioji ir vėliausioji data, kurių duomenis galima perkelti (transporto priemonės bloko duomenys),

— kortelių buvimo transporto priemonės bloke ženklas,

— ankstesnis duomenų perkėlimas į įmonę,

— įmonės užraktai,

— pirmiau atlikta kontrolė.

▼B

2.2.2.11 Request Transfer Exit (SID 37)

DDP_013 Pranešimą Request transfer exit IDE siunčia, kad transporto priemonės blokui praneštų apie duomenų perkėlimo seanso nutraukimą.

2.2.2.12 Positive Response Request Transfer Exit (SID 77)

DDP_014 Pranešimą Positive response request transfer exit transporto priemonės blokas siunčia pareikalavimui patvirtinti.

2.2.2.13 Stop Communication Request (SID 82)

DDP_015 Pranešimą Stop Communication Request IDE siunčia, kad nutrauktų ryšį su transporto priemonės bloku.

2.2.2.14 Positive Response Stop Communication (SID C2)

DDP_016 Pranešimą Positive Response Stop Communication transporto priemonės blokas siunčia, kad patvirtintų pareikalavimą.

2.2.2.15 Acknowledge Sub Message (SID 83)

DDP_017 Pranešimą Acknowledge Sub Message IDE siunčia, kad patvirtintų kiekvienos pranešimo dalies gavimą, kai pranešimas siunčiamas keliomis dalimis. Duomenų laukelyje yra iš transporto priemonės bloko gautas SID ir 2 baitų kodas:

— MsgC+1 reiškia, kad pranešimo dalis Nr. MsgC gauta tinkamai,

IDE siunčia reikalavimą transporto priemonės blokui atsiųsti kitą pranešimo dalį,

— MsgC reiškia, kad pranešimo dalis Nr. MsgC priimta nesklandžiai,

IDE siunčia reikalavimą transporto priemonės blokui dar kartą atsiųsti pranešimo dalį,

— FFFF reiškia reikalavimą nutraukti pranešimą.

Šį kodą IDE gali naudoti transporto priemonės bloko pranešimo siuntimui nutraukti dėl bet kokios priežasties.

Paskutinė pranešimo dalis (LEN baitas < 255) gali būti patvirtinta naudojant bet kurį iš pirmiau nurodytų kodų arba visai nepatvirtinta.

Transporto priemonės bloko atsakymai, sudaryti iš kelių pranešimo dalių, yra:

— Positive Response Transfer Data (SID 76)

▼B

2.2.2.16 Negative Response (SID 7F)

DDP_018 Neigiamo atsakymo pranešimą transporto priemonės blokas siunčia atsakydamas į pirmiau išvardytus pranešimus, jei transporto priemonės blokas 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 subfunkcija netinkama.

Nesuprantamas pareikalavimo DS_ arba TRTP arba nėra kitų pranešimo dalių, kurias reikia persiųsti;

— 13 neteisingas pranešimo ilgis.

Gauto pranešimo ilgis yra neteisingas;

— 22 netinkamos sąlygos arba pareikalavimo sekos klaida.

Pareikalauta paslauga neaktyvi arba pareikalavimo pranešimų seka yra neteisinga;

— 31 pareikalavimas neatitinka srities.

Pareikalavimo parametro įrašas (duomenų laukelis) negalioja;

— 50 nusiuntimas nepriimtas.

Pareikalavimo negalima patenkinti (transporto priemonės blokas veikia ne tuo režimu arba įvyko vidinė triktis);

— 78 laukiama atsakymo.

Pareikalauto veiksmo negalima užbaigti laiku ir transporto priemonės blokas nepasirengęs priimti kito pareikalavimo;

— FA duomenų negalima gauti.

Transporto priemonės bloke nėra duomenų perdavimo pareikalavimo duomenų objekto (pvz…, neįstatyta kortelė).

2.2.3 *Pranešimų srautas*

Įprastinės duomenų perkėlimo procedūros pranešimų srautas paprastai būna toks:

IDE		VU
Start Communication Request	⇨	
	⇦	Positive Response
Start Diagnostic Service Request	⇨	
	⇦	Positive Response
Request Upload	⇨	
	⇦	Positive Response

▼B

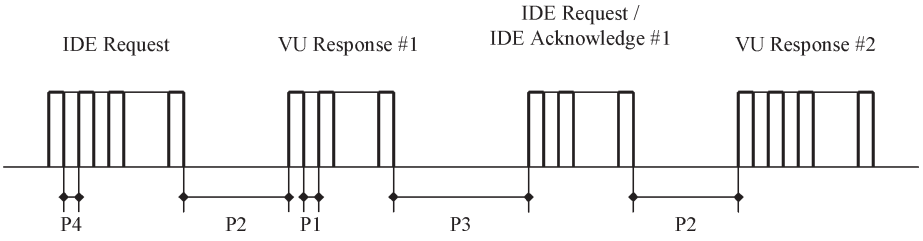
IDE		VU
Transfer Data Request Overview	⇨	
	⇦	Positive Response
Transfer Data Request #2	⇨	
	⇦	Positive Response #1
Acknowledge Sub Message #1	⇨	
	⇦	Positive Response #2
Acknowledge Sub Message #2	⇨	
	⇦	Positive Response #m
Acknowledge Sub Message #m	⇨	
	⇦	Positive Response (Data Field<255 Bytes)
Acknowledge Sub Message (optional)	⇨	
…		
Transfer Data Request #n	⇨	
	⇦	Positive Response
Request Transfer Exit	⇨	
	⇦	Positive Response
Stop Communication Request	⇨	
	⇦	Positive Response

2.2.4 *Sinchronizavimas*

DDP_019 Įprasto veikimo metu naudojami paveiksle pavaizduoti sinchronizavimo parametrai.

1 pav.

Pranešimų srauto sinchronizavimas



Čia:

P1 = laikas tarp baitų transporto priemonės bloko atsakymui.

P2 = laikas tarp IDE pareikalavimo pabaigos ir transporto priemonės bloko atsakymo pradžios arba tarp IDE patvirtinimo pabaigos ir transporto priemonės bloko kito atsakymo pradžios.

P3 = laikas tarp transporto priemonės bloko atsakymo pabaigos ir naujo IDE pareikalavimo pradžios arba tarp transporto priemonės bloko atsakymo pabaigos ir IDE patvirtinimo pradžios arba tarp IDE pareikalavimo pabaigos ir naujo IDE pareikalavimo pradžios (jei transporto priemonės blokas neatsako).

P4 = laikas tarp baitų IDE pareikalavimui.

P5 = pailginta P3 trukmė duomenų perkėlimui iš kortelės.

▼B

Sinchronizavimo parametrų leidžiamosios vertės pateiktos toliau esančioje lentelėje (KWP išplėstasis sinchronizavimo parametrų rinkinys, naudojamas fizinio adresavimo atveju spartesniam ryšiui).

Sinchronizavimas Parametras	Apatinė riba Vertė (ms)	Viršutinė riba Vertė (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minučių

(*) jei transporto priemonės blokas pateikia neigiamą atsakymą su kodu, kurio reikšmė „pareikalavimas gautas, laukiama atsakymo“, ši vertė didinama iki tos pačios P3 viršutinės ribos.

2.2.5 *Klaidų valdymas*

Jei keičiantis pranešimais įvyksta klaida, pranešimų srauto schema pakeičiama atsižvelgiant į tai, kurioje įrangoje aptikta klaida, ir į pranešimą, dėl kurio atsirado klaida.

2 ir 3 paveiksluose pavaizduotos atitinkamai transporto priemonės bloko 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 IDE laukia P3min laikotarpį ir pakartoja pareikalavimą.

DDP_021 Jei transporto priemonės blokas aptinka klaidą iš IDE atėjusioje sekoje, jis nesiunčia atsakymo ir P3max laikotarpį laukia kito pareikalavimo pradėti ryšį.

2.2.5.2 Ryšio etapas

Yra dvi klaidų valdymo sritys.

1. **Transporto priemonės blokas aptinka IDE siuntimo klaidą.**

DDP_022 Transporto priemonės blokas 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).

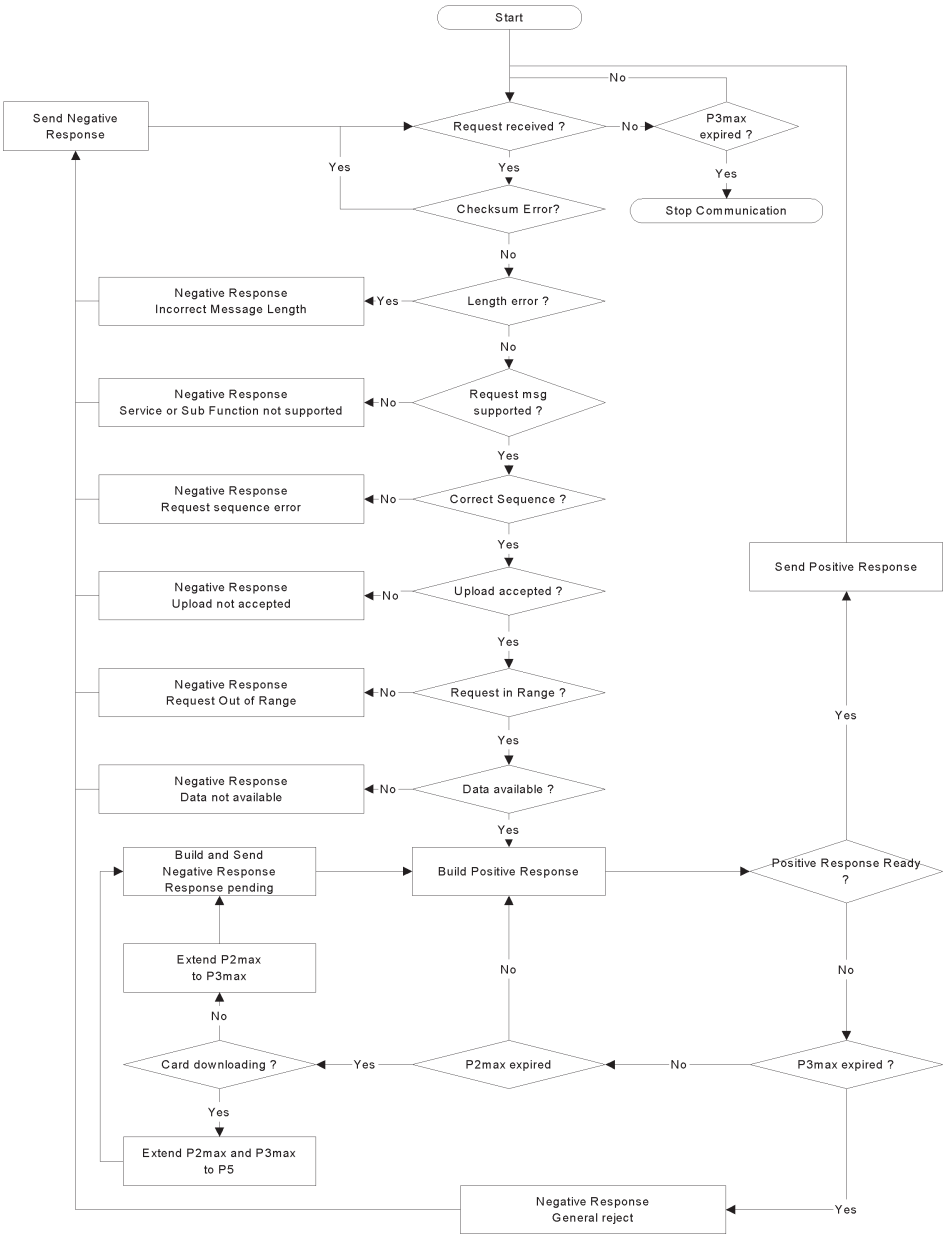
DDP_023 Jei transporto priemonės blokas aptinka vieną iš pirmiau išvardytų klaidų, jis nesiunčia atsakymo ir ignoruoja priimtą pranešimą.

DDP_024 Transporto priemonės blokas gali aptikti ir kitas gauto pranešimo formato arba turinio klaidas (pvz., pranešimas netinkamas) net jei pranešimas atitinka ilgio ir kontrolinės sumos reikalavimus; tokiu atveju transporto priemonės blokas atsako neigiamo atsakymo pranešimu ir nurodo klaidos pobūdį.

▼B

2 pav.

Transporto priemonės bloko klaidų valdymas



2. **IDE aptinka transporto priemonės bloko 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 pranešimo dalių skaitiklio kitimą vienas po kito gautuose pranešimuose.

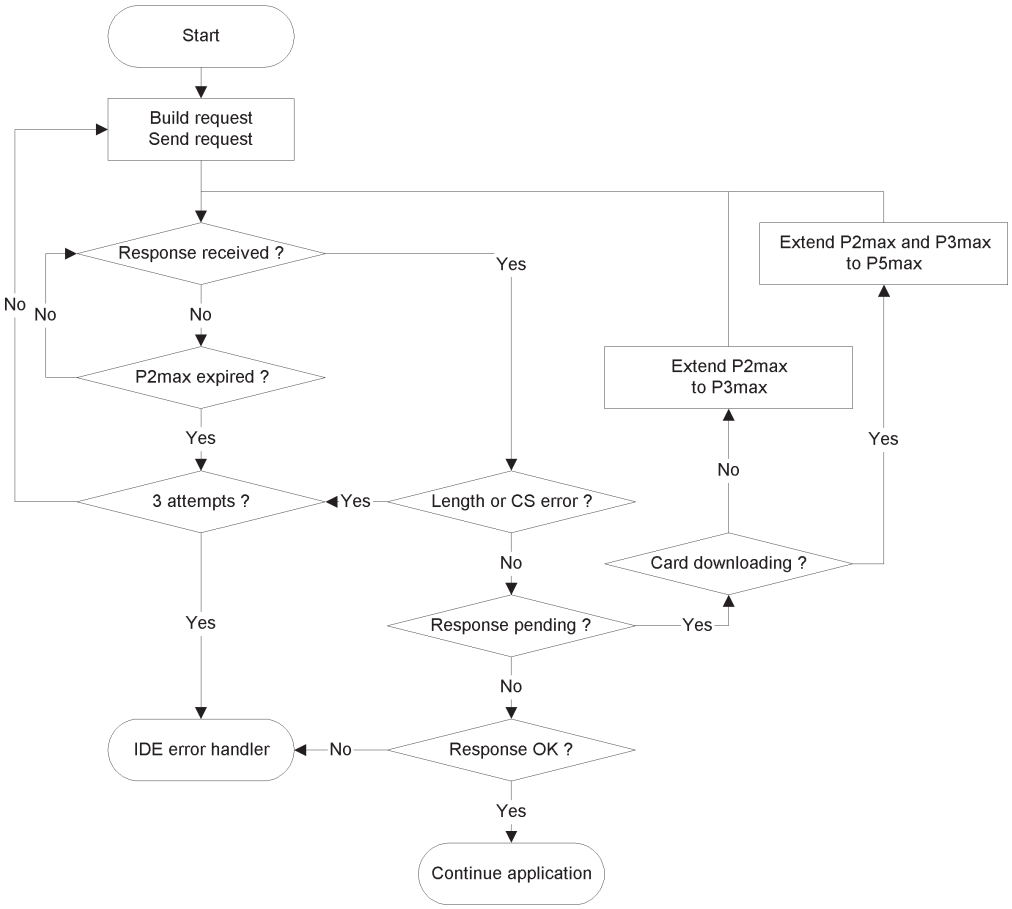
DDP_027 Jei IDE aptinka klaidą arba transporto priemonės blokas neatsako per laikotarpį P2max, pareikalavimo pranešimas siunčiamas pakartotiniai (iš viso ne daugiau kaip tris kartus). Kad būtų galima aptikti šią klaidą, pranešimo dalies patvirtinimas yra pareikalavimas transporto priemonės blokui.

▼B

DDP_028 Prieš naują siuntimą IDE turi palaukti ne trumpiau kaip laikotarpį P3min; laukimo laikotarpis skaičiuojamas nuo paskutinio apskaičiuoto pabaigos bito pasirodymo aptikus klaidą.

3 pav.

IDE klaidų valdymas



2.2.6 *Atsakymo pranešimo turinys*

Šiame punkte aprašytas įvairių teigiamo atsakymo pranešimų duomenų laukelių turinys.

Duomenų elementų apibrėžtys pateiktos 1 priedėlyje „Duomenų žinynas“.

Pastaba. 2-osios kartos parsisiuntimui taikomas reikalavimas – kiekvienas aukščiausio lygio duomenų elementas pateikiamas kaip įrašų masyvas, net jei jame yra tik vienas įrašas. Įrašų masyvas prasideda nuo antraštės; antraštėje nurodomas įrašo tipas, įrašo dydis ir įrašų skaičius. Šiose lentelėse įrašų masyvai (su antraštėmis) pažymėti priedėlių „…RecordArray“.

2.2.6.1 Positive Response Transfer Data Overview

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 pranešimo dalis:

▼B

1-osios kartos duomenų struktūra

Duomenų elementas	Pastaba
MemberStateCertificate VUCertificate	Transporto priemonės bloko saugumo pažymėjimai
VehicleIdentificationNumber VehicleRegistrationIdentification	Transporto priemonės identifikacija
CurrentDateTime	Transporto priemonės bloko esama data ir laikas
VuDownloadablePeriod	Laikotarpis, kurio duomenis galima perkelti
CardSlotsStatus	Į transporto priemonės bloką įstatytų kortelių rūšis
VuDownloadActivityData	Ankstesnis transporto priemonės bloko duomenų perkėlimas
VuCompanyLocksData	Visi laikomi įmonės užraktai. Jei skirsnis tuščias, siunčiama tik noOfLocks = 0.
VuControlActivityData	Visi transporto priemonės bloke laikomi kontrolės įrašai. Jei skirsnis tuščias, siunčiama tik noOfControls = 0.
Signature	Visų duomenų (išskyrus pažymėjimus), pradedant nuo VehicleIdentificationNumber iki paskutinio VuControlActivityData paskutinio baito, RSA parašas.

2-osios kartos duomenų struktūra

Duomenų elementas	Pastaba
MemberStateCertificateRecordArray	Valstybės narės pažymėjimas
VUCertificateRecordArray	Transporto priemonės bloko pažymėjimas
VehicleIdentificationNumberRecordArray	Transporto priemonės identifikacija
VehicleRegistrationNumberRecordArray	Transporto priemonės registracijos numeris
CurrentDateTimeRecordArray	Transporto priemonės bloko esama data ir laikas
VuDownloadablePeriodRecordArray	Laikotarpis, kurio duomenis galima perkelti
CardSlotsStatusRecordArray	Į transporto priemonės bloką įstatytų kortelių rūšis
VuDownloadActivityDataRecordArray	Ankstesnis transporto priemonės bloko duomenų perkėlimas
VuCompanyLocksRecordArray	Visi laikomi įmonės užraktai. Jei skirsnis tuščias, siunčiama tik masyvo antraštė su noOfRecords = 0.
VuControlActivityRecordArray	Visi transporto priemonės bloke laikomi kontrolės įrašai. Jei skirsnis tuščias, siunčiama tik masyvo antraštė su noOfRecords = 0.
SignatureRecordArray	Visų ankstesnių duomenų, išskyrus pažymėjimus, ECC parašas.

2.2.6.2 Positive Response Transfer Data Activities

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 pranešimo dalis:

▼B

1-osios kartos duomenų struktūra

Duomenų elementas	Pastaba
TimeReal	Perkeltų dienos duomenų data
OdometerValueMidnight	Odometras dienos, kurios duomenys perkelti, pabaigoje
VuCardIWData	Kortelių įstatymo ir išėmimo ciklų duomenys. — Jei šiame skirsnyje duomenų nėra, siunčiama tik noOfVuCardIWRecords = 0. — Jei duomenų elementas VuCardIWRecord viršija 00:00 (kortelė įstatyta ankstesnę dieną) arba 24:00 (kortelė išimta kitą dieną), jis rodomas visas per dvi susijusias dienas.
VuActivityDailyData	Kortelės lizdo būsena 00:00 ir veiklos pokyčiai, užregistruoti dieną, kurios duomenys perkelti.
VuPlaceDailyWorkPeriodData	Su vietomis susiję duomenys, užregistruoti dieną, kurios duomenys perkelti. Jei skirsnis tuščias, siunčiama tik noOfPlaceRecords = 0.
VuSpecificConditionData	Duomenys apie ypatingas būsenas, užregistruoti dieną, kurios duomenys perkelti. Jei skirsnis tuščias, siunčiama tik noOfSpecificConditionRecords = 0.
Signature	Visų duomenų, pradedant nuo TimeReal iki paskutinio ypatingos būsenos įrašo paskutinio baito, RSA parašas.

2-osios kartos duomenų struktūra

Duomenų elementas	Pastaba
DateOfDayDownloadedRecordArray	Perkeltų dienos duomenų data
OdometerValueMidnightRecordArray	Odometras dienos, kurios duomenys perkelti, pabaigoje
VuCardIWRecordArray	Kortelių įstatymo ir išėmimo ciklų duomenys. — Jei skirsnyje nėra duomenų, siunčiama tik masyvo antraštė su noOfRecords = 0. — Jei duomenų elementas VuCardIWRecord viršija 00:00 (kortelė įstatyta ankstesnę dieną) arba 24:00 (kortelė išimta kitą dieną), jis rodomas visas per dvi susijusias dienas.
VuActivityDailyRecordArray	Kortelės lizdo būsena 00:00 ir veiklos pokyčiai, užregistruoti dieną, kurios duomenys perkelti.
VuPlaceDailyWorkPeriodRecordArray	Su vietomis susiję duomenys, užregistruoti dieną, kurios duomenys perkelti. Jei skirsnis tuščias, siunčiama tik masyvo antraštė su noOfRecords = 0.
VuGNSSCDRecordArray	Transporto priemonės buvimo vietos pagal GNSS, jei vairuotojo nepertraukiamo vairavimo trukmė pasiekia trijų valandų kartotinį. Jei skirsnis tuščias, siunčiama tik masyvo antraštė su noOfRecords = 0.
VuSpecificConditionRecordArray	Duomenys apie ypatingas būsenas, užregistruoti dieną, kurios duomenys perkelti. Jei skirsnis tuščias, siunčiama tik masyvo antraštė su noOfRecords = 0.
SignatureRecordArray	Visų ankstesnių duomenų ECC parašas.

▼B

2.2.6.3 Positive Response Transfer Data Events and Faults

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 pranešimo dalis.

1-osios kartos duomenų struktūra

Duomenų elementas	Pastaba
VuFaultData	Visos transporto priemonės bloke laikomos arba vykstančios triktys. Jei skirsnis tuščias, siunčiama tik noOfVuFaults = 0.
VuEventData	Visi (išskyrus greičio viršijimą) transporto priemonės bloke laikomi arba vykstantys įvykiai. Jei skirsnis tuščias, siunčiama tik noOfVuEvents = 0.
VuOverSpeedingControlData	Su paskutine greičio viršijimo kontrole susiję duomenys (numatytoji reikšmė, jei duomenų nėra)
VuOverSpeedingEventData	Visi transporto priemonės bloke laikomi greičio viršijimo įvykiai. Jei skirsnis tuščias, siunčiama tik noOfVuOverSpeedingEvents = 0.
VuTimeAdjustmentData	Visi transporto priemonės bloke laikomi laiko koregavimo įvykiai (nepriskiriami prie visiško kalibravimo). Jei skirsnis tuščias, siunčiama tik noOfVuTimeAdjRecords = 0.
Signature	Visų duomenų, pradedant nuo noOfVuFaults iki paskutinio laiko koregavimo įrašo paskutinio baito, RSA parašas.

2-osios kartos duomenų struktūra

Duomenų elementas	Pastaba
VuFaultRecordArray	Visos transporto priemonės bloke laikomos arba vykstančios triktys. Jei skirsnis tuščias, siunčiama tik masyvo antraštė su noOfRecords = 0.
VuEventRecordArray	Visi (išskyrus greičio viršijimą) transporto priemonės bloke laikomi arba vykstantys įvykiai. Jei skirsnis tuščias, siunčiama tik masyvo antraštė su noOfRecords = 0.
VuOverSpeedingControlDataRecordArray	Su paskutine greičio viršijimo kontrole susiję duomenys (numatytoji reikšmė, jei duomenų nėra)
VuOverSpeedingEventRecordArray	Visi transporto priemonės bloke laikomi greičio viršijimo įvykiai. Jei skirsnis tuščias, siunčiama tik masyvo antraštė su noOfRecords = 0.
VuTimeAdjustmentRecordArray	Visi transporto priemonės bloke laikomi laiko koregavimo įvykiai (nepriskiriami prie visiško kalibravimo). Jei skirsnis tuščias, siunčiama tik masyvo antraštė su noOfRecords = 0.
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	Visų ankstesnių duomenų ECC parašas.

▼B

2.2.6.4 Positive Response Transfer Data Detailed Speed

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 pranešimo dalis.

1-osios kartos duomenų struktūra

Duomenų elementas	Pastaba
VuDetailedSpeedData	Visi tikslaus greičio duomenys, laikomi transporto priemonės bloke (vienas greičio blokas per minutę, kurią transporto priemonė važiavo). 60 greičio verčių per minutę (viena per sekundę).
Signature	Visų duomenų, pradedant nuo noOfSpeedBlocks iki paskutinio greičio bloko paskutinio baito, RSA parašas.

2-osios kartos duomenų struktūra

Duomenų elementas	Pastaba
VuDetailedSpeedBlockRecordArray	Visi tikslaus greičio duomenys, laikomi transporto priemonės bloke (vienas greičio blokas per minutę, kurią transporto priemonė važiavo). 60 greičio verčių per minutę (viena per sekundę).
SignatureRecordArray	Visų ankstesnių duomenų ECC parašas.

2.2.6.5 Positive Response Transfer Data Technical Data

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 pranešimo dalis.

1-osios kartos duomenų struktūra

Duomenų elementas	Pastaba
VuIdentification	
SensorPaired	
VuCalibrationData	Visi transporto priemonės bloke laikomi įrašai apie kalibravimą.
Signature	Visų duomenų, pradedant nuo vuManufacturerName iki paskutinio VuCalibrationRecord paskutinio baito, RSA parašas.

▼B

2-osios kartos duomenų struktūra

Duomenų elementas	Pastaba
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Visi transporto priemonės bloke laikomi judesio jutiklių susiejimo įrašai.
VuSensorExternalGNSSCoupledRecordArray	Visi transporto priemonės bloke laikomi išorinio GNSS įrenginio sujungimo įrašai.
VuCalibrationRecordArray	Visi transporto priemonės bloke laikomi įrašai apie kalibravimą.
VuCardRecordArray	Visi transporto priemonės bloke laikomi kortelės įstatymo duomenys.
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	Visų ankstesnių duomenų ECC parašas.

2.3. **ESM rinkmenų laikymas**

DDP_034 Kai duomenų perkėlimo seanse perduodami duomenys iš transporto priemonės bloko, IDE turi įrašyti vienoje pavienėje fizinėje rinkmenoje visus per duomenų perkėlimo seansą pranešimuose Positive Response Transfer Data iš transporto priemonės bloko gautus duomenis. Neįrašomos tik pranešimų antraštės, pranešimo dalių skaitikliai, tuščios pranešimo dalys ir kontrolinės sumos, tačiau įrašomi SID ir TREP (jei yra kelios pranešimų dalys – tik pirmosios pranešimo dalies).

3. DUOMENŲ PERKĖLIMO IŠ TACHOGRAFO KORTELIŲ PROTOKOLAS

3.1. **Taikymo sritis**

Šiame skyriuje aprašyta, kaip duomenys tiesiogiai perkeliami iš tachografo kortelės į IDE. IDE nėra apsaugos aplinkos dalis, todėl tarp kortelės ir IDE autentiškumas netikrinamas.

3.2. **Apibrėžtys**

Duomenų perkėlimo seansas. Laikas, kai iš ICC perkeliami duomenys. Seansas aprėpia visą procedūrą nuo ICC perkrovimo, kurį atlieka IFD, iki ICC pasyvinimo (kortelės ištraukimo arba kitos atstatos).

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 perkeliami tokiais etapais:

— bendra kortelės informacija perkeliama į EF ICCir IC. Ši informacija yra neprivaloma, ji neapsaugota skaitmeniniu parašu;

▼B

— perkeliami EF Card_Certificate (arba CardSignCertificate) ir CA_Certificate. Ši informacija neapsaugota skaitmeniniu parašu;

kiekvieną duomenų perkėlimo seansą privaloma perkelti šias rinkmenas;

— perkeliamos kitų programos duomenų rinkmenos EF (Tachograph DF ir Tachograph_G2 DF, jei reikia) išskyrus EF Card_Download. Ši informacija apsaugota skaitmeniniu parašu;

— kiekvieną duomenų perkėlimo seansą privaloma perkelti EF Application_Identificationir ID;

— perkeliant duomenis iš vairuotojo kortelės taip pat privaloma perkelti šiuos EF:

- Events_Data,
- Faults_Data,
- Driver_Activity_Data,
- Vehicles_Used,
- Places,
- GNSS_Places (if relevant),
- Control_Activity_Data,
- Specific_Conditions.

— perkeliant duomenis iš vairuotojo kortelės, atnaujinama EF LastCardDownload esanti data Card_Download;

— perkeliant duomenis iš dirbtuvių kortelės, atstatoma EF Card_Download esančio kalibravimo skaitiklio pradinė būsena;

— perkeliant duomenis iš dirbtuvių kortelės, neperkeliama EF Sensor_Installation_Data.

3.3.1 *Inicijavimo seka*

DDP_036 IDE turi inicijuoti seką taip:

Kortelė	Kryptis	IDE/IFD	Reikšmė/pastabos
	⇦	Techninės įrangos atstata	
ATR	⇨		

Galima naudoti PPS didesniam perdavimo greičiui pasirinkti, jei ji yra tinkama ICC.

3.3.2 *Duomenų rinkmenų be parašo seka*

DDP_037 EF ICC, IC, Card_Certificate (arba CardSignCertificate) ir CA_Certificate duomenų perkėlimo seka yra tokia:

Kortelė	Kryptis	IDE/IFD	Reikšmė/pastabos
	⇦	**Select File**	Pasirenkama rinkmena pagal identifikatorių
OK	⇨		

▼B

Kortelė	Kryptis	IDE/IFD	Reikšmė/pastabos
	⇦	**Nuskaityti dvejetainį**	Jei rinkmenoje yra daugiau duomenų, nei telpa skaitytuvo arba kortelės buferyje, komanda kartojama tol, kol nuskaitomi visi duomenys.
File Data OK	⇨	Įrašyti duomenis į ESM	pagal **3.4** Data storage format

1 pastaba. prieš pasirenkant EF Card_Certificate (arba Card-SignCertificate) reikia pasirinkti tachografo programą (pasirenkama pagal AID).

2 pastaba. Pasirinkti ir perskaityti rinkmeną galima vienu etapu, pasinaudojus komanda Read Binary su trumpuoju rinkmenos EF identifikatoriumi.

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	Dir	IDE/IFD	Reikšmė/pastabos
	⇦	**Select File**	
OK	⇨		
	⇦	**Perform Hash of File**	Pagal nustatytą maišos algoritmą (11 priedėlis) apskaičiuojama pasirinktos rinkmenos duomenų maišos vertė. Ši komanda nenumatyta pagal ISO.
Apskaičiuojama rinkmenos maiša ir laikinai įrašoma į atmintį maišos vertė			
OK	⇨		
	⇦	**Nuskaityti dvejetainį**	Jei rinkmenoje yra daugiau duomenų, nei telpa skaitytuvo arba kortelės buferyje, komanda kartojama tol, kol nuskaitomi visi duomenys.
File Data OK	⇨	Įrašomi duomenys į ESM	pagal **3.4** Data storage format

▼B

Kortelė	Dir	IDE/IFD	Reikšmė/pastabos
	⇦	**PSO: Compute Digital Signature**	
Atliekama apsaugos operacija „Compute Digital Signature“ panaudojant laikinai saugomą maišos vertę.			
Signature OK	⇨	Prirašomi duomenys prie anksčiau į ESM įrašytų duomenų	pagal **3.4** Data storage format

Pastaba. Pasirinkti ir perskaityti rinkmeną galima vienu etapu, pasinaudojus komanda Read Binary su trumpuoju rinkmenos EF identifikatoriumi. Šiuo atveju galima rinkmeną EF pasirinkti ir perskaityti pirmiau nei vykdoma komanda Perform Hash of File.

3.3.4 *Kalibravimo skaitiklio atstatos seka*

DDP_039 Dirbtuvių kortelės `Card_Download` skaitiklio `NoOfCalibrationsSinceDownload` atstatos seka yra tokia:

Kortelė	Dir	IDE/IFD	Reikšmė/pastabos
	⇦	**Select File** EF Card_ Download	Pasirenkama rinkmena pagal identifikatorių
OK	⇨		
	⇦	**Atnaujinti dvejetainį** NoOfCalibrationsSinceDownload = ‘00 00’	
Atstatoma duomenų perkėlimo iš kortelės skaitiklio pradinė būsena			
OK	⇨		

Pastaba. Pasirinkti ir atnaujinti rinkmeną galima vienu etapu, pasinaudojus komanda Update Binary su trumpuoju rinkmenos EF identifikatoriumi.

3.4. **Duomenų laikymo formatas**

3.4.1 *Įvadas*

DDP_040 Perkelti duomenys turi būti įrašomi pagal tokius reikalavimus:

— duomenys turi būti įrašomi skaidriai. 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 iš kortelės perkelti duomenys įrašomi vienoje ESM rinkmenoje.

▼B

3.4.2 *Rinkmenos formatas*

DDP_041 Rinkmenų formatas yra keleto TLV objektų junginys.

DDP_042 EF žymena yra FID ir prierašas „00“.

DDP_043 EF parašo žymena yra FID ir prierašas „01“.

DDP_044 Ilgis yra dviejų baitų vertė. Ši vertė apibrėžia baitų skaičių verčių laukelyje. Vertė „FF FF“ ilgio laukelyje yra rezervuota panaudoti vėliau.

DDP_045 Kai duomenys iš rinkmenos neperkeliami, į atmintį neturi būti įrašoma jokia su ja susijusi informacija (jokios žymenos ir jokio nulinio ilgio).

DDP_046 Parašas turi būti įrašomas kaip TLV objektas, esantis iškart po TLV objekto, kuriame yra rinkmenos duomenys.

Apibrėžtis	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 perkeltoje 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 duomenys Vehicles_Used
05 05 01	00 80	EF parašas Vehicles_Used

4. DUOMENŲ PERKĖLIMAS IŠ TACHOGRAFO KORTELĖS PER TRANSPORTO PRIEMONĖS BLOKĄ

DDP_047 Transporto priemonės blokas turi leisti perkelti duomenis iš vairuotojo kortelės, įkištos į prijungtą IDE.

DDP_048 IDE turi išsiųsti į transporto priemonės bloką 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 dalyje nustatytą protokolą transporto priemonės blokas 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 data.

▼B

DDP_050 IDE turi išrinkti kortelės duomenis iš pranešimo Positive Response Transfer Data (pašalindama visas antraštes, SID, TREP, pranešimo dalių skaitiklius ir kontrolines sumas) ir įrašyti juos į vieną fizinę rinkmeną, kaip aprašyta 2.3 poskyryje.

DDP_051 Tuomet transporto priemonės blokas turi atnaujinti vairuotojo kortelės rinkmenas `Control_Activity_Data` arba `Card_Download`.

▼B

8 priedėlis

KALIBRAVIMO PROTOKOLAS

TURINYS

1. ĮVADAS

2. TERMINAI, APIBRĖŽTYS IR NUORODOS

3. PASLAUGŲ APŽVALGA

3.1. Galimos paslaugos

3.2. Atsakymo kodai

4. RYŠIO PASLAUGOS

4.1. Paslauga StartCommunication

4.2. Paslauga StopCommunication

4.2.1 Pranešimo aprašymas

4.2.2 Pranešimo formatas

4.2.3 Parametro apibrėžimas

4.3. Paslauga TesterPresent

4.3.1 Pranešimo aprašymas

4.3.2 Pranešimo formatas

5. VALDYMO PASLAUGOS

5.1. Paslauga StartDiagnosticSession

5.1.1 Pranešimo aprašymas

5.1.2 Pranešimo formatas

5.1.3 Parametro apibrėžimas

5.2. Paslauga SecurityAccess

5.2.1 Pranešimų aprašymas

5.2.2 SecurityAccess pranešimo requestSeed formatas

5.2.3 SecurityAccess pranešimo sendKey formatas

6. DUOMENŲ PERDAVIMO PASLAUGOS

6.1. Paslauga ReadDataByIdentifier

6.1.1 Pranešimo aprašymas

6.1.2 Pranešimo formatas

6.1.3 Parametro apibrėžimas

6.2. Paslauga WriteDataByIdentifier

6.2.1 Pranešimo aprašymas

6.2.2 Pranešimo formatas

6.2.3 Parametro apibrėžimas

▼B

7. BANDOMŲJŲ IMPULSŲ VALDYMAS. ĮVESTIES IR IŠVESTIES VALDYMO FUNKCINIS BLOKAS

7.1. Paslauga InputOutputControlByIdentifier

7.1.1 Pranešimo aprašymas

7.1.2 Pranešimo formatas

7.1.3 Parametro apibrėžimas

8. DATARECORDS FORMATAI

8.1. Siunčiamų parametrų grupės

8.2. dataRecords formatai

1. ĮVADAS

Šiame priedėlyje aprašyta, kaip vyksta keitimasis duomenimis tarp transporto priemonės bloko ir tikrintuvo per K liniją, kuri yra 6 priedėlyje aprašytos kalibravimo sąsajos dalis. Čia taip pat aprašytas įvesties ir išvesties signalo linijos valdymas per kalibravimo jungtį.

Kaip užmezgamas ryšys per K liniją aprašyta 4 skyriuje „Communication Services“.

Šiame priedėlyje K linijos valdymo taikymo sritį įvairiomis sąlygomis apibrėžia diagnostikos „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 „Management Services“.

Pagal šiame reglamente nustatytus sąveikos reikalavimus laikoma, kad šis priedėlis yra aktualus abiejų kartų transporto priemonės blokams ir dirbtuvių kortelėms,

CPR_001 Seanso ECUProgrammingSession metu galima rašyti duomenis į transporto priemonės bloką. Norint įvesti duomenis apie kalibravimą, transporto priemonės blokas turi veikti režimu CALIBRATION.

Kaip duomenys perduodami per K liniją, aprašyta 6 skyriuje „Data Transmission Services“. Duomenų perdavimo formatai išsamiai aprašyti 8 skyriuje „dataRecords formats“.

CPR_002 Seanso ECUAdjustmentSession metu per K linijos sąsają galima pasirinkti kalibravimo I/O signalo linijos I/O režimą. Kalibravimo I/O signalo linijos valdymas aprašytas 7 skyriuje „Control of Test Pulses – Input/Output Control functional unit“.

CPR_003 Šiame dokumente tikrintuvo adresas žymimas „tt“. Nors tikrintuvų adresai gali būti privilegijuoti, transporto priemonės blokas turi teisingai atsakyti į bet kokį tikrintuvo adresą. Transporto priemonės bloko fizinis adresas yra 0xEE.

▼B

2. TERMINAI, APIBRĖŽTYS IR NUORODOS

Protokolai, pranešimai ir klaidų kodai daugiausia remiasi ISO 14229-1 projektu („Kelių transporto priemonės. Diagnostikos sistemos“. 1 dalis. „Diagnostikos paslaugos“. 2001 m. vasario 22 d. 6 versija).

Paslaugų identifikatoriams, paslaugų pareikalavimams bei atsakymams ir standartiniams parametrams naudojamas baitų kodavimas ir šešioliktainės vertės.

Terminas „tikrintuvas“ reiškia įrangą, naudojamą programavimo (kalibravimo) duomenims įvesti į transporto priemonės bloką.

Terminai „klientas“ ir „serveris“ atitinkamai reiškia tikrintuvą ir transporto priemonės bloką.

Santrumpa EVB reiškia „elektroninį valdymo bloką“ ir žymi transporto priemonės bloką.

Nuorodos.

ISO 14230-2 Kelių transporto priemonės. Diagnostikos sistemos. Raktažodžių protokolas 2000, 2 dalis. Duomenų perdavimo kanalo lygmuo.

Pirmasis leidimas. 1999 m.

Transporto priemonės, diagnostika.

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 identifikatoriaus vertės,

— **ketvirtoje skiltyje** nurodytos **StandardDiagnosticSession (SD)** paslaugos, kurios turi būti įdiegtos kiekviename transporto priemonės bloke,

— **penktoje skiltyje** nurodytos **ECUAdjustmentSession (ECUAS)** paslaugos, kurios turi būti įdiegtos, kad I/O signalo liniją būtų galima valdyti per transporto priemonės bloko priekinėje plokštelėje esančią kalibravimo jungtį,

— **šeštoje skiltyje** nurodytos **ECUProgrammingSession (ECUPS)** paslaugos, kurios turi būti įdiegtos, kad būtų galima programuoti transporto priemonės bloko parametrus.

▼B

1 lentelė

Paslaugų identifikatorių verčių lentelė

			Diagnostikos seansai		
Diagnostikos paslaugos pavadinimas	Skyriaus Nr.	SId Req. vertė	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 ženklas reiškia, kad šiam diagnostikos seansui paslauga privaloma. Jei nėra jokio ženklo, šiam diagnostikos seansui paslauga negalima.

3.2. **Atsakymo kodai**

Kiekvienai paslaugai nustatyti atsakymo kodai.

4. RYŠIO PASLAUGOS

Kai kurios paslaugos reikalingos pagrindiniam ryšiui užmegzti. Jų nematyti taikomajame lygmenyje. Galimos paslaugos nurodytos toliau esančioje lentelėje:

2 lentelė

Ryšio paslaugos

Paslaugos pavadinimas	Aprašymas
StartCommunication	Klientas reikalauja pradėti ryšio su serveriu(-iais) seansą.
StopCommunication	Klientas reikalauja nutraukti esamą ryšio seansą.
TesterPresent	Klientas nurodo serveriui, kad jis vis dar yra

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**

CPR_006 Gavęs StartCommunication nurodomąjį bazinį elementą, transporto priemonės blokas turi patikrinti, ar reikalaujamas ryšys gali būti užmegztas esamomis sąlygomis. Ryšiui užmegzti tinkamos sąlygos aprašytos dokumente ISO 14230-2.

▼B

CPR_007 Tuomet transporto priemonės blokas turi atlikti visus veiksmus, kurių reikia ryšiui užmegzti, ir išsiųsti StartCommunication atsakomąjį bazinį elementą su parinktais teigiamo atsakymo parametrais.

CPR_008 Jei jau inicijuotas (ir pradėjęs diagnostikos seansą) transporto priemonės blokas gauna naują pareikalavimą StartCommunication (pvz., dėl klaidos ištaisymo tikrintuve), tas pareikalavimas turi būti priimtas, o transporto priemonės blokas inicijuotas iš naujo.

CPR_009 Jei dėl kokios nors priežasties ryšio pradėti negalima, transporto priemonės blokas turi toliau vykdyti funkcijas, kurias jis atliko prieš pat bandymą užmegzti ryšį.

CPR_010 Pranešimas StartCommunication turi būti fiziškai adresuotas.

CPR_011 Transporto priemonės bloko paslaugos inicijuojamos taikant „greitojo inicijavimo“ metodą:

— prieš bet kurią veiklą yra prastovos laikas,

— tuomet tikrintuvas išsiunčia inicijavimo šabloną,

— transporto priemonės bloko atsakyme pateikiama visa informacija, reikalinga ryšiui užmegzti.

CPR_012 Pasibaigus inicijavimui:

— pagal raktinius baitus nustatomos Table 4 nurodytos visų ryšio parametrų vertės,

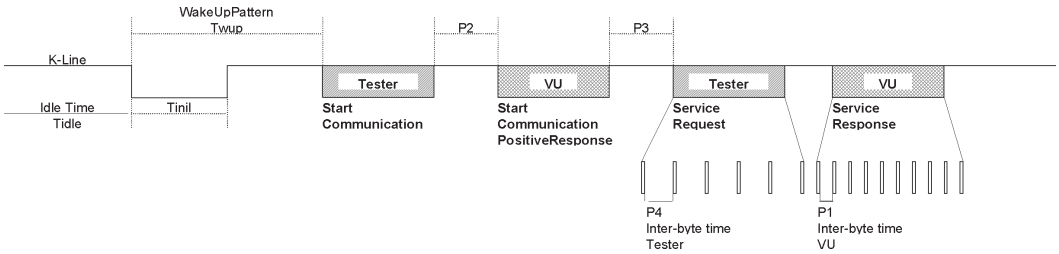
— transporto priemonės blokas laukia tikrintuvo pirmojo pareikalavimo,

— transporto priemonės blokas veikia numatytuoju diagnostikos režimu, t. y. StandardDiagnosticSession,

— kalibravimo I/O signalo linija yra numatytosios būsenos, t. y. neaktyvi.

CPR_014 Duomenų perdavimo sparta K linijoje turi būti 10 400 bodų.

CPR_016 Greitasis inicijavimas prasideda tada, kai tikrintuvas nusiunčia į K liniją sužadinimo šabloną (Wup). Šablonas prasideda po prastovos laiko K linijoje žemuoju laiku Tinil. Tikrintuvas siunčia pirmąjį paslaugos StartCommunication bitą po pirmojo nuolydžio praėjus laikui Twup.



▼B

CPR_017 Greitojo inicijavimo ir ryšio bendrai sinchronizavimo vertės nurodytos toliau pateikiamose lentelėse. Prastovos trukmė gali būti įvairi:

— pirmasis siuntimas po maitinimo įjungimo, Tidle = 300 ms,

— užbaigus paslaugą StopCommunication, Tidle = P3min.,

— nutraukus ryšį dėl to, kad baigėsi skirtas laikas P3max, Tidle = 0.

3 lentelė

Greitojo inicijavimo sinchronizavimo vertės

Parametras		min. vertė	maks. vertė
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

4 lentelė

Ryšio sinchronizavimo vertės

Sinchronizavimas Parametras	Parametro aprašymas	apatinės ribos vertės [ms]	viršutinės ribos vertės [ms]
		min.	maks.
P1	Tarpbaitinis laikas transporto priemonės bloko atsakymui	0	20
P2	Laikas tarp tikrintuvo pareikalavimo ir transporto priemonės bloko atsakymo arba dviejų transporto priemonės bloko atsakymų	25	250
P3	Laikas tarp transporto priemonės bloko atsakymų pabaigos ir tikrintuvo naujo pareikalavimo pradžios	55	5 000
P4	Tarpbaitinis laikas tikrintuvo pareikalavimui	5	20

CPR_018 Greitojo inicijavimo pranešimų formatas nurodytas toliau pateikiamose lentelėse: (Pastaba. Hex reiškia „šešioliktainis“)

5 lentelė

StartCommunication pareikalavimo pranešimas

Baito Nr.	Parametro pavadinimas	Hex vertė	Mnemoninis žymuo
#1	Formato baitas – fizinis adresas	81	FMT
#2	Paskirties adreso baitas	EE	TGT
#3	Šaltinio adreso baitas	tt	SRC

▼B

Baito Nr.	Parametro pavadinimas	Hex vertė	Mnemoninis žymuo
#4	**StartCommunication pareikalavimo paslaugos identifikatorius**	**81**	**SCR**
#5	Kontrolinė suma	00-FF	CS

6 lentelė

StartCommunication teigiamo atsakymo pranešimas

Baito Nr.	Parametro pavadinimas	Hex 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	**StartCommunication teigiamo atsakymo paslaugos identifikatorius**	**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 transporto priemonės blokas nėra inicijuotas, niekas nesiunčiama ir transporto priemonės blokas veikia įprastu režimu.

4.2. **Paslauga StopCommunication**

4.2.1 *Pranešimo aprašymas*

Šios ryšio lygmens paslaugos paskirtis – nutraukti ryšio seansą.

CPR_020 Gavęs StopCommunication nurodomąjį bazinį elementą, transporto priemonės blokas turi patikrinti, ar esamomis sąlygomis galima nutraukti ryšį. Jei taip, transporto priemonės blokas turi atlikti visus veiksmus, kurių reikia ryšiui nutraukti.

CPR_021 Jei ryšį nutraukti įmanoma, transporto priemonės blokas turi išsiųsti StopCommunication atsakomąjį bazinį elementą su parinktais teigiamo atsakymo parametrais ir tuomet nutraukti ryšį.

CPR_022 Jei ryšio dėl kokios nors priežasties nutraukti negalima, transporto priemonės blokas turi siųsti StopCommunication atsakomąjį bazinį elementą su pasirinktu neigiamo atsakymo parametru.

CPR_023 Jei transporto priemonės blokas aptinka, kad baigėsi laikas P3max, ryšys nutraukiamas nesiunčiant atsakomojo bazinio elemento.

▼B

4.2.2 *Pranešimo formatas*

CPR_024 StopCommunication bazinių elementų pranešimo formatai nurodyti toliau pateikiamose lentelėse:

7 lentelė

StopCommunication pareikalavimo pranešimas

Baito Nr.	Parametro pavadinimas	Hex 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	**StopCommunication pareikalavimo paslaugos identifikatorius**	**82**	**SPR**
#6	Kontrolinė suma	00-FF	CS

8 lentelė

StopCommunication teigiamo atsakymo pranešimas

Baito Nr.	Parametro pavadinimas	Hex 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	**StopCommunication teigiamo atsakymo paslaugos identifikatorius**	**C2**	**SPRPR**
#6	Kontrolinė suma	00-FF	CS

9 lentelė

StopCommunication neigiamo atsakymo pranešimas

Baito Nr.	Parametro pavadinimas	Hex 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

▼B

Baito Nr.	Parametro pavadinimas	Hex vertė	Mnemoninis žymuo
#5	**Neigiamo atsakymo paslaugos identifikatorius**	**7F**	**NR**
#6	StopCommunication pareikalavimo paslaugos identifikatorius	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Kontrolinė suma	00-FF	CS

4.2.3 *Parametro apibrėžimas*

Šiai paslaugai parametrų apibrėžti nereikia.

4.3. **Paslauga TesterPresent**

4.3.1 *Pranešimo aprašymas*

Paslaugą TesterPresent tikrintuvas naudoja tam, kad serveriui nurodytų, kad jis vis dar yra, ir kad serveris automatiškai vėl neimtų veikti įprastu režimu ir nenutrauktų ryšio. Ši periodiškai siunčiama paslauga išlaiko aktyvų diagnostikos seansą (ryšį) grąžindama nulinę P3 laikmačio vertę kiekvieną kartą, kai gaunamas šios paslaugos pareikalavimas.

4.3.2 *Pranešimo formatas*

CPR_079 TesterPresent bazinių elementų pranešimo formatai nurodyti toliau pateikiamose lentelėse.

10 lentelė

TesterPresent pareikalavimo pranešimas

Baito Nr.	Parametro pavadinimas	Hex 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	**TesterPresent pareikalavimo paslaugos identifikatorius**	**3E**	**TP**
#6	Sub Function = responseRequired = [yes	01	RESPREQ_Y
	no]	02	RESPREQ_NO
#7	Kontrolinė suma	00-FF	CS

CPR_080 Jei parametro responseRequired vertė yra „yes“, tuomet serveris turi atsakyti toliau nurodytu teigiamo atsakymo pranešimu. Jei vertė yra „no“, serveris atsakymo nesiunčia.

▼B

11 lentelė

TesterPresent teigiamo atsakymo pranešimas

Baito Nr.	Parametro pavadinimas	Hex 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	**TesterPresent teigiamo atsakymo paslaugos identifikatorius**	**7E**	**TPPR**
#6	Kontrolinė suma	00-FF	CS

CPR_081 Tarnybinei stočiai turi būti tinkami tokie neigiamų atsakymų kodai:

12 lentelė

TesterPresent neigiamo atsakymo pranešimas

Baito Nr.	Parametro pavadinimas		Hex 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 identifikatorius**		**7F**	**NR**
#6	TesterPresent identifikatorius	pareikalavimo paslaugos	3E	TP
#7	responseCode =	[SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
		incorrectMessageLength]	13	RC_IML
#8	Kontrolinė suma		00-FF	CS

▼B

5. VALDYMO PASLAUGOS

Galimos paslaugos nurodytos toliau esančioje lentelėje:

13 lentelė

Valdymo paslaugos

Paslaugos pavadinimas	Aprašymas
StartDiagnosticSession	Klientas reikalauja pradėti diagnostikos seansą su transporto priemonės bloku.
SecurityAccess	Klientas reikalauja prieigos prie funkcijų, kuriomis leista naudotis tik įgaliotiems naudotojams.

5.1. **Paslauga StartDiagnosticSession**

5.1.1 *Pranešimo aprašymas*

CPR_025 Paslauga StartDiagnosticSession naudojama įvairiems diagnostikos seansams pradėti serveryje. Diagnostikos seanso metu aktyvuojamas specialių paslaugų rinkinys, kaip nurodyta Table 17. Gali būti aktyvuojamos transporto priemonės gamintojo nustatytos paslaugos, kurios šiame dokumente neaprašytos. Taikymo taisyklės turi atitikti tokius reikalavimus:

— Transporto priemonės bloke visuomet turi būti aktyvus tiksliai vienas diagnostikos seansas,

— įjungus transporto priemonės bloko maitinimą, jis visuomet turi pradėti seansą StartDiagnosticSession. Jei kiti diagnostikos seansai nepradedami, tuomet StartDiagnosticSession turi veikti tol, kol transporto priemonės blokas būna įjungtas,

— jei tikrintuvas pareikalauja jau vykstančio diagnostikos seanso, tuomet transporto priemonės blokas turi išsiųsti teigiamo atsakymo pranešimą,

— kai tikrintuvas pareikalauja naujo diagnostikos seanso, transporto priemonės blokas iš pradžių turi išsiųsti teigiamo atsakymo pranešimą StartDiagnosticSession ir tik po to pradėti naują seansą. Jei transporto priemonės blokas negali pradėti pareikalauto naujo diagnostikos seanso, tuomet jis turi išsiųsti StartDiagnosticSession neigiamo atsakymo pranešimą ir tęsti esamąjį.

CPR_026 Diagnostikos seansas turi būti pradedamas tik tuomet, jei tarp kliento ir transporto priemonės bloko užmegztas ryšys.

CPR_027 Sėkmingai pradėjus paslaugą StartDiagnosticSession, turi galioti Table 4 nustatyti sinchronizavimo parametrai, o jei anksčiau vyko kitas diagnostikos seansas, turi būti nustatyta parametro diagnosticSession vertė StandardDiagnosticSession.

5.1.2 *Pranešimo formatas*

CPR_028 StartDiagnosticSession bazinių elementų pranešimo formatai nurodyti toliau pateikiamose lentelėse.

▼B

14 lentelė

StartDiagnosticSession pareikalavimo pranešimas

Baito Nr.	Parametro pavadinimas	Hex 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	**StartDiagnosticSession pareikalavimo paslaugos identifikatorius**	**10**	**STDS**
#6	diagnosticSession = (viena iš Table 17 nurodytų verčių)	xx	DS_…
#7	Kontrolinė suma	00-FF	CS

15 lentelė

StartDiagnosticSession teigiamo atsakymo pranešimas

Baito Nr.	Parametro pavadinimas	Hex 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	**StartDiagnosticSession teigiamo atsakymo paslaugos identifikatorius**	**50**	**STDSPR**
#6	diagnosticSession = (ta pati vertė, kaip ir 6 baito Table 14)	xx	DS_…
#7	Kontrolinė suma	00-FF	CS

16 lentelė

StartDiagnosticSession neigiamo atsakymo pranešimas

Baito Nr.	Parametro pavadinimas	Hex vertė	Mnemoninis žymuo
#1	Formato baitas – fizinis adresas	80	FMT
#2	Paskirties adreso baitas	tt	TGT
#3	Šaltinio adreso baitas	EE	SRC

▼B

Baito Nr.	Parametro pavadinimas		Hex vertė	Mnemoninis žymuo
#4	Papildomas ilgio baitas		03	LEN
#5	**Neigiamo atsakymo paslaugos identifikatorius**		**7F**	**NR**
#6	StartDiagnosticSession pareikalavimo paslaugos identifikatorius		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]) – į pareikalavimo pranešimo 6 baitą įrašyta vertė netinkama, t. y. jos nėra Table 17,
([b]) – pranešimo ilgis yra netinkamas,
([c]) – neįvykdyti pranešimo StartDiagnosticSession kriterijai.

5.1.3 *Parametro apibrėžimas*

CPR_029 Parametrą ***diagnosticSession (DS_)*** paslauga StartDiagnosticSession naudoja tam tikram serverio(-ių) veikimo būdui pasirinkti. Šiame dokumente nustatyti tokie diagnostikos seansai:

17 lentelė

diagnosticSession verčių apibrėžtis

Šešioliktainė vertė	Aprašymas	Mnemoninis žymuo
81	**StandardDiagnosticSession** Per šį diagnostikos seansą galima naudoti visas **Table 1 4 skiltyje (SD)** pažymėtas paslaugas. Šios paslaugos leidžia nuskaityti iš serverio (transporto priemonės bloko) visus duomenis. Šis diagnostikos seansas veikia sėkmingai atlikus inicijavimą tarp kliento (tikrintuvo) ir serverio (transporto priemonės bloko). Šį diagnostikos seansą gali pakeisti kiti šiame skyriuje nurodyti diagnostikos seansai.	**SD**
85	**ECUProgrammingSession** Per šį diagnostikos seansą galima naudoti visas **Table 1 6 skiltyje (ECUPS)** pažymėtas paslaugas. Šios paslaugos leidžia programuoti serverio (transporto priemonės bloko) atmintį. Šį diagnostikos seansą gali pakeisti kiti šiame skyriuje nurodyti diagnostikos seansai.	**ECUPS**

▼B

Šešioliktainė vertė	Aprašymas	Mnemoninis žymuo
87	**ECUAdjustmentSession** Per šį diagnostikos seansą galima naudoti visas **Table 1 5 skiltyje (ECUAS)** pažymėtas paslaugas. Šios paslaugos leidžia valdyti serverio (transporto priemonės bloko) įvestį ir išvestį. Šį diagnostikos seansą gali pakeisti kiti šiame skyriuje nurodyti diagnostikos seansai.	**ECUAS**

5.2. **Paslauga SecurityAccess**

Jei transporto priemonės blokas veikia ne režimu CALIBRATION, neįmanoma įrašyti duomenų apie kalibravimą. Į transporto priemonės bloką įstačius galiojančią dirbtuvių kortelę dar reikia įvesti atitinkamą PIN ir tik tuomet suteikiama galimybė naudotis režimu CALIBRATION.

Jei transporto priemonės blokas veikia režimu CALIBRATION arba CONTROL, įmanoma prieiga prie įvesties ir išvesties linijos.

Paslauga SecurityAccess suteikia galimybę įvesti PIN ir nurodyti tikrintuvui, ar transporto priemonės blokas veikia režimu CALIBRATION, ar ne.

PIN leidžiama įvesti ir kitais būdais.

5.2.1 *Pranešimų aprašymas*

Paslaugą SecurityAccess sudaro pranešimas requestSeed, po kurio gali būti siunčiamas pranešimas sendKey. Paslauga SecurityAccess turi būti vykdoma po paslaugos StartDiagnosticSession.

CPR_033 Tikrintuvas turi SecurityAccess pranešimu requestSeed patikrinti, ar transporto priemonės blokas yra pasirengęs priimti PIN.

CPR_034 Jei transporto priemonės blokas jau veikia režimu CALIBRATION, jis turi atsakyti į pareikalavimą pasinaudodamas SecurityAccess teigiamo atsakymo paslauga 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 SecurityAccess teigiamo atsakymo paslauga ir išsiųsdamas „seed“, didesnį kaip 0x0000.

CPR_036 Jei transporto priemonės blokas nepasirengęs priimti PIN iš tikrintuvo dėl to, kad įstatyta dirbtuvių kortelė negalioja, ji neįstatyta arba transporto priemonės blokas tikisi, kad PIN bus įvestas kitu būdu, jis turi atsakyti į pareikalavimą neigiamo atsakymo pranešimu, kuriame nustatytas atsakymo kodas conditionsNotCorrectOrRequestSequenceError.

CPR_037 Tuomet tikrintuvas naudodamasis SecurityAccess pranešimu sendKey turi nusiųsti transporto priemonės blokui PIN. Tam, kad galėtų būti atliktas kortelės autentiškumo tikrinimo procesas, transporto priemonės blokas turi naudoti neigiamo atsakymo kodą requestCorrectlyReceived-ResponsePending atsakymo laikui pratęsti. Tačiau tas laikas negali būti ilgesnis kaip 5 minutės. Kai tik pareikalauta paslauga

▼B

užbaigiama, transporto priemonės blokas turi išsiųsti teigiamo arba neigiamo atsakymo pranešimą, kurio kodas skiriasi nuo nurodytojo. Neigiamo atsakymo kodą requestCorrectlyReceived-ResponsePending transporto priemonės blokas gali kartoti tol, kol reikalaujamoji paslauga užbaigiama ir išsiunčiamas galutinio atsakymo pranešimas.

CPR_038 Transporto priemonės blokas turi atsakyti į šį pareikalavimą pasinaudodamas SecurityAccess teigiamo atsakymo paslauga tik veikdamas režimu CALIBRATION.

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 *SecurityAccess pranešimo requestSeed formatas*

CPR_040 SecurityAccess requestSeed bazinių elementų pranešimo formatai nurodyti toliau pateikiamose lentelėse.

18 lentelė

SecurityAccess pareikalavimo pranešimas requestSeed

Baito Nr.	Parametro pavadinimas	Hex 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	**SecurityAccess pareikalavimo paslaugos identifikatorius**	**27**	**SA**
#6	accessType – requestSeed	7D	AT_RSD
#7	Kontrolinė suma	00-FF	CS

▼B

19 lentelė

Teigiamo atsakymo pranešimas SecurityAccess – requestSeed

Baito Nr.	Parametro pavadinimas	Hex 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	04	LEN
#5	**SecurityAccess teigiamo atsakymo paslaugos identifikatorius**	**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

SecurityAccess neigiamo atsakymo pranešimas

Baito Nr.	Parametro pavadinimas	Hex 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 identifikatorius**	**7F**	**NR**
#6	SecurityAccess pareikalavimo paslaugos identifikatorius	27	SA
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength]	13	RC_IML
#8	Kontrolinė suma	00-FF	CS

▼B

5.2.3 *SecurityAccess pranešimo sendKey formatas*

CPR_041 SecurityAccess sendKey bazinių elementų pranešimo formatai nurodyti toliau pateikiamose lentelėse.

21 lentelė

SecurityAccess pareikalavimo sendKey pranešimas

Baito Nr.	Parametro pavadinimas	Hex 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	**SecurityAccess pareikalavimo paslaugos identifikatorius**	**27**	**SA**
#6	accessType – sendKey	7E	AT_SK
nuo #7 iki #m+6	Raktas #1 (High) … Raktas #m (low, m turi būti nuo 4 iki 8)	xx … xx	KEY
#m+7	Kontrolinė suma	00-FF	CS

22 lentelė

SecurityAccess teigiamo sendKey atsakymo pranešimas

Baito Nr.	Parametro pavadinimas	Hex 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	**SecurityAccess teigiamo atsakymo paslaugos identifikatorius**	**67**	**SAPR**
#6	accessType – sendKey	7E	AT_SK
#7	Kontrolinė suma	00-FF	CS

▼B

23 lentelė

SecurityAccess neigiamo atsakymo pranešimas

Baito Nr.	Parametro pavadinimas		Hex 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 identifikatorius**		**7F**	**NR**
#6	SecurityAccess pareikalavimo paslaugos identifikatorius		27	SA
#7	ResponseCode =	[generalReject	10	RC_GR
		subFunctionNotSupp-orted	12	RC_SFNS
		incorrectMessageLen-gth	13	RC_IML
		conditionsNotCorrect-OrRequestSequenceE-rror	22	RC_CNC
		invalidKey	35	RC_IK
		exceededNumberOf-Attempts	36	RC_ENA
		requestCorrectlyRe-ceived-ResponsePending]	78	RC_RCR_RP
#8	Kontrolinė suma		00-FF	CS

6. DUOMENŲ PERDAVIMO PASLAUGOS

Galimos paslaugos nurodytos toliau esančioje lentelėje:

24 lentelė

Duomenų perdavimo paslaugos

Paslaugos pavadinimas	Aprašymas
ReadDataByIdentifier	Klientas reikalauja persiųsti esamą įrašo, pasiekiamo su recordDataIdentifier, vertę
WriteDataByIdentifier	Klientas reikalauja įrašyti įrašą, pasiekiamą su recordDataIdentifier.

▼B

6.1. **Paslauga ReadDataByIdentifier**

6.1.1 *Pranešimo aprašymas*

CPR_050 Naudodamas paslaugą ReadDataByIdentifier, klientas reikalauja duomenų įrašų verčių iš serverio. Duomenys identifikuojami pagal recordDataIdentifier. Transporto priemonės bloko gamintojas atsako už tai, kad atliekant šią paslaugą būtų laikomasi serveriui keliamų reikalavimų.

6.1.2 *Pranešimo formatas*

CPR_051 ReadDataByIdentifier bazinių elementų pranešimo formatai nurodyti toliau pateikiamose lentelėse.

25 lentelė

ReadDataByIdentifier pareikalavimo pranešimas

Baito Nr.	Parametro pavadinimas	Hex 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	**ReadDataByIdentifier pareikalavimo paslaugos identifikatorius**	**22**	**RDBI**
nuo #6 iki #7	recordDataIdentifier = [viena iš Table 28 nurodytų verčių]	xxxx	RDI_…
#8	Kontrolinė suma	00-FF	CS

26 lentelė

ReadDataByIdentifier teigiamo atsakymo pranešimas

Baito Nr.	Parametro pavadinimas	Hex 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	**ReadDataByIdentifier teigiamo atsakymo paslaugos identifikatorius**	**62**	**RDBIPR**
nuo #6 iki #7	recordDataIdentifier = (ta pati vertė kaip 6 ir 7 baitų Table 25)	xxxx	RDI_…

▼B

Baito Nr.	Parametro pavadinimas		Hex vertė	Mnemoninis žymuo
nuo #8 iki #m+7	dataRecord[] =	[data#1	xx	DREC_DAT-A1
		:	:	:
		data#m]	xx	DREC_DAT-Am
#m+8	Kontrolinė suma		00-FF	CS

27 lentelė

ReadDataByIdentifier neigiamo atsakymo pranešimas

Baito Nr.	Parametro pavadinimas		Hex 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 identifikatorius**		**7F**	**NR**
#6	ReadDataByIdentifier pareikalavimo paslaugos identifikatorius		22	RDBI
#7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Kontrolinė suma		00-FF	CS

6.1.3 *Parametro apibrėžimas*

CPR_052 Parametras ***recordDataIdentifier (RDI_)*** ReadDataByIdentifier pareikalavimo pranešime 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 šešioliktainės vertės,

— **antroje skiltyje (Duomenų elementas)** nurodytas duomenų elementas pagal 1 priedėlį, kuriuo paremtas recordDataIdentifier (kartais reikia perkoduoti),

▼B

— **trečioje skiltyje (Aprašymas)** nurodytas atitinkamo recordDataIdentifier pavadinimas,

— **ketvirtoje skiltyje (Mnemoninis žymuo)** nurodytas šio recordDataIdentifier mnemoninis žymuo.

28 lentelė

recordDataIdentifier verčių apibrėžtis

Šešioliktainė vertė	Duomenų elementas	recordDataIdentifier pavadinimas (žr. Formatą 8.2 skyriuje)	Mnemoninis žymuo
F90B	CurrentDateTime	TimeDate	RDI_TD
F912	HighResOdometer	HighResolutionTotalVehicle-Distance	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Kfactor	RDI_KF
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_ VRN
F190	VehicleIdentificationNumber	VIN	RDI_ VIN

CPR_054 Naudojant parametrą ***dataRecord (DREC_)***, ReadDataByIdentifier teigiamo atsakymo pranešime klientui (tikrintuvui) pateikiamos duomenų įrašo vertės, nurodytos identifikatoriumi recordDataIdentifier. Duomenų formatai nurodyti 8 skyriuje. Galima naudoti papildomus parametrus dataRecord, skirtus papildomiems naudotojams, įskaitant transporto priemonės blokui pritaikytus įvesties, vidinius ir išvesties duomenis, tačiau šiame dokumente jie neaprašyti.

6.2. Paslauga WriteDataByIdentifier

6.2.1 *Pranešimo aprašymas*

CPR_056 Paslaugą WriteDataByIdentifier klientas naudoja duomenų įrašų vertėms įrašyti serveryje. Duomenys identifikuojami pagal recordDataIdentifier. Transporto priemonės bloko gamintojas atsako už tai, kad atliekant šią paslaugą būtų laikomasi serveriui keliamų reikalavimų. Norint atnaujinti Table 28 išvardytus parametrus transporto priemonės blokas turi veikti režimu CALIBRATION.

6.2.2 *Pranešimo formatas*

CPR_057 WriteDataByIdentifier bazinių elementų pranešimo formatai nurodyti toliau pateikiamose lentelėse.

▼B

29 lentelė

WriteDataByIdentifier pareikalavimo pranešimas

Baito Nr.	Parametro pavadinimas	Hex 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	**WriteDataByIdentifier pareikalavimo paslaugos identifikatorius**	**2E**	**WDBI**
nuo #6 iki #7	recordDataIdentifier = [viena iš Table 28 nurodytų verčių]	xxxx	RDI_…
nuo #8 iki m+7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DAT-A1 : DREC_DAT-Am
#m+8	Kontrolinė suma	00-FF	CS

30 lentelė

WriteDataByIdentifier teigiamo atsakymo pranešimas

Baito Nr.	Parametro pavadinimas	Hex 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	**WriteDataByIdentifier teigiamo atsakymo paslaugos identifikatorius**	**6E**	**WDBIPR**
nuo #6 iki #7	recordDataIdentifier = (ta pati vertė kaip 6 ir 7 baitų Table 29)	xxxx	RDI_…
#8	Kontrolinė suma	00-FF	CS

▼B

31 lentelė

WriteDataByIdentifier neigiamo atsakymo pranešimas

Baito Nr.	Parametro pavadinimas		Hex 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 identifikatorius**		**7F**	**NR**
#6	WriteDataByIdentifier pareikalavimo paslaugos identifikatorius		2E	WDBI
#7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Kontrolinė suma		00-FF	CS

6.2.3 *Parametro apibrėžimas*

Parametras ***recordDataIdentifier (RDI_)*** apibrėžtas Table 28.

Naudojant parametrą ***dataRecord (DREC_)***, WriteDataByIdentifier teigiamo atsakymo pranešime serveriui (transporto priemonės blokui) pateikiamos duomenų įrašo vertės, nurodytos identifikatoriumi 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 tik tam serveriui būdingą įvestį ir išvestį.

7.1. **Paslauga InputOutputControlByIdentifier**

7.1.1 *Pranešimo aprašymas*

Priekinėje jungtyje yra sujungimas, per kurį galima kontroliuoti arba stebėti bandymų impulsus naudojant tinkamą tikrintuvą.

▼B

CPR_058 Šį kalibravimo I/O signalą galima konfigūruoti K linijos komanda, kad naudojant paslaugą InputOutputControlByIdentifier būtų parenkama reikiama linijos įvesties arba išvesties funkcija. Galimos tokios linijos būsenos:

— disabled,

— speedSignalInput, kai kalibravimo I/O signalo linija naudojama greičio signalui (bandomajam signalui) įvesti vietoje judesio jutiklio greičio signalo; ši funkcija negalima režime CONTROL,

— 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; ši funkcija negalima režime CONTROL.

CPR_059 Tam, kad būtų galima sukonfigūruoti linijos būseną, transporto priemonės bloke turi būti prasidėjęs reguliavimo seansas ir jis turi veikti režimu CALIBRATION arba CONTROL. Jei transporto priemonės blokas veikia režimu CALIBRATION, galima rinktis keturias linijos būsenas (disabled, speedSignalInput, realTimeSpeedSignalOutputSensor, RTCOutput). Jei transporto priemonės blokas veikia režimu CONTROL, galima rinktis tik dvi linijos būsenas (disabled, realTimeSpeedOutputSensor). Baigdamas reguliavimo seansą ar režimą CALIBRATION arba CONTROL transporto priemonės blokas turi užtikrinti, kad kalibravimo I/O signalo linija būtų grąžinta į (numatytąją) būseną „disabled“.

CPR_060 Jei greičio impulsai transporto priemonės bloko 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 būseną „disabled“.

CPR_061 Seka turi būti tokia:

— naudojantis paslauga StartCommunication užmezgamas ryšys,

— naudojantis paslauga StartDiagnosticSession pradedamas reguliavimo seansas ir nustatomas režimas CALIBRATION arba CONTROL (šių dviejų operacijų eiliškumas nesvarbus),

— naudojantis paslauga InputOutputControlByIdentifier pakeičiama išvesties būsena.

7.1.2 *Pranešimo formatas*

CPR_062 InputOutputControlByIdentifier bazinių elementų pranešimo formatai nurodyti toliau pateikiamose lentelėse.

▼B

33 lentelė

InputOutputControlByIdentifier pareikalavimo pranešimas

Baito Nr.	Parametro pavadinimas	Hex 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	**InputOutputControlByIdentifier pareikalavimo paslaugos identifikatorius**	**2F**	**IOCBI**
nuo #6 iki #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 arba nuo #8 iki #9	ControlOptionRecord = [inputOutputControlParameter – viena iš Table 36 verčių controlState – viena iš Table 37 verčių (žr. pastabą toliau)]	 xx xx	COR_… IOCP_… CS_…
9 arba 10	Kontrolinė suma	00-FF	CS

Pastaba: Parametras controlState būna tik kai kuriais atvejais (žr. 7.1.3).

34 lentelė

InputOutputControlByIdentifier teigiamo atsakymo pranešimas

Baito Nr.	Parametro pavadinimas	Hex 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	**inputOutputControlByIdentifier teigiamo atsakymo paslaugos identifikatorius**	**6F**	**IOCBIPR**
nuo #6 iki #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 arba nuo #8 iki #9	controlStatusRecord = [inputOutputControlParameter (ta pati vertė kaip 8 baito Table 33) controlState (ta pati vertė, kaip ir 9 baito Table 33)] (jei taikytina)	 xx xx	CSR_ IOCP_… CS_…
9 arba 10	Kontrolinė suma	00-FF	CS

▼B

35 lentelė

InputOutputControlByIdentifier neigiamo atsakymo pranešimas

Baito Nr.	Parametro pavadinimas	Hex 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 identifikatorius**	**7F**	**NR**
#6	inputOutputControlByIdentifier Request SId	2F	IOCBI
#7	responseCode=[		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
#8	Kontrolinė suma	00-FF	CS

7.1.3 *Parametro apibrėžimas*

CPR_064 Parametras ***inputOutputControlParameter (IOCP_)*** apibrėžtas toliau esančioje lentelėje.

36 lentelė

inputOutputControlParameter verčių apibrėžtis

Šešioliktainė vertė	Aprašymas	Mnemoninis žymuo
00	**ReturnControlToECU** Ši vertė serveriui (transporto priemonės blokui) turi nurodyti, kad tikrintuvas nebevaldo kalibravimo I/O signalo linijos.	RCTECU
01	**ResetToDefault** Ši vertė serveriui (transporto priemonės blokui) turi nurodyti, kad reikalaujama atstatyti kalibravimo I/O signalo linijos numatytąją būseną.	RTD

▼B

Šešioliktainė vertė	Aprašymas	Mnemoninis žymuo
03	**ShortTermAdjustment** Ši vertė serveriui (transporto priemonės blokui) turi nurodyti, kad reikalaujama suderinti kalibravimo I/O signalo liniją su verte, nurodyta parametru controlState.	STA

CPR_065 Parametras ***controlState*** yra tik tuomet, kai nustatyta parametro inputOutputControlParameter vertė ShortTermAdjustment; jis apibrėžtas toliau esančioje lentelėje:

37 lentelė

controlState verčių apibrėžtis

Režimas	Hex vertė	Aprašymas
Pasyvintas	00	I/O linija yra neaktyvi („disabled“, numatytoji būsena)
Aktyvintas	01	Kalibravimo I/O linija aktyvinta režimu speedSignalInput
Aktyvintas	02	Kalibravimo I/O linija aktyvinta režimu realTimeSpeedSignalOutputSensor
Aktyvintas	03	Kalibravimo I/O linija aktyvinta režimu RTCOutput

8. DATARECORDS FORMATAI

Skyriuje aprašyta:

— bendrosios taisyklės, kurias reikia taikyti transporto priemonės bloko tikrintuvui siunčiamų signalų parametrų grupėms,

— formatai, kuriuos reikia naudoti 6 skyriuje aprašytomis duomenų perdavimo paslaugomis siunčiamiems duomenims.

CPR_067 Visi nurodyti parametrai turi būti tinkami transporto priemonės blokui.

CPR_068 Kai transporto priemonės blokas atsako į pareikalavimo pranešimus, tikrintuvui, siunčiami duomenys turi būti išmatuotojo tipo (t. y. esama reikalaujamo parametro vertė, kurią išmatavo arba nustatė transporto priemonės blokas).

8.1. **Siunčiamų parametrų grupės**

CPR_069 Table 38 lentelėje apibrėžtos grupės, naudojamos siunčiamų parametrų galiojimui nustatyti.

CPR_070 Grupės „error indicator“ vertės skirtos tam, kad transporto priemonės blokas galėtų iš karto nurodyti, kad galiojantys parametrų duomenys šiuo metu neprieinami dėl tam tikros rūšies klaidos tachografe.

CPR_071 Grupės „not available“ vertės skirtos tam, kad transporto priemonės blokas galėtų išsiųsti pranešimą, kuriame yra tame modulyje neturimas arba netinkamas parametras. Grupės „not requested“ vertės skirtos tam, kad įrenginys galėtų siųsti komandos pranešimą ir identifikuoti tuos parametrus, kai iš priimančiojo įtaiso nelaukiama atsakymo.

▼B

CPR_072 Jei dėl komponento gedimo negalima persiųsti galiojančių parametro duomenų, vietoj tų parametro duomenų turi būti naudojamas klaidos indikatorius, kaip nurodyta Table 38. 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 (šešioliktainė vertė)	2 baitai (šešioliktainė vertė)	4 baitai (Hex 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 nereikalaujama	FF	nuo FF00 iki FFFF	nuo FF000000 iki FFFFFFFF	FF

CPR_073 ASCII koduotiems parametrams ASCII rašmuo „*“ rezervuotas kaip skirtukas.

8.2. **dataRecords formatai**

Toliau esančiose Table 39–Table 42 lentelėse nurodyti formatai, kuriuose reikia naudoti su paslaugomis ReadDataByIdentifier ir WriteDataByIdentifier.

CPR_074 Table 39 lentelėje nurodytas kiekvieno pagal savo recordDataIdentifier identifikuojamo parametro ilgis, skiriamoji geba ir naudojimo ribos:

39 lentelė

DataRecords formatas

Parametro pavadinimas	Duomenų ilgis (baitais)	Skiriamoji geba	Naudojimo ribos
TimeDate	8	Daugiau žr. Table 40.	
HighResolutionTotalVehicleDistance	4	5 m/bit prieaugis, 0 m poslinkis	nuo 0 iki +21 055 406 km
Kfactor	2	0,001 impulso/m/bit prieaugis, poslinkis – 0	nuo 0 iki 64,255 impulsų/m
LfactorTyreCircumference	2	$0{,}125 \times 10^{-3}$ m/bit prieaugis, poslinkis – 0	nuo 0 iki 8,031 m
WvehicleCharacteristicFactor	2	0,001 impulso/m/bit prieaugis, poslinkis – 0	nuo 0 iki 64,255 impulsų/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Daugiau žr. Table 41.	
SpeedAuthorised	2	1/256 km/h/bit prieaugis, poslinkis – 0	nuo 0 iki 250,996 km/h

▼B

Parametro pavadinimas	Duomenų ilgis (baitais)	Skiriamoji geba	Naudojimo ribos
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Daugiau žr. Table 42.	
VIN	17	ASCII	ASCII

CPR_075 Table 40 lentelėje nurodyti parametro TimeDate įvairių baitų formatai.

40 lentelė

TimeDate išsamus formatas (recordDataIdentifier vertė # F90B)

Baitas	Parametro apibrėžimas	Skiriamoji geba	Naudojimo ribos
1	Sekundės	0,25 s/bit prieaugis, 0 s poslinkis	nuo 0 iki 59,75 s
2	Minutės	1 min./bit prieaugis, 0 min. poslinkis	nuo 0 iki 59 min.
3	Valandos	1 h/bit prieaugis, 0 h poslinkis	nuo 0 iki 23 h
4	Mėnuo	1 mėn./bit prieaugis, 0 mėn. poslinkis	nuo 1 iki 12 mėnesių
5	Diena	0,25 dienos/bit prieaugis, 0 dienų poslinkis (žr. PASTABĄ Table 41)	nuo 0,25 iki 31,75 dienos
6	Metai	1 metai/bit prieaugis, +1985 metų poslinkis (Žr. PASTABĄ toliau Table 41)	nuo 1985 iki 2235 m.
7	Minučių vietos laiku poslinkis	1 min./bit prieaugis, – 125 min. poslinkis	nuo – 59 iki + 59 min.
8	Valandų vietos laiku poslinkis	1 h/bit prieaugis, – 125 h poslinkis	nuo – 23 iki + 23 h

CPR_076 Table 41 lentelėje nurodyti parametro NextCalibrationDate įvairių baitų formatai.

41 lentelė

NextCalibrationDate išsamus formatas (recordDataIdentifier vertė # F922)

Baitas	Parametro apibrėžimas	Skiriamoji geba	Naudojimo ribos
1	Mėnuo	1 mėn./bit prieaugis, 0 mėn. poslinkis	nuo 1 iki 12 mėnesių
2	Diena	0,25 dienos/bit prieaugis, 0 dienų poslinkis (žr. PASTABĄ toliau)	nuo 0,25 iki 31,75 dienos
3	Metai	1 metai/bit prieaugis, + 1985 metų poslinkis (žr. PASTABĄ toliau)	nuo 1985 iki 2235 m.

▼B

PASTABA dėl parametro „diena“ naudojimo.

1) Datos vertė 0 yra neapibrėžtoji vertė. Vertės 1, 2, 3 ir 4 naudojamos pirmajai mėnesio dienai žymėti; 5, 6, 7 ir 8 žymi antrąją mėnesio dieną ir t. t.

2) 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 Table 42 lentelėje nurodyti parametro VehicleRegistrationNumber įvairių baitų formatai.

42 lentelė

VehicleRegistrationNumber išsamus formatas (recordDataIdentifier vertė # F97E)

Baitas	Parametro apibrėžimas	Skiriamoji geba	Naudojimo ribos
1	Kodo puslapis (kaip apibrėžta 1 priedėlyje)	ASCII	nuo 01 iki 0A
2–14	Transporto priemonės registracijos numeris (kaip apibrėžta 1 priedėlyje)	ASCII	ASCII

▼B

9 priedėlis.

TIPO PATVIRTINIMAS BŪTINŲJŲ BANDYMŲ SĄRAŠAS

TURINYS

1. ĮVADAS

2. TRANSPORTO PRIEMONĖS BLOKO VEIKIMO BANDYMAI

3. JUDESIO JUTIKLIO VEIKIMO BANDYMAI

4. TACHOGRAFO KORTELIŲ VEIKIMO BANDYMAI

5. IŠORINIO GNSS ĮRENGINIO BANDYMAI

6. NUOTOLINIO RYŠIO ĮRENGINIO BANDYMAI

7. POPIERIAUS FUNKCINIAI BANDYMAI

8. SĄVEIKUMO BANDYMAI

1. ĮVADAS

1.1. **Tipo patvirtinimas**

Tachografo (ar jo komponento) arba tachografo kortelės EB tipo patvirtinimas grindžiamas:

— **saugumo sertifikavimu** remiantis bendrų kriterijų specifikacijomis pagal saugumo tikslą, atitinkantį šio priedo 10 priedėlio reikalavimus (turi būti užpildytas/iš dalies pakeistas),

— **veikimo sertifikavimu**, kurį atlieka valstybės narės institucija ir kuriuo patvirtinama, kad bandomas vienetas atitinka šio priedo reikalavimus dėl atliekamų funkcijų, matavimo tikslumo ir atsparumo aplinkos poveikiui,

— **sąveikumo sertifikavimu**, kurį atlieka kompetentinga institucija ir kuriuo patvirtinama, kad tachografas (arba tachografo kortelė) yra visiškai sąveikus su reikiamais tachografo kortelės (ar tachografo) modeliais (žr. šio priedo 8 skyrių).

Šiame priedėlyje nurodyta, kuriuos būtinuosius veikimo bandymus privalo atlikti valstybės narės institucija ir kuriuos būtinuosius sąveikumo bandymus turi atlikti kompetentinga institucija. Bandymų atlikimo tvarka ir jų rūšys išsamiau neaprašytos.

Saugumo sertifikavimo klausimai šiame priedėlyje neaptariami. Jei kai kurie tipo patvirtinimui reikalingi bandymai atliekami vykdant saugumo vertinimo ir sertifikavimo procesą, šių bandymų kartoti nereikia. Tokiu atveju galima tik patikrinti tokių bandymų rezultatus. Informacijos tikslais reikalavimai, kurie turėtų būti tikrinami (arba labai susiję su bandymais, kuriuos numatyta atlikti) atliekant saugumo sertifikavimą, šiame priedėlyje pažymėti žvaigždute.

Numeriais pažymėti reikalavimai nurodyti priede, o kiti reikalavimai – kituose priedėliuose (pvz., PIC_001 nurodo 3 priedėlio „Piktogramos“ reikalavimą PIC_001).

Priedėlyje atskirai aptariamas judesio jutiklio, transporto priemonės bloko ir išorinio GNSS įrenginio, kaip tachografo komponentų, tipo patvirtinimas. Išduodamas atskiras kiekvieno komponento tipo patvirtinimo pažymėjimas,

▼B

kuriame nurodomi kiti suderinami komponentai. Judesio jutiklio (arba išorinio GNSS įrenginio) veikimo bandymas atliekamas kartu su transporto priemonės bloku, o transporto priemonės bloko – kartu su judesio jutikliu (arba išoriniu GNSS įrenginiu).

Užtikrinti kiekvieno judesio jutiklio (arba išorinio GNSS įrenginio) modelio ir kiekvieno transporto priemonės bloko modelio sąveikumą nereikalaujama. Tokiu atveju judesio jutiklio (arba išorinio GNSS įrenginio) tipas gali būti patvirtintas tik kartu su atitinkamo transporto priemonės bloko tipo patvirtinimu, o transporto priemonės bloko tipas – tik kartu su judesio jutiklio (arba išorinio GNSS įrenginio) tipo patvirtinimu.

1.2. **Nuorodos**

Šiame priedėlyje naudoti šaltiniai:

IEC 60068-2-1 Aplinkos poveikio bandymai. 2-1 dalis. Bandymai. A bandymas. Šaltis.

IEC 60068-2-2 Pagrindinės aplinkos poveikio bandymų procedūros. 2 dalis. Bandymai. B bandymai. Sausasis kaitinimas (sinusinis).

IEC 60068-2-6 Aplinkos poveikio bandymai. 2 dalis. Bandymai. Fc bandymas. Vibracija.

IEC 60068-2-14 Aplinkos poveikio bandymai. 2-14 dalis. Bandymai. N bandymas. Temperatūros kitimas.

IEC 60068-2-27 Aplinkos poveikio bandymai. 2 dalis. Bandymai. Ea bandymas ir nurodymai. Smūgis.

IEC 60068-2-30 Aplinkos poveikio bandymai. 2-30 dalis. Bandymai. Db bandymas. Drėgnasis ciklinis kaitinimas (12 h + 12 h ciklas).

IEC 60068-2-64 Aplinkos poveikio bandymai. 2-64 dalis. Bandymai. Fh bandymas. Plačiajuostė atsitiktinė vibracija ir nurodymai.

IEC 60068-2-78 Aplinkos poveikio bandymai. 2-78 dalis. Bandymai. Bandymo kamera. Drėgnoji šiluma, nuostovioji būsena.

ISO 16750-3 Mechaninės apkrovos (2012 m. gruodžio mėn.).

ISO 16750-4 Klimatinės apkrovos (2010 m. balandžio mėn.).

ISO 20653 Kelių transporto priemonės. Apsaugos laipsnis (IP kodas). Elektros įrenginių apsauga nuo svetimkūnių, vandens ir prieigos.

ISO 10605:2008 + 2010 m. techninė pataisa + 2014 m. pakeitimas Nr. 1 Kelių transporto priemonės. Elektrostatinio išlydžio keliamų elektrinių trikdžių bandymo metodai.

ISO 7637-1:2002 + 2008 m. pakeitimas Nr. 1 Kelių transporto priemonės. Elektrinio laidumo ir sujungimo sukeliami elektriniai trikdžiai. 1 dalis. Apibrėžtys ir bendrosios nuostatos.

ISO 7637-2 Kelių transporto priemonės. Elektrinio laidumo ir sujungimo sukeliami elektriniai trikdžiai. 2 dalis. Elektrinio trumpojo pavienio impulso perdavimas tik maitinimo laidais.

ISO 7637-3 Kelių transporto priemonės. Elektrinio laidumo ir sujungimo sukeliami elektriniai trikdžiai. 3 dalis. Elektrinio trumpojo pavienio impulso perdavimas dėl talpinio arba indukcinio ryšio ne per maitinimo linijas.

ISO/IEC 7816-1 Atpažinimo kortelės. Lustinės kortelės su kontaktais. 1 dalis. Fizinės charakteristikos.

▼B

ISO/IEC 7816-2 Informacijos technologija. Atpažinimo kortelės. Lustinės kortelės su kontaktais. 2 dalis. Kontaktų matmenys ir vieta.

ISO/IEC 7816-3 Informacijos technologija. Atpažinimo kortelės. Lustinės kortelės su kontaktais. 3 dalis. Elektroniniai signalai ir siuntimo protokolai.

ISO/IEC 10373-1:2006 + 2012 m. pakeitimas Nr. 1 Atpažinimo kortelės. Bandymo metodai. 1 dalis. Bendrosios charakteristikos

ISO/IEC 10373-3:2010 + 2013 m. techninė pataisa Atpažinimo kortelės. Bandymo metodai. 3 dalis. Lustinės kortelės su kontaktais ir atitinkami sietuvų įtaisai.

ISO 16844-3:2004 + 2006 m. pataisa Nr. 1 Kelių transporto priemonės. Tachografų sistemos. 3 dalis. Judesio jutiklio sąsaja (su transporto priemonės blokais).

ISO 16844-4 Kelių transporto priemonės. Tachografų sistemos. 4 dalis. CAN sąsaja.

ISO 16844-6 Kelių transporto priemonės. Tachografų sistemos. 6 dalis. Diagnostika.

ISO 16844-7 Kelių transporto priemonės. Tachografų sistemos. 7 dalis. Parametrai.

ISO 534 Popierius ir kartonas. Storio, tankio ir savitojo tūrio nustatymas.

JT EEK R10 Vienodos transporto priemonių patvirtinimo nuostatos dėl elektromagnetinio suderinamumo (Jungtinių Tautų Europos ekonomikos komisija).

2. TRANSPORTO PRIEMONĖS BLOKO VEIKIMO BANDYMAI

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
1.	**Administracinis patikrinimas**		
1.1.	Dokumentai	Dokumentų tinkamumas	
1.2.	Gamintojo atliktų bandymų rezultatai	Įrengimo metu gamintojo atliktų bandymų rezultatai. Įrodymas popieriuje.	88, 89, 91
2.	**Apžiūra**		
2.1.	Atitiktis dokumentams		
2.2.	Identifikavimas/ženklinimas		224–226
2.3.	Medžiagos		219–223
2.4.	Plombavimas		398, 401–405
2.5.	Išorinės sąsajos		
3.	**Veikimo bandymai**		
3.1.	Užtikrinamos funkcijos		03, 04, 05, 07, 382
3.2.	Veikimo režimai		09–11*, 132, 133
3.3.	Funkcijų ir duomenų prieigos teisės		12*, 13*, 382, 383, 386–389
3.4.	Kortelės įkišimo ir ištraukimo stebėsena		15, 16, 17, 18, 19*, 20*, 132
3.5.	Greičio ir nuvažiuoto atstumo matavimas		21–31

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
3.6.	Laiko matavimas (bandymas atliekamas esant 20 °C)		38–43
3.7.	Vairuotojo veiklos stebėsena		44–53, 132
3.8.	Važiavimo būsenos stebėsena		54, 55, 132
3.9.	Rankomis įvedami duomenys		56–62
3.10.	Įmonės užraktų valdymas		63–68
3.11.	Kontrolės veiklos stebėsena		69, 70
3.12.	Įvykių ir (arba) trikčių aptikimas		71–88 132
3.13.	Įrangos identifikacijos duomenys		93*, 94*, 97, 100
3.14.	Duomenys apie vairuotojo kortelės įkišimą ir ištraukimą		102* – 104*
3.15.	Duomenys apie vairuotojo veiklą		105* – 107*
3.16.	Buvimo vietos duomenys		108* – 112*
3.17.	Odometro duomenys		113* – 115*
3.18.	Tikslaus greičio duomenys		116*
3.19.	Duomenys apie įvykius		117*
3.20.	Duomenys apie triktis		118*
3.21.	Kalibravimo duomenys		119* – 121*
3.22.	Laiko koregavimo duomenys		124*, 125*
3.23.	Duomenys apie kontrolės veiklą		126*, 127*
3.24.	Duomenys apie įmonės užraktus		128*
3.25.	Duomenų perkėlimo veiklos duomenys		129*
3.26.	Duomenys apie ypatingas būsenas		130*, 131*
3.27.	Informacijos įrašymas į tachografo korteles ir laikymas		134, 135, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148
3.28.	Rodymas ekrane		90, 132, 149–166, PIC_001, DIS_001
3.29.	Spausdinimas		90, 132, 167–179, PIC_001, PRT_001 – PRT_014
3.30.	Įspėjimas		132, 180–189, PIC_001
3.31.	Duomenų perkėlimas į išorines laikmenas		90, 132, 190–194
3.32.	Nuotolinis ryšys tikslinėms patikroms kelyje atlikti		195–197
3.33.	Duomenų persiuntimas į papildomus išorinius įtaisus		198, 199

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
3.34.	Kalibravimas		202–206*, 383, 384, 386–391
3.35.	Kalibravimo tikrinimas kelyje		207–209
3.36.	Laiko koregavimas		210–212*
3.37.	Papildomų funkcijų netrukdymas		06, 425
3.38.	Judesio jutiklio sąsaja		02, 122
3.39.	Išorinis GNSS įrenginys		03, 123
3.40.	Patikrinti, ar transporto priemonės blokas aptinka, užregistruoja ir saugo atmintyje transporto priemonės bloko gamintojo nustatytą (-us) įvykį (-ius) ir (arba) triktį (-is), kai poruotas judesio jutiklis reaguoja į magnetinius laukus, trukdančius fiksuoti transporto priemonės judėjimą.		217
3.41.	Šifravimo rinkinys ir standartiniai domeno parametrai		CSM_48, CSM_50
4.	**Aplinkos poveikio bandymai**		
4.1.	Temperatūra	Veikimas tikrinamas taip: Atliekamas bandymas pagal ISO 16750-4 5.1.1.2 skyrių: veikimo žemoje temperatūroje bandymas (72 h esant – 20 °C). Tai bandymas, aprašytas IEC 60068-2-1. Aplinkos poveikio bandymai. 2-1 dalis. Bandymai. A bandymas. Šaltis. Atliekamas bandymas pagal ISO 16750-4 5.1.2.2 skyrių: veikimo aukštoje temperatūroje bandymas (72 h esant 70 °C). Tai bandymas, aprašytas IEC 60068-2-2. Pagrindinės aplinkos poveikio bandymų procedūros. 2 dalis. Bandymai. B bandymai. Sausasis kaitinimas Atliekamas bandymas pagal ISO 16750-4 5.3.2 skyrių: Staigus nustatytos trukmės temperatūros pokytis (– 20 °C/70 °C, 20 ciklų, išlaikymo kiekvienoje temperatūroje trukmė 2 h). Bandant žemesnėje, aukštesnėje temperatūroje ir per temperatūros ciklus gali būti atliekami sumažinto rinkinio bandymai (iš nurodytųjų šios lentelės 3 skyriuje).	213
4.2.	Drėgmė	Patikrinama, ar transporto priemonės blokas gali išlaikyti ciklinę drėgmę (karščio bandymą), pagal IEC 60068-2-30 Db bandymą atliekant šešis 24 valandų ciklus, kai kiekvieno ciklo metu temperatūra kinta nuo + 25 °C iki + 55 °C, o santykinis drėgnis esant + 25 °C temperatūrai yra 97 %, o esant + 55 °C temperatūrai – 93 %.	214

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
4.3.	Mechaninis poveikis	1. Sinusiniai virpesiai: patikrinama, ar transporto priemonės blokas gali išlaikyti tokius sinusinius virpesius: nuolatinį 10 mm amplitudės 5–11 Hz dažnio poslinkį, nuolatinį 5g pagreitį, kai dažnis yra 11–300 Hz. Šis reikalavimas patikrinamas atliekant IEC 60068-2-6 Fc bandymą, trunkantį bent 3 × 12 valandų (po 12 valandų išilgai kiekvienos koordinačių ašies). ISO 16750-3 nereikalaujama atlikti sinusinių virpesių bandymo, jei prietaisas įrengtas atskiroje transporto priemonės vairuotojo kabinoje. 2. Atsitiktiniai virpesiai: atliekamas bandymas pagal ISO 16750-3 4.1.2.8 skyrių: VIII bandymas. Komercinė transporto priemonė, atskira vairuotojo kabina. Atsitiktinės vibracijos bandymas, 10–2 000 Hz, pagreičio vertikalia kryptimi kvadratinis vidurkis 21,3 m/s^2, išilgine kryptimi – 11,8 m/s^2, skersine kryptimi – 13,1 m/s^2, 3 kryptimis, po 32 h kiekviena kryptimi, įskaitant temperatūros ciklą – 20 – 70 °C. Tai bandymas, aprašytas IEC 60068-2-64. Aplinkos poveikio bandymai. 2-64 dalis. Bandymai. Fh bandymas. Plačiajuostė atsitiktinė vibracija ir nurodymai. 3. Smūgiai: mechaninio pusės sinusoidės 3g smūgio bandymas pagal ISO 16750. Pirmiau nurodyti bandymai atliekami su skirtingais bandomo įrangos tipo pavyzdžiais.	219
4.4.	Apsauga nuo vandens ir svetimkūnių	Atliekamas bandymas pagal ISO 20653. Kelių transporto priemonės. Apsaugos laipsnis (IP kodas). Elektros įrenginių apsauga nuo svetimkūnių, vandens ir prieigos (parametrai nekeičiami). Mažiausioji vertė IP 40.	220, 221
4.5.	Apsauga nuo viršįtampio	Patikrinama, ar transporto priemonės blokas gali išlaikyti maitinimą tokiomis sąlygomis: 24 V modeliai: 34 V, + 40 °C temperatūroje 1 valandą 12 V modeliai: 17 V, + 40 °C temperatūroje 1 valandą (ISO 16750-2)	216

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
4.6.	Apsauga nuo poliškumo pakeitimo	Patikrinama, ar transporto priemonės blokas gali išlaikyti jo maitinimo įtampos poliškumo pakeitimą (ISO 16750-2)	216
4.7.	Apsauga nuo trumpojo jungimo	Patikrinama, ar įvesties ir išvesties signalai apsaugoti nuo trumpojo jungimo su maitinimo ir įžeminimo linijomis (ISO 16750-2)	216
5.	**Elektromagnetinio suderinamumo bandymai**		
5.1.	Spinduliavimas ir imlumas	Atitiktis JT EEK R10 taisyklei	218
5.2.	Elektrostatinis išlydis	Atitiktis ISO 10605:2008 + 2010 m. techninių klaidų ištaisymas + 2014 m. pakeitimas Nr. 1 +/–4 kV kontaktiniam ir +/–8 kV oriniam išlydžiui	218
5.3.	Imlumas trumpojo pavienio impulso perdavimui per maitinimo linijas	24 V modeliams: atitiktis ISO 7637-2 + JT EEK taisyklė Nr. 10 3 red.: 1a impulsas: Vs = – 450 V, Ri = 50 omų 2a impulsas: Vs = + 37 V, Ri = 2 omai 2b impulsas: Vs = + 20 V, Ri = 0,05 omo 3a impulsas: Vs = – 150 V, Ri = 50 omų 3b impulsas: Vs = + 150 V, Ri = 50 omų 4 impulsas: Vs = – 16 V, Va = – 12 V, t6 = 100 ms 5 impulsas: Vs = + 120 V, Ri = 2,2 omo, td = 250 ms 12 V modeliams: atitiktis ISO 7637-1 + JT EEK taisyklė Nr. 10 3 red.: 1 impulsas: Vs = – 75 V, Ri = 10 omų 2a impulsas: Vs = + 37 V, Ri = 2 omai 2b impulsas: Vs = + 10 V, Ri = 0,05 omo 3a impulsas: Vs = – 112 V, Ri = 50 omų 3b impulsas: Vs = + 75 V, Ri = 50 omų 4 impulsas: Vs = – 6 V, Va = –5 V, t6 = 15 ms 5 impulsas: Vs = + 65 V, Ri = 3 omai, td = 100 ms 5 impulso bandymas turi būti atliekamas tik jei transporto priemonės blokas yra skirtas įrengti transporto priemonėje, kurioje nenaudojama jokia bendroji išorinė apsauga nuo susikaupusio krūvio. Siūlomą apsaugą nuo susikaupusio krūvio žr. ISO 16750-2, 4 redakcija, 4.6.4 skyrius.	218

▼B

3. JUDESIO JUTIKLIO VEIKIMO BANDYMAI

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
1.	**Administracinis patikrinimas**		
1.1.	Dokumentai	Dokumentų tinkamumas	
2.	**Apžiūra**		
2.1.	Atitiktis dokumentams		
2.2.	Identifikavimas/ženklinimas		225, 226
2.3.	Medžiagos		219–223
2.4.	Plombavimas		398, 401–405
3.	**Veikimo bandymai**		
3.1.	Jutiklio identifikavimo duomenys		95–97*
3.2.	Judesio jutiklio siejimas su transporto priemonės bloku		122*, 204
3.3.	Judėjimo aptikimas Judėjimo matavimo tikslumas		30–35
3.4.	Transporto priemonės bloko sąsaja		02
3.5.	Patikrinti, ar judesio jutiklis atsparus nuolatiniam magnetiniam laukui. Arba patikrinti, ar judesio jutiklis reaguoja į nuolatinius magnetinius laukus, trukdančius fiksuoti transporto priemonės judėjimą, kad prijungtas transporto priemonės blokas galėtų nustatyti, registruoti ir saugoti atmintyje jutiklio triktis.		217
4.	**Aplinkos poveikio bandymai**		
4.1.	Veikimo temperatūra	Veikimas tikrinamas (kaip nurodyta bandyme Nr. 3.3) [–40 °C – +135 °C] temperatūros intervale: pagal IEC 60068-2-1 atliekamas Ad bandymas, trunkantis 96 valandas esant žemiausiai To_{min} temperatūrai, pagal IEC 60068-2-2 atliekamas Bd bandymas, trunkantis 96 valandas esant aukščiausiai To_{max} temperatūrai, atliekamas bandymas pagal ISO 16750-4 5.1.1.2 skyrių: veikimo žemoje temperatūroje bandymas (24 h esant –40 °C). Tai bandymas, aprašytas IEC 60068-2-1. Aplinkos poveikio bandymai. 2-1 dalis. Bandymai. A bandymas. Šalčio IEC 68-2-2 Bd bandymas, trunkantis 96 valandas esant žemiausiai –40 °C temperatūrai, atliekamas bandymas pagal ISO 16750-4 5.1.2.2 skyrių: veikimo aukštoje temperatūroje bandymas (96 h esant 135 °C). Tai bandymas, aprašytas IEC 60068-2-2. Pagrindinės aplinkos poveikio bandymų procedūros. 2 dalis. Bandymai. B bandymai. Sausasis kaitinimas	213

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
4.2.	Temperatūros ciklai	Atliekamas bandymas pagal ISO 16750-4 5.3.2 skyrių: Staigus nustatytos trukmės temperatūros pokytis (–40 °C/135 °C, 20 ciklų, išlaikymo kiekvienoje temperatūroje trukmė 30 minučių). IEC 60068-2-14 Aplinkos poveikio bandymai. 2-14 dalis. Bandymai. N bandymas. Temperatūros kitimas.	213
4.3.	Drėgmės ciklai	Patikrinamas veikimas (kaip nustatyta bandyme Nr. 3.3) pagal IEC 60068-2-30 Db bandymą atliekant šešis 24 valandų ciklus, kai kiekvieno ciklo metu temperatūra kinta nuo +25 °C iki +55 °C, o santykinis drėgnis esant +25 °C temperatūrai yra 97 %, o esant +55 °C temperatūrai – 93 %.	214
4.4.	Vibracija	ISO 16750-3 4.1.2.6 skyrius. VI bandymas. Komercinė transporto priemonė, variklis, pavarų dėžė. Mišraus režimo vibracijos bandymas, apimantis: a) sinusinių virpesių bandymą, 20–520 Hz, 11,4–120 m/s^2, <= 0,5 oktavos/min; b) atsitiktinių virpesių bandymą, 10–2 000 Hz, RMS 177 m/s^2, 94 h kiekviena ašimi, įskaitant temperatūros ciklą –20 – 70 °C). Tai bandymas, aprašytas IEC 60068-2-80. Aplinkos poveikio bandymai. 2-80 dalis. Bandymai. Fi bandymas. Vibracija. Mišrus režimas.	219
4.5.	Mechaninis smūgis	ISO 16750-3 4.2.3 skyrius. VI bandymas. Pavarų dėžėje ar ant jos sumontuotų įtaisų bandymas pusės sinusoidės smūgiais, esant sutartam pagreičiui 3 000–15 000 m/s^2 intervale, sutartai, tačiau < 1 ms, impulso trukmei ir sutartam smūgių skaičiui. Tai bandymas, aprašytas IEC 60068-2-27. Aplinkos poveikio bandymai. 2 dalis. Bandymai. Ea bandymas ir nurodymai. Smūgis.	219
4.6.	Apsauga nuo vandens ir svetimkūnių	Atliekamas bandymas pagal ISO 20653. Kelių transporto priemonės. Apsaugos laipsnis (IP kodas). Elektros įrenginių apsauga nuo svetimkūnių, vandens ir prieigos. (Tikslinė vertė IP 64)	220, 221
4.7.	Apsauga nuo poliškumo pakeitimo	Patikrinama, ar judesio jutiklis gali išlaikyti jo maitinimo įtampos poliškumo pakeitimą.	216
4.8.	Apsauga nuo trumpojo jungimo	Patikrinama, ar įvesties ir išvesties signalai apsaugoti nuo trumpojo jungimo su maitinimo ir įžeminimo linijomis	216

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
5.	**Elektromagnetinis suderinamumas**		
5.1.	Spinduliavimas ir imlumas	Patikrinama atitiktis JT EEK R10 taisyklei	218
5.2.	Elektrostatinis išlydis	Atitiktis ISO 10605:2008 + 2010 m. techninių klaidų ištaisymas + 2014 m. pakeitimas Nr. 1 +/–4 kV kontaktiniam ir +/–8 kV oriniam išlydžiui	218
5.3.	Imlumas trumpojo pavienio impulso perdavimui per duomenų linijas	24 V modeliams: atitiktis ISO 7637-2 + JT EEK taisyklė Nr. 10 3 red.: 1a impulsas: Vs = –450 V, Ri = 50 omų 2 a impulsas: Vs = +37 V, Ri = 2 omai 2b impulsas: Vs = +20 V, Ri = 0,05 omo 3 a impulsas: Vs = -150 V, Ri = 50 omų 3b impulsas: Vs = +150 V, Ri = 50 omų 4 impulsas: Vs = –16 V, Va = –12 V, t6 = 100 ms 5 impulsas: Vs = +120 V, Ri = 2,2 omo, td = 250 ms 12 V modeliams: atitiktis ISO 7637-1 + JT EEK taisyklė Nr. 10 3 red.: 1 impulsas: Vs = –75 V, Ri = 10 omų 2 a impulsas: Vs = +37 V, Ri = 2 omai 2b impulsas: Vs = +10 V, Ri = 0,05 omo 3 a impulsas: Vs = –112 V, Ri = 50 omų 3b impulsas: Vs = +75 V, Ri = 50 omų 4 impulsas: Vs = –6 V, Va = –5 V, t6 = 15 ms 5 impulsas: Vs = +65 V, Ri = 3 omai, td = 100 ms 5 impulso bandymas turi būti atliekamas tik jei transporto priemonės blokas skirtas įrengti transporto priemonėje, kurioje nenaudojama jokia bendroji išorinė apsauga nuo susikaupusio krūvio. Siūlomą apsaugą nuo susikaupusio krūvio žr. ISO 16750-2, 4 redakcija, 4.6.4 skyrius.	218

4. TACHOGRAFO KORTELIŲ VEIKIMO BANDYMAI

Šiame (4) skyriuje nurodytus bandymus

Nr. 5 „Protokolo bandymai“,

Nr. 6 „Kortelės sandara“ ir

Nr. 7 „Veikimo bandymai“

gali atlikti vertintojas arba sertifikuotojas, vykdydami lusto modulio bendrų kriterijų (CC) saugumo sertifikavimo procesą.

Bandymai Nr. 2.3 ir 4.2 yra tokie patys. Tai kortelės pagrindo ir lusto modulio derinio mechaniniai bandymai. Jei vienas iš šių komponentų (kortelės pagrindas, lusto modulis) pakeičiamas, šie bandymai būtini.

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
1.	**Administracinis patikrinimas**		
1.1.	Dokumentai	Dokumentų tinkamumas	
2.	**Kortelės pagrindas**		
2.1.	Spausdintiniai elementai	Patikrinti, ar visos apsaugos priemonės ir matomi duomenys ant kortelės išspausdinti teisingai ir atitinka reikalavimus. [žymuo] 1C priedas, 4.1 skyrius „Matomi duomenys“, 227) Kortelės priekyje: kortelę išdavusios valstybės narės valstybine kalba arba kalbomis didžiosiomis raidėmis išspausdinti žodžiai „Vairuotojo kortelė“, „Kontrolės kortelė“, „Dirbtuvių kortelė“ arba „Įmonės kortelė“. [valstybės narės pavadinimas] 1C priedas, 4.1 skyrius „Matomi duomenys“, 228) Kortelės priekyje: kortelę išdavusios valstybės narės pavadinimas (neprivalomas). [ženklas] 1C priedas, 4.1 skyrius „Matomi duomenys“, 229) Kortelės priekyje: kortelę išdavusios valstybės narės skiriamasis ženklas, išspausdintas negatyvo atvaizdu mėlyname stačiakampyje ir apsuptas dvylikos geltonų žvaigždučių. [sąrašas] 1C priedas, 4.1 skyrius „Matomi duomenys“, 232) Kitoje kortelės pusėje: pateikiamas kortelės priekyje sunumeruotų punktų paaiškinimas. [spalva] 1C priedas, 4.1 skyrius „Matomi duomenys“, 234) Tachografo kortelių fone turi vyrauti šios spalvos: — vairuotojo kortelės – balta, — dirbtuvių kortelės – raudona, — kontrolės kortelės – mėlyna, — įmonės kortelės – geltona.	227–229, 232, 234–236

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
		[saugumas] 1C priedas, 4.1 skyrius „Matomi duomenys“, 235) Tachografo kortelės turi turėti bent tokius apsaugos nuo klastojimo ir neteisėto keitimo elementus: — apsauginio dizaino foną su smulkiu ornamentiniu raštu ir spalvotais spaudiniais, — bent vieną dvispalvę mikrospaudos eilutę.	
		[žymos] 1C priedas, 4.1 skyrius „Matomi duomenys“, 236) Valstybės narės gali naudoti papildomas spalvas ir ženklus, pvz., nacionalinius simbolius ir apsaugos elementus.	
		[patvirtinimo ženklas] Tachografo kortelės turi turėti patvirtinimo ženklą. Patvirtinimo ženklą sudaro: — stačiakampis, kuriame yra raidė „e“, po jos nurodomas patvirtinimą išdavusios šalies skiriamasis skaičius arba raidė, — patvirtinimo numeris, atitinkantis tachografo kortelės patvirtinimo pažymėjimo numerį, nurodomas bet kurioje vietoje kuo arčiau to stačiakampio.	
2.2.	Mechaniniai bandymai	[kortelės dydis] Tachografo kortelės turi atitikti standartą ISO/IEC 7810 Atpažinimo kortelės. Fizikinės charakteristikos. [5] Kortelės matmenys, [5.1] Kortelės dydis, [5.1.1] Kortelės matmenys ir leidžiamosios nuokrypos, kortelės tipas ID-1. Nenaudota kortelė	240, 243 ISO/IEC 7810
		[kortelės kraštai] Tachografo kortelės turi atitikti standartą ISO/IEC 7810 Atpažinimo kortelės. Fizikinės charakteristikos. [5] Kortelės matmenys, [5.1] Kortelės dydis, [5.1.2] Kortelės kraštai	

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
		[kortelės konstrukcija] Tachografo kortelės turi atitikti standartą ISO/IEC 7810 Atpažinimo kortelės. Fizikinės charakteristikos. [6] Kortelės konstrukcija	
		[kortelės medžiagos] Tachografo kortelės turi atitikti standartą ISO/IEC 7810 Atpažinimo kortelės. Fizikinės charakteristikos. [7] Kortelės medžiagos	
		[lenkiamasis standis] Tachografo kortelės turi atitikti standartą ISO/IEC 7810 Atpažinimo kortelės. Fizikinės charakteristikos. [8] Kortelės charakteristikos, [8.1] Lenkiamasis standis	
		[toksiškumas] Tachografo kortelės turi atitikti standartą ISO/IEC 7810 Atpažinimo kortelės. Fizikinės charakteristikos. [8] Kortelės charakteristikos, [8.3] Toksiškumas	
		[cheminis atsparumas] Tachografo kortelės turi atitikti standartą ISO/IEC 7810 Atpažinimo kortelės. Fizikinės charakteristikos. [8] Kortelės charakteristikos, [8.4] Cheminis atsparumas	
		[kortelės stabilumas] Tachografo kortelės turi atitikti standartą ISO/IEC 7810 Atpažinimo kortelės. Fizikinės charakteristikos. [8] Kortelės charakteristikos, [8.5] Kortelės matmenų stabilumas ir persimetimas dėl temperatūros ir drėgmės.	

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
		[šviesa] Tachografo kortelės turi atitikti standartą ISO/IEC 7810 Atpažinimo kortelės. Fizikinės charakteristikos. [8] Kortelės charakteristikos, [8.6] Šviesa	
		[patvarumas] 1C priedas, 4.4 skyrius „Aplinkos ir elektrinės specifikacijos“, 241) Pagal aplinkos ir elektrines specifikacijas naudojamos tachografo kortelės turi tinkamai veikti penkerius metus.	
		[atlupimo stipris] Tachografo kortelės turi atitikti standartą ISO/IEC 7810 Atpažinimo kortelės. Fizikinės charakteristikos. [8] Kortelės charakteristikos, [8.8] Atlupimo stipris	
		[sukibimas arba sulipimas] Tachografo kortelės turi atitikti standartą ISO/IEC 7810 Atpažinimo kortelės. Fizikinės charakteristikos. [8] Kortelės charakteristikos, [8.9] Sukibimas arba sulipimas	
		[persimetimas] Tachografo kortelės turi atitikti standartą ISO/IEC 7810 Atpažinimo kortelės. Fizikinės charakteristikos. [8] Kortelės charakteristikos, [8.11] Bendras kortelės persimetimas	
		[atsparumas šilumai] Tachografo kortelės turi atitikti standartą ISO/IEC 7810 Atpažinimo kortelės. Fizikinės charakteristikos. [8] Kortelės charakteristikos, [8.12] Atsparumas šilumai	

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
		[paviršiaus iškraipymai] Tachografo kortelės turi atitikti standartą ISO/IEC 7810 Atpažinimo kortelės. Fizikinės charakteristikos. [8] Kortelės charakteristikos, [8.13] Paviršiaus iškraipymai	
		[tarša] Tachografo kortelės turi atitikti standartą ISO/IEC 7810 Atpažinimo kortelės. Fizikinės charakteristikos. [8] Kortelės charakteristikos, [8.14] Tarša ir kortelės komponentų sąveika	
2.3.	Mechaniniai bandymai su įterptuoju lusto moduliu	[lenkimas] Tachografo kortelės turi atitikti standartą ISO/IEC 7810:2003/2009 m. pakeitimas Nr. 1. Atpažinimo kortelės. Fizikinės charakteristikos. 1 keitinys. Lustinėms kortelėms taikomi kriterijai. [9.2] Dinaminis lenkimo įtempis Bendras lenkimo ciklų skaičius 4 000.	ISO/IEC 7810
		[susukimas] Tachografo kortelės turi atitikti standartą ISO/IEC 7810:2003/2009 m. pakeitimas Nr. 1. Atpažinimo kortelės. Fizikinės charakteristikos. 1 keitinys. Lustinėms kortelėms taikomi kriterijai. [9.3] Dinaminis sukimo įtempis Bendras susukimo ciklų skaičius 4 000.	
3.	**Modulis**		
3.1.	Modulis	Modulis – tai lusto korpusas ir kontaktų plokštelė. [paviršiaus profilis] Tachografo kortelės turi atitikti standartą ISO/IEC 7816-1:2011. Atpažinimo kortelės. Lustinės kortelės. 1 dalis. Kortelės su kontaktais. Fizikinės charakteristikos. [4.2] Kontaktų paviršiaus profilis	ISO/IEC 7816

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
		[mechaninis atsparumas] Tachografo kortelės turi atitikti standartą ISO/IEC 7816-1:2011. Atpažinimo kortelės. Lustinės kortelės. 1 dalis. Kortelės su kontaktais. Fizikinės charakteristikos. [4.3] Mechaninis atsparumas (kortelės ir kontaktų)	
		[elektrinė varža] Tachografo kortelės turi atitikti standartą ISO/IEC 7816-1:2011. Atpažinimo kortelės. Lustinės kortelės. 1 dalis. Kortelės su kontaktais. Fizikinės charakteristikos. [4.4] Elektrinė varža (kontaktų)	
		[matmenys] Tachografo kortelės turi atitikti standartą ISO/IEC 7816-2:2007. Atpažinimo kortelės. Lustinės kortelės. 2 dalis. Kortelės su kontaktais. Kontaktų matmenys ir vieta. [3] Kontaktų matmenys	
		[vieta] Tachografo kortelės turi atitikti standartą ISO/IEC 7816-2:2007. Atpažinimo kortelės. Lustinės kortelės. 2 dalis. Kortelės su kontaktais. Kontaktų matmenys ir vieta. [4] Kontaktų skaičius ir vieta Jei modulis yra šešių kontaktų, C4 ir C8 kontaktams šio bandymo reikalavimas netaikomas.	
4.	**Lustas**		
4.1.	Lustas	[veikimo temperatūra] Tachografo kortelės lustas turi veikti aplinkos temperatūrai esant – 25 °C – + 85 °C intervale.	241–244 JT EEK R10 ISO/IEC 7810 ISO/IEC 10373

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
		[temperatūra ir drėgmė] 1C priedas, 4.4 skyrius „Aplinkos ir elektrinės specifikacijos“, 241) Tachografo kortelės turi gebėti tinkamai veikti visomis Bendrijos teritorijai būdingomis klimato sąlygomis ir bent jau temperatūroje nuo – 25 °C iki + 70 °C, o trumpam – iki + 85 °C temperatūroje. „Trumpam“ reiškia ne ilgiau kaip 4 valandas kiekvienąkart ir ne daugiau kaip 100 kartų per visą kortelės naudojimo laiką. Tachografo kortelės nuosekliais etapais nustatytą laiką laikomos aplinkoje, kurioje užtikrinama toliau nurodyta temperatūra ir drėgmė. Po kiekvieno etapo išbandomas tachografo kortelių elektrinis veikimas. 1. Temperatūra – 20 °C, trukmė 2 h. 2. Temperatūra +/–0 °C, trukmė 2 h. 3. Temperatūra + 20 °C, santykinis drėgnis 50 %, trukmė 2 h. 4. Temperatūra + 50 °C, santykinis drėgnis 50 %, trukmė 2 h. 5. Temperatūra +7 0 °C, santykinis drėgnis 50 %, trukmė 2 h. Trumpam temperatūra padidinama iki + 85 °C, santykinis drėgnis 50 %, trukmė 60 min. 6. Temperatūra + 70 °C, santykinis drėgnis 85 %, trukmė 2 h. Trumpam temperatūra padidinama iki + 85 °C, santykinis drėgnis 85 %, trukmė 30 min.	
		[drėgmė] 1C priedas, 4.4 skyrius „Aplinkos ir elektrinės specifikacijos“, 242) Tachografo kortelės turi tinkamai veikti esant 10–90 % drėgniui.	
		[elektromagnetinis suderinamumas (EMS)] 1C priedas, 4.4 skyrius „Aplinkos ir elektrinės specifikacijos“, 244) Naudojamos tachografo kortelės turi atitikti EEK taisyklę R10, susijusią su elektromagnetiniu suderinamumu.	

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
		[statinė elektra] 1C priedas, 4.4 skyrius „Aplinkos ir elektrinės specifikacijos“, 244) Naudojamos tachografo kortelės turi būti apsaugotos nuo elektrostatinių išlydžių. Tachografo kortelės turi atitikti standartą ISO/IEC 7810:2003/2009 m. pakeitimas Nr. 1. Atpažinimo kortelės. Fizikinės charakteristikos. 1 keitinys. Lustinėms kortelėms taikomi kriterijai. [9.4] Statinė elektra [9.4.1] Lustinės kortelės su kontaktais Bandymo įtampa 4 000 V.	
		[rentgeno spinduliuotė] Tachografo kortelės turi atitikti standartą ISO/IEC 7810:2003/2009 m. pakeitimas Nr. 1. Atpažinimo kortelės. Fizikinės charakteristikos. 1 keitinys. Lustinėms kortelėms taikomi kriterijai. [9.1] Rentgeno spinduliuotė	
		[ultravioletinė spinduliuotė] ISO/IEC 10373-1:2006. Atpažinimo kortelės. Bandymo metodai. 1 dalis. Bendrosios charakteristikos [5.11] Ultravioletinė spinduliuotė	
		[3 ratai] Tachografo kortelės turi atitikti standartą ISO/IEC 10373-1:2006/2012 m. pakeitimas Nr. 1. Atpažinimo kortelės. Bandymo metodai. 1 dalis. Bendrosios charakteristikos. 1 keitinys. [5.22] Lustinės kortelės. Mechaninis atsparumas. Lustinių kortelių su kontaktais 3 ratų bandymas.	
		[vyniojimas] Tachografo kortelės turi atitikti standartą MasterCard CQM V2.03:2013 [11.1.3] R-L3-14-8: Vyniojimo bandymo tvirtumas. [13.2.1.32] TM-422: Mechaninis atsparumas. Vyniojimo bandymas.	

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
4.2.	Į kortelės pagrindą įterptojo lusto modulio mechaniniai bandymai-> tas pats kaip 2.3	[lenkimas] Tachografo kortelės turi atitikti standartą ISO/IEC 7810:2003/2009 m. pakeitimas Nr. 1. Atpažinimo kortelės. Fizikinės charakteristikos. 1 keitinys. Lustinėms kortelėms taikomi kriterijai. [9.2] Dinaminis lenkimo įtempis Bendras lenkimo ciklų skaičius 4 000. [susukimas] Tachografo kortelės turi atitikti standartą ISO/IEC 7810:2003/2009 m. pakeitimas Nr. 1. Atpažinimo kortelės. Fizikinės charakteristikos. 1 keitinys. Lustinėms kortelėms taikomi kriterijai. [9.3] Dinaminis sukimo įtempis Bendras susukimo ciklų skaičius 4 000.	ISO/IEC 7810
5.	**Protokolo bandymai**		
5.1.	ATR	Patikrinama, ar ATR atitinka reikalavimus.	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2.	T=0	Patikrinama, ar protokolas T=0 atitinka reikalavimus.	ISO/IEC 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3.	PTS	Patikrinama, ar komanda PTS atitinka reikalavimus nustatant T=1 iš T=0.	ISO/IEC 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4.	T=1	Patikrinama, ar protokolas T=1 atitinka reikalavimus.	ISO/IEC 7816-3 TCS_11, TCS_13, TCS_16
6.	**Kortelės struktūra**		
6.1.		Išbandoma, ar kortelės rinkmenų struktūra atitinka reikalavimus – ar kortelėje yra privalomosios rinkmenos ir jų prieigos sąlygos.	TCS_22 – TCS_28 TCS_140 – TCS_179
7.	**Veikimo bandymai**		
7.1.	Įprastas apdorojimas	Bent po kartą išbandomas kiekvienos komandos leidžiamasis naudojimas (pvz.: išbandoma UPDATE_BINARY komanda su CLA = „00“, CLA = „0C“ ir su skirtingais P1, P2 ir Lc) parametrais). Patikrinama, ar kortelėje faktiškai buvo atlikti veiksmai (pvz.: nuskaitant rinkmeną, kuri buvo paveikta duota komanda)	TCS_29 – TCS_139

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
7.2.	Klaidų pranešimai	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 saugumo sertifikavimą).	
7.3.	Šifravimo rinkinys ir standartiniai domeno parametrai		CSM_48, CSM_50
8.	**Individualizavimas**		
8.1.	Optinis individualizavimas	1C priedas, 4.1 skyrius „Matomi duomenys“, 230) Kortelės priekyje: informacija, nurodoma išduodamoje kortelėje.	230, 231, 235
		1C priedas, 4.1 skyrius „Matomi duomenys“, 231) Kortelės priekyje: datos rašomos formatu „dd/mm/yyyy“ arba „dd.mm.yyyy“ (diena, mėnesis, metai).	
		1C priedas, 4.1 skyrius „Matomi duomenys“, 235) Tachografo kortelės turi turėti bent tokius apsaugos nuo klastojimo ir neteisėto keitimo elementus: — nuotraukos plote apsauginio dizaino fonas ir nuotrauka turi persikloti.	

5. IŠORINIO GNSS ĮRENGINIO BANDYMAI

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
1.	**Administracinis patikrinimas**		
1.1.	Dokumentai	Dokumentų tinkamumas	
2.	**Išorinio GNSS įrenginio apžiūra**		
2.1.	Atitiktis dokumentams		
2.2.	Identifikavimas/ženklinimas		224–226
2.3.	Medžiagos		219–223
3.	**Veikimo bandymai**		
3.1.	Jutiklio identifikavimo duomenys		98, 99
3.2.	Išorinio GNSS įrenginio sujungimas su transporto priemonės bloku		123, 205

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
3.3.	GNSS vieta		36, 37
3.4.	Transporto priemonės bloko sąsaja, kai GNSS imtuvas yra transporto priemonės bloko išorėje		03
3.5.	Šifravimo rinkinys ir standartiniai domeno parametrai		CSM_48, CSM_50
4.	**Aplinkos poveikio bandymai**		
4.1.	Temperatūra	Veikimas tikrinamas taip: Atliekamas bandymas pagal ISO 16750-4 5.1.1.2 skyrių: veikimo žemoje temperatūroje bandymas (72 h esant – 20 °C). Tai bandymas, aprašytas IEC 60068-2-1. Aplinkos poveikio bandymai. 2-1 dalis. Bandymai. A bandymas. Šaltis. Atliekamas bandymas pagal ISO 16750-4 5.1.2.2 skyrių: veikimo aukštoje temperatūroje bandymas (72 h esant 70 °C). Tai bandymas, aprašytas IEC 60068-2-2. Pagrindinės aplinkos poveikio bandymų procedūros. 2 dalis. Bandymai. B bandymai. Sausasis kaitinimas Atliekamas bandymas pagal ISO 16750-4 5.3.2 skyrių. Staigus nustatytos trukmės temperatūros pokytis (– 20 °C/ 70 °C, 20 ciklų, išlaikymo kiekvienoje temperatūroje trukmė 1 h). Bandant žemesnėje, aukštesnėje temperatūroje ir per temperatūros ciklus gali būti atliekami sumažinto rinkinio bandymai (iš nurodytųjų šios lentelės 3 skyriuje).	213
4.2.	Drėgmė	Patikrinama, ar transporto priemonės blokas gali išlaikyti ciklišką drėgmės poveikį (karščio bandymą), pagal IEC 60068-2-30 Db bandymą atliekant šešis 24 valandų ciklus, kai kiekvieno ciklo metu temperatūra kinta nuo + 25 °C iki + 55 °C, o santykinis drėgnis esant + 25 °C temperatūrai yra 97 %, o esant + 55 °C temperatūrai – 93 %.	214
4.3.	Mechaninis poveikis	1. Sinusiniai virpesiai: patikrinama, ar transporto priemonės blokas gali išlaikyti tokius sinusinius virpesius: nuolatinį 10 mm amplitudės 5–11 Hz dažnio poslinkį, nuolatinį 5g pagreitį, kai dažnis yra 11–300 Hz. Šis reikalavimas patikrinamas atliekant IEC 60068-2-6 Fc bandymą, trunkantį bent 3 × 12 valandų (po 12 valandų išilgai kiekvienos koordinačių ašies). ISO 16750-3 nereikalaujama atlikti sinusinių virpesių bandymo, jei prietaisas įrengtas atskiroje transporto priemonės vairuotojo kabinoje.	219

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
		2. Atsitiktiniai virpesiai: atliekamas bandymas pagal ISO 16750-3 4.1.2.8 skyrių: VIII bandymas. Komercinė transporto priemonė, atskira vairuotojo kabina. Atsitiktinės vibracijos bandymas, 10–2 000 Hz, pagreičio vertikalia kryptimi kvadratinis vidurkis 21,3 m/s^2, išilgine kryptimi – 11,8 m/s^2, skersine kryptimi – 13,1 m/s^2, 3 kryptimis, po 32 h kiekviena kryptimi, įskaitant temperatūros ciklą – 20 – 70 °C. Tai bandymas, aprašytas IEC 60068-2-64. Aplinkos poveikio bandymai. 2-64 dalis. Bandymai. Fh bandymas. Plačiajuostė atsitiktinė vibracija ir nurodymai. 3. Smūgiai: mechaninio pusės sinusoidės 3g smūgio bandymas pagal ISO 16750. Pirmiau nurodyti bandymai atliekami su skirtingais bandomo įrangos tipo pavyzdžiais.	
4.4.	Apsauga nuo vandens ir svetimkūnių	Atliekamas bandymas pagal ISO 20653. Kelių transporto priemonės. Apsaugos laipsnis (IP kodas). Elektros įrenginių apsauga nuo svetimkūnių, vandens ir prieigos (parametrai nekeičiami)	220, 221
4.5.	Apsauga nuo viršįtampio	Patikrinama, ar transporto priemonės blokas gali išlaikyti maitinimą tokiomis sąlygomis: 24 V modeliai: 34 V, + 40 °C temperatūroje 1 valandą 12 V modeliai: 17 V, + 40 °C temperatūroje 1 valandą (ISO 16750-2, 4.3 skyrius)	216
4.6.	Apsauga nuo poliškumo pakeitimo	Patikrinama, ar transporto priemonės blokas gali išlaikyti jo maitinimo įtampos poliškumo pakeitimą (ISO 16750-2, 4.7 skyrius)	216
4.7.	Apsauga nuo trumpojo jungimo	Patikrinama, ar įvesties ir išvesties signalai apsaugoti nuo trumpojo jungimo su maitinimo ir įžeminimo linijomis (ISO 16750-2, 4.10 skyrius)	216
5.	**Elektromagnetinio suderinamumo bandymai**		
5.1.	Spinduliavimas ir imlumas	Atitiktis JT EEK R10 taisyklei	218

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
5.2.	Elektrostatinis išlydis	Atitiktis ISO 10605:2008 + 2010 m. techninių klaidų ištaisymas + 2014 m. pakeitimas Nr. 1 +/–4 kV kontaktiniam ir +/–8 kV oriniam išlydžiui	218
5.3.	Imlumas trumpojo pavienio impulso perdavimui per maitinimo linijas	24 V modeliams: atitiktis ISO 7637-2 + JT EEK taisyklė Nr. 10 3 red.: 1a impulsas: Vs = – 450 V, Ri = 50 omų 2 a impulsas: Vs = + 37 V, Ri = 2 omai 2b impulsas: Vs = + 20 V, Ri = 0,05 omo 3 a impulsas: Vs = – 150 V, Ri = 50 omų 3b impulsas: Vs = + 150 V, Ri = 50 omų 4 impulsas: Vs = – 16 V, Va = –12 V, t6 = 100 ms 5 impulsas: Vs = + 120 V, Ri = 2,2 omo, td = 250 ms 12 V modeliams: atitiktis ISO 7637-1 + JT EEK taisyklė Nr. 10 3 red.: 1 impulsas: Vs = – 75 V, Ri = 10 omų 2 a impulsas: Vs = + 37 V, Ri = 2 omai 2b impulsas: Vs = + 10 V, Ri = 0,05 omo 3 a impulsas: Vs = – 112 V, Ri = 50 omų 3b impulsas: Vs = + 75 V, Ri = 50 omų 4 impulsas: Vs = – 6 V, Va = –5 V, t6 = 15 ms 5 impulsas: Vs = + 65 V, Ri = 3 omai, td = 100 ms 5 impulso bandymas turi būti atliekamas tik jei transporto priemonės blokas yra skirtas įrengti transporto priemonėje, kurioje nenaudojama jokia bendroji išorinė apsauga nuo susikaupusio krūvio. Siūlomą apsaugą nuo susikaupusio krūvio žr. ISO 16750-2, 4 redakcija, 4.6.4 skyrius.	218

6. NUOTOLINIO RYŠIO ĮRENGINIO BANDYMAI

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
1.	**Administracinis patikrinimas**		
1.1.	Dokumentai	Dokumentų tinkamumas	
2.	**Apžiūra**		
2.1.	Atitiktis dokumentams		
2.2.	Identifikavimas/ženklinimas		225, 226
2.3.	Medžiagos		219–223
4.	**Aplinkos poveikio bandymai**		
4.1.	Temperatūra	Veikimas tikrinamas taip: Atliekamas bandymas pagal ISO 16750-4 5.1.1.2 skyrių: veikimo žemoje temperatūroje bandymas (72 h esant –20 °C). Tai bandymas, aprašytas IEC 60068-2-1. Aplinkos poveikio bandymai. 2-1 dalis. Bandymai. A bandymas. Šaltis.	213

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
		Atliekamas bandymas pagal ISO 16750-4 5.1.2.2 skyrių: veikimo aukštoje temperatūroje bandymas (72 h esant 70 °C). Tai bandymas, aprašytas IEC 60068-2-2. Pagrindinės aplinkos poveikio bandymų procedūros. 2 dalis. Bandymai. B bandymai. Sausasis kaitinimas Atliekamas bandymas pagal ISO 16750-4 5.3.2 skyrių. Staigus nustatytos trukmės temperatūros pokytis (–20 °C/ 70 °C, 20 ciklų, išlaikymo kiekvienoje temperatūroje trukmė 1 h). Bandant žemesnėje, aukštesnėje temperatūroje ir per temperatūros ciklus gali būti atliekami sumažinto rinkinio bandymai (iš nurodytųjų šios lentelės 3 skyriuje).	
4.4.	Apsauga nuo vandens ir svetimkūnių	Atliekamas bandymas pagal ISO 20653. Kelių transporto priemonės. Apsaugos laipsnis (IP kodas). Elektros įrenginių apsauga nuo svetimkūnių, vandens ir prieigos (tikslinė vertė IP 40).	220, 221
5.	**Elektromagnetinio suderinamumo bandymai**		
5.1.	Spinduliavimas ir imlumas	Atitiktis JT EEK R10 taisyklei	218
5.2.	Elektrostatinis išlydis	Atitiktis ISO 10605:2008 + 2010 m. techninių klaidų ištaisymas + 2014 m. pakeitimas Nr. 1 +/–4 kV kontaktiniam ir +/–8 kV oriniam išlydžiui	218
5.3.	Imlumas trumpojo pavienio impulso perdavimui per maitinimo linijas	24 V modeliams: atitiktis ISO 7637-2 + JT EEK taisyklė Nr. 10 3 red.: 1a impulsas: Vs = –450 V, Ri = 50 omų 2 a impulsas: Vs = +37 V, Ri = 2 omai 2b impulsas: Vs = +20 V, Ri = 0,05 omo 3 a impulsas: Vs = –150 V, Ri = 50 omų 3b impulsas: Vs = +150 V, Ri = 50 omų 4 impulsas: Vs = –16 V, Va = –12 V, t6 = 100 ms 5 impulsas: Vs = +120 V, Ri = 2,2 omo, td = 250 ms 12 V modeliams: atitiktis ISO 7637-1 + JT EEK taisyklė Nr. 10 3 red.: 1 impulsas: Vs = –75 V, Ri = 10 omų 2 a impulsas: Vs = +37 V, Ri = 2 omai 2b impulsas: Vs = +10 V, Ri = 0,05 omo 3 a impulsas: Vs = –112 V, Ri = 50 omų 3b impulsas: Vs = +75 V, Ri = 50 omų 4 impulsas: Vs = –6 V, Va = –5 V, t6 = 15 ms 5 impulsas: Vs = +65 V, Ri = 3 omai, td = 100 ms 5 impulso bandymas turi būti atliekamas tik jei transporto priemonės blokas yra skirtas įrengti transporto priemonėje, kurioje nenaudojama jokia bendroji išorinė apsauga nuo susikaupusio krūvio. Siūlomą apsaugą nuo susikaupusio krūvio žr. ISO 16750-2, 4 redakcija, 4.6.4 skyrius.	218

▼B

7. POPIERIAUS FUNKCINIAI BANDYMAI

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
1.	**Administracinis patikrinimas**		
1.1.	Dokumentai	Dokumentų tinkamumas	
2.	**Bendrieji bandymai**		
2.1.	Ženklų skaičius eilutėje	Spaudinių apžiūra	172
2.2.	Minimalus ženklo dydis	Spaudinio apžiūra ir ženklų patikra	173
2.3.	Suderinami ženklų rinkiniai	Spausdintuvu turi būti įmanoma spausdinti ženklus, nurodytus 1 priedėlio 4 skyriuje „Ženklų rinkiniai“.	174
2.4.	Spaudinių raiška	Patikrinamas tachografo tipo patvirtinimas ir apžiūrimi spaudiniai	174
2.5.	Spaudinių skaitomumas ir identifikavimas	Spaudinių apžiūra. Įrodo gamintojas, pateikdamas bandymų ataskaitas ir protokolus. Tachografų, su kuriais gali būti naudojamas spausdintuvo popierius, patvirtinimo numeris (-iai) įspausti popieriuje.	175, 177, 178
2.6.	Pastabų įrašymas ranka	Apžiūra – yra laukelis vairuotojo parašui. Yra laukelių kitiems papildomiems įrašams ranka.	180
2.7.	Papildoma informacija lapo pusėse	Abiejose lapo pusėse gali būti papildomų duomenų ir informacijos. Šie papildomi duomenys ir informacija neturi trukdyti skaityti spaudinius. Apžiūra.	177, 178
3.	**Atmintinės bandymai**		
3.1.	Sausasis kaitinimas	Parengimas: 16 valandų esant + 23 °C ± 2 °C temperatūrai ir 55 % ±3 % santykiniam drėgniui. Bandymo aplinka: 72 valandos esant + 70 °C ±2 °C. Atkūrimas: 16 valandų esant + 23 °C ±2 °C temperatūrai ir 55 % ±3 % santykiniam drėgniui.	176, 178 IEC 60068-2-2-Bb
2.2.	Drėgnasis kaitinimas	Parengimas: 16 valandų esant + 23 °C ±2 °C temperatūrai ir 55 % ±3 % santykiniam drėgniui. Bandymo aplinka: 144 valandos esant +55 °C ±2 °C temperatūrai ir 93 % ±3 % santykiniam drėgniui. Atkūrimas: 16 valandų esant + 23 °C ± 2 °C temperatūrai ir 55 % ±3 % santykiniam drėgniui.	176, 178 IEC 60068-2-78-Cab

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
4.	**Popieriaus eksploataciniai bandymai**		
4.1.	Pagrindo (švaraus popieriaus) atsparumas drėgmei	Parengimas: 16 valandų esant + 23 °C ± 2 °C temperatūrai ir 55 % ±3 % santykiniam drėgniui. Bandymo aplinka: 144 valandos esant +55 °C ±2 °C temperatūrai ir 93 % ± 3 % santykiniam drėgniui. Atkūrimas: 16 valandų esant + 23 °C ± 2 °C temperatūrai ir 55 % ±3 % santykiniam drėgniui.	176, 178 IEC 60068-2-78-Cab
4.2.	Tinkamumas spausdinti	Parengimas: 24 valandų esant + 40 °C ± 2 °C temperatūrai ir 93 % ±3 % santykiniam drėgniui. Bandymo aplinka: spausdinama esant + 23 °C ± 2 °C temperatūrai. Atkūrimas: 16 valandų esant + 23 °C ± 2 °C temperatūrai ir 55 % ±3 % santykiniam drėgniui.	176, 178
4.3.	Atsparumas kaitinimui	Parengimas: 16 valandų esant + 23 °C ± 2 °C temperatūrai ir 55 % ±3 % santykiniam drėgniui. Bandymo aplinka: 2 valandos esant + 70 °C ± 2 °C temperatūrai, sausasis kaitinimas. Atkūrimas: 16 valandų esant + 23 °C ± 2 °C temperatūrai ir 55 % ± 3 % santykiniam drėgniui.	176, 178 IEC 60068-2-2-Bb
4.4.	Atsparumas žemai temperatūrai	Parengimas: 16 valandų esant + 23 °C ± 2 °C temperatūrai ir 55 % ±3 % santykiniam drėgniui. Bandymo aplinka: 24 valandos esant – 20 °C ± 3 °C temperatūrai, sausasis šaltis. Atkūrimas: 16 valandų esant + 23 °C ± 2 °C temperatūrai ir 55 % ± 3 % santykiniam drėgniui.	176, 178 ISO 60068-2-1-Ab
4.5.	Atsparumas šviesai	Parengimas: 16 valandų esant + 23 °C ± 2 °C temperatūrai ir 55 % ±3 % santykiniam drėgniui. Bandymo aplinka: 100 valandų esant 5 000 liuksų apšviestumui, +23 °C ± 2 °C temperatūrai ir 55 % ±3 % santykiniam drėgniui. Atkūrimas: 16 valandų esant + 23 °C ± 2 °C temperatūrai ir 55 % ± 3 % santykiniam drėgniui.	176, 178

Įskaitomumo kriterijai 3.x ir 4.x bandymams:

spaudinio įskaitomumas užtikrintas, jei optinis tankis atitinka šias ribas:

spausdintiniai ženklai – min. 1,0;

fonas (švarus popierius) – maks. 0,2.

Optinis gautų spaudinių tankis matuojamas pagal DIN EN ISO 534.

Spaudinių matmenys turi būti nepakitę ir ženklai turi būti aiškiai įskaitomi.

8. SĄVEIKUMO BANDYMAI

Nr.	Bandymas	Aprašymas
9.1. Transporto priemonės blokų ir tachografo kortelių sąveikumo bandymai		
1.	Abipusis autentiškumo tikrinimas	Patikrinama, ar abipusis transporto priemonės bloko ir tachografo kortelės autentiškumo tikrinimas vyksta tinkamai.

▼B

Nr.	Bandymas	Aprašymas
2.	Įrašymo ir nuskaitymo bandymai	Atliekamas transporto priemonės bloko tipinės veiklos scenarijus. Veiklos scenarijus priderinamas prie bandomos kortelės tipo, o į kortelę turi būti įrašoma kiek įmanoma daugiau rinkmenų EF. Perkeliant duomenis iš transporto priemonės bloko patikrinama, ar visi atitinkami įrašai atlikti tinkamai. Perkeliant duomenis iš kortelės patikrinama, ar visi atitinkami įrašai atlikti tinkamai. Pagal kasdienius spaudinius patikrinama, ar visus atitinkamus įrašus galima tinkamai perskaityti.
	9.2. Transporto priemonės blokų ir judesio jutiklių sąveikumo bandymai	
1.	Siejimas	Patikrinama, ar transporto priemonės blokai ir judesio jutikliai susieti tinkamai.
2.	Veiklos bandymai	Atliekamas judesio jutiklio tipinės veiklos scenarijus. Veiklos scenarijus turi apimti normalią veiklą ir kuo daugiau įvykių ar trikčių. Perkeliant duomenis iš transporto priemonės bloko patikrinama, ar visi atitinkami įrašai atlikti tinkamai. Perkeliant duomenis iš kortelės patikrinama, ar visi atitinkami įrašai atlikti tinkamai. Pagal kasdienius spaudinius patikrinama, ar visus atitinkamus įrašus galima tinkamai perskaityti.
	9.3. Transporto priemonės blokų ir išorinių GNSS įrenginių sąveikumo bandymai (kai taikoma)	
1.	Abipusis autentiškumo tikrinimas	Patikrinama, ar abipusis transporto priemonės bloko ir tachografo kortelės autentiškumo tikrinimas (susiejimas) vyksta tinkamai.
2.	Veiklos bandymai	Atliekamas išorinio GNSS įrenginio tipinės veiklos scenarijus. Veiklos scenarijus turi apimti normalią veiklą ir kuo daugiau įvykių ar trikčių. Perkeliant duomenis iš transporto priemonės bloko patikrinama, ar visi atitinkami įrašai atlikti tinkamai. Perkeliant duomenis iš kortelės patikrinama, ar visi atitinkami įrašai atlikti tinkamai. Pagal kasdienius spaudinius patikrinama, ar visus atitinkamus įrašus galima tinkamai perskaityti.

▼B

10 priedėlis

SAUGUMO REIKALAVIMAI

Šiame priedėlyje nurodyti IT saugumo reikalavimai išmaniojo tachografo sistemos komponentams (antrosios kartos tachografams).

SEC_001 Pagal bendrų kriterijų sistemą išduotą saugumo pažymėjimą turi turėti šie išmaniojo tachografo sistemos komponentai:

— transporto priemonės blokas

— tachografo kortelė,

— judesio jutiklis,

— išorinis GNSS įrenginys.

SEC_002 Būtinieji IT saugumo reikalavimai, kuriuos turi atitikti kiekvienas komponentas, kuriam būtinas saugumo pažymėjimas, nustatomi komponento apsaugos profilyje pagal bendrų kriterijų sistemą.

SEC_003 Europos Komisija užtikrina, kad būtų remiami, parengiami ir vyriausybinių IT saugumo pažymėjimų įstaigų, dalyvaujančių bendro aiškinimo darbo grupėje (*Joint Interpretation Working Group*, JIWG), kuri remia pažymėjimų tarpusavio pripažinimą pagal Europos susitarimą dėl informacinių technologijų saugumo vertinimo pažymėjimų tarpusavio pripažinimo(SOGIS-MRA), užregistruoti keturi šio priedo nuostatas atitinkantys apsaugos profiliai:

— transporto priemonės bloko apsaugos profilis,

— tachografo kortelės apsaugos profilis,

— judesio jutiklio apsaugos profilis,

— išorinio GNSS įrenginio apsaugos profilis.

Transporto priemonės bloko apsaugos profilis skirtas tiems atvejams, kai transporto priemonės blokas yra skirtas naudoti su išoriniu GNSS įrenginiu arba be šio įrenginio. Pirmuoju atveju išoriniam GNSS įrenginiui keliami saugumo reikalavimai pateikiami specialiame apsaugos profilyje.

SEC_004 Komponentų gamintojai prireikus patikslina ir užpildo atitinkamą komponento apsaugos profilį, nekeisdami ir neišbraukdami esamų grėsmių, tikslų, procedūrinių priemonių ir apsaugos užtikrinimo funkcijų specifikacijų, ir taip parengia saugumo tikslą, pagal kurį siekia komponento saugumo sertifikavimo.

SEC_005 Atliekant vertinimo procesą būtina patvirtinti, kad toks konkretus saugumo tikslas griežtai atitinka taikomą apsaugos profilį.

SEC_006 Kiekvieno apsaugos profilio patikimumo lygis turi būti EAL4, papildytas patikinimo komponentais ATE_DPT.2 ir AVA_VAN.5.

▼B

11 priedėlis.

BENDRIEJI APSAUGOS MECHANIZMAI

TURINYS

PREAMBULĖ

A DALIS. PIRMOSIOS KARTOS TACHOGRAFO SISTEMA

1. ĮVADAS

1.1. Nuorodos

1.2. Žymenys ir terminų santrumpos

2. KRIPTOGRAFINĖS SISTEMOS IR ALGORITMAI

2.1. Kriptografinės sistemos

2.2. Kriptografiniai algoritmai

2.2.1 RSA algoritmas

2.2.2 Maišos algoritmas

2.2.3 Duomenų šifravimo algoritmas

3. RAKTAI IR PAŽYMĖJIMAI

3.1. Raktų generavimas ir platinimas

3.1.1 RSA raktų generavimas ir platinimas

3.1.2 RSA bandymų raktai

3.1.3 Judesio jutiklių raktai

3.1.4 T-DES seanso raktų generavimas ir platinimas

3.2. Raktai

3.3. Pažymėjimai

3.3.1 Pažymėjimų turinys

3.3.2 Išduodami pažymėjimai

3.3.3 Pažymėjimo tikrinimas ir išnagrinėjimas

4. ABIPUSIO AUTENTIŠKUMO TIKRINIMO MECHANIZMAS

5. IŠ TRANSPORTO PRIEMONĖS BLOKO Į KORTELES (IR ATVIRKŠČIAI) PERDUODAMŲ DUOMENŲ KONFIDENCIALUMAS, NEPAŽEISTUMAS IR AUTENTIŠKUMO TIKRINIMO MECHANIZMAI

5.1. Saugusis keitimasis pranešimais

5.2. Saugiojo keitimosi pranešimais klaidų tvarkymas

5.3. Kriptografinių kontrolinių sumų apskaičiavimo algoritmas

5.4. Kriptogramų, skirtų konfidencialumo DO, skaičiavimo algoritmas

6. DUOMENŲ PERKĖLIMO SKAITMENINIO PARAŠO MECHANIZMAI

6.1. Parašo generavimas

▼B

6.2. Parašo tikrinimas

B DALIS. ANTROSIOS KARTOS TACHOGRAFO SISTEMA

7. ĮVADAS

7.1. Nuorodos

7.2. Žymenys ir terminų santrumpos

7.3. Terminų apibrėžtys

8. KRIPTOGRAFINĖS SISTEMOS IR ALGORITMAI

8.1. Kriptografinės sistemos

8.2. Kriptografiniai algoritmai

8.2.1 Simetriniai algoritmai

8.2.2 Asimetriniai algoritmai ir standartiniai domeno parametrai

8.2.3 Maišos algoritmai

8.2.4 Šifravimo deriniai

9. RAKTAI IR PAŽYMĖJIMAI

9.1. Asimetrinės raktų poros ir viešųjų raktų pažymėjimai

9.1.1 Bendrosios nuostatos

9.1.2 Europos lygmuo

9.1.3 Valstybių narių lygmuo

9.1.4 Įrangos lygmuo. Transporto priemonės blokai

9.1.5 Įrangos lygmuo. Tachografo kortelės

9.1.6 Įrangos lygmuo. Išoriniai GNSS įrenginiai

9.1.7 Apžvalga. Pažymėjimo keitimas

9.2. Simetriniai raktai

9.2.1 Transporto priemonės bloko ir judesio jutiklio ryšio apsaugos raktai

9.2.2 DSRC ryšio apsaugos raktai

9.3. Pažymėjimai

9.3.1 Bendrosios nuostatos

9.3.2 Pažymėjimo turinys

9.3.3 Pažymėjimų prašymas

10. TRANSPORTO PRIEMONĖS BLOKO IR KORTELĖS ABIPUSIS AUTENTIŠKUMO TIKRINIMAS IR SAUGUSIS KEITIMASIS PRANEŠIMAIS

10.1. Bendrosios nuostatos

10.2. Abipusis pažymėjimų sekos tikrinimas

10.2.1 Transporto priemonės bloko atliekamas kortelės pažymėjimų sekos tikrinimas

▼B

10.2.2	Kortelės atliekamas transporto priemonės bloko pažymėjimų sekos tikrinimas
10.3.	Transporto priemonės bloko autentiškumo tikrinimas
10.4.	Lusto autentiškumo tikrinimas ir seanso raktų derinimas
10.5.	Saugusis keitimasis pranešimais
10.5.1	Bendrosios nuostatos
10.5.2	Saugiojo pranešimo struktūra
10.5.3	Saugiojo keitimosi pranešimais seanso nutraukimas
11.	TRANSPORTO PRIEMONĖS BLOKO IR IŠORINIO GNSS ĮRENGINIO SUJUNGIMAS, ABIPUSIS AUTENTIŠKUMO TIKRINIMAS IR SAUGUSIS KEITIMASIS PRANEŠIMAIS
11.1.	Bendrosios nuostatos
11.2.	Transporto priemonės bloko ir išorinio GNSS įrenginio sujungimas
11.3.	Abipusis pažymėjimų sekos tikrinimas
11.3.1	Bendrosios nuostatos
11.3.2	Transporto priemonės bloko ir EGF sujungimas
11.3.3	Įprastas veikimo režimas
11.4.	Transporto priemonės bloko autentiškumo tikrinimas, lusto autentiškumo tikrinimas ir seanso raktų derinimas
11.5.	Saugusis keitimasis pranešimais
12.	TRANSPORTO PRIEMONĖS BLOKO IR JUDESIO JUTIKLIO SIEJIMAS IR RYŠYS
12.1.	Bendrosios nuostatos
12.2.	Transporto priemonės bloko ir judesio jutiklio siejimas naudojant skirtingų kartų raktus
12.3.	Transporto priemonės bloko ir judesio jutiklio siejimas ir ryšys taikant AES
12.4.	Transporto priemonės bloko ir judesio jutiklio siejimas naudojant skirtingų kartų įrangą
13.	DSRC PAGRĮSTO NUOTOLINIO RYŠIO SAUGUMAS
13.1.	Bendrosios nuostatos
13.2.	Tachografo informacinio turinio užšifravimas ir MAC generavimas
13.3.	Tachografo informacinio turinio tikrinimas ir iššifravimas
14.	PERKELIAMŲ DUOMENŲ PASIRAŠYMAS IR PARAŠŲ TIKRINIMAS
14.1.	Bendrosios nuostatos
14.2.	Parašo generavimas
14.3.	Parašo tikrinimas

▼B

PREAMBULĖ

Šiame priedėlyje nustatyti apsaugos mechanizmai, kuriais užtikrinama:

— įvairių tachografo sistemos komponentų abipusis autentiškumo tikrinimas;

— iš vieno tachografo sistemos komponento į kitą tachografo sistemos komponentą perduodamų arba į išorinę laikmeną perkeliamų duomenų konfidencialumas, nepažeistumas, autentiškumas ir (arba) su šiais duomenimis susijusios atsakomybės prisiėmimas.

Šis priedėlis sudarytas iš dviejų dalių. A dalyje nustatyti pirmosios kartos tachografo sistemos (skaitmeninio tachografo) apsaugos mechanizmai. B dalyje nustatyti antrosios kartos tachografo sistemos (išmaniojo tachografo) apsaugos mechanizmai.

Šio priedėlio A dalyje nustatyti mechanizmai taikomi, jei bent vienas iš tachografo sistemos komponentų, susijusių su abipusiu autentiškumo tikrinimu ir (arba) duomenų perdavimu, yra pirmosios kartos.

Šio priedėlio B dalyje nustatyti mechanizmai taikomi, jei abu tachografo sistemos komponentai, susiję su abipusiu autentiškumo tikrinimu ir (arba) duomenų perdavimu, yra antrosios kartos.

15 priedėlyje pateikta daugiau informacijos apie pirmosios kartos komponentų naudojimą kartu su antrosios kartos komponentais.

A DALIS.

PIRMOSIOS KARTOS TACHOGRAFO SISTEMA

1. ĮVADAS

1.1. **Nuorodos**

Šiame priedėlyje naudoti šaltiniai

SHA-1	Nacionalinis standartų ir technologijos institutas (NIST). *FIPS leidinys Nr. 180-1: Saugios maišos standartas*. 1995 m. balandžio mėn.
PKCS1	RSA laboratorijos. PKCS # 1: *RSA šifravimo standartas*. 2.0 versija. 1998 m. spalio mėn.
TDES	Nacionalinis standartų ir technologijos institutas (NIST). *FIPS leidinys Nr. 46-3: Duomenų šifravimo standartas*. 1999 m. projektas.
TDES-OP	ANSI X9.52. Trigubo duomenų šifravimo algoritmo naudojimo režimai. 1998.
ISO/IEC 7816-4	Informacijos technologija. Atpažinimo kortelės. Lustinės kortelės su kontaktais. 4 dalis. Tarpsektorinės mainų komandos. Pirmoji laida 1995 m. ir 1-as keitinys 1997 m.
ISO/IEC 7816-6	Informacijos technologija. Atpažinimo kortelės. Lustinės kortelės su kontaktais. 6 dalis. Tarpsektoriniai duomenų elementai. Pirmoji laida 1996 m. ir 1-a pataisa 1998 m.
ISO/IEC 7816-8	Informacijos technologija. Atpažinimo kortelės. Lustinės kortelės su kontaktais. 8 dalis. Su saugumu susijusios tarpsektorinės komandos. Pirmoji laida 1999 m.
ISO/IEC 9796-2	Informacijos technologija. Saugumo metodai. Skaitmeninio parašo schema, atkurianti pranešimą. 2 dalis. Būdai, naudojant maišos funkciją. Pirmoji laida 1997 m.

▼B

ISO/IEC 9798-3	Informacijos technologija. Saugumo metodai. Objekto tapatumo nustatymas. 3 dalis. Objekto autentiškumo tikrinimas naudojant atvirojo rakto algoritmą. Antroji laida 1998 m.
ISO 16844-3	Kelių transporto priemonės. Tachografų sistemos. 3 dalis. Judesio jutiklio sąsaja.

1.2. **Žymenys ir terminų santrumpos**

Šiame priedėlyje vartojami žymenys ir terminų santrumpos

(K_a, K_b, K_c)	raktų rinkinys, skirtas naudoti pagal trigubo duomenų šifravimo algoritmą
CA	pažymėjimų įstaiga
CAR	pažymėjimų įstaigos žymuo
CC	kriptografinė kontrolinė suma
CG	kriptograma
CH	komandos antraštė
CHA	pažymėjimo turėtojo įgaliojimas
CHR	pažymėjimo turėtojo žymuo
D()	iššifravimas naudojant DES
DE	duomenų elementas
DO	duomenų objektas
d	RSA privatusis raktas, privačioji eksponentė
e	RSA viešasis raktas, viešoji eksponentė
E()	šifravimas naudojant DES
EQT	įranga
Hash()	maišos vertė, *hash* išvestis
Hash	maišos funkcija
KID	rakto identifikatorius
Km	TDES raktas. Pagrindinis raktas, apibrėžtas standarte ISO 16844-3
Km_{VU}	transporto priemonės bloke įdiegtas TDES raktas
Km_{WC}	dirbtuvių kortelėse įdiegtas TDES raktas
m	pranešimo simbolis, sveikasis skaičius nuo 0 iki *n*-1
n	RSA raktai, modulis
PB	užpildo baitai
PI	užpildo 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 nuosekliojo blokinio šifravimo režimas

▼B

TDEA	trigubo duomenų šifravimo algoritmas
TLV	žymenos ilgio vertė
VU	transporto priemonės blokas
X.C	pažymėjimų įstaigos išduotas naudotojo X pažymėjimas
X.CA	naudotojo X pažymėjimų įstaiga
X.CA.PK $_{o}$ X.C	pažymėjimo išnagrinėjimo operacija viešajam raktui išskirti. Tai infiksinis operatorius, kurio kairysis operandas yra pažymėjimų įstaigos viešasis raktas, o dešinysis operandas – tos pažymėjimų įstaigos išduotas pažymėjimas. Rezultatas – naudotojo X, kurio pažymėjimas yra dešinysis operandas, viešasis raktas
X.PK	naudotojo X viešasis RSA raktas
X.PK[I]	tam tikros informacijos I šifruotė RSA, gauta naudojant naudotojo X viešąjį raktą
X.SK	naudotojo X privatusis RSA raktas
X.SK[I]	tam tikros informacijos I šifruotė RSA, gauta naudojant naudotojo X privatųjį raktą
‘xx’	šešioliktainė vertė
||	sujungimo ženklas

2. KRIPTOGRAFINĖS SISTEMOS IR ALGORITMAI

2.1. **Kriptografinės sistemos**

CSM_001 Transporto priemonės blokuose ir tachografo kortelėse taikoma įprasta RSA viešaraktė kriptografinė sistema, kuria užtikrinami šie apsaugos mechanizmai:

— transporto priemonės blokų ir kortelių abipusio autentiškumo tikrinimas,

— trigubo DES seanso raktų perdavimas iš transporto priemonės blokų į tachografų korteles (ir atvirkščiai),

— iš transporto priemonės blokų arba tachografų kortelių į išorines laikmenas perkeliamų duomenų skaitmeninis parašas.

CSM_002 Transporto priemonės blokuose ir tachografo kortelėse taikoma trigubo DES simetrinė kriptografinė sistema, kuria užtikrinamas duomenų nepažeistumo apsaugos mechanizmas, kai duomenys apie naudotoją perduodami iš transporto priemonės blokų į tachografo korteles (ir atvirkščiai), ir (kai taikytina) užtikrinamas duomenų, perduodamų iš transporto priemonės blokų į tachografo korteles (ir atvirkščiai), konfidencialumas.

2.2. **Kriptografiniai algoritmai**

2.2.1 *RSA algoritmas*

CSM_003 RSA algoritmas išsamiai apibrėžiamas tokiais sąryšiais:

▼B

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

Išsamesnis RSA funkcijos apibūdinimas pateiktas šaltinyje [PKCS1]. Apskaičiuojant RSA, viešoji eksponentė e yra sveikasis skaičius nuo 3 iki n-1, atitinkantis sąlygą gcd(e, lcm(p-1, q-1))=1.

2.2.2 *Maišos algoritmas*

CSM_004 Skaitmeninio parašo mechanizmuose taikomas maišos algoritmas SHA-1, apibrėžtas šaltinyje [SHA-1].

2.2.3 *Duomenų šifravimo algoritmas*

CSM_005 DES pagrįsti algoritmai taikomi nuosekliojo blokinio šifravimo režimu.

3. RAKTAI IR PAŽYMĖJIMAI

3.1. **Raktų generavimas ir platinimas**

3.1.1 *RSA raktų generavimas ir platinimas*

CSM_006 RSA raktai generuojami trimis funkciniais hierarchijos lygmenimis:

— Europos lygmeniu,

— valstybių narių lygmeniu,

— įrangos lygmeniu.

CSM_007 Europos lygmeniu sugeneruojama viena Europos raktų pora (EUR.SK ir EUR.PK). Europos privatusis raktas yra skirtas valstybių narių viešiesiems raktams sertifikuoti. Turi būti tvarkomas visų sertifikuotų raktų registras. Šią užduotį Europos Komisijos įgaliojimu ir atsakomybe atlieka Europos pažymėjimų įstaiga.

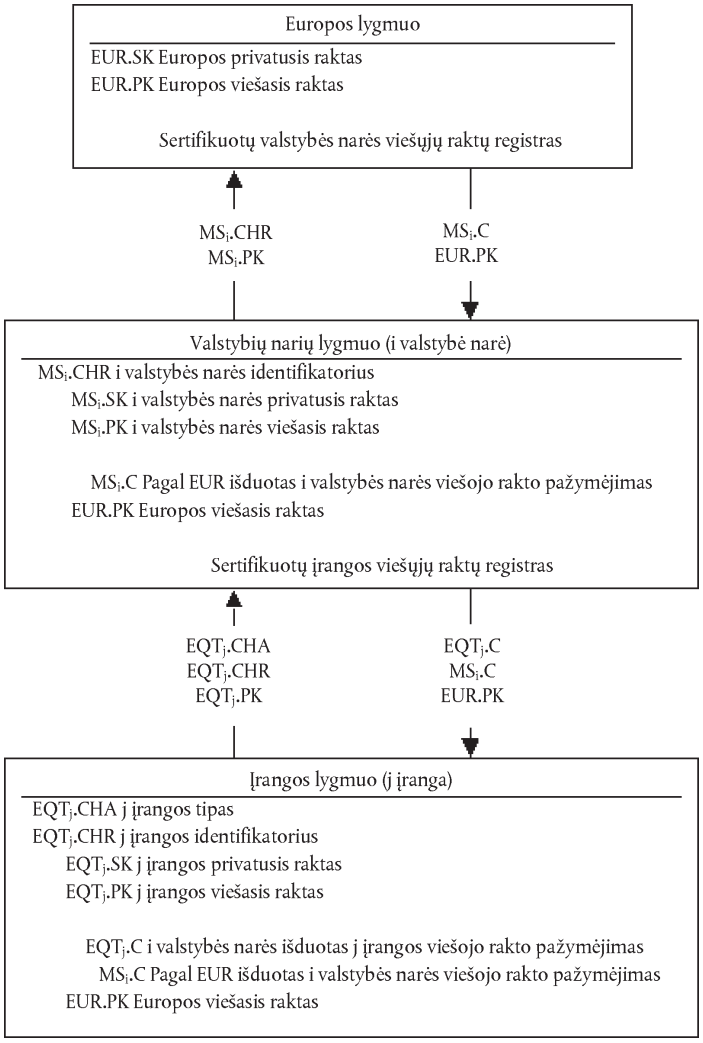
CSM_008 Valstybių narių lygmeniu sugeneruojama valstybės narės raktų pora (MS.SK ir MS.PK). Valstybių narių viešuosius raktus sertifikuoja Europos pažymėjimų įstaigos. Valstybės narės privatusis raktas yra skirtas viešiesiems raktams, įdiegtiniems į įrangą (transporto priemonės bloką arba tachografo kortelę), sertifikuoti. Turi būti tvarkomas visų sertifikuotų viešųjų raktų registras su įrangos, kurioje jie įdiegti, identifikavimo duomenimis. Šią užduotį atlieka valstybės narės pažymėjimų įstaigos. Valstybė narė gali reguliariai keisti savo raktų porą.

CSM_009 Įrangos lygmeniu sugeneruojama ir į įrangą įdiegiama viena raktų pora (EQT.SK ir EQT.PK). Įrangos viešuosius raktus sertifikuoja valstybės narės pažymėjimų įstaiga. Tai gali atlikti įrangos gamintojai, individualizuotojai arba valstybės narės institucijos. Ši raktų pora naudojama autentiškumo tikrinimo, skaitmeninio parašo ir šifravimo paslaugoms.

CSM_010 Turi būti užtikrinamas generuojamų, perduodamų (jei reikia) ir saugomų privačiųjų raktų konfidencialumas.

▼B

Toliau pateiktame paveiksle bendrai pavaizduotas šio proceso duomenų srautas.



3.1.2 *RSA bandymų raktai*

CSM_011 Įrangos bandymams (įskaitant sąveikumo bandymus) Europos pažymėjimų įstaiga sugeneruoja vieną Europos bandymų raktų porą ir ne mažiau kaip dvi valstybių narių bandymų raktų poras, kurių viešieji raktai sertifikuojami Europos privačiuoju bandymų raktu. Į įrangą, kurios tipo patvirtinimo bandymai atliekami, gamintojai turi įdiegti bandymų raktus, sertifikuotus vienu iš šių valstybių narių bandymų raktu.

3.1.3 *Judesio jutiklių raktai*

Turi būti tinkamai užtikrintas generuojamų, perduodamų (jei reikia) ir saugomų toliau apibūdintų trijų trigubo DES raktų konfidencialumas.

Siekdama populiarinti standartą ISO 16844 atitinkančius tachografų komponentus, Europos pažymėjimų įstaiga ir valstybių narių pažymėjimų įstaigos taip pat turi užtikrinti:

CSM_036 Europos pažymėjimų įstaiga generuoja du nepriklausomus ir unikalius trigubo DES raktus – KmVU ir KmWC, ir suge neruoja Km, kaip nurodyta toliau: $Km = Km_{VU}\ XOR\ Km_{WC}$. Šiuos raktus valstybių narių prašymu Europos pažymėjimų įstaiga, taikydamas tinkamas apsaugos procedūras, perduoda tų šalių pažymėjimų įstaigoms.

▼B

CSM_037 Valstybių narių pažymėjimų įstaigos:

— naudoja Km judesio jutiklio gamintojų reikalaujamiems duomenims apie judesio jutiklį užšifruoti (naudojant Km užšifruotini duomenys apibrėžti standarte ISO 16844-3);

— taikydamos tinkamas apsaugos procedūras, perduoda Km_{VU} transporto priemonės blokų gamintojams, kad šie juos įdiegtų į transporto priemonės blokus;

— užtikrina, kad Km_{WC} būtų įdiegtas į visas dirbtuvių korteles, kai jos individualizuojamos (kaip `SensorInstallationSecData` elementariojoje rinkmenoje `Sensor_Installation_Data`).

3.1.4 *T-DES seanso raktų generavimas ir platinimas*

CSM_012 Transporto priemonės blokai ir tachografo kortelės abipusio autentiškumo tikrinimo proceso metu generuoja būtinus duomenis ir jais keičiasi bendrajam trigubo DES seanso raktui sukurti. Šio keitimosi duomenimis konfidencialumas turi būti užtikrintas taikant RSA šifravimo mechanizmą.

CSM_013 Šis raktas naudojamas visose tolesnėse kriptografinėse operacijose, kai taikomas saugusis keitimasis pranešimais. Jo galiojimas turi baigtis pasibaigus seansui (ištraukus kortelę arba perkrovus ją) ir (arba) panaudojus jį 240 kartų (rakto panaudojimas vieną kartą – tai viena saugiojo keitimosi pranešimais būdu kortelei perduoda komanda ir atsakas į ją).

3.2. **Raktai**

CSM_014 RSA raktų (bet kurio lygmens) ilgis yra toks: modulis n – 1 024 bitai, viešoji eksponentė e – ne daugiau kaip 64 bitai, privačioji eksponentė d – 1 024 bitai.

CSM_015 Trigubo DES raktų forma turi būti (K_a, K_b, K_a), čia K_a ir K_b – nepriklausomi 64 bitų ilgio raktai. Lyginumo klaidos nustatymo bitai nenustatomi.

3.3. **Pažymėjimai**

CSM_016 RSA viešųjų raktų pažymėjimai turi būti „neautonominio aprašo“ „kortele patikrinami“ pažymėjimai (remiantis ISO/IEC 7816-8).

3.3.1 *Pažymėjimų turinys*

CSM_017 RSA viešųjų raktų pažymėjimuose pateikiami tokie duomenys, išdėstyti tokia tvarka:

Duomenys	Formatas	Baitai	Pastaba
CPI	INTEGER	1	Pažymėjimo profilio identifikatorius (šios versijos – ‘01’)
CAR	OCTET STRING	8	Pažymėjimų įstaigos žymuo
CHA	OCTET STRING	7	pažymėjimo turėtojo įgaliojimas

▼B

Duomenys	Formatas	Baitai	Pastaba
EOV	TimeReal	4	Pažymėjimo galiojimo pabaiga. Neprivaloma; jei nenaudojama, užpildoma vertėmis FF
CHR	OCTET STRING	8	pažymėjimo turėtojo žymuo
n	OCTET STRING	128	Viešasis raktas (modulis)
e	OCTET STRING	8	Viešasis raktas (viešoji eksponentė)
		164	

Pastabos

1. Pažymėjimo profilio identifikatoriumi (CPI) apibrėžiama tiksli autentiškumo tikrinimo pažymėjimo struktūra. Jį galima naudoti kaip įrangos atitinkamų antraščių sąrašo vidinį identifikatorių, kuriuo apibūdinamas duomenų elementų sujungimas 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’
Išplėstinio 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	Viešojo rakto žymena (sudaryta)	Paskesnių DO ilgis	Modulio žymena	Modulio ilgis	Viešosios eksponentės žymena	Viešosios eksponentės ilgis

2. Pažymėjimų įstaigos žymens (CAR) paskirtis – identifikuoti pažymėjimą išdavusią CA, kad duomenų elementą būtų galima naudoti kartu su institucijos rakto identifikatoriumi pažymėjimų įstaigos viešajam raktui nurodyti (dėl kodavimo žr. tolesnį punktą apie rakto identifikatorių).

3. Pažymėjimo turėtojo įgaliojimas (CHA) yra skirtas pažymėjimo turėtojo teisėms identifikuoti. Jis sudarytas iš tachografo taikomosios programos identifikatoriaus ir įrangos, kuriai skirtas pažymėjimas, tipo (pagal duomenų elementą `EquipmentType`; valstybės narės – ‘00’).

▼B

4. Pažymėjimo turėtojo žymens (CHR) paskirtis – unikaliai identifikuoti pažymėjimo turėtoją, kad duomenų elementą būtų galima naudoti kartu su subjekto rakto identifikatoriumi pažymėjimo turėtojo viešajam raktui nurodyti.

5. Raktų identifikatoriais unikaliai identifikuojamas pažymėjimo turėtojas arba pažymėjimų įstaigos. Jie koduojami taip:

5.1. Įranga (transporto priemonės blokas arba kortelė):

Duomenys	Įrangos serijos numeris	Data	Tipas	Gamintojas
Ilgis	4 baitai	2 baitai	1 baitas	1 baitas
Vertė	Sveikasis skaičius	mm yy BCD kodu	Nustato gamintojas	Gamintojo kodas

Kiek tai susiję su VU, prašydamas pažymėjimų gamintojas gali žinoti įrangos, į kurią bus įdiegti raktai, identifikavimo duomenis arba jų nežinoti.

Pirmuoju atveju gamintojas perduoda įrangos identifikavimo duomenis su viešuoju raktu savo valstybės narės institucijai sertifikuoti. Tuomet pažymėjime bus nurodyti įrangos identifikavimo duomenys, o gamintojas privalo užtikrinti, kad raktai ir pažymėjimas būtų įdiegti į reikiamą įrangą. Rakto identifikatoriaus forma yra tokia, kaip nurodyta pirmiau.

Antruoju atveju gamintojas privalo priskirti unikalų identifikatorių kiekvienam pažymėjimo prašymui ir perduoti šiuos identifikavimo duomenis su viešuoju raktu savo valstybės narės institucijai sertifikuoti. Pažymėjime bus nurodyti prašymo identifikavimo duomenys. Įdiegęs raktą į įrangą, gamintojas privalo pranešti savo valstybės narės institucijai apie rakto priskyrimą įrangai (t. y. nurodyti pažymėjimo prašymo identifikavimo duomenis, įrangos identifikavimo duomenis). Rakto identifikatorius yra tokios formos:

Duomenys	Pažymėjimo prašymo serijos numeris	Data	Tipas	Gamintojas
Ilgis	4 baitai	2 baitai	1 baitas	1 baitas
Vertė	Sveikasis skaičius	mm yy BCD kodu	‘FF’	Gamintojo kodas

▼B

5.2. Pažymėjimų įstaiga:

Duomenys	Institucijos identifikavimo duomenys	Rakto serijos numeris	Papildoma informacija	Identifikatorius
Ilgis	4 baitai	1 baitas	2 baitai	1 baitas
Vertė	1 baito skaitinis valstybės kodas 3 baitų raidinis skaitinis valstybės kodas	Sveikasis skaičius	Papildomas kodas (pagal CA) jei nenaudojama – ‘FF FF’	‘01’

Rakto serijos numeris naudojamas įvairiems valstybės narės raktams atskirti, jei raktas būtų pakeistas.

6. Pažymėjimų tikrintojai privalo žinoti, kad sertifikuotas viešasis raktas yra RSA raktas, susijęs su autentiškumo tikrinimu, skaitmeninio parašo tikrinimu ir šifravimu konfidencialumui užtikrinti (pažymėjime nėra tokių objektų identifikatorių, kuriais tai būtų nurodoma).

3.3.2 *Išduodami pažymėjimai*

CSM_018 Išduodamas pažymėjimas – tai skaitmeninis parašas su iš dalies atkartotu pažymėjimo turiniu pagal standartą ISO/IEC 9796-2 (išskyrus jo A4 priedą) ir su pridėtu pažymėjimų įstaigos žymeniu.

$$X.C = X.CA.SK[‘6A’ \parallel C_r \parallel \mathit{Hash}(Cc) \parallel ‘BC’] \parallel C_n \parallel X.CAR$$

Pažymėjimo turinys: $Cc = C_r \parallel C_n$

C_r	C_n
106 baitai	58 baitai

Pastabos

1. Šis pažymėjimas yra 194 baitų ilgio.

2. CAR, kuris slepiamas parašu, taip pat pridedamas prie parašo, kad pažymėjimų įstaigos viešąjį raktą būtų galima pasirinkti pažymėjimui patikrinti.

3. Pažymėjimo tikrintojas privalo žinoti algoritmą, kurį pažymėjimų įstaiga taikė pažymėjimui pasirašyti.

4. Su išduodamu 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

▼B

3.3.3 *Pažymėjimo tikrinimas ir išnagrinėjimas*

Pažymėjimo tikrinimas ir išnagrinėjimas susideda iš parašo patikrinimo pagal standartą ISO/IEC 9796-2, pažymėjimo turinio bei įdiegto viešojo rakto atkūrimo pagal formulę X.PK = X.CA.PK $_{o}$ X.C ir pažymėjimo galiojimo patikrinimo.

CSM_019 Šio proceso metu atliekami tokie veiksmai:

parašo patikrinimas ir turinio atkūrimas:

— iš X.C atkuriamas *Sign*, Cn' ir CAR': X.C = Sign (128 baitai) || C_n' (58 baitai) || CAR' (8 baitai)

— iš CAR' pasirenkamas atitinkamas pažymėjimų įstaigos viešasis raktas (jei tai nepadaryta anksčiau kitais būdais),

— *Sign* atidaromas CA viešuoju raktu: Sr'= X.CA.PK [Sign],

— patikrinama, ar Sr' prasideda simboliais ‘6A’, o baigiasi – ‘BC’,

— apskaičiuojami C_r' ir H': Sr' = ‘6A’ || C_r' (106 baitai) || H' (20 baitų) || ‘BC’

— 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. Remiantis C':

— jei taikytina, patikrinama galiojimo pabaigos data,

iš C' atkuriamas ir išsaugomas viešasis raktas, rakto identifikatorius, pažymėjimo turėtojo įgaliojimas ir pažymėjimo galiojimo pabaigos data:

— X.PK = *n* || *e*

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. ABIPUSIO AUTENTIŠKUMO TIKRINIMO MECHANIZMAS

Tachografo kortelių ir transporto priemonės blokų abipusis autentiškumo tikrinimas atliekamas tokiu principu:

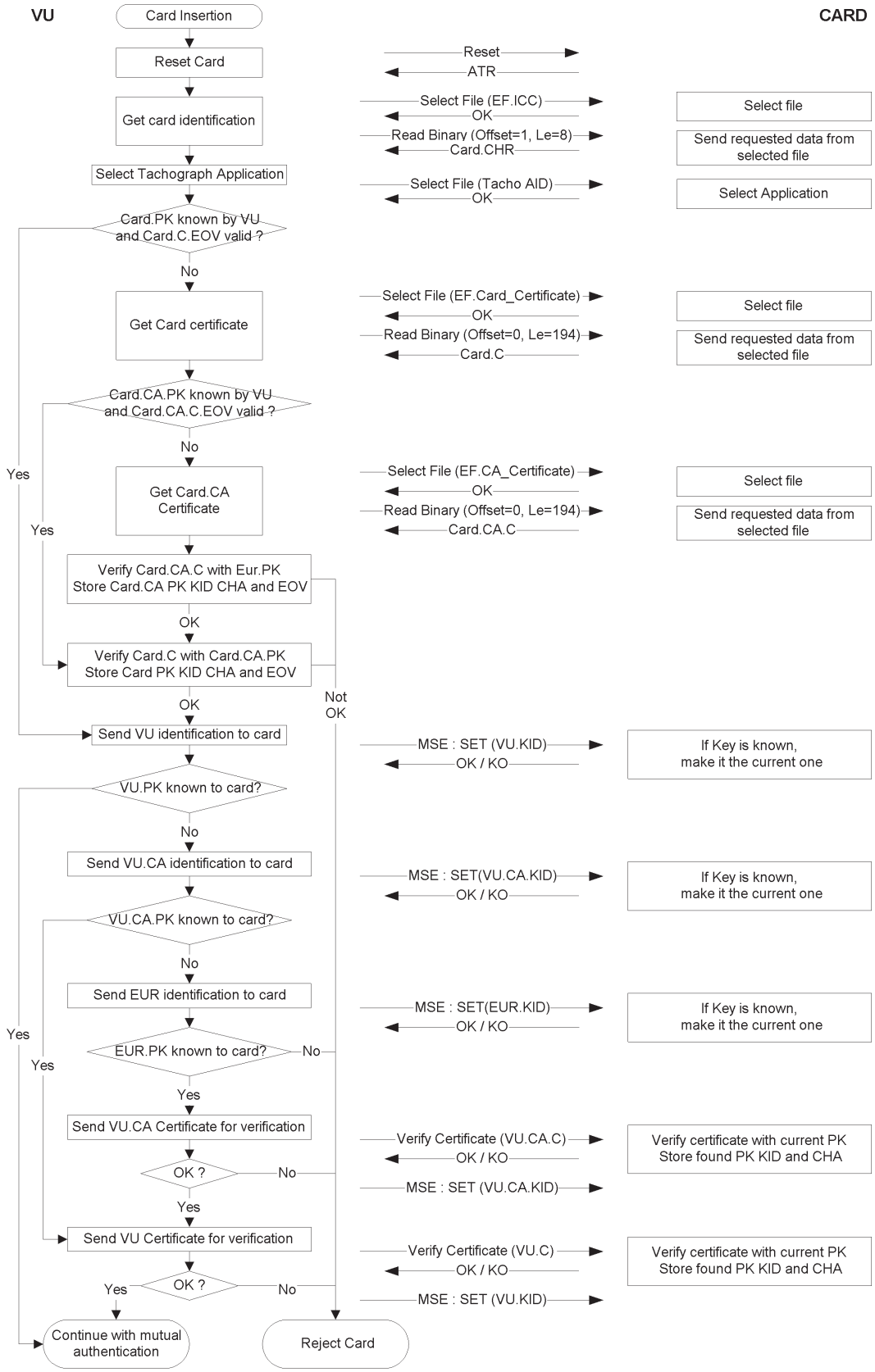
kiekvienas subjektas turi įrodyti kitam, kad turi galiojančių raktų porą, kurios viešąjį raktą sertifikavo valstybės narės pažymėjimų įstaiga, kurią savo ruožtu sertifikavo Europos pažymėjimų įstaiga;

įrodoma privačiuoju raktu pasirašant kito subjekto atsiųstą atsitiktinį skaičių, šis subjektas turi atkurti tą skaičių tikrindamas parašą.

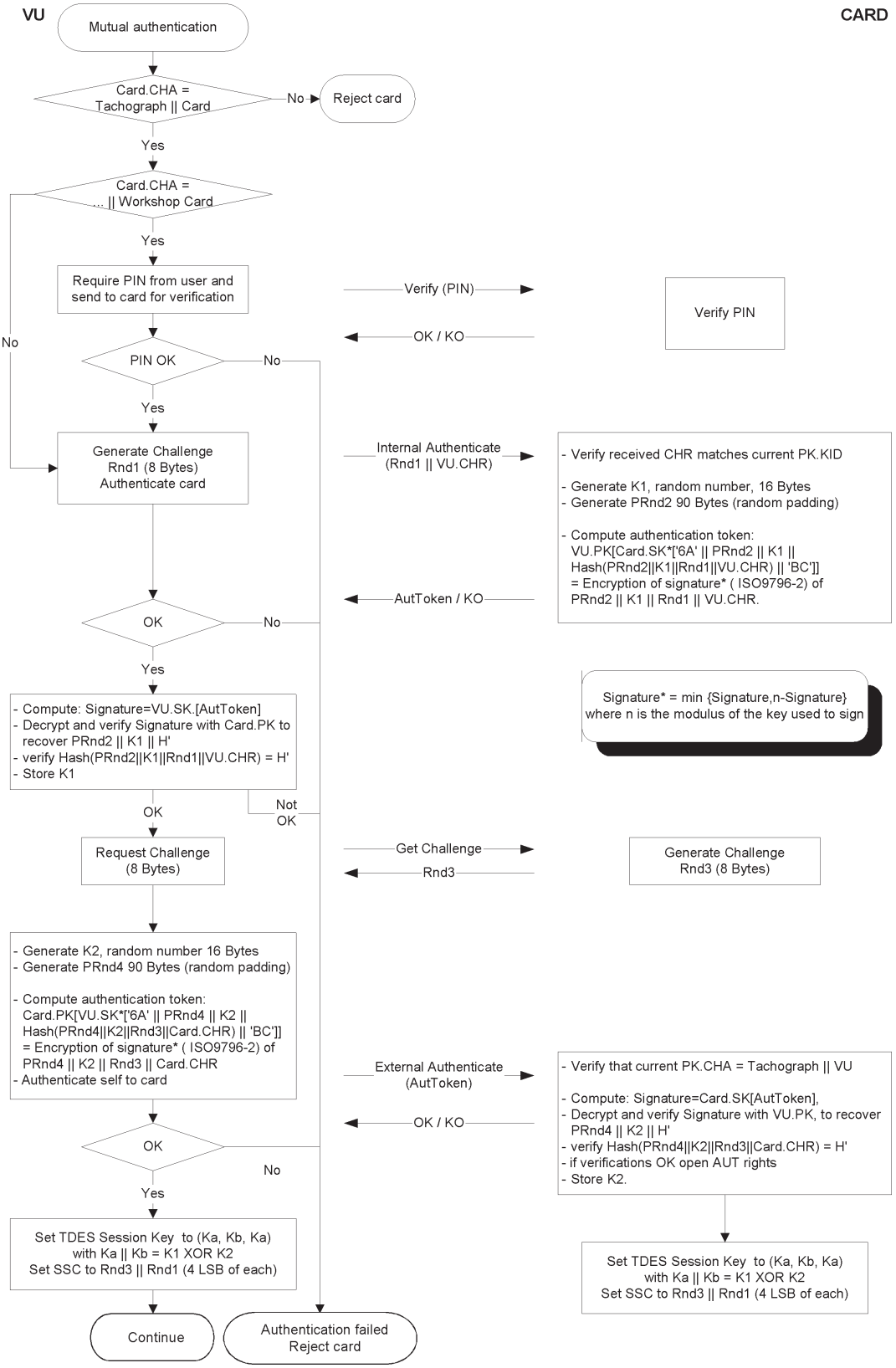
Šį mechanizmą transporto priemonės blokas aktyvina įstačius kortelę. Procesas pradedamas apsikeitimu pažymėjimais ir viešųjų raktų išnagrinėjimu, o baigiamas seanso rakto nustatymu.

▼B

CSM_020 Taikomas toliau nurodytas protokolas (rodyklėmis rodomos komandos ir duomenys, kuriais keičiamasi (žr. 2 priedėlį).



▼B


VU
CARD
Mutual authentication
Card.CHA = Tachograph || Card
No
Reject card
Yes
Card.CHA = ... || Workshop Card
Yes
Require PIN from user and send to card for verification
Verify (PIN)
Verify PIN
OK / KO
No
PIN OK
No
Yes
Generate Challenge Rnd1 (8 Bytes) Authenticate card
Internal Authenticate (Rnd1 || VU.CHR)
- Verify received CHR matches current PK.KID
- Generate K1, random number, 16 Bytes
- Generate PRnd2 90 Bytes (random padding)
- Compute authentication token: VU.PK[Card.SK*['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd2 || K1 || Rnd1 || VU.CHR.
AutToken / KO
OK
No
Yes
Signature* = min {Signature,n-Signature} where n is the modulus of the key used to sign
- Compute: Signature=VU.SK.[AutToken]
- Decrypt and verify Signature with Card.PK to recover PRnd2 || K1 || H'
- verify Hash(PRnd2||K1||Rnd1||VU.CHR) = H'
- Store K1
Not OK
OK
Request Challenge (8 Bytes)
Get Challenge
Rnd3
Generate Challenge Rnd3 (8 Bytes)
- Generate K2, random number 16 Bytes
- Generate PRnd4 90 Bytes (random padding)
- Compute authentication token: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd4 || K2 || Rnd3 || Card.CHR
- Authenticate self to card
External Authenticate (AutToken)
- Verify that current PK.CHA = Tachograph || VU
- Compute: Signature=Card.SK[AutToken],
- Decrypt and verify Signature with VU.PK, to recover PRnd4 || K2 || H'
- verify Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- if verifications OK open AUT rights
- Store K2.
OK / KO
OK
No
Yes
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2 Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2 Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Continue
Authentication failed Reject card

▼B

5. IŠ TRANSPORTO PRIEMONĖS BLOKO Į KORTELES (IR ATVIRKŠČIAI) PERDUODAMŲ DUOMENŲ KONFIDENCIALUMAS, NEPAŽEISTUMAS IR AUTENTIŠKUMO TIKRINIMO MECHANIZMAI

5.1. **Saugusis keitimasis pranešimais**

CSM_021 Iš transporto priemonės bloko į korteles (ir atvirkščiai) perduodamų duomenų nepažeistumas užtikrinamas taikant saugųjį keitimąsi pranešimais, kaip nurodyta standartuose [ISO/IEC 7816-4] ir [ISO/IEC 7816-8].

CSM_022 Jei perduodamus duomenis reikia apsaugoti, prie duomenų objektų, perduodamų su komanda arba atsaku, pridedama kriptografinė kontrolinė suma. Kriptografinę kontrolinę sumą patikrina gavėjas.

CSM_023 Su komanda perduodamų duomenų kriptografinė kontrolinė suma apskaičiuojama įtraukiant komandos antraštę ir visus perduodamus duomenų objektus (=> CLA = ‘0C’, o visi duomenų objektai turi būti su žymenomis, kurių b1 = 1).

CSM_024 Jei atsake nėra duomenų lauko, atsako būsenos informacijos baitai apsaugomi kriptografine kontroline suma.

CSM_025 Kriptografinės kontrolinės sumos turi būti 4 baitų ilgio.

Taigi, taikant saugųjį keitimąsi pranešimais, komandų ir atsakų struktūra yra tokia:

Naudojami DO – standarte ISO/IEC 7816-4 aprašytų saugiojo keitimosi pranešimais DO dalinė imtis:

Žymena	Mnemoninis žymuo	Reikšmė
‘81’	T_{PV}	Paprastoji vertė, BER-TLV metodu neužkoduoti duomenys (turi būti apsaugota naudojant CC)
‘97’	$\mathbf{T_{LE}}$	Le vertė neapsaugotoje komandoje (turi būti apsaugota naudojant CC)
‘99’	T_{SW}	Informacija apie būseną (turi būti apsaugota naudojant CC)
‘8E’	T_{CC}	Kriptografinė kontrolinė suma
‘87’	$T_{PI\ CG}$	Užpildo indikacinis baitas || Kriptograma (Paprastoji vertė, neužkoduota BER-TLV metodu)

▼B

Jei neapsaugota atsako į komandą pora yra:

Komandos antraštė				Komandos pagrindinė dalis		
CLA	INS	P1	P2	[L_c laukas]	[Duomenų laukas]	[L_e laukas]
keturi baitai				L baitai, žymimi simboliais nuo B_1 iki B_L		

Atsako pagrindinė dalis	Atsako papildymas	
[Duomenų laukas]	SW1	SW2
L_r duomenų baitai	du baitai	

Atitinkama apsaugota atsako į komandą pora yra:

Apsaugota komanda

Komandos antraštė (CH)				Komandos pagrindinė dalis										
CLA	INS	P1	P2	[Naujas L_c laukas]	[Naujas duomenų laukas]									[Naujas L_e laukas]
‘OC’				Naujo duomenų lauko ilgis	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	‘00’
					‘81’	L_c	Duomenų laukas	‘97’	‘01’	L_e	‘8E’	‘04’	CC	

Duomenys, įtrauktini į kontrolinę sumą: CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = užpildo baitai (80 .. 00), taikant standartuose ISO/IEC 7816-4 ir ISO 9797 nustatytą 2-ą metodą.

DO PV ir LE yra tik tuomet, kai neapsaugotoje komandoje yra atitinkamų duomenų.

Apsaugotas atsakas

1. Atvejis, kai atsako duomenų laukas netuščias ir jo konfidencialumo užtikrinti nereikia:

Atsako pagrindinė dalis						Atsako papildymas
[Naujas duomenų laukas]						nauji SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
‘81’	L_r	Duomenų laukas	‘8E’	‘04’	CC	

Duomenys, įtrauktini į kontrolinę sumą: T_{PV} || L_{PV} || PV || PB

2. Atvejis, kai atsako duomenų laukas nėra tuščias ir reikia užtikrinti jo konfidencialumą:

▼B

Atsako pagrindinė dalis						Atsako papildymas
[Naujas duomenų laukas]						nauji SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
‘87’		PI ‖ CG	‘8E’	‘04’	CC	

Duomenys, perduotini naudojant CG: BER-TLV metodu neužkoduoti duomenys ir užpildo baitai.

Duomenys, įtrauktini į kontrolinę sumą: $T_{PI\ CG}$ ‖ $L_{PI\ CG}$ ‖ PI CG ‖ PB

3. Atvejis, kai atsako duomenų laukas yra tuščias:

Atsako pagrindinė dalis						Atsako papildymas
[Naujas duomenų laukas]						nauji SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
‘99’	‘02’	Nauji SW1 SW2	‘8E’	‘04’	CC	

Duomenys, įtrauktini į kontrolinę sumą: T_{SW} ‖ L_{SW} ‖ SW ‖ PB

5.2. **Saugiojo keitimosi pranešimais klaidų tvarkymas**

CSM_026 Kai tachografo kortelė interpretuodama komandą atpažįsta SM klaidą, tuomet netaikant SM turi būti pateikti būsenos baitai. Standarte ISO/IEC 7816-4 apibrėžti tokie būsenos baitai, kuriais nurodomos SM klaidos:

‘66 88’: kriptografinės kontrolinės sumos patikrinti nepavyko;

‘69 87’: nėra lauktų SM duomenų objektų;

‘69 88’: SM duomenų objektai neteisingi.

CSM_027 Kai tachografo kortelė pateikia būsenos baitus be SM DO arba su klaidingais SM DO, transporto priemonės blokas turi nutraukti seansą.

5.3. **Kriptografinių kontrolinių sumų apskaičiavimo algoritmas**

CSM_028 Kriptografinės sumos apskaičiuojamos naudojant mažmeninius MAC, kaip nustatyta ANSI X9.19, kai taikomas DES:

— pradinis etapas: pradinis kontrolinis blokas y0 yra E(Ka, SSC);

— kitas etapas: naudojant Ka, apskaičiuojami kontroliniai blokai y1, ..., yn;

— galutinis etapas: naudojant paskutinį kontrolinį bloką yn apskaičiuojama kontrolinė suma: E(Ka, D(Kb, yn));

čia E() reiškia užšifravimą taikant DES, o D() – iššifravimą taikant DES;

perduodami keturi svarbiausieji kriptografinės kontrolinės sumos baitai.

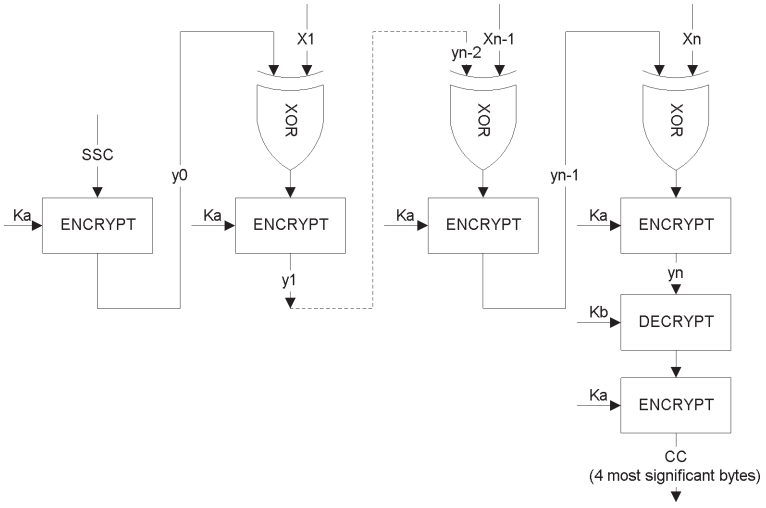
▼B

CSM_029 Per raktų derinimo procedūrą aktyvinamas siuntimo sekos skaitiklis (SSC):

pradinis SSC: Rnd3 (4 nesvarbiausieji baitai) || Rnd1 (4 nesvarbiausieji baitai).

CSM_030 Prieš kiekvieną MAC skaičiavimą siuntimo sekos skaitiklis padidinamas vienetu (t. y. pirmosios komandos SSC yra pradinis SSC + 1, pirmojo atsako SSC — pradinis SSC + 2).

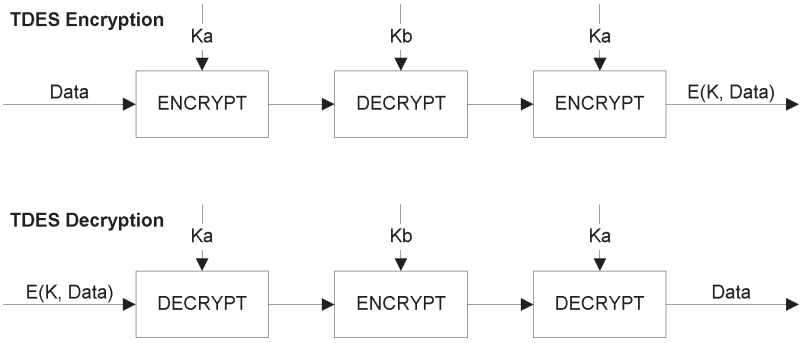
Toliau pateiktame paveiksle pavaizduota mažmeninio MAC apskaičiavimo schema.



5.4. **Kriptogramų, skirtų konfidencialumo DO, skaičiavimo algoritmas**

CSM_031 Kriptogramos skaičiuojamos TCBC režimu taikant TDEA, kaip nurodyta [TDES] ir [TDES-OP], pradinės vertės bloku pasirenkant nulinį vektorių.

Toliau pateiktame paveiksle pavaizduota raktų naudojimo pagal TDES schema.



▼B

6. DUOMENŲ PERKĖLIMO SKAITMENINIO PARAŠO MECHANIZMAI

CSM_032 Specializuota įranga su mikroprocesoriumi (IDE) išsaugo vieno duomenų perkėlimo seanso metu iš įrangos (transporto priemonės bloko arba kortelės) gautus duomenis vienoje fizinėje duomenų rinkmenoje. Ši rinkmena turi turėti pažymėjimus MS_i.C ir EQT.C. Rinkmenoje yra skaitmeniniai duomenų blokų parašai, nustatyti 7 priedėlyje „Duomenų perkėlimo protokolai“.

CSM_033 Perkeltų duomenų skaitmeninių parašų struktūra su papildymu turi būti tokia, kad, jei reikia, perkeltus duomenis galima būtų perskaityti jų neiššifruojant.

6.1. **Parašo generavimas**

CSM_034 Duomenų parašus įranga generuoja pagal parašų su papildymu sistemą, kaip apibrėžta [PKCS1], taikant SHA-1 maišos funkciją:

Parašas = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1(Duomenys))]

PS = užpildymo oktetais ‘FF’ eilutė, kad ilgis sudarytų 128.

DER(SHA-1(*M*)) yra algoritmo ID užkodavimas maišos funkcijai ir maišos vertės užkodavimas DigestInfo tipo 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**

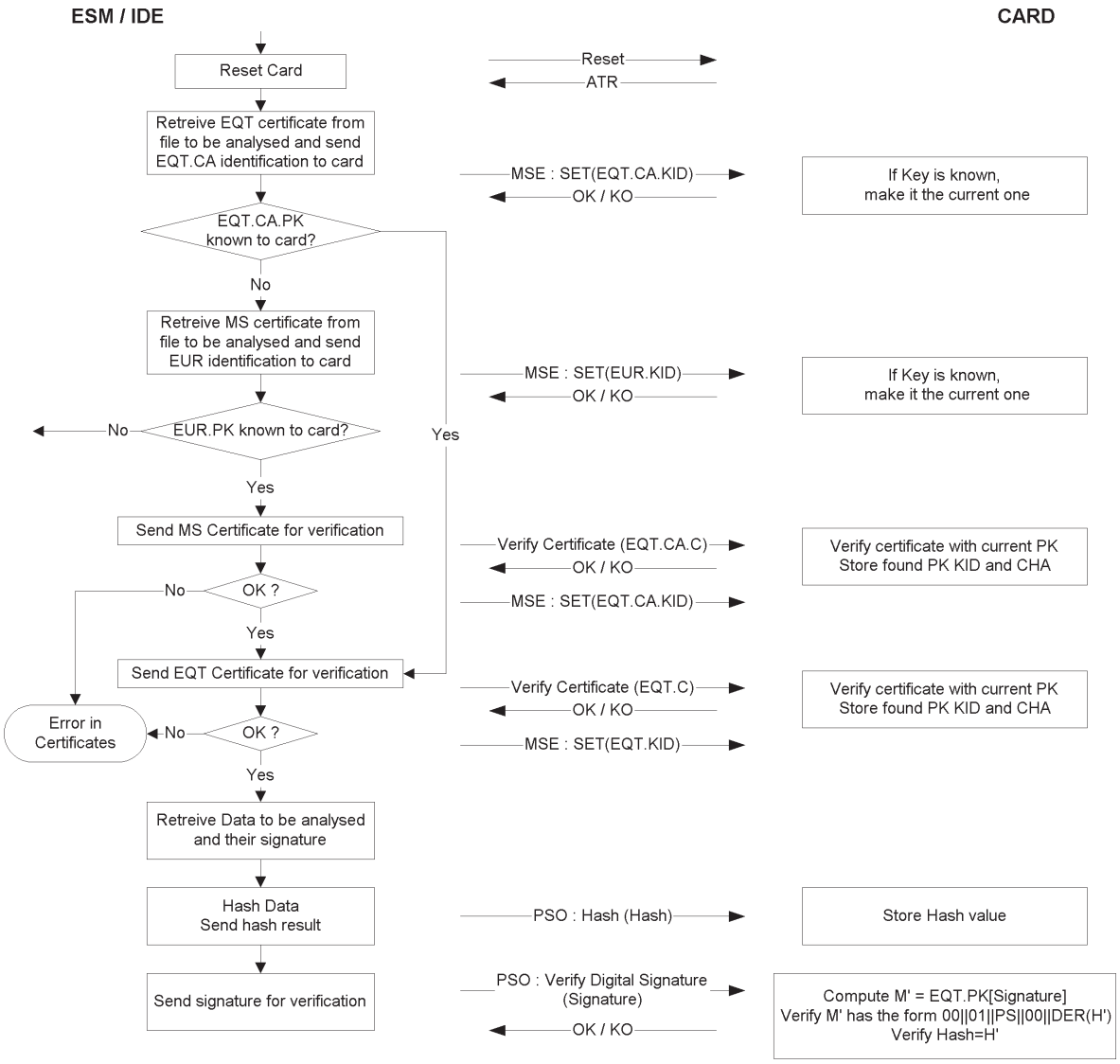
CSM_035 Perkeltų duomenų parašo tikrinimas atliekamas pagal parašų su papildymu sistemą, kaip nurodyta PKCS1, taikant SHA-1 maišos funkciją.

Tikrintojas privalo pats žinoti Europos viešąjį raktą EUR.PK (ir juo pasikliauti).

Toliau pateiktoje schemoje pavaizduotas protokolas, kurį IDE su kontrolės kortele gali naudoti į ESM (išorines laikmenas) perkeltų ir saugomų duomenų nepažeistumui tikrinti. Kontrolės kortelė naudojama skaitmeniniams parašams iššifruoti. Tokiu atveju ši funkcija gali būti neįdiegta į IDE.

Duomenims, kurie bus analizuojami, perkelti ir pasirašyti naudota įranga žymima EQT.

▼B



B DALIS.

ANTROSIOS KARTOS TACHOGRAFO SISTEMA

7. ĮVADAS

7.1. **Nuorodos**

Šioje šio priedėlio dalyje naudoti tokie šaltiniai:

AES	Nacionalinis standartų ir technologijos institutas (NIST), FIPS leidinys Nr. 197. Patobulintas šifravimo standartas (angl. *Advanced Encryption Standard*, AES), 2001 m. lapkričio 26 d.
DSS	Nacionalinis standartų ir technologijos institutas (NIST). FIPS leidinys Nr. 186-4. Skaitmeninio parašo standartas (angl. *Digital Signature Standard*, DSS), 2013 m. liepos mėn.
ISO 7816-4	ISO/IEC 7816-4. Atpažinimo kortelės. Lustinės kortelės. 4 dalis. Struktūra, saugumas ir mainų komandos. Trečioji laida, 2013 4 15.
ISO 7816-8	ISO/IEC 7816-8. Atpažinimo kortelės. Lustinės kortelės. 8 dalis. Saugumo operacijų komandos. Antroji laida, 2004 6 1.

▼B

ISO 8825-1	ISO/IEC 8825-1. Informacijos technologija. ASN.1 kodavimo taisyklės. Pagrindinio, kanoninio ir skiriamojo kodavimo taisyklių aprašas. Ketvirtoji laida, 2008 12 15.
ISO 9797-1	ISO/IEC 9797-1. Informacinės technologijos. Saugumo metodai. Pranešimų tapatumo nustatymo kodai. 1 dalis. Mechanizmai, pagrįsti blokiniu šifru. Antroji laida, 2011 3 1.
ISO 10116	ISO/IEC 10116. Informacijos technologija. Saugumo metodai. Veiksenos, skirtos n bitų blokiniam šifrui. Trečioji laida.2006 2 1.
ISO 16844-3	ISO/IEC 16844-3. Kelių transporto priemonės. Tachografų sistemos. 3 dalis. Judesio jutiklio sąsaja. Pirmoji laida 2004 m., įskaitant 1-ąją techninę pataisą 2006 m.
RFC 5480	Elipsinės kreivės kriptografija pagrįsto viešojo rakto informacija, 2009 m. kovo mėn.
RFC 5639	Elipsinių kreivių kriptografija (ECC). „Brainpool“ standartinės kreivės ir kreivių generavimas, 2010 m.
RFC 5869	HMAC pagrįsta išskyrimo ir išplėtimo rakto darybos funkcija (angl. *HMAC-based Extract-and-Expand Key Derivation Function*, HKDF), 2010 m. gegužės mėn.
SHS	Nacionalinis standartų ir technologijos institutas (NIST). FIPS leidinys Nr. 180-4. Saugios maišos standartas, 2012 m. kovo mėn.
SP 800-38B	Nacionalinis standartų ir technologijos institutas (NIST). Specialusis leidinys Nr. 800-38B. Rekomendacija dėl blokinio šifravimo būdų. CMAC autentiškumo tikrinimo būdas, 2005 m.
TR-03111	BSI techninės gairės TR-03111. Elipsinių kreivių kriptografija. 2.00 versija, 2012 m. birželio 28 d.

7.2. **Žymenys ir terminų santrumpos**

Šiame priedėlyje vartojami žymenys ir terminų santrumpos

AES	patobulintas šifravimo standartas
CA	pažymėjimų įstaiga
CAR	pažymėjimų įstaigos žymuo
CBC	nuoseklusis blokinis šifravimas (režimas)
CH	komandos antraštė
CHA	pažymėjimo turėtojo įgaliojimas
CHR	pažymėjimo turėtojo žymuo
CV	pastovus vektorius
DER	išskirtinės kodavimo taisyklės
DO	duomenų objektas
DSRC	skirtasis trumpojo nuotolio ryšys
ECC	elipsinių kreivių kriptografija
ECDSA	elipsinių kreivių kriptografija pagrįsto skaitmeninio parašo algoritmas
ECDH	elipsinių kreivių kriptografija pagrįstas Diffie-Hellmano algoritmas (raktų derinimo algoritmas)
EGF	išorinis GNSS įrenginys
EQT	įranga

▼B

IDE	specializuota įranga su mikroprocesoriumi
K_M	judesio jutiklio pagrindinis raktas, suteikiantis galimybę transporto priemonės bloką susieti su judesio jutikliu
K_{M-VU}	į transporto priemonės bloką įdiegtas raktas, transporto priemonės blokui suteikiantis galimybę apskaičiuoti judesio jutiklio pagrindinį raktą, kai į transporto priemonės bloką įstatoma dirbtuvių kortelė
K_{M-WC}	į dirbtuvių korteles įdiegtas raktas, transporto priemonės blokui suteikiantis galimybę apskaičiuoti judesio jutiklio pagrindinį raktą, kai į transporto priemonės bloką įstatoma dirbtuvių kortelė
MAC	pranešimo atpažinimo kodas
MoS	judesio jutiklis
MSB	svarbiausias bitas
PKI	viešojo rakto infrastruktūra
RCF	nuotolinio ryšio įrenginys
SSC	siuntimo sekos skaitiklis
SM	saugusis keitimasis pranešimais
TDES	trigubo duomenų šifravimo standartas
TLV	žymenos ilgio vertė
VU	transporto priemonės blokas
X.C	naudotojo X viešojo rakto pažymėjimas
X.CA	naudotojo X pažymėjimą išdavusi pažymėjimų įstaiga
X.CAR	naudotojo X pažymėjime nurodytas pažymėjimų įstaigos žymuo
X.CHR	naudotojo X pažymėjime nurodytas pažymėjimo turėtojo žymuo
X.PK	naudotojo X viešasis raktas
X.SK	naudotojo X privatusis raktas
$X.PK_{eph}$	naudotojo X trumpalaikis viešasis raktas
$X.SK_{eph}$	naudotojo X trumpalaikis privatusis raktas
‘xx’	šešioliktainė vertė
||	sujungimo ženklas

7.3. **Terminų apibrėžtys**

Šiame priedėlyje vartojamų terminų apibrėžtys pateiktos 1C priedo I skirsnyje.

8. KRIPTOGRAFINĖS SISTEMOS IR ALGORITMAI

8.1. **Kriptografinės sistemos**

CSM_38 Transporto priemonės blokuose ir tachografo kortelėse taikoma elipsinėmis kreivėmis pagrįsta viešaraktė kriptografinė sistema, kuria teikiamos šios apsaugos paslaugos:

— transporto priemonės bloko ir kortelės abipusis autentiškumo tikrinimas;

▼B

— AES seanso raktų derinimas tarp transporto priemonės bloko ir kortelės;

— iš transporto priemonės blokų arba tachografų kortelių į išorines laikmenas perkeliamų duomenų autentiškumo, nepažeistumo ir su šiais duomenimis susijusios atsakomybės prisiėmimo užtikrinimas.

CSM_39 Transporto priemonės blokuose ir išoriniuose GNSS įrenginiuose taikoma elipsinėmis kreivėmis pagrįsta viešaraktė kriptografinė sistema, kuria teikiamos šios apsaugos paslaugos:

— transporto priemonės bloko ir išorinio GNSS įrenginio sujungimas;

— transporto priemonės bloko ir išorinio GNSS įrenginio abipusis autentiškumo tikrinimas;

— AES seanso raktų derinimas tarp transporto priemonės bloko ir išorinio GNSS įrenginio.

CSM_40 Transporto priemonės blokuose ir tachografo kortelėse taikoma AES pagrįsta simetrinė kriptografinė sistema, kuria teikiamos šios apsaugos paslaugos:

— duomenų, kuriais tarpusavyje keičiasi transporto priemonės blokas ir tachografo kortelė, autentiškumo ir nepažeistumo užtikrinimas;

— jeigu taikytina, duomenų, kuriais tarpusavyje keičiasi transporto priemonės blokas ir tachografo kortelė, konfidencialumo užtikrinimas.

CSM_41 Transporto priemonės blokuose ir išoriniuose GNSS įrenginiuose taikoma AES pagrįsta simetrinė kriptografinė sistema, kuria teikiamos šios apsaugos paslaugos:

— duomenų, kuriais tarpusavyje keičiasi transporto priemonės blokas ir išorinis GNSS įrenginys, autentiškumo ir nepažeistumo užtikrinimas.

CSM_42 Transporto priemonės blokuose ir judesio jutikliuose taikoma AES pagrįsta simetrinė kriptografinė sistema, kuria teikiamos šios apsaugos paslaugos:

— transporto priemonės bloko ir judesio jutiklio siejimas;

— transporto priemonės bloko ir judesio jutiklio abipusis autentiškumo tikrinimas;

— duomenų, kuriais tarpusavyje keičiasi transporto priemonės blokas ir judesio jutiklis, konfidencialumo užtikrinimas.

CSM_43 Transporto priemonės blokuose ir kontrolės kortelėse taikoma AES pagrįsta simetrinė kriptografinė sistema, kuria teikiamos šios nuotolinio ryšio sąsajos apsaugos paslaugos:

— iš transporto priemonės bloko ir tachografo kortelę perduodamų duomenų konfidencialumo, autentiškumo ir nepažeistumo užtikrinimas.

Pastabos

— Tiksliau sakant, duomenys iš transporto priemonės bloko nuotolinio ryšio įrenginiu, kuris transporto priemonės bloko atžvilgiu gali būti tiek vidinis, tiek išorinis (žr. 14 priedėlį), perduodami į nuotolinį užklausiklį,

▼B

valdomą kontrolės pareigūno. Tačiau nuotolinis užklausiklis gautus duomenis persiunčia į kontrolės kortelę, kad jie būtų iššifruoti ir patikrintas jų autentiškumas. Saugumo požiūriu nuotolinio ryšio įrenginys ir nuotolinis užklausiklis yra visiškai skaidrūs.

— Naudojant dirbtuvių kortelę teikiamos tokios pat DSRC sąsajos apsaugos paslaugos, kaip ir naudojant kontrolės kortelę. Taip dirbtuvėms suteikiama galimybė patikrinti, ar tinkamai veikia transporto priemonės bloko nuotolinio ryšio sąsaja ir ar ji saugi. Daugiau informacijos pateikta 9.2.2 skirsnyje.

8.2. **Kriptografiniai algoritmai**

8.2.1 *Simetriniai algoritmai*

CSM_44 Transporto priemonės blokai, tachografo kortelės, judesio jutikliai ir išoriniai GNSS įrenginiai turi būti suderinami su AES algoritmu, nustatytu [AES], taikant 128, 192 ir 256 bitų ilgio raktus.

8.2.2 *Asimetriniai algoritmai ir standartiniai domeno parametrai*

CSM_45 Transporto priemonės blokai, tachografo kortelės ir išoriniai GNSS įrenginiai turi būti suderinami su elipsinių kreivių kriptografija taikant 256, 384 ir 512/521 bitų dydžio raktus.

CSM_46 Transporto priemonės blokai, tachografo kortelės ir išoriniai GNSS įrenginiai turi būti suderinami su ECDSA parašo algoritmu, nustatytu [DSS].

CSM_47 Transporto priemonės blokai, tachografo kortelės ir išoriniai GNSS įrenginiai turi būti suderinami su ECKA-EB raktų derinimo algoritmu, nustatytu [TR 03111].

CSM_48 Transporto priemonės blokai, tachografo kortelės ir išoriniai GNSS įrenginiai turi būti suderinami su visais standartiniais domeno parametrais, nurodytais toliau pateiktoje 1 lentelėje ir susijusiais su elipsinių kreivių kriptografija.

1 lentelė.

Standartiniai domeno parametrai

Pavadinimas	Dydis (bitais)	Nuoroda	Objekto identifikatorius
NIST P-256	256	[DSS], [RFC 5480]	`secp256r1`
BrainpoolP256r1	256	[RFC 5639]	`brainpoolP256r1`
NIST P-384	384	[DSS], [RFC 5480]	`secp384r1`
BrainpoolP384r1	384	[RFC 5639]	`brainpoolP384r1`
BrainpoolP512r1	512	[RFC 5639]	`brainpoolP512r1`
NIST P-521	521	[DSS], [RFC 5480]	`secp521r1`

▼B

Pastaba. Paskutinėje 1 lentelės skiltyje nurodyti objektų identifikatoriai, susiję su „Brainpool“ kreivėmis, yra nustatyti [RFC 5639], o susiję su NIST kreivėmis – [RFC 5480].

1 pavyzdys. BrainpoolP256r1 kreivės objekto identifikatorius yra: `{iso(1) identified-organization(3) teletrust(36) algorithm(3) signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8) ellipticCurve(1) versionOne(1) 7}`.

Atitinkamas adresas su taškiniais skirtukais: `1.3.36.3.3.2.8.1.1.7`.

2 pavyzdys. NIST P-384 kreivės objekto identifikatorius yra:

`{iso(1) identified-organization(3) certicom(132) curve(0) 34}`.

Atitinkamas adresas su taškiniais skirtukais: `1.3.132.0.34`.

8.2.3 *Maišos algoritmai*

CSM_49 Transporto priemonės blokai ir tachografo kortelės turi būti suderinami su SHA-256, SHA-384 ir SHA-512 algoritmais, nustatytais [SHS].

8.2.4 *Šifravimo deriniai*

CSM_50 Jei saugumo protokolui sudaryti kartu taikomi simetrinis algoritmas, asimetrinis algoritmas ir (arba) maišos algoritmas, jų atitinkami raktų ilgiai ir maišos dydžiai turi būti (iš esmės) tokio pat stiprumo. 2 lentelėje nurodyti leidžiami šifravimo deriniai:

2 lentelė.

Leidžiami šifravimo deriniai

Šifravimo derinio ID	ECC rakto dydis (bitais)	AES rakto dydis (bitais)	Maišos algoritmas	MAC ilgis (baitais)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Pastaba. Šiame priedėlyje 512 ir 521 bitų ilgio ECC raktai laikomi vienodo stiprumo.

9. RAKTAI IR PAŽYMĖJIMAI

9.1. **Asimetrinės raktų poros ir viešųjų raktų pažymėjimai**

9.1.1 *Bendrosios nuostatos*

Pastaba. Šiame skirsnyje aprašyti raktai skirti abipusiam autentiškumo tikrinimui ir saugiajam keitimuisi pranešimais tarp transporto priemonės blokų ir tachografo kortelių bei tarp transporto priemonės blokų ir išorinių GNSS įrenginių. Šie procesai išsamiai aprašyti šio priedėlio 10 ir 11 skyriuose.

CSM_51 Europos išmaniojo tachografo sistemoje ECC raktų poros ir atitinkami pažymėjimai generuojami ir tvarkomi trim funkciniais lygmenimis:

— Europos lygmeniu,

— valstybių narių lygmeniu,

— įrangos lygmeniu.

▼B

CSM_52 Visoje Europos išmaniojo tachografo sistemoje viešieji bei privatieji raktai ir pažymėjimai generuojami, tvarkomi ir perduodami taikant standartinius, saugius metodus.

9.1.2 *Europos lygmuo*

CSM_53 Europos lygmeniu sugeneruojama viena unikali ECC raktų pora, žymima EUR. Ji sudaroma iš privačiojo rakto (EUR.SK) ir viešojo rakto (EUR.PK). Ši raktų pora yra visos Europos išmaniojo tachografo PKI pagrindinė raktų pora. Šią užduotį Europos Komisijos įgaliojimu ir atsakomybe atlieka Europos vyriausioji pažymėjimų įstaiga (ERCA).

CSM_54 Naudodama Europos privatųjį raktą, ERCA (pati) pasirašo Europos viešojo rakto pagrindinį pažymėjimą ir jį perduoda visoms valstybėms narėms.

CSM_55 Naudodama Europos privatųjį raktą, ERCA, gavusi prašymą, pasirašo valstybių narių viešųjų raktų pažymėjimus. ERCA tvarko visų pasirašytų valstybių narių viešųjų raktų pažymėjimų registrą.

CSM_56 Kaip nurodyta 9.1.7 skirsnyje pateiktame 1 paveiksle, ERCA kas 17 metų sugeneruoja naują Europos pagrindinę raktų porą. ERCA, sugeneravusi naują Europos pagrindinę raktų porą, sukuria naują jos pačios pasirašytą pagrindinį pažymėjimą, skirtą naujam Europos viešajam raktui. Europos pagrindinio pažymėjimo galiojimo laikotarpis – 34 metai ir 3 mėnesiai.

Pastaba. Nustačiusi naują pagrindinę raktų porą, ERCA sugeneruoja naują judesio jutiklių pagrindinį raktą ir naują DSRC pagrindinį raktą; žr. 9.2.1.2 ir 9.2.2.2 skirsnius.

CSM_57 Prieš sugeneruodama naują pagrindinę raktų porą, ERCA atlieka reikiamo naujosios raktų poros, kuri turėtų išlikti saugi kitus 34 metus, kriptografinio stiprumo analizę. Nustačiusi, kad tai būtina, ERCA pradeda taikyti šifravimo rinkinį, kuris yra stipresnis už dabartinį, kaip nustatyta CSM_50 punkte.

CSM_58 ERCA, sugeneravusi naują Europos pagrindinę raktų porą, sukuria naujo Europos viešojo rakto sąsajos pažymėjimą ir pasirašo jį naudodama ankstesnį Europos privatųjį raktą. Šio sąsajos pažymėjimo galiojimo laikotarpis – 17 metų. Ši tvarka taip pat pavaizduota 9.1.7 skirsnyje pateiktame 1 paveiksle.

Pastaba. Kadangi sąsajos pažymėjime yra ERCA *X* kartos viešasis raktas ir šis pažymėjimas yra pasirašytas naudojant ERCA *X-1* kartos privatųjį raktą, sąsajos pažymėjimu *X-1* kartos įrangai siūlomas būdas, kuriuo galima užtikrinti pasitikėjimą *X* kartos įranga.

CSM_59 Įsigaliojus naujo pagrindinio rakto pažymėjimui, ERCA jokiais tikslais nenaudoja pagrindinės raktų poros privačiojo rakto.

▼B

CSM_60 ERCA visada disponuoja tokiais kriptografiniais raktais ir pažymėjimais:

— dabartine EUR raktų pora ir atitinkamu pažymėjimu;

— visais ankstesniais EUR pažymėjimais, naudotinais tebegaliojantiems MSCA pažymėjimams patikrinti;

— sąsajos pažymėjimais, skirtais visų kartų EUR pažymėjimams, išskyrus pirmosios kartos pažymėjimus.

9.1.3 *Valstybių narių lygmuo*

CSM_61 Valstybių narių lygmeniu visos valstybės narės, kurios privalo pasirašyti tachografo kortelės pažymėjimus, sugeneruoja vieną arba daugiau unikalių ECC raktų porų, žymimų MSCA_Card. Visos valstybės narės, kurios privalo pasirašyti transporto priemonės blokų arba išorinių GNSS įrenginių pažymėjimus, taip pat sugeneruoja vieną arba daugiau unikalių ECC raktų porų, žymimų MSCA_VU-EGF.

CSM_62 Valstybių narių raktų poras generuoja valstybės narės pažymėjimų įstaiga (MSCA). MSCA, sugeneravusi valstybės narės raktų porą, viešąjį raktą perduoda ERCA, kad gautų ERCA pasirašytą atitinkamą valstybės narės pažymėjimą.

CSM_63 MSCA parenka tokį valstybės narės raktų poros stiprumą, kuris būtų lygiavertis Europos pagrindinės raktų poros, skirtos atitinkamam valstybės narės pažymėjimui pasirašyti, stiprumui.

CSM_64 MSCA_VU-EGF raktų pora, jei tokia yra, sudaroma iš privačiojo rakto MSCA_VU-EGF.SK ir viešojo rakto MSCA_VU-EGF.PK. MSCA naudoja privatųjį raktą MSCA_VU-EGF.SK tik transporto priemonės blokų ir išorinių GNSS įrenginių viešojo rakto pažymėjimams pasirašyti.

CSM_65 MSCA_Card raktų pora sudaroma iš privačiojo rakto MSCA_Card.SK ir viešojo rakto MSCA_Card.PK. MSCA naudoja privatųjį raktą MSCA_Card.SK tik tachografo kortelių viešojo rakto pažymėjimams pasirašyti.

CSM_66 MSCA tvarko visų pasirašytų transporto priemonės blokų pažymėjimų, išorinių GNSS įrenginių pažymėjimų ir kortelės pažymėjimų registrą, taip pat įrangos, kuriai yra skirtas pažymėjimas, identifikavimo duomenis.

CSM_67 MSCA_VU-EGF pažymėjimo galiojimo laikotarpis – 17 metų ir 3 mėnesiai. MSCA_Card pažymėjimo galiojimo laikotarpis – 7 metai ir 1 mėnuo.

CSM_68 Kaip parodyta 9.1.7 skirsnyje pateiktame 1 paveiksle, MSCA_VU-EGF raktų poros privačiojo rakto ir MSCA_Card raktų poros privačiojo rakto naudojimo laikotarpis – dveji metai.

▼B

CSM_69 Pasibaigus MSCA_VU-EGF raktų poros privačiojo rakto naudojimo laikotarpiui, MSCA jokiais tikslais nenaudoja šio rakto. Pasibaigus MSCA_Card raktų poros privačiojo rakto naudojimo laikotarpiui, MSCA jokiais tikslais nenaudoja šio rakto.

CSM_70 MSCA visada disponuoja tokiais kriptografiniais raktais ir pažymėjimais:

— dabartine MSCA_Card raktų pora ir atitinkamu pažymėjimu;

— visais ankstesniais MSCA_Card pažymėjimais, naudotinais tebegaliojantiems tachografo kortelės pažymėjimams patikrinti;

— dabartiniu EUR pažymėjimu, reikalingu dabartiniam MSCA pažymėjimui patikrinti;

— visais ankstesniais EUR pažymėjimais, reikalingais visiems MSCA išduotiems tebegaliojantiems pažymėjimams patikrinti.

CSM_71 Jei MSCA privalo pasirašyti transporto priemonės blokų arba išorinių GNSS įrenginių pažymėjimus, ji papildomai disponuoja šiais raktais ir pažymėjimais:

— dabartine MSCA_VU-EGF raktų pora ir atitinkamu pažymėjimu;

— visais ankstesniais MSCA_VU-EGF viešaisiais raktais, naudotinais tebegaliojantiems transporto priemonės blokų arba išorinių GNSS įrenginių pažymėjimams patikrinti.

9.1.4 *Įrangos lygmuo. Transporto priemonės blokai*

CSM_72 Kiekvienam transporto priemonės blokui sugeneruojama po dvi unikalias ECC raktų poras, žymimas VU_MA ir VU_Sign. Tai atlieka transporto priemonės blokų gamintojai. Sugeneravę transporto priemonės bloko raktų porą, raktą generuojantis subjektas viešąjį raktą perduoda šalies, kurioje jis yra įsisteigęs, MSCA, kad gautų MSCA pasirašytą atitinkamą transporto priemonės bloko pažymėjimą. Privatusis raktas naudojamas tik transporto priemonės bloke.

CSM_73 Tam tikro transporto priemonės bloko VU_MA ir VU_Sign pažymėjimų įsigaliojimo data turi būti ta pati.

CSM_74 Transporto priemonės bloko gamintojas parenka tokį transporto priemonės bloko raktų poros stiprumą, kuris būtų lygiavertis MSCA raktų poros, skirtos atitinkamam transporto priemonės bloko pažymėjimui pasirašyti, stiprumui.

CSM_75 Transporto priemonės bloke jam skirta raktų pora VU_MA, sudaryta iš privačiojo rakto VU_MA.SK ir viešojo rakto VU_MA.PK, naudojama tik transporto priemonės bloko autentiškumui patvirtinti tachografo kortelių ir išorinių GNSS įrenginių atžvilgiu, kaip nustatyta šio priedėlio 10.3 ir 11.4 skirsniuose.

CSM_76 Transporto priemonės blokas turi galėti generuoti trumpalaikių ECC raktų poras ir trumpalaikių raktų porą naudoja tik seanso raktui derinti su tachografo kortele arba išoriniu GNSS įrenginiu, kaip nustatyta šio priedėlio 10.4 ir 11.4 skirsniuose.

▼B

CSM_77 Transporto priemonės bloke jo VU_Sign raktų poros privatusis raktas VU_Sign.SK naudojamas tik perkeltų duomenų rinkmenoms pasirašyti, kaip nustatyta šio priedėlio 14 skyriuje. Atitinkamas viešasis raktas VU_Sign.PK naudojamas tik transporto priemonės bloko sukurtiems parašams patikrinti.

CSM_78 Kaip nurodyta 9.1.7 skirsnyje pateiktame 1 paveiksle, VU_MA pažymėjimo galiojimo laikotarpis – 15 metų ir 3 mėnesiai. VU_Sign pažymėjimo galiojimo laikotarpis – taip pat 15 metų ir 3 mėnesiai.

Pastabos

— Nustatant ilgesnį VU_Sign pažymėjimo galiojimo laikotarpį transporto priemonės blokas gali galiojančius perkeltų duomenų parašus kurti dar tris mėnesius nuo šio pažymėjimo galiojimo pabaigos, kaip reikalaujama Reglamente (ES) Nr. 581/2010.

— Ilgesnis VU_MA pažymėjimo galiojimo laikotarpis reikalingas tam, kad dar tris mėnesius nuo šio pažymėjimo galiojimo pabaigos būtų galima patvirtinti transporto priemonės bloko autentiškumą kontrolės kortelės arba įmonės kortelės atžvilgiu, taip suteikiant galimybę perkelti duomenis.

CSM_79 Pasibaigus atitinkamo pažymėjimo galiojimui, transporto priemonės blokas jokiais tikslais nenaudoja transporto priemonės bloko raktų poros privačiojo rakto.

CSM_80 Pradėjus naudoti transporto priemonės bloką, transporto priemonės bloko raktų poros (išskyrus trumpalaikių raktų poras) ir atitinkami to transporto priemonės bloko pažymėjimai darbo sąlygomis nekeičiami ir neatnaujinami.

Pastabos

— Trumpalaikių raktų poroms šis reikalavimas netaikomas, nes kaskart, kai atliekamas lusto autentiškumo tikrinimas ir seanso raktų derinimas, transporto priemonės blokas sugeneruoja naują trumpalaikių raktų porą; žr. 10.4 skirsnį. Pažymėtina, kad trumpalaikių raktų poroms atitinkami pažymėjimai neišduodami.

— Šiuo reikalavimu neatimama galimybė transporto priemonės bloko statinių raktų poras keisti saugioje transporto priemonės bloko gamintojo kontroliuojamoje aplinkoje atliekant atnaujinimo arba taisymo darbus.

CSM_81 Pradedamuose naudoti transporto priemonės blokuose turi būti tokie kriptografiniai raktai ir pažymėjimai:

— privatusis raktas VU_MA ir atitinkamas pažymėjimas;

— privatusis raktas VU_Sign ir atitinkamas pažymėjimas;

— MSCA_VU-EGF pažymėjimas su MSCA_VU-EGF.PK viešuoju raktu, skirtu VU_MA pažymėjimui ir VU_Sign pažymėjimui patikrinti;

▼B

— EUR pažymėjimas su EUR.PK viešuoju raktu, skirtu MSCA_VU-EGF pažymėjimui patikrinti;

— EUR pažymėjimas, kurio galiojimo laikotarpis yra prieš pat EUR pažymėjimo, skirto MSCA_VU-EGF pažymėjimui patikrinti, galiojimo laikotarpį, jei toks pažymėjimas yra;

— sąsajos pažymėjimas, kuriuo susiejami šie du EUR pažymėjimai, jei toks yra.

CSM_82 Be CSM_81 punkte nurodytų kriptografinių raktų ir pažymėjimų, transporto priemonės blokuose taip pat turi būti šio priedėlio A dalyje nurodyti raktai ir pažymėjimai, kad transporto priemonės blokas galėtų sąveikauti su pirmosios kartos tachografo kortelėmis.

9.1.5 *Įrangos lygmuo. Tachografo kortelės*

CSM_83 Kiekvienai tachografo kortelei sugeneruojama unikali ECC raktų pora, žymima Card_MA. Kiekvienai vairuotojo kortelei ir kiekvienai dirbtuvių kortelei sugeneruojama antra unikali ECC raktų pora, žymima Card_Sign. Tai gali atlikti kortelių gamintojai arba kortelių individualizuotojai. Sugeneravęs kortelės raktų porą, raktą generuojantis subjektas viešąjį raktą perduoda šalies, kurioje jis yra įsisteigęs, MSCA, kad gautų MSCA pasirašytą atitinkamą kortelės pažymėjimą. Privatusis raktas naudojamas tik tachografo kortelėje.

CSM_84 Tam tikros vairuotojo kortelės arba dirbtuvių kortelės Card_MA ir Card_Sign pažymėjimų įsigaliojimo data turi būti ta pati.

CSM_85 Kortelės gamintojas arba kortelės individualizuotoja parenka tokį kortelės raktų poros stiprumą, kuris būtų lygiavertis MSCA raktų poros, skirtos atitinkamam kortelės pažymėjimui pasirašyti, stiprumui.

CSM_86 Tachografo kortelėje jai skirta Card_MA raktų pora, sudaryta iš privačiojo rakto Card_MA.SK ir viešojo rakto Card_MA.PK, naudojama tik abipusiam autentiškumo tikrinimui ir seanso raktų derinimui transporto priemonės blokų atžvilgiu, kaip nustatyta šio priedėlio 10.3 ir 10.4 skirsniuose.

CSM_87 Vairuotojo kortelėje arba dirbtuvių kortelėje jos Card_Sign raktų poros privatusis raktas Card_Sign.SK naudojamas tik perkeltų duomenų rinkmenoms pasirašyti, kaip nustatyta šio priedėlio 14 skyriuje. Atitinkamas viešasis raktas Card_Sign.PK naudojamas tik kortelės sukurtiems parašams patikrinti.

CSM_88 Card_MA pažymėjimo galiojimo laikotarpis yra toks:

— vairuotojo kortelės: 5 metai,

— įmonės kortelės: 2 metai,

— kontrolės kortelės: 2 metai,

— dirbtuvių kortelės: 1 metai.

▼B

CSM_89 Card_Sign pažymėjimo galiojimo laikotarpis yra toks:

— vairuotojo kortelės:	5 metai ir 1 mėnuo,
— dirbtuvių kortelės:	1 metai ir 1 mėnuo.

Pastaba. Nustatant ilgesnį Card_Sign pažymėjimo galiojimo laikotarpį, vairuotojo kortelė gali galiojančius perkeltų duomenų parašus kurti dar mėnesį nuo šio pažymėjimo galiojimo pabaigos. Tai būtina pagal Reglamentą (ES) Nr. 581/2010, kuriame reikalaujama, kad duomenis iš vairuotojo kortelės būtų galima perkelti dar 28 dienas nuo tos dienos, kai į ją paskutinį kartą buvo įrašyti duomenys.

CSM_90 Išdavus kortelę, tos tachografo kortelės raktų poros ir atitinkami pažymėjimai nekeičiami ir neatnaujinami.

CSM_91 Išduotose tachografo kortelėse turi būti tokie kriptografiniai raktai ir pažymėjimai:

— Card_MA privatusis raktas ir atitinkamas pažymėjimas;

— be to, vairuotojų kortelėse ir dirbtuvių kortelėse – Card_Sign privatusis raktas ir atitinkams pažymėjimas;

— MSCA_Card pažymėjimas su MSCA_Card.PK viešuoju raktu, skirtu Card_MA pažymėjimui ir Card_Sign pažymėjimui patikrinti;

— EUR pažymėjimas su EUR.PK viešuoju raktu, skirtu MSCA_Card pažymėjimui patikrinti;

— EUR pažymėjimas, kurio galiojimo laikotarpis yra prieš pat EUR pažymėjimo, skirto MSCA_Card pažymėjimui, patikrinti, galiojimo laikotarpį, jei toks pažymėjimas yra.

— sąsajos pažymėjimas, kuriuo susiejami šie du EUR pažymėjimai, jei toks yra.

CSM_92 Be CSM_91 punkte nurodytų kriptografinių raktų ir pažymėjimų, tachografo kortelėse taip pat turi būti šio priedėlio A dalyje nurodyti raktai ir pažymėjimai, kad šios kortelės galėtų sąveikauti su pirmosios kartos transporto priemonės blokais.

9.1.6 *Įrangos lygmuo. Išoriniai GNSS įrenginiai*

CSM_93 Kiekvienam išoriniam GNSS įrenginiui sugeneruojama po unikalią ECC raktų porą, žymimą EGF_MA. Tai atlieka išorinių GNSS įrenginių gamintojai. Sugeneravus EGF_MA raktų porą, viešasis raktas perduodamas šalies, kurioje įsisteigęs gamintojas, MSCA, kad būtų gautas MSCA pasirašytas atitinkamas EGF_MA pažymėjimas. Privatusis raktas naudojamas tik išoriniame GNSS įrenginyje.

CSM_94 EGF gamintojas parenka tokį EGF_MA raktų poros stiprumą, kuris būtų lygiavertis MSCA raktų poros, skirtos atitinkamam EGF_MA pažymėjimui pasirašyti, stiprumui.

▼B

CSM_95 Išoriniame GNSS įrenginyje jam skirta raktų pora EGF_MA, sudaryta iš privačiojo rakto EGF_MA.SK ir viešojo rakto EGF_MA.PK, naudojama tik abipusiam autentiškumo tikrinimui ir seanso raktų derinimui transporto priemonės blokų atžvilgiu, kaip nustatyta šio priedėlio 11.4 ir 11.4 skirsniuose.

CSM_96 EGF_MA pažymėjimo galiojimo laikotarpis – 15 metų.

CSM_97 Pasibaigus atitinkamo pažymėjimo galiojimui, išorinis GNSS įrenginys nenaudoja EGF_MA raktų poros privačiojo rakto sujungimo su transporto priemonės bloku tikslais.

Pastaba. Kaip paaiškinta 11.3.3 skirsnyje, EGF jam skirtą privatųjį raktą savo autentiškumui patvirtinti transporto priemonės bloko, su kuriuo jis jau sujungtas, atžvilgiu gali naudoti net ir pasibaigus atitinkamo pažymėjimo galiojimui.

CSM_98 Pradėjus naudoti EGF, EGF_MA raktų pora ir atitinkamas to išorinio GNSS įrenginio pažymėjimas darbo sąlygomis nekeičiami ir neatnaujinami.

Pastaba. Šiuo reikalavimu neatimama galimybė EGF raktų poras keisti saugioje EGF gamintojo kontroliuojamoje aplinkoje atliekant atnaujinimo arba taisymo darbus.

CSM_99 Pradedamame naudoti išoriniame GNSS įrenginyje turi būti tokie kriptografiniai raktai ir pažymėjimai:

— EGF_MA privatusis raktas ir atitinkamas pažymėjimas;

— MSCA_VU-EGF pažymėjimas su MSCA_VU-EGF.PK viešuoju raktu, skirtu EGF_MA pažymėjimui patikrinti;

— EUR pažymėjimas su EUR.PK viešuoju raktu, skirtu MSCA_VU-EGF pažymėjimui patikrinti;

— EUR pažymėjimas, kurio galiojimo laikotarpis yra prieš pat EUR pažymėjimo, skirto MSCA_VU-EGF pažymėjimui patikrinti, galiojimo laikotarpį, jei toks pažymėjimas yra;

— sąsajos pažymėjimas, kuriuo susiejami šie du EUR pažymėjimai, jei toks yra.

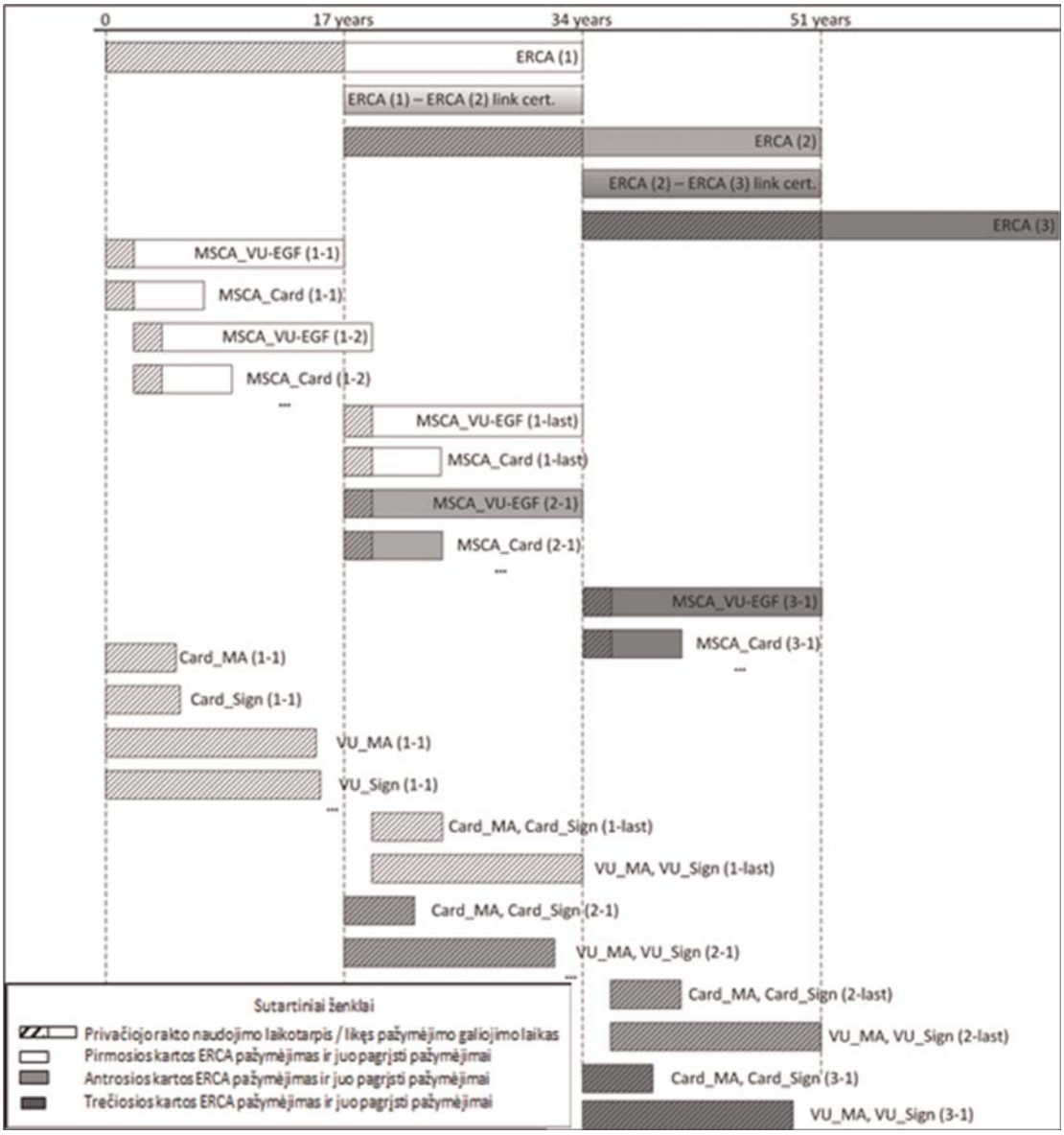
9.1.7 *Apžvalga. Pažymėjimo keitimas*

Toliau pateiktame 1 paveiksle parodyta, kaip išduodami ir laikui bėgant naudojami įvairių kartų ERCA pagrindiniai pažymėjimai, ERCA sąsajos pažymėjimai, MSCA pažymėjimai ir įrangos (transporto priemonės blokų ir kortelių) pažymėjimai:

▼B

1 pav.

Įvairių kartų ERCA pagrindinių pažymėjimų, ERCA sąsajos pažymėjimų, MSCA pažymėjimų ir įrangos pažymėjimų išdavimas ir naudojimas



Pastabos dėl 1 paveikslo

1. Pagrindinių pažymėjimų karta nurodoma skliaustuose pateiktu skaičiumi. Pvz., ERCA (1) yra pirmosios kartos ERCA pagrindinis pažymėjimas; ERCA (2) – antrosios kartos pažymėjimas ir t. t.

2. Kiti pažymėjimai nurodyti dviem skliaustuose pateiktais skaičiais: pirmuoju skaičiumi nurodoma pagrindinio pažymėjimo, kuriuo remiantis buvo išduotas atitinkamas pažymėjimas, karta, antruoju – paties pažymėjimo karta. Pvz., MSCA_Card (1-1) yra pirmasis MSCA_Card pažymėjimas, išduotas remiantis ERCA (1); MSCA_Card (2-1) yra pirmasis MSCA_Card pažymėjimas, išduotas remiantis ERCA (2); MSCA_Card (2-last) yra paskutinysis MSCA_Card pažymėjimas, išduotas remiantis ERCA (2); Card_MA(2-1) yra pirmasis kortelės pažymėjimas, remiantis ERCA (2) išduotas abipusio autentiškumo tikrinimo tikslais, ir t. t.

▼B

3. MSCA_Card (2-1) ir MSCA_Card (1-last) pažymėjimai išduodami beveik tuo pat metu, tačiau jų išdavimo datos šiek tiek skiriasi. MSCA_Card (2-1) yra pirmasis MSCA_Card pažymėjimas, išduotas remiantis ERCA (2), jis bus išduotas šiek tiek vėliau nei MSCA_Card (1-last) – paskutinis MSCA_Card pažymėjimas, išduotas remiantis ERCA (1).

4. Kaip parodyta paveiksle, pirmieji transporto priemonės bloko ir kortelės pažymėjimai, išduoti remiantis ERCA (2), pasirodys likus beveik dvejiems metams iki to laiko, kai pasirodys paskutinieji transporto priemonės bloko ir kortelės pažymėjimai, išduoti remiantis ERCA (1). Taip yra dėl to, kad transporto priemonės bloko ir kortelės pažymėjimai išduodami remiantis MSCA pažymėjimu, o ne tiesiogiai remiantis ERCA pažymėjimu. MSCA (2-1) pažymėjimas bus išduotas iš karto po to, kai įsigalios ERCA (2), o MSCA (1-last) pažymėjimas bus išduotas šiek tiek anksčiau, paskutiniu ERCA (1) pažymėjimo galiojimo momentu. Todėl šių dviejų MSCA pažymėjimų galiojimo laikotarpiai bus beveik vienodi, nors šie pažymėjimai ir skirtingų kartų.

5. Nurodytas kortelių galiojimo laikotarpis yra vairuotojo kortelių galioji laikotarpis (5 metai).

6. Siekiant sutaupyti vietos, parodyti tik pirmosios kartos Card_MA ir Card_Sign pažymėjimų ir VU_MA ir VU_Sign pažymėjimų galiojimo laikotarpių skirtumai.

9.2. **Simetriniai raktai**

9.2.1 *Transporto priemonės bloko ir judesio jutiklio ryšio apsaugos raktai*

9.2.1.1 *Bendrosios nuostatos*

Pastaba. Šio skirsnio skaitytojai turėtų būti susipažinę su standarto [ISO 16844-3], kuriame aprašoma transporto priemonės bloko ir judesio jutiklio sąsaja, turiniu. Transporto priemonės bloko ir judesio jutiklio siejimas išsamiai aprašytas šio priedėlio 12 skyriuje.

CSM_100 Kaip parodyta 3 lentelėje, transporto priemonės blokams ir judesio jutikliams susieti, transporto priemonės blokų ir judesio jutiklių abipusiam autentiškumo tikrinimui atlikti ir transporto priemonės blokų ir judesio jutiklių tarpusavio ryšiui užšifruoti reikalingi įvairūs simetriniai raktai. Visi šie raktai yra AES raktai, jų ilgis lygus judesio jutiklio pagrindinio rakto ilgiui ir yra susijęs su CSM_50 punkte aprašytos (numatytos) Europos pagrindinės raktų poros, ilgiu.

3 lentelė.

Transporto priemonės bloko ir judesio jutiklio ryšio apsaugos raktai

Raktas	Simbolis	Generuoja	Generavimo metodas	Kur saugoma
Judesio jutiklio pagrindinis raktas, transporto priemonės bloko dalis	$K_{M\text{-}VU}$	ERCA	Atsitiktinis	ERCA, su transporto priemonės blokų pažymėjimų išdavimu susijusios MSCA, transporto priemonės blokų gamintojai, transporto priemonės blokai
Judesio jutiklio pagrindinis raktas, dirbtuvių dalis	$K_{M\text{-}WC}$	ERCA	Atsitiktinis	ERCA, MSCA, kortelių gamintojai, dirbtuvių kortelės

▼B

Raktas	Simbolis	Generuoja	Generavimo metodas	Kur saugoma
Judesio jutiklio pagrindinis raktas	K_M	Generuojamas neautonomiškai	Apskaičiuojama pagal formulę: $K_M = K_{M\text{-}VU}$ XOR $K_{M\text{-}WC}$	ERCA, su judesio jutiklių pažymėjimų išdavimu susijusios MSCA (neprivaloma) (*)
Identifikavimo raktas	K_{ID}	Generuojamas neautonomiškai	Apskaičiuojama pagal formulę: $K_{ID} = K_M$ XOR CV; CV turi būti tokia, kaip nurodyta CSM_106 punkte	ERCA, su judesio jutiklių pažymėjimų išdavimu susijusios MSCA (neprivaloma) (*)
Siejimo raktas	K_P	Judesio jutiklio gamintojas	Atsitiktinis	Vienas judesio jutiklis
Seanso raktas	K_S	Transporto priemonės blokas (siejant transporto priemonės bloką ir judesio jutiklį)	Atsitiktinis	Vienas transporto priemonės blokas ir vienas judesio jutiklis

(*) K_M ir K_{ID} saugoti neprivaloma, nes šiuos raktus galima apskaičiuoti remiantis $K_{M\text{-}VU}$, $K_{M\text{-}WC}$ ir CV.

CSM_101 Europos vyriausioji pažymėjimų įstaiga sugeneruoja $K_{M\text{-}VU}$ ir $K_{M\text{-}WC}$ – du atsitiktinius unikalius AES raktus, kuriais remiantis pagal formulę $K_{M\text{-}VU}$ XOR $K_{M\text{-}WC}$ galima apskaičiuoti judesio jutiklio pagrindinį raktą K_M. Valstybių narių pažymėjimų įstaigų prašymu ERCA joms perduoda raktus K_M, $K_{M\text{-}VU}$ ir $K_{M\text{-}WC}$.

CSM_102 Kiekvienam judesio jutiklio pagrindiniam raktui K_M ERCA priskiria unikalų versijos numerį, kuris taip pat taikomas jį sudarantiems raktams $K_{M\text{-}VU}$ ir $K_{M\text{-}WC}$ ir susijusiam identifikavimo raktui K_{ID}. ERCA nurodo versijos numerį valstybių narių pažymėjimų įstaigoms, kai joms perduoda $K_{M\text{-}VU}$ ir $K_{M\text{-}WC}$.

Pastaba. Versijos numeris naudojamas įvairioms šių raktų kartoms atskirti, kaip išsamiai paaiškinta 9.2.1.2 skirsnyje.

CSM_103 Gamintojų prašymu valstybės narės pažymėjimų įstaiga jiems perduoda raktą $K_{M\text{-}VU,,}$ nurodydama jo versijos numerį. Transporto priemonės blokų gamintojai įdiegia raktą $K_{M\text{-}VU}$ ir jo versijos numerį į visus gaminamus transporto priemonės blokus.

CSM_104 Valstybės narės pažymėjimų įstaiga užtikrina, kad raktas $K_{M\text{-}WC}$ ir jo versijos numeris būtų įdiegti į kiekvieną jos atsakomybe išduodamą dirbtuvių kortelę.

Pastabos

— Žr. 2 priedėlyje pateiktą duomenų tipo `SensorInstallationSecData` aprašymą.

— Kaip paaiškinta 9.2.1.2 skirsnyje, į vieną dirbtuvių kortelę iš tikrųjų gali būti įdiegti kelių kartų $K_{M\text{-}WC}$.

▼B

CSM_105 Be CSM_104 punkte nurodyto AES rakto, MSCA užtikrina, kad į kiekvieną jos atsakomybe išduodamą dirbtuvių kortelę būtų įdiegtas šio priedėlio A dalies CSM_037 reikalavime nurodytas TDES raktas Km_{WC}.

Pastabos

— Taip suteikiama galimybė antrosios kartos dirbtuvių kortelę naudoti pirmosios kartos transporto priemonės blokui sujungti.

— Antrosios kartos dirbtuvių kortelėje bus įdiegtos dvi skirtingos taikomosios programos – viena, atitinkanti šio priedėlio B dalies reikalavimus, ir kita, atitinkanti A dalies reikalavimus. Pastarojoje programoje bus įdiegtas TDES raktas Km_{WC}.

CSM_106 MSCA, susijusi su judesio jutiklių išdavimu, identifikavimo raktą apskaičiuoja remdamasi judesio jutiklio pagrindiniu raktu – atlikdama XOR operaciją su pastoviuoju vektoriumi CV. CV vertė turi būti tokia:

— jei tai 128 bitų judesio jutiklio pagrindinis raktas: CV = ‘B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5E 83’

— jei tai 192 bitų judesio jutiklio pagrindinis raktas: CV = ‘72 AD EA FA 00 BB F4 EE F4 99 15 70 5B 7E EE BB 1C 54 ED 46 8B 0E F8 25’

— jei tai 256 bitų judesio jutiklio pagrindinis raktas: CV = ‘1D 74 DB F0 34 C7 37 2F 65 55 DE D5 DC D1 9A C3 23 D6 A6 25 64 CD BE 2D 42 0D 85 D2 32 63 AD 60’

Pastaba. Šie pastovieji vektoriai sugeneruoti taip:

Pi_10 =matematinės konstantos π trupmeninės dalies pirmieji 10 baitų = ‘24 3F 6A 88 85 A3 08 D3 13 19’

CV_128-bits = SHA-256(Pi_10) pirmieji 16 baitų

CV_192-bits = SHA-384(Pi_10) pirmieji 24 baitai

CV_256-bits = SHA-512(Pi_10) pirmieji 32 baitai

CSM_107 Judesio jutiklių gamintojai kiekvienam judesio jutikliui sugeneruoja atsitiktinį unikalų siejimo raktą K_P ir kiekvieną siejimo raktą perduoda valstybės narės pažymėjimų įstaigai. MSCA kiekvieną siejimo raktą atskirai užšifruoja naudodama judesio jutiklio pagrindinį raktą K_M ir šį užšifruotą raktą pateikia judesio jutiklio gamintojui. MSCA judesio jutiklio gamintojui praneša su kiekvienu užšifruotu raktu susijusio K_M versijos numerį.

Pastaba. Kaip paaiškinta 9.2.1.2 skirsnyje, judesio jutiklio gamintojui iš tikrųjų gali reikėti vienam judesio jutikliui sugeneruoti daug unikalių siejimo raktų.

▼B

CSM_108 Judesio jutiklių gamintojai kiekvienam judesio jutikliui sugeneruoja unikalų serijos numerį ir visus serijos numerius perduoda valstybės narės pažymėjimų įstaigai. MSCA kiekvieną serijos numerį atskirai užšifruoja naudodama identifikavimo raktą K_{ID} ir šį užšifruotą serijos numerį pateikia judesio jutiklio gamintojui. MSCA judesio jutiklio gamintojui praneša su kiekvienu užšifruotu serijos numeriu susijusio K_{ID} versijos numerį.

CSM_109 Vykdydama CSM_107 ir CSM_108 reikalavimus, MSCA nuosekliojo blokinio šifravimo režimu taiko AES algoritmą, kaip apibrėžta standarte [ISO 10116], naudodama kaitaliojimo parametrą m = 1 ir inicializacijos vektorių SV = ‘00’ {16}, t. y. 16 baitų, kurių dvejetainė vertė lygi 0. Prireikus MSCA taiko standarte [ISO 9797-1] nustatytą 2 užpildymo metodą.

CSM_110 Judesio jutiklio gamintojas užšifruotą siejimo raktą ir užšifruotą serijos numerį išsaugo judesio jutiklyje, kuriam jie yra skirti, kartu su atitinkamomis šifravimo tikslais naudotų raktų K_M ir K_{ID} grynojo teksto vertėmis ir versijos numeriais.

Pastaba. Kaip paaiškinta 9.2.1.2 skirsnyje, judesio jutiklio gamintojui iš tikrųjų gali reikėti į vieną judesio jutiklį įdiegti daug užšifruotų siejimo raktų ir daug užšifruotų serijos numerių.

CSM_111 Be CSM_110 punkte nurodytos AES pagrįstos kriptografinės informacijos, judesio jutiklio gamintojas kiekviename judesio jutiklyje taip pat gali išsaugoti TDES algoritmu pagrįstą kriptografinę informaciją, nurodytą šio priedėlio A dalies CSM_037 reikalavime.

Pastaba. Tai padarius antrosios kartos judesio jutiklį bus galima sujungti su pirmosios kartos transporto priemonės bloku.

CSM_112 Siejant su judesio jutikliu transporto priemonės bloko sugeneruoto seanso rakto K_S ilgis turi būti susietas su jo $K_{M\text{-}VU}$ ilgiu, kaip aprašyta CSM_50.

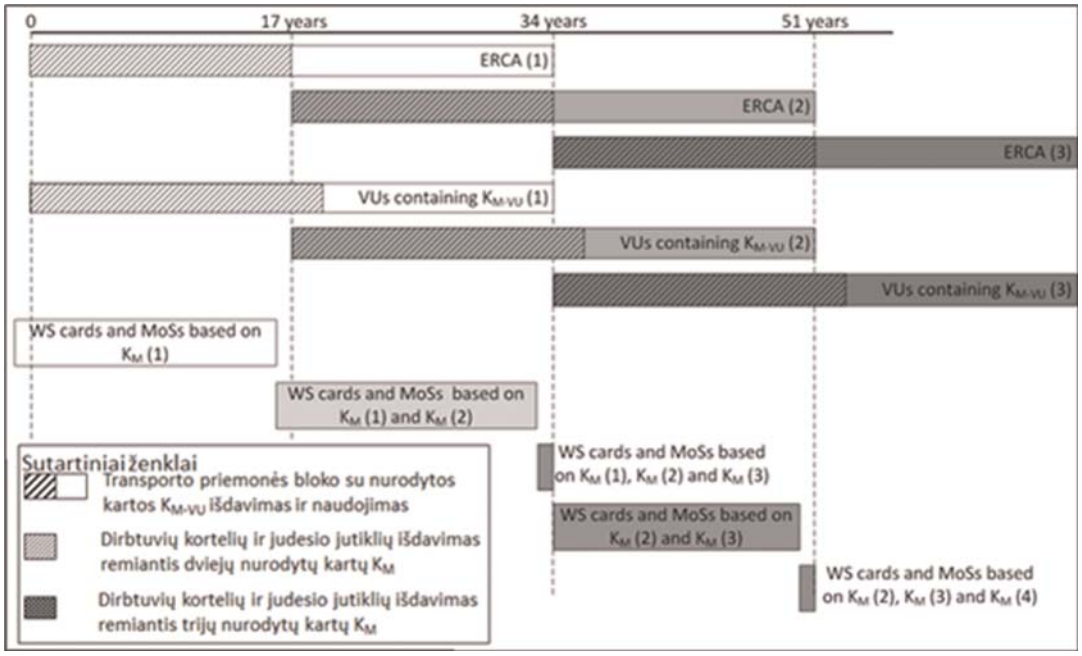
9.2.1.2 *Judesio jutiklio pagrindinio rakto keitimas antrosios kartos įrangoje*

CSM_113 Kiekvienas judesio jutiklio pagrindinis raktas ir visi susiję raktai (žr. 3 lentelę) yra susieti su tam tikra ERCA pagrindinės raktų poros karta. Todėl kas 17 metų šie raktai turi būti keičiami. Kiekvienos kartos judesio jutiklio pagrindinio rakto galiojimo laikotarpis prasideda likus vieniems metams iki susijusios ERCA pagrindinės raktų poros įsigaliojimo ir pasibaigia, kai baigia galioti susijusi ERCA pagrindinė raktų pora. Tai parodyta 2 paveiksle.

▼B

2 pav.

Įvairių kartų judesio jutiklių pagrindinių raktų išdavimas ir naudojimas transporto priemonės blokuose, judesio jutikliuose ir dirbtuvių kortelėse



CSM_114 Likus ne mažiau kaip vieniems metams iki naujos Europos pagrindinės raktų poros sugeneravimo, kaip aprašyta CSM_56 punkte, ERCA, sugeneruodama naujus K_{M-VU} ir K_{M-WC}, sugeneruoja naują judesio jutiklio pagrindinį raktą K_M. Judesio jutiklio pagrindinio rakto ilgis turi būti susietas su numatomu naujos Europos pagrindinės raktų poros stiprumu, kaip nustatyta CSM_50 punkte. MSCA prašymu ERCA joms perduoda raktus K_M, K_{M-VU} ir K_{M-WC}, nurodydama jų versijos numerius.

CSM_115 MSCA užtikrina, kad kiekvienoje jos įgaliojimu išduotoje dirbtuvių kortelėje būtų saugomi visų galiojančių kartų K_{M-WC} ir jų versijos numeriai, kaip parodyta 2 paveiksle.

Pastaba. Tai reiškia, kad paskutiniaisiais ERCA pažymėjimo galiojimo metais dirbtuvių kortelės bus išduodamos su trijų skirtingų kartų K_{M-WC}, kaip parodyta 2 paveiksle.

CSM_116 Su CSM_107 ir CSM_108 punktuose aprašytu procesu susiję reikalavimai: kiekvieną iš judesio jutiklio gamintojo gautą siejimo raktą K_P MSCA atskirai užšifruoja naudodama kiekvienos galiojančios kartos judesio jutiklio pagrindinį raktą K_M. Be to, kiekvieną iš judesio jutiklio gamintojo gautą serijos numerį MSCA atskirai užšifruoja naudodama kiekvieną galiojančios kartos identifikavimo raktą K_{ID}. Judesio jutiklio gamintojas visus užšifruotus siejimo raktus ir visus užšifruotus serijos numerius išsaugo judesio jutiklyje, kuriam jie yra skirti, kartu su atitinkamomis šifravimo tikslais naudotų raktų K_M ir K_{ID} grynojo teksto vertėmis ir versijos numeriu (-iais).

▼B

Pastaba. Tai reiškia, kad paskutiniaisiais ERCA pažymėjimo galiojimo metais judesio jutikliai bus išduodami su užšifruotais duomenimis, pagrįstais trijų skirtingų kartų K_M, kaip parodyta 2 paveiksle.

CSM_117 Su CSM_107 punkte aprašytu procesu susiję reikalavimai: kadangi siejimo rakto K_P ilgis susiejamas su K_M ilgiu (žr. CSM_100 punktą), judesio jutiklio gamintojui gali reikėti vienam judesio jutikliui sugeneruoti tris skirtingus siejimo raktus (skirtingo ilgio), jei vėlesnių kartų K_M būtų kitokio ilgio. Tokiu atveju kiekvieną siejimo raktą gamintojas perduoda MSCA. MSCA užtikrina, kad kiekvienas siejimo raktas būtų užšifruotas naudojant tinkamos kartos judesio jutiklio pagrindinį raktą, t. y. tokio pat ilgio raktą.

Pastaba. Jei judesio jutiklio gamintojas nusprendžia antrosios kartos judesio jutikliui sugeneruoti TDES algoritmu pagrįstą siejimo raktą (žr. CSM_111 punktą), gamintojas MSCA nurodo, kad šiam siejimo raktui užšifruoti turi būti naudojamas TDES algoritmu pagrįstas judesio jutiklio pagrindinis raktas. Taip daroma dėl to, kad TDES rakto ilgis gali atitikti AES rakto ilgį, todėl MSCA negalės to suprasti tik iš rakto ilgio.

CSM_118 Transporto priemonės blokų gamintojai į kiekvieną transporto priemonės bloką įdiegia tik vienos kartos $K_{M\text{-}VU}$, nurodydami jo versijos numerį. Šios kartos $K_{M\text{-}VU}$ susiejamas su ERCA pažymėjimu, kuriuo remiantis išduoti transporto priemonės bloko pažymėjimai.

Pastabos

— *X* kartos ERCA pažymėjimu pagrįstame transporto priemonės bloke įdiegiamas tik *X* kartos $K_{M\text{-}VU}$, net jei jis išduodamas jau prasidėjus *X+1* kartos ERCA pažymėjimo galiojimo laikotarpiui. Tai parodyta 2 paveiksle.

— *X* kartos transporto priemonės blokas negali būti siejamas su *X-1* kartos judesio jutikliu.

— Kadangi dirbtuvių kortelių galiojimo laikotarpis yra vieni metai, atsižvelgiant į CSM_113–CSM_118 punktus, kai bus išduotas pirmasis transporto priemonės blokas su nauju $K_{M\text{-}VU}$, visose dirbtuvių kortelėse bus įdiegtas naujas $K_{M\text{-}WC.}$ Todėl toks transporto priemonės blokas visada galės apskaičiuoti naują K_M. Be to, iki to laiko daugelyje naujų judesio jutiklių jau bus duomenys, užšifruoti remiantis nauju K_M.

9.2.2 *DSRC ryšio apsaugos raktai*

9.2.2.1 *Bendrosios nuostatos*

CSM_119 Iš transporto priemonės bloko kontrolės institucijai DSRC nuotolinio ryšio kanalu perduodamų duomenų autentiškumas ir konfidencialumas užtikrinamas naudojant konkrečiam transporto priemonės blokui skirtų AES raktų, apskaičiuotų remiantis bendru DSRC pagrindiniu raktu KM_{DSRC}, rinkinį.

▼B

CSM_120 DSRC pagrindinis raktas KM_{DSRC} – tai ERCA saugiai sugeneruotas, saugomas ir platinamas AES raktas. Šio rakto ilgis gali būti 128, 192 arba 256 bitai, jis susiejamas su Europos pagrindine raktų pora, kaip aprašyta CSM_50 punkte.

CSM_121 Valstybių narių pažymėjimų įstaigų prašymu ERCA joms saugiai perduoda šį DSRC pagrindinį raktą, kad jos galėtų apskaičiuoti konkrečiam transporto priemonės blokui skirtus DSRC raktus ir užtikrinti, kad DSRC pagrindinis raktas būtų įdiegtas į visas jų atsakomybe išduodamas kontrolės korteles ir dirbtuvių korteles.

CSM_122 Kiekvienam DSRC pagrindiniam raktui ERCA priskiria unikalų versijos numerį. ERCA, valstybių narių pažymėjimų įstaigoms perduodama DSRC pagrindinį raktą, joms nurodo versijos numerį.

Pastaba. Versijos numeris naudojamas įvairioms DSRC pagrindinio rakto kartoms atskirti, kaip išsamiai paaiškinta 9.2.2.2 skirsnyje.

CSM_123 Kiekvienam transporto priemonės blokui jo gamintojas sukuria unikalų serijos numerį ir jį perduoda atitinkamos valstybės narės pažymėjimų įstaigai, prašydamas išduoti dviejų konkrečiam transporto priemonės blokui skirtų DSRC raktų rinkinį. Transporto priemonės bloko serijos numerio duomenų tipas turi būti `VuSerialNumber`, koduojama pagal išskirtines kodavimo taisykles (DER), nustatytas standarte [ISO 8825-1].

CSM_124 Gavusi prašymą išduoti konkrečiam transporto priemonės blokui skirtų DSRC raktų rinkinį, MSCA apskaičiuoja transporto priemonės blokui skirtus du AES raktus – $K_VU_{DSRC}_ENC$ ir $K_VU_{DSRC}_MAC$. Šių konkrečiam transporto priemonės blokui skirtų raktų ilgis turi atitikti DSRC pagrindinio rakto ilgį. MSCA taiko [RFC 5869] nustatytą raktų darybos funkciją. *HMAC-Hash* funkcijai vykdyti reikalinga maišos funkcija turi būti susieta su DSRC pagrindinio rakto ilgiu, kaip aprašyta CSM_50 punkte. [RFC 5869] nustatyta raktų darybos funkcija taikoma taip:

1 etapas (išskyrimas):

— *PRK* = HMAC-Hash (*salt, IKM*), čia: *salt* – tuščia eilutė (‘’), *IKM* – KM_{DSRC}.

2 etapas (išplėtimas):

— *OKM* = *T(1)*, čia:

T(1) = HMAC-Hash (*PRK*, *T(0)* || *info* || ‘01’), kai

▼B

— *T(0)* = tuščia eilutė (‘’),

— *info* = transporto priemonės bloko serijos numeris, nurodytas CSM_123 punkte,

— K_VU_{DSRC}_ENC = pirmieji *OKM L* oktetai,

K_VU_{DSRC}_MAC = paskutinieji *OKM L;*

čia: *L* – privalomas K_VU_{DSRC}_ENC ir K_VU_{DSRC}_MAC ilgis oktetais.

CSM_125 MSCA saugiai perduoda K_VU_{DSRC}_ENC ir K_VU_{DSRC}_MAC transporto priemonės bloko gamintojui, kad šis juos įdiegtų transporto priemonės bloką, kuriam jie yra skirti.

CSM_126 Išduoti K_VU_{DSRC}_ENC ir K_VU_{DSRC}_MAC išsaugomi transporto priemonės bloko saugiojoje atmintinėje, kad būtų galima užtikrinti nuotolinio ryšio kanalu perduotų duomenų nepažeistumą, autentiškumą ir konfidencialumą. Transporto priemonės bloke taip pat turi būti saugomas DSRC pagrindinio rakto, naudoto šiems konkrečiam transporto priemonės blokui skirtiems raktams apskaičiuoti, versijos numeris.

CSM_127 Išduotas KM_{DSRC} turi būti saugomas kontrolės kortelių ir dirbtuvių kortelių saugioje atmintinėje, kad būtų galima patikrinti nuotolinio ryšio kanalu transporto priemonės bloko perduotų duomenų nepažeistumą ir autentiškumą ir šiuos duomenis iššifruoti. Kontrolės kortelėse ir dirbtuvių kortelėse taip pat turi būti saugomas DSRC pagrindinio rakto versijos numeris.

Pastaba. Kaip paaiškinta 9.2.2.2 skirsnyje, į vieną dirbtuvių kortelę arba kontrolės kortelę iš tikrųjų gali būti įdiegti kelių kartų K_{DSRC}.

CSM_128 MSCA tvarko visų jos sugeneruotų konkrečiam transporto priemonės blokui skirtų DSRC raktų, jų versijos numerių ir transporto priemonės bloko, kuriam yra skirtas raktų rinkinys, identifikavimo duomenų registrą.

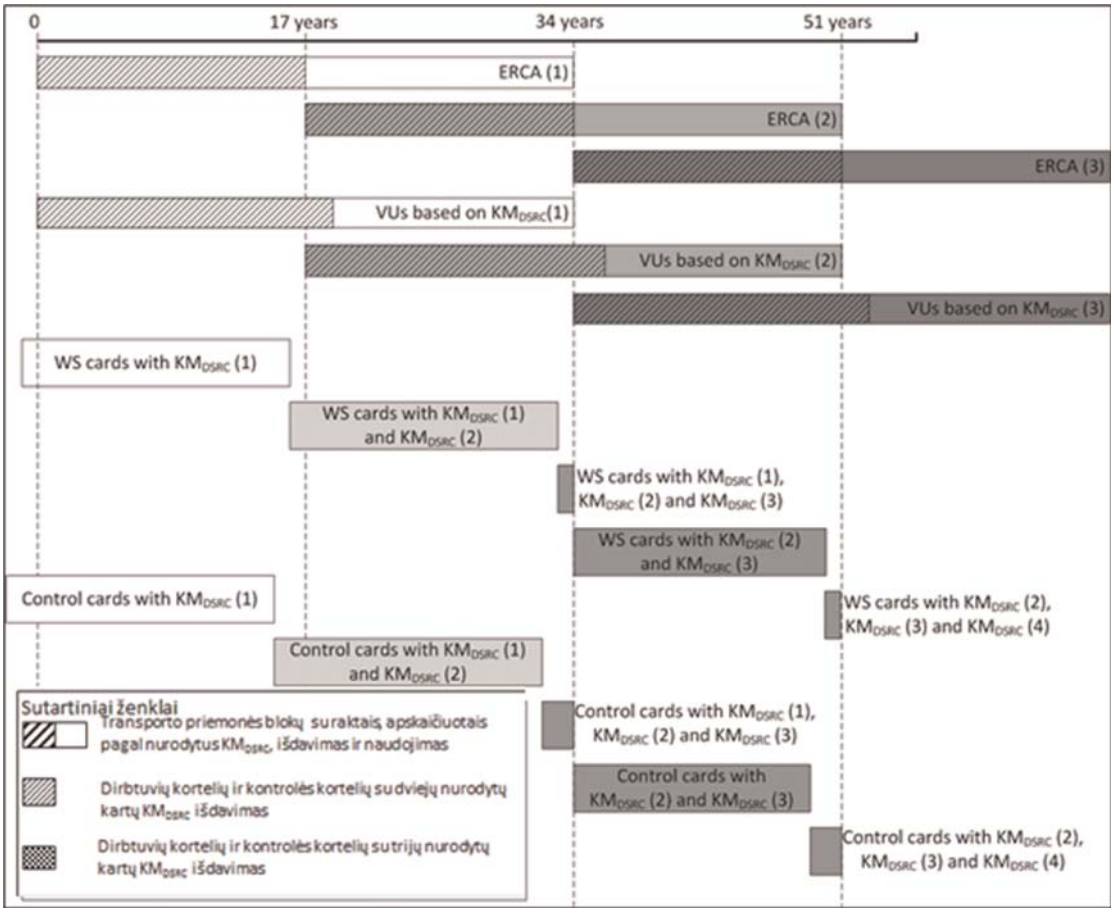
9.2.2.2 *DSRC pagrindinio rakto keitimas*

CSM_129 Kiekvienas DSRC raktas yra susietas su tam tikra ERCA pagrindinės raktų poros karta. Todėl ERCA privalo kas 17 metų pakeisti DSRC pagrindinį raktą. Kiekvienos kartos DSRC pagrindinio rakto galiojimo laikotarpis prasideda likus dvejiems metams iki susijusios ERCA pagrindinės raktų poros įsigaliojimo ir pasibaigia, kai baigia galioti susijusi ERCA pagrindinė raktų pora. Tai parodyta 3 paveiksle.

▼B

3 pav.

Įvairių kartų DSRC pagrindinių raktų išdavimas ir naudojimas transporto priemonės blokuose, dirbtuvių kortelėse ir kontrolės kortelėse



CSM_130 Likus ne mažiau kaip dvejiems metams iki naujos Europos pagrindinės raktų poros sugeneravimo, kaip aprašyta CSM_56, ERCA sugeneruoja naują DSRC pagrindinį raktą. DSRC rakto ilgis turi būti susietas su numatomu naujos Europos pagrindinės raktų poros stiprumu, kaip nustatyta CSM_50 punkte. MSCA prašymu ERCA joms perduoda naują DSRC pagrindinį raktą, nurodydama jo versijos numerį.

CSM_131 MSCA užtikrina, kad kiekvienoje jos įgaliojimu išduodamoje kontrolės kortelėje būtų išsaugoti visų galiojančių kartų KM_{DSRC} ir jų versijos numeriai, kaip parodyta 3 paveiksle.

Pastaba. Tai reiškia, kad paskutiniuosius dvejus ERCA pažymėjimo galiojimo metus kontrolės kortelės bus išduodamos su trijų skirtingų kartų KM_{DSRC}, kaip parodyta 3 paveiksle.

CSM_132 MSCA užtikrina, kad visų kartų KM_{DSRC}, kurie galiojo ne trumpiau kaip vienus metus ir vis dar galioja, būtų įdiegti į kiekvieną jos įgaliojimu išduodamą dirbtuvių kortelę, taip pat nurodant jų versijos numerius, kaip parodyta 3 paveiksle.

▼B

Pastaba. Tai reiškia, kad paskutiniaisiais ERCA pažymėjimo galiojimo metais dirbtuvių kortelės bus išduodamos su trijų skirtingų kartų KM_{DSRC}, kaip parodyta 3 paveiksle.

CSM_133 Transporto priemonės blokų gamintojai į kiekvieną transporto priemonės bloką įdiegia tik vieną konkrečiam transporto priemonės blokui skirtų DSRC raktų rinkinį, nurodydami jo versijos numerį. Raktų rinkinys apskaičiuojamas remiantis tos kartos KM_{DSRC}, kuri yra susieta su ERCA pažymėjimu, kuriuo remiantis išduoti transporto priemonės bloko pažymėjimai.

Pastabos

— Tai reiškia, kad *X* kartos ERCA pažymėjimu pagrįstame transporto priemonės bloke įdiegiamas tik *X* kartos K_VU_{DSRC} ir K_VU_{DSRC}_MAC, net jei transporto priemonės blokas išduodamas jau prasidėjus *X+1* kartos ERCA pažymėjimo galiojimo laikotarpiui. Tai parodyta 3 paveiksle.

— Kadangi dirbtuvių kortelių galiojimo laikotarpis yra vieni metai, o kontrolės kortelių – dveji metai, atsižvelgiant į CSM_131–CSM_133 punktus, kai bus išduotas pirmasis transporto priemonės blokas su šiuo pagrindiniu raktu pagrįstais konkrečiam transporto priemonės blokui skirtais raktais, visose dirbtuvių kortelėse ir kontrolės kortelėse bus įdiegtas naujas DSRC pagrindinis raktas.

9.3. **Pažymėjimai**

9.3.1 *Bendrosios nuostatos*

CSM_134 Visi Europos išmaniojo tachografo sistemoje naudojami pažymėjimai turi būti autonominio aprašo, kortele patikrinami (CV) pažymėjimai, atitinkantys standartus [ISO 7816-4] ir [ISO 7816-8].

CSM_135 Pažymėjimų ASN.1 duomenų struktūroms ir (konkrečioms taikomosioms programoms skirtiems) duomenų objektams koduoti taikomos išskirtinės kodavimo taisyklės (DER), nustatytos standartu [ISO 8825-1].

Pastaba. Atlikus tokį kodavimą gaunama toliau nurodytos struktūros žymenos ilgio vertė (TLV).

Žymena: žymena užkoduojama vienu arba dviem oktetais, ja nurodomas turinys.

Ilgis: ilgis užkoduojamas vienu, dviem arba trim oktetais kaip nepasirašytas sveikasis skaičius, jo didžiausias galimas ilgis – 65 535 oktetai. Naudojama kuo mažiau oktetų.

Vertė: vertė užkoduojama nuliu arba daugiau oktetų.

9.3.2 *Pažymėjimo turinys*

CSM_136 Visų pažymėjimų struktūra turi būti tokia, kaip nurodyta 4 lentelėje pateiktame pažymėjimo profilyje.

4 lentelė.

1 versijos pažymėjimo profilis

Laukas	Lauko identifikatorius	Žymena	Ilgis (baitais)	ASN.1 duomenų tipas (žr. 1 priedėlį)
ECC pažymėjimas	C	‘7F 21’	Kintamas	
ECC pažymėjimo pagrindinė dalis	B	‘7F 4E’	Kintamas	

▼B

Laukas	Lauko identifikatorius	Žymena	Ilgis (baitais)	ASN.1 duomenų tipas (žr. 1 priedėlį)
Pažymėjimo profilio identifikatorius	CPI	‘5F 29’	‘01’	`INTEGER(0..255)`
Pažymėjimų įstaigos žymuo	CAR	‘42’	‘08’	`KeyIdentifier`
Pažymėjimo turėtojo įgaliojimas	CHA	‘5F 4C’	‘07’	`CertificateHolder Authorisation`
Viešasis raktas	PK	‘7F 49’	Kintamas	
Domeno parametrai	DP	‘06’	Kintamas	`OBJECT IDENTIFIER`
Viešasis taškas	PP	‘86’	Kintamas	`OCTET STRING`
Pažymėjimo turėtojo žymuo	CHR	‘5F 20’	‘08’	`KeyIdentifier`
Pažymėjimo įsigaliojimo data	CEfD	‘5F 25’	‘04’	`TimeReal`
Pažymėjimo galiojimo pabaigos data	CExD	‘5F 24’	‘04’	`TimeReal`
ECC pažymėjimo parašas	S	‘5F 37’	Kintamas	`OCTET STRING`

Pastaba. Lauko identifikatorius tolesniuose šio priedėlio skirsniuose bus naudojamas atskiriems pažymėjimo laukams nurodyti, pvz., X.CAR yra naudotojo X pažymėjime nurodytos pažymėjimų įstaigos žymuo.

9.3.2.1 Pažymėjimo profilio identifikatorius

CSM_137 Pažymėjimo profilio identifikatorius naudojamas pažymėjime naudotam pažymėjimo profiliui nurodyti. 4 lentelėje nurodyta 1 versija žymima verte ‘00’.

9.3.2.2 Pažymėjimų įstaigos žymuo

CSM_138 Pažymėjimų įstaigos žymuo naudojamas viešajam raktui, skirtam pažymėjimo parašui patikrinti, identifikuoti. Taigi pažymėjimų įstaigos žymuo atitinka atitinkamos pažymėjimų įstaigos pažymėjime nurodytą pažymėjimo turėtojo žymenį.

CSM_139 ERCA pagrindinį pažymėjimą pasirašo pati ERCA, t. y. pažymėjimų įstaigos žymuo ir pažymėjimo turėtojo žymuo yra vienodi.

▼B

CSM_140 ERCA sąsajos pažymėjime nurodomas pažymėjimo turėtojo žymuo atitinka naujojo ERCA pagrindinio pažymėjimo CHR. Sąsajos pažymėjimui skirtas pažymėjimo turėtojo žymuo atitinka ankstesnio ERCA pagrindinio pažymėjimo CHR.

9.3.2.3 Pažymėjimo turėtojo įgaliojimas

CSM_141 Pažymėjimo turėtojo įgaliojimas naudojamas pažymėjimo rūšiai identifikuoti. Jis sudaromas iš šešių svarbiausiųjų tachografo taikomosios programos identifikatoriaus baitų, susietų su įrangos, kuriai skirtas pažymėjimas, tipu.

9.3.2.4 Viešasis raktas

Į viešąjį raktą įeina du duomenų elementai: su viešuoju raktu pažymėjime naudotini standartiniai domeno parametrai ir viešojo taško vertė.

CSM_142 Domeno parametrų duomenų elementas sudaromas iš 1 lentelėje nurodytų objekto identifikatorių, kuriais nurodomas standartinių domeno parametrų rinkinys.

CSM_143 Viešojo taško duomenų elementas sudaromas iš viešojo taško. Elipsinės kreivės viešieji taškai konvertuojami į oktetų eilutes, kaip nustatyta [TR-03111]. Naudojamas neglaudintas kodavimo formatas. Iš užkoduoto formato atkuriant elipsinės kreivės tašką, visada atliekami [TR-03111] aprašyti tikrinimai.

9.3.2.5 Pažymėjimo turėtojo žymuo

CSM_144 Pažymėjimo turėtojo žymuo yra pažymėjime nurodytas viešojo rakto identifikatorius. Jis naudojamas šiam viešajam raktui nurodyti kituose pažymėjimuose.

CSM_145 Kortelių pažymėjimuose ir išorinių GNSS įrenginių pažymėjimuose nurodomo pažymėjimo turėtojo žymens duomenys turi būti 1 priedėlyje nurodyto `ExtendedSerialNumber` duomenų tipo.

CSM_146 Dėl transporto priemonės blokų reikia pasakyti, kad gamintojas, prašydamas pažymėjimo, gali žinoti gamintojo suteikiamą transporto priemonės bloko, kuriam skirtas tas pažymėjimas ir susijęs privatusis raktas, serijos numerį arba jo nežinoti. Pirmuoju atveju pažymėjimo turėtojo žymens duomenys turi būti 1 priedėlyje nurodyto `ExtendedSerialNumber` duomenų tipo. Antruoju atveju pažymėjimo turėtojo žymens duomenys turi būti 1 priedėlyje nurodyto `CertificateRequestID` duomenų tipo.

CSM_147 ERCA ir MSCA pažymėjimuose nurodomo pažymėjimo turėtojo žymens duomenys turi būti 1 priedėlyje nurodyto `CertificationAuthorityKID` duomenų tipo.

▼B

9.3.2.6 Pažymėjimo įsigaliojimo data

CSM_148 Pažymėjimo įsigaliojimo data – data ir laikas, kai prasideda pažymėjimo galiojimo laikotarpis. Pažymėjimo įsigaliojimo data turi būti pažymėjimo sugeneravimo data.

9.3.2.7 Pažymėjimo galiojimo pabaigos data

CSM_149 Pažymėjimo galiojimo pabaigos data – data ir laikas, kai baigiasi pažymėjimo galiojimo laikotarpis.

9.3.2.8 Pažymėjimo parašas

CSM_150 Pažymėjimo parašas sukuriamas pažymėjimo pagrindinei daliai, įskaitant pažymėjimo pagrindinės dalies žymeną ir ilgį. Parašas kuriamas pagal ECDSA algoritmą, kaip nurodyta [DSS], taikant maišos algoritmą, susietą su pasirašančiosios institucijos rakto dydžiu, nurodytu CSM_50 punkte. Parašo formatas turi būti paprastas, kaip nurodyta [TR-03111].

9.3.3 *Pažymėjimų prašymas*

CSM_151 Prašydamas pažymėjimo, prašytojas savo pažymėjimų įstaigai perduoda tokius duomenis:

— prašomo pažymėjimo profilio identifikatorių;

— pažymėjimų įstaigos žymenį, kurį numatoma naudoti pasirašant pažymėjimą;

— pasirašytiną viešąjį raktą.

CSM_152 Be CSM_151 punkte nurodytų duomenų, MSCA, prašydama ERCA išduoti pažymėjimą, perduoda tokius duomenis, suteikiančius ERCA galimybę naujame MSCA pažymėjime sukurti pažymėjimo turėtojo žymenį:

— pažymėjimų įstaigos skaitinį valstybės kodą (1 priedėlyje nurodytas duomenų tipas `NationNumeric`);

— pažymėjimų įstaigos raidinį skaitinį valstybės kodą (1 priedėlyje nurodytas duomenų tipas `NationAlpha`);

— vieno baito serijos numerį įvairiems pažymėjimų įstaigos raktams atskirti, jei jie būtų keičiami;

— dviejų baitų lauką su papildoma informacija apie pažymėjimų įstaigą.

CSM_153 Be CSM_151 punkte nurodytų duomenų, įrangos gamintojas, prašydamas MSCA išduoti pažymėjimą, perduoda tokius duomenis, suteikiančius MSCA galimybę naujame įrangos pažymėjime sukurti pažymėjimo turėtojo žymenį:

— gamintojo suteiktą įrangos tipo identifikatorių;

— jei žinoma (žr. CSM_154 punktą), įrangos serijos numerį, skirtingą kiekvienam gamintojui, įrangos tipui ir gamybos mėnesiui. Jei ne, unikalų pažymėjimo prašymo identifikatorių;

▼B

— įrangos pagaminimo arba pažymėjimo prašymo metus ir mėnesį.

Gamintojas užtikrina, kad šie duomenys būtų teisingi ir kad MSCA pateiktas pažymėjimas būtų įdiegtas į įrangą, kuriai jis yra skirtas.

CSM_154 Dėl transporto priemonės blokų reikia pasakyti, kad gamintojas, prašydamas pažymėjimo, gali žinoti gamintojo suteikiamą transporto priemonės bloko, kuriam yra skirtas tas pažymėjimas ir susijęs privatusis raktas, serijos numerį arba jo nežinoti. Jeigu serijos numeris yra žinomas, transporto priemonės bloko gamintojas jį perduoda MSCA. Jei ne, gamintojas unikaliai identifikuoja kiekvieną pažymėjimo prašymą ir šį pažymėjimo prašymo serijos numerį perduoda MSCA. Tokiu atveju atitinkamame pažymėjime bus nurodytas pažymėjimo prašymo serijos numeris. Įdiegęs pažymėjimą į konkretų transporto priemonės bloką, gamintojas MSCA informuoja apie pažymėjimo prašymo numerio sąryšį su transporto priemonės bloko identifikavimo duomenimis.

10. TRANSPORTO PRIEMONĖS BLOKO IR KORTELĖS ABIPUSIS AUTENTIŠKUMO TIKRINIMAS IR SAUGUSIS KEITIMASIS PRANEŠIMAIS

10.1. **Bendrosios nuostatos**

CSM_155 Aukšto lygio saugus transporto priemonės bloko ir tachografo kortelės ryšys užtikrinimas tokiais etapais:

— pirma, kiekviena šalis kitai šaliai įrodo turinti valstybės narės pažymėjimų įstaigos pasirašytą galiojantį viešojo rakto pažymėjimą. MSCA viešojo rakto pažymėjimas savo ruožtu turi būti pasirašytas Europos vyriausiosios pažymėjimų įstaigos. Šis etapas vadinamas pažymėjimų sekos tikrinimu ir yra išsamiai aprašytas 10.2 skirsnyje;

— antra, transporto priemonės blokas kortelei turi įrodyti turįs privatųjį raktą, atitinkantį pateiktame pažymėjime esantį viešąjį raktą. Jis tai padaro pasirašydamas kortelės siunčiamą atsitiktinį skaičių. Kortelė patikrina šio atsitiktinio skaičiaus parašą. Jei patikrinimas sėkmingas, patvirtinamas transporto priemonės bloko autentiškumas. Šis etapas vadinamas transporto priemonės bloko autentiškumo tikrinimu ir yra išsamiai aprašytas 10.3 skirsnyje;

— trečia, abi šalys, taikydamos asimetrinį raktų derinimo algoritmą, savarankiškai apskaičiuoja du AES seanso raktus. Naudodama vieną iš šių raktų, kortelė sukuria pranešimo atpažinimo kodą (MAC), susijusį su kokiais nors transporto priemonės bloko siunčiamais duomenimis. Transporto priemonės blokas patikrina šį MAC. Jei patikrinimas sėkmingas, patvirtinamas kortelės autentiškumas. Šis etapas vadinamas kortelės autentiškumo tikrinimu ir yra išsamiai aprašytas 10.4 skirsnyje;

— ketvirta, transporto priemonės blokas ir kortelė naudoja suderintus seanso raktus visų pranešimų, kuriais keičiamasi, konfidencialumui, vientisumui ir autentiškumui užtikrinti. Šis etapas vadinamas saugiuoju keitimusi pranešimais ir išsamiai aprašytas 10.5 skirsnyje.

CSM_156 CSM_155 punkte aprašytą mechanizmą transporto priemonės blokas pradeda taikyti kaskart, kai į kurį nors kortelės lizdą įstatoma kortelė.

▼B

10.2. **Abipusis pažymėjimų sekos tikrinimas**

10.2.1 *Transporto priemonės bloko atliekamas kortelės pažymėjimų sekos tikrinimas*

CSM_157 Transporto priemonės blokuose taikomas 4 paveiksle pavaizduotas tachografo kortelės pažymėjimų sekos tikrinimo protokolas.

Pastabos dėl 4 paveikslo

— Paveiksle nurodyti kortelės pažymėjimai ir viešieji raktai yra skirti abipusiam autentiškumo tikrinimui. 9.1.5 skirsnyje jie žymimi Card_MA.

— Paveiksle nurodyti Card.CA pažymėjimai ir viešieji raktai naudojami kortelės pažymėjimams pasirašyti, jie nurodomi kortelės pažymėjimo CAR. 9.1.3 skirsnyje jie žymimi MSCA_Card.

— Paveiksle nurodytas Card.CA.EUR pažymėjimas yra Card.CA pažymėjimo CAR nurodytas Europos pagrindinis pažymėjimas.

— Paveiksle nurodytas Card.Link pažymėjimas yra kortelės sąsajos pažymėjimas, jei toks yra. Kaip nurodyta 9.1.2 skirsnyje, tai sąsajos pažymėjimas, skirtas ERCA sukurtai ir naudojant ankstesnį Europos privatųjį raktą pasirašytai naujai Europos pagrindinei raktų porai.

— Card.Link.EUR pažymėjimas yra Card.Link pažymėjimo CAR nurodytas Europos pagrindinis pažymėjimas.

CSM_158 Kaip parodyta 4 paveiksle, kortelės pažymėjimų sekos tikrinimas pradedamas įdėjus kortelę. Transporto priemonės blokas nuskaito EF ICC esantį kortelės turėtojo žymenį (`cardExtendedSerialNumber`). Transporto priemonės blokas patikrina, ar kortelė jam yra žinoma, t. y. ar jis anksčiau jau yra sėkmingai patikrinęs šią kortelės pažymėjimų seką ir ją išsaugojęs būsimiems patikrinimams. Jei kortelė yra žinoma ir kortelės pažymėjimas tebegalioja, procesas tęsiamas – atliekamas transporto priemonės bloko pažymėjimų sekos tikrinimas. Jei kortelė nėra žinoma, transporto priemonės blokas paeiliui nuskaito kortelėje esantį MSCA_Card pažymėjimą, skirtą kortelės pažymėjimui patikrinti, Card.CA.EUR pažymėjimą, skirtą MSCA_Card pažymėjimui patikrinti, ir galbūt sąsajos pažymėjimą, kol randa pažymėjimą, kuris jam yra žinomas arba kurį jis gali patikrinti. Jei toks pažymėjimas randamas, transporto priemonės blokas, remdamasis šiuo pažymėjimu, patikrina pirminius kortelės pažymėjimus, kuriuos nuskaitė iš kortelės. Jei patikrinimas sėkmingas, procesas tęsiamas – atliekamas transporto priemonės bloko pažymėjimų sekos patikrinimas. Jei ne, transporto priemonės blokas atmeta kortelę.

▼B

Pastaba. Card.CA.EUR pažymėjimą transporto priemonės blokas gali atpažinti trim būdais:

— Card.CA.EUR pažymėjimas yra toks pats pažymėjimas, kaip ir paties transporto priemonės bloko EUR pažymėjimas;

— Card.CA.EUR pažymėjimas yra ankstesnis už paties transporto priemonės bloko EUR pažymėjimą, jis buvo įdiegtas į transporto priemonės bloką, kai šis buvo išduodamas (žr. CSM_81 punktą);

— Card.CA.EUR pažymėjimas yra vėlesnis už paties transporto priemonės bloko EUR pažymėjimą, transporto priemonės blokas iš kitos tachografo kortelės jau yra gavęs sąsajos pažymėjimą, jį patikrinęs ir išsaugojęs būsimiems patikrinimams.

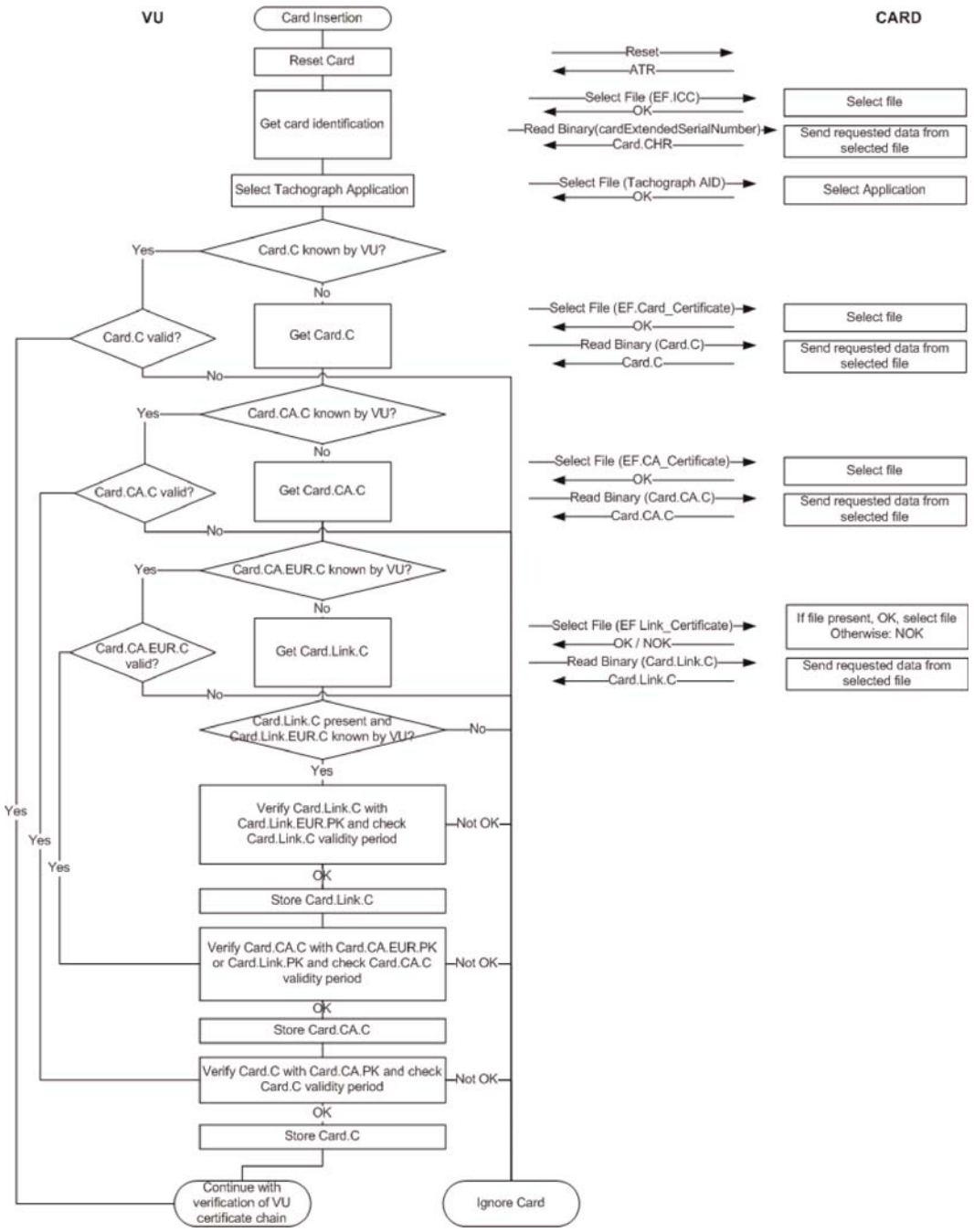
CSM_159 Kaip nurodyta 4 paveiksle, transporto priemonės blokas, patikrinęs dar nežinomo pažymėjimo autentiškumą ir galiojimą, gali jį išsaugoti būsimiems patikrinimams, kad to pažymėjimo autentiškumo nereikėtų dar kartą tikrinti, kai jis vėl bus pateiktas transporto priemonės blokui. Transporto priemonės blokas gali išsaugoti ne visą pažymėjimą, o tik pagrindinės pažymėjimo dalies turinį, kaip nurodyta 9.3.2 skirsnyje.

CSM_160 Transporto priemonės blokas patikrina iš kortelės nuskaitytų arba jo atmintyje saugomų pažymėjimų galiojimo laiką ir atmeta pažymėjimus, kurių galiojimo laikas baigėsi. Kortelės pateikto pažymėjimo galiojimo laikui tikrinti transporto priemonės blokas naudoja savo vidinį laikrodį.

▼B

4 pav.

Transporto priemonės bloko atliekamo kortelės pažymėjimų sekos tikrinimo protokolas



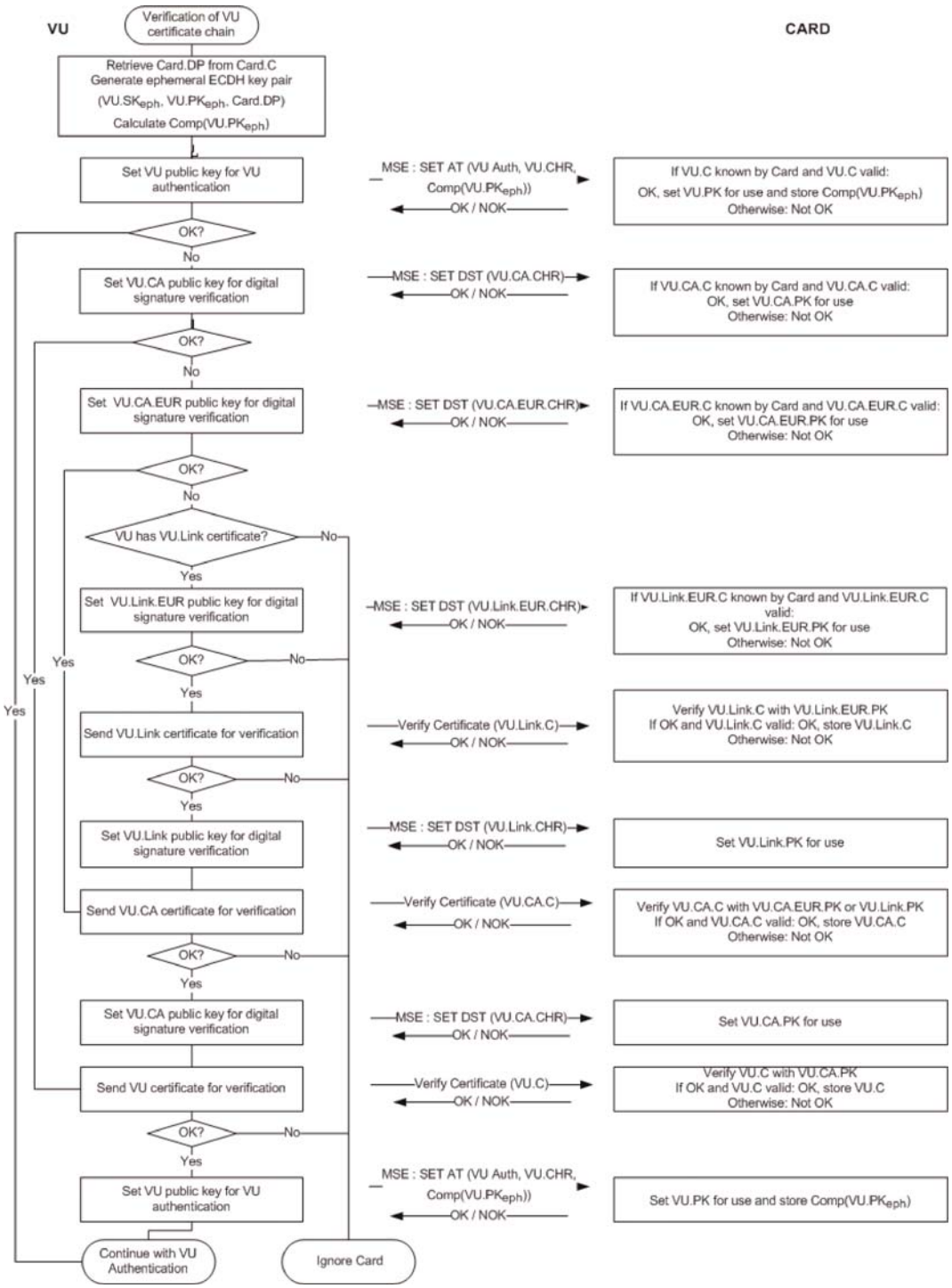
10.2.2 *Kortelės atliekamas transporto priemonės bloko pažymėjimų sekos tikrinimas*

CSM_161 Tachografo kortelėse taikomas 5 paveiksle pavaizduotas transporto priemonės bloko pažymėjimų sekos tikrinimo protokolas.

▼B

5 pav.

Kortelės atliekamo transporto priemonės bloko pažymėjimų sekos tikrinimo protokolas



Pastabos dėl 5 paveikslo

— Paveiksle nurodyti transporto priemonės bloko pažymėjimai ir viešieji raktai yra skirti abipusiam autentiškumo tikrinimui. 9.1.4 skirsnyje jie žymimi VU_MA.

▼B

— Paveiksle nurodyti VU.CA pažymėjimai ir viešieji raktai yra skirti transporto priemonės bloko ir išorinio GNSS įrenginio pažymėjimams pasirašyti. 9.1.3 skirsnyje jie žymimi MSCA_VU-EGF;

— Paveiksle nurodytas VU.CA.EUR pažymėjimas yra VU.CA pažymėjimo CAR nurodytas Europos pagrindinis pažymėjimas.

— paveiksle nurodytas VU.Link pažymėjimas yra transporto priemonės bloko sąsajos pažymėjimas, jei toks yra. Kaip nurodyta 9.1.2 skirsnyje, tai sąsajos pažymėjimas, skirtas ERCA sukurtai ir naudojant ankstesnį Europos privatųjį raktą pasirašytai naujai Europos pagrindinei raktų porai.

— VU.Link.EUR pažymėjimas yra VU.Link pažymėjimo CAR nurodytas Europos pagrindinis pažymėjimas.

CSM_162 Kaip parodyta 5 paveiksle, transporto priemonės bloko pažymėjimų sekos tikrinimas pradedamas nuo transporto priemonės bloko bandymo nustatyti savo viešąjį raktą, kuris bus naudojamas tachografo kortelėje. Jei tai pavyksta, tai reiškia, kad kortelė anksčiau jau yra sėkmingai patikrinusi šią transporto priemonės bloko pažymėjimų seką ir ją išsaugojusi būsimiems patikrinimams. Tokiu atveju transporto priemonės bloko pažymėjimas yra parengtas naudoti ir procesas tęsiamas – atliekamas transporto priemonės bloko autentiškumo tikrinimas. Jei transporto priemonės bloko pažymėjimas kortelei nėra žinomas, transporto priemonės blokas paeiliui pateikia VU.CA pažymėjimą, skirtą to transporto priemonės bloko pažymėjimui patikrinti, VU.CA.EUR pažymėjimą, skirtą VU.CA pažymėjimui patikrinti, ir galbūt sąsajos pažymėjimą, taip siekiant rasti pažymėjimą, kuris kortelei būtų žinomas arba kurį ji galėtų patikrinti. Jei toks pažymėjimas randamas, kortelė, remdamasi šiuo pažymėjimu, patikrina jai pateiktus pirminius transporto priemonės bloko pažymėjimus. Jei patikra sėkminga, transporto priemonės bloko viešojo rakto, kuris bus naudojamas tachografo kortelėje, nustatymas baigiamas. Jei ne, transporto priemonės blokas atmeta kortelę.

Pastaba. VU.CA.EUR pažymėjimą kortelė gali atpažinti trim būdais:

— VU.CA.EUR pažymėjimas yra toks pats pažymėjimas, kaip ir pačios kortelės EUR pažymėjimas;

— VU.CA.EUR pažymėjimas yra ankstesnis už pačios kortelės EUR pažymėjimą, jis buvo įdiegtas į kortelę, kai ši buvo išduota (žr. CSM_91 punktą);

— VU.CA.EUR pažymėjimas yra vėlesnis už pačios kortelės EUR pažymėjimą, kortelė iš kito transporto priemonės bloko jau yra gavusi sąsajos pažymėjimą, jį patikrinusi ir išsaugojusi būsimiems patikrinimams.

CSM_163 Savo viešajam raktui, kuris bus naudojamas tachografo kortelėje, nustatyti transporto priemonės blokas taiko komandą *MSE:Set AT*. Kaip nustatyta 2 priedėlyje, taikant šią komandą nurodomas kriptografinis mechanizmas, kuris bus taikomas naudojant nustatytą raktą. Šis mechanizmas – tai transporto priemonės bloko autentiškumo patikrinimas pagal ECDSA algoritmą, kartu taikant maišos algoritmą, susietą su transporto priemonės bloko VU_MA raktų poros raktų dydžiu, kaip nurodyta CSM_50 punkte.

▼B

CSM_164 Be to, taikant komandą *MSE:Set AT* nurodoma trumpalaikių raktų pora, kurią transporto priemonės blokas naudos derindamas seanso raktus (žr. 10.4 skirsnį). Todėl, prieš perduodant komandą *MSE:Set AT*, transporto priemonės blokas sugeneruoja trumpalaikių ECC raktų porą. Trumpalaikių raktų porai sugeneruoti transporto priemonės blokas naudoja kortelės pažymėjime nurodytus standartinius domeno parametrus. Trumpalaikių raktų pora žymima taip: (VU.SK_{eph}, VU.PK_{eph}, Card.DP). Kaip rakto identifikatorių transporto priemonės blokas naudoja ECDH trumpalaikio viešojo taško x koordinatę; tai vadinama glausta viešojo rakto išraiška ir žymima Comp(VU.PK_{eph}).

CSM_165 Jei komanda *MSE:Set AT* įvykdoma sėkmingai, kortelė nurodytą VU.PK nustato kaip naudotiną atliekant transporto priemonės autentiškumo tikrinimą ir laikinai išsaugo Comp(VU.PK_{eph}). Jei seanso raktas suderinamas tik perdavus dvi arba daugiau komandų *MSE:Set AT*, kortelė išsaugo tik paskutinįjį gautą Comp(VU.PK_{eph}).

CSM_166 Kortelė patikrina transporto priemonės bloko pateikto arba jo nurodyto kortelės atmintyje saugomo pažymėjimo galiojimo laiką ir atmeta pažymėjimus, kurių galiojimo laikas baigėsi.

CSM_167 Tikrindama transporto priemonės bloko pateikto pažymėjimo galiojimo laiką, kiekviena tachografo kortelė savo atmintyje išsaugo duomenis, kuriais nurodomas dabartinis laikas. Transporto priemonės blokas neturi galėti tiesiogiai atnaujinti šių duomenų. Išduodant kortelę dabartinis kortelės laikas nustatomas toks, kokia yra kortelės Card_MA pažymėjimo įsigaliojimo data. Jei transporto priemonės bloko pateikto autentiško pažymėjimo, kaip tinkamo laiko šaltinio, įsigaliojimo data yra vėlesnė už kortelės dabartinį laiką, kortelė atnaujina savo dabartinį laiką. Tokiu atveju kortelė nustato tokį savo dabartinį laiką, kokia yra to pažymėjimo įsigaliojimo data. Kortelė kaip tinkamus laiko šaltinius priima tik tokius pažymėjimus:

— antrosios kartos ERCA sąsajos pažymėjimus;

— antrosios kartos MSCA pažymėjimus;

— antrosios kartos transporto priemonės bloko pažymėjimus, kuriuos išdavė ta pati šalis, kaip ir pačios kortelės pažymėjimą (-us).

Pastaba. Paskutinysis reikalavimas reiškia, kad kortelė turi galėti atpažinti transporto priemonės bloko pažymėjimo CAR, t. y. MSCA_VU-EGF pažymėjimą. Šis CAR bus ne toks pat, kaip pačios kortelės pažymėjimo, t. y. MSCA_-Card pažymėjimo.

CSM_168 Kaip nurodyta 5 paveiksle, kortelė, patikrinusi dar nežinomo pažymėjimo autentiškumą ir galiojimą, gali jį išsaugoti būsimiems patikrinimams, kad to pažymėjimo autentiškumo

▼B

nereikėtų dar kartą tikrinti, kai jis vėl bus pateiktas kortelei. Kortelė gali išsaugoti ne visą pažymėjimą, o tik pagrindinės pažymėjimo dalies turinį, kaip nurodyta 9.3.2 skirsnyje.

10.3. **Transporto priemonės bloko autentiškumo tikrinimas**

CSM_169 Transporto priemonės blokuose ir kortelėse taikomas 6 paveiksle pavaizduotas transporto priemonės bloko autentiškumo tikrinimo kortelės atžvilgiu protokolas. Transporto priemonės bloko autentiškumo tikrinimas tachografo kortelei suteikia galimybę aiškiai patvirtinti, kad transporto priemonės blokas yra autentiškas. Šiuo tikslu kortelės pateiktai tikrinamajai užklausai pasirašyti transporto priemonės blokas naudoja savo privatųjį raktą.

CSM_170 Pasirašydamas kortelės teikiamą tikrinamąją užklausą, transporto priemonės blokas taip pat pateikia iš kortelės pažymėjimo paimtą kortelės turėtojo žymenį.

Pastaba. Taip užtikrinama, kad kortelė, kurios atžvilgiu transporto priemonės blokas patvirtina savo autentiškumą, būtų ta pati kortelė, kurios pažymėjimų seką transporto priemonės blokas jau yra patikrinęs.

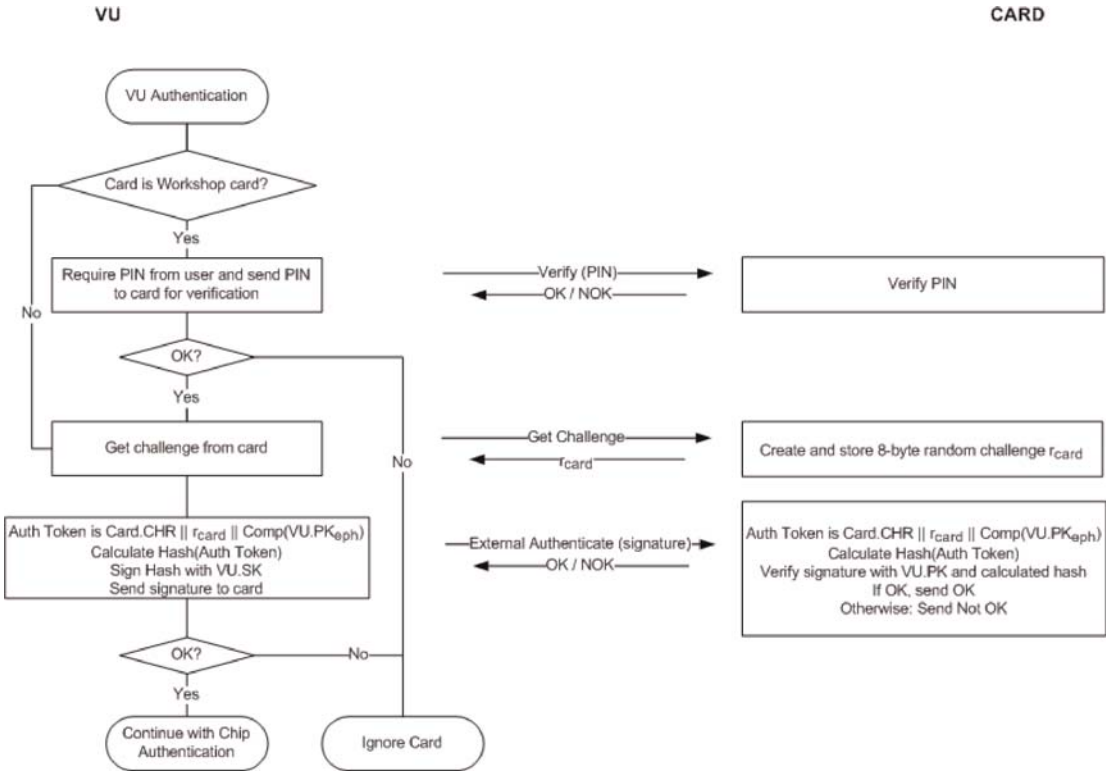
CSM_171 Pasirašydamas transporto priemonės blokas taip pateikia trumpalaikio viešojo rakto Comp($VU.PK_{eph}$) identifikatorių, kurį transporto priemonės blokas naudos saugiajam keitimuisi pranešimais užtikrinti, kai bus vykdomas 10.4 skirsnyje aprašytas lusto autentiškumo tikrinimas.

Pastaba. Taip užtikrinama, kad transporto priemonės blokas, su kuriuo kortelė užmezga ryšį per saugiojo keitimosi pranešimais seansą, būtų tas pats transporto priemonės blokas, kurio autentiškumą kortelė patvirtino.

▼B

6 pav.

Transporto priemonės bloko autentiškumo tikrinimo protokolas



CSM_172 Jei atliekant transporto priemonės bloko autentiškumo tikrinimą transporto priemonės blokas perduoda daug komandų GET CHALLENGE, kortelė kiekvieną kartą atsakydama pateikia naują 8 baitų atsitiktinę tikrinamąją užklausą, tačiau išsaugo tik paskutinę tikrinamąją užklausą.

CSM_173 Transporto priemonės blokas savo autentiškumui patvirtinti taiko pasirašymo algoritmą ECDSA, nurodytą [DSS], ir maišos algoritmą, susietą su transporto priemonės bloko VU_MA raktų poros raktų dydžiu, nurodytu CSM_50 punkte. Parašo formatas turi būti paprastas, kaip nurodyta [TR-03111]. Taip sukurtą parašą transporto priemonės blokas perduoda kortelei.

CSM_174 Pagal komandą EXTERNAL AUTHENTICATE gavusi transporto priemonės bloko parašą, kortelė:

— apskaičiuoja autentiškumo tikrinimo raktą, susiedama Card.CHR, kortelės tikrinamąją užklausą r_{card} ir transporto priemonės bloko trumpalaikio viešojo rakto Comp(VU.P-K_{eph}) identifikatorių;

— apskaičiuoja autentiškumo tikrinimo rakto maišos vertę, taikydama maišos algoritmą, susietą su transporto priemonės bloko VU_MA raktų poros raktų dydžiu, nurodytu CSM_50 punkte;

— pagal ECDSA algoritmą patikrina transporto priemonės bloko parašą, naudodama VU.PK ir apskaičiuotąją maišos vertę.

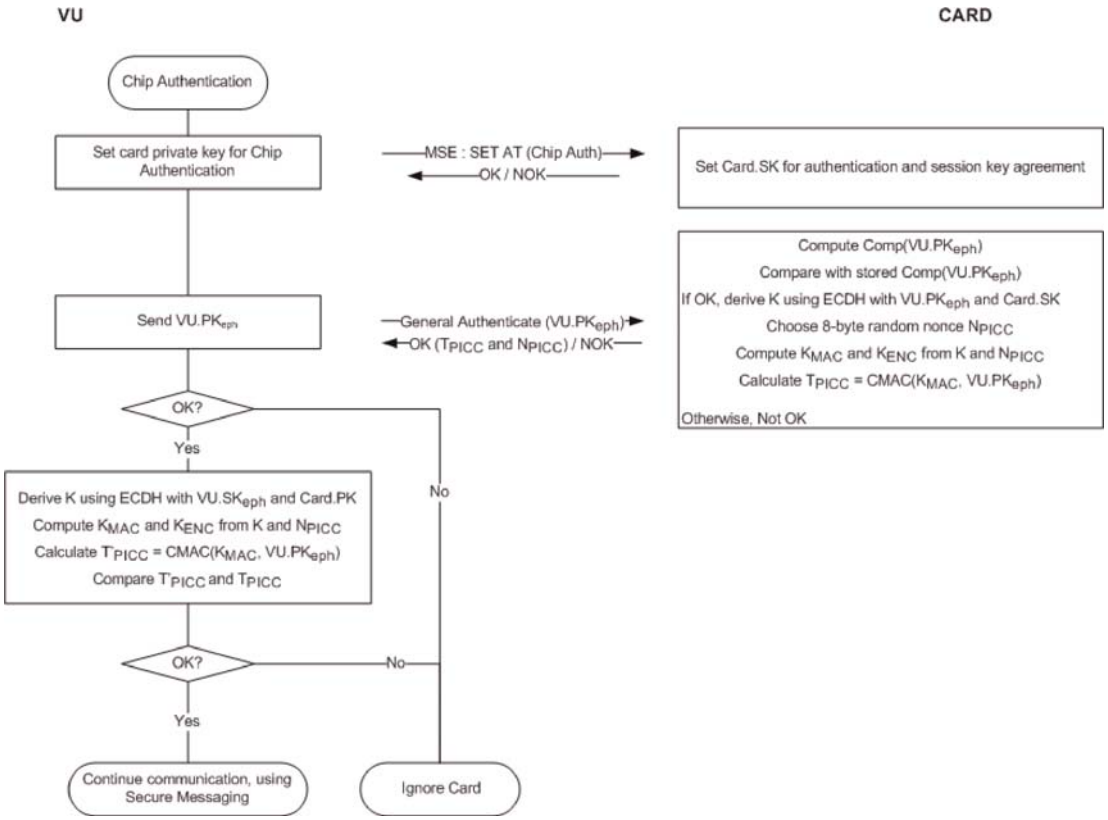
▼B

10.4. **Lusto autentiškumo tikrinimas ir seanso raktų derinimas**

CSM_175 Transporto priemonės blokuose ir kortelėse taikomas **7** paveiksle pavaizduotas kortelės autentiškumo tikrinimo transporto priemonės bloko atžvilgiu protokolas. Lusto autentiškumo tikrinimas transporto priemonės blokui suteikia galimybę aiškiai patvirtinti, kad kortelė yra autentiška.

7 pav.

Lusto autentiškumo tikrinimas ir seanso raktų derinimas



CSM_176 Transporto priemonės blokas ir kortelė atlieka toliau nurodytus veiksmus.

1. Transporto priemonės blokas pradeda lusto autentiškumo tikrinimo procesą perduodamas komandą *MSE:Set AT*, kuria nurodomas lusto autentiškumo patikrinimas pagal ECDH algoritmą, siekiant gauti AES seanso raktą, kurio ilgis susietas su kortelės Card_MA raktų poros raktų dydžiu, nurodytu CSM_50 punkte. Remdamasis kortelės pažymėjimu, transporto priemonės blokas nustato kortelės raktų poros raktų dydį.

2. Transporto priemonės blokas kortelei perduoda savo trumpalaikių raktų poros viešąjį tašką $VU.PK_{eph}$. Kaip paaiškinta CSM_164 punkte, šią trumpalaikių raktų porą transporto priemonės blokas sugeneravo prieš transporto priemonės bloko pažymėjimų sekos patikrinimą. Transporto priemonės blokas kortelei perdavė trumpalaikį viešąjį raktą $Comp(VU.PK_{eph})$ ir ši jį išsaugojo.

▼B

3. Remdamasi $VU.PK_{eph}$, kortelė apskaičiuoja Comp($VU.PK_{eph}$) ir jį palygina su išsaugota Comp($VU.PK_{eph}$) verte.

4. Taikydama ECDH algoritmą ir naudodama kortelės statinį privatųjį raktą bei transporto priemonės bloko trumpalaikį viešąjį raktą, kortelė apskaičiuoja slaptąjį K.

5. Kortelė parenka atsitiktinį 8 baitų vienkartinį N_{PICC} ir naudodama jį bei remdamasi K apskaičiuoja du AES seanso raktus – K_{MAC} ir K_{ENC}. Žr. CSM_179 punktą.

6. Naudodama K_{MAC}, kortelė apskaičiuoja transporto priemonės bloko trumpalaikio viešojo rakto identifikatoriaus autentiškumo tikrinimo raktą: T_{PICC} = CMAC(K_{MAC}, $VU.PK_{eph}$). Kortelė transporto priemonės blokui perduoda N_{PICC} ir T_{PICC}.

7. Taikydamas ECDH algoritmą ir naudodamas kortelės statinį viešąjį raktą bei transporto priemonės bloko trumpalaikį privatųjį raktą, transporto priemonės blokas apskaičiuoja tą patį slaptąjį K, kurį kortelė apskaičiavo atliekant 4 veiksmą.

8. Remdamasis K ir N_{PICC}, transporto priemonės blokas apskaičiuoja seanso raktus K_{MAC} ir K_{ENC}; žr. CSM_179 punktą.

9. Transporto priemonės blokas patikrina autentiškumo tikrinimo raktą T_{PICC}.

CSM_177 Atliekant pirmiau aprašytą 3 veiksmą, kortelė apskaičiuoja Comp(VU.PKeph) kaip viešojo taško VU.PKeph koordinatę x.

CSM_178 Atliekant pirmiau aprašytus 4 ir 7 veiksmus, kortelė ir transporto priemonės blokas taiko algoritmą ECKA-EG, apibrėžtą [TR-03111].

CSM_179 Atliekant pirmiau aprašytus 5 ir 8 veiksmus, kortelė ir transporto priemonės blokas AES seanso raktus apskaičiuoja pagal [TR-03111] nustatytą raktų darybos funkciją, užtikrindami tokį tikslumą ir atlikdami tokius pakeitimus:

— K_{ENC} skaitiklio vertė turi būti ‘00 00 00 01’, $K_{MAC.}$ – ‘00 00 00 02’.

— Naudojamas pasirenkamas vienkartinis *r*, jis turi būti lygus $N_{PICC.}$

— 128 bitų AES raktams skaičiuoti taikomas maišos algoritmas SHA-256.

— 192 bitų AES raktams skaičiuoti taikomas maišos algoritmas SHA-384.

— 256 bitų AES raktams skaičiuoti taikomas maišos algoritmas SHA-512.

Seanso raktų ilgis (t. y. ilgis, kurį pasiekus nupjaunama maišos vertė) susiejamas su Card_MA raktų poros ilgiu, nustatytu CSM_50 punkte.

▼B

CSM_180 Atliekant pirmiau aprašytus 6 ir 9 veiksmus, kortelė ir transporto priemonės blokas CMAC režimu taiko AES algoritmą, kaip nustatyta [SP 800-38B]. T_{PICC} ilgis susiejamas su AES seanso raktų ilgiu, nustatytu CSM_50 punkte.

10.5. **Saugusis keitimasis pranešimais**

10.5.1 *Bendrosios nuostatos*

CSM_181 Visos komandos ir atsakai, kuriais transporto priemonės blokas ir tachografo kortelė iki seanso pabaigos apsikeitė sėkmingai patvirtinus lusto autentiškumą, apsaugomi taikant saugųjį keitimąsi pranešimais.

CSM_182 Išskyrus rinkmenos, kurios prieigos sąlyga yra SM-R-ENC-MAC-G2 (žr. 2 priedėlio 4 skirsnį), nuskaitymą, saugusis keitimasis pranešimais turi būti atliekamas tik autentiškumo tikrinimo režimu. Taikant šį režimą, pranešimų autentiškumui ir vientisumui užtikrinti prie visų komandų ir atsakų pridedama kriptografinė kontrolinė suma (dar vadinama MAC).

CSM_183 Nuskaitant rinkmenos, kurios prieigos sąlyga yra SM-R-ENC-MAC-G2, duomenis, saugusis keitimasis pranešimais atliekamas užšifravimo ir autentiškumo tikrinimo režimu, t. y. pirmiausia užšifruojami atsakymo duomenys, kad būtų užtikrintas pranešimo konfidencialumas, o tada, siekiant užtikrinti autentiškumą ir vientisumą, apskaičiuojami formatiniai užšifruoti duomenys.

CSM_184 Saugusis keitimasis pranešimais grindžiamas AES algoritmu, nustatytu [AES], jam naudojami seanso raktai K_{MAC} ir K_{ENC}, suderinti atliekant lusto autentiškumo tikrinimą.

CSM_185 Siekiant išvengti pakartojimo atakų, kaip siuntimo sekos skaitiklis (SSC) naudojamas nepasirašytas sveikasis skaičius. SSC dydis turi atitikti AES bloko dydį, t. y. jis turi būti 128 bitų. SSC turi būti „MSB-first“ formato. Pradedant saugųjį keitimąsi pranešimais, pradinė siuntimo sekos skaitiklio vertė turi būti nulis (t. y. ‘00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00’). SSC didinamas prieš kiekvieną atvejį, kai sugeneruojamas komandos arba atsako APDU, t. y. kadangi SM seanso pradinė SSC vertė yra 0, perduodant pirmąją komandą SSC vertė bus 1. Pirmojo atsako SSC vertė bus 2.

CSM_186 Pranešimų šifravimo tikslais nuosekliojo blokinio šifravimo (CBC) režimu taikant AES algoritmą, kaip apibrėžta standarte [ISO 10116], naudojamas K_{ENC}, kaitaliojimo parametras m = 1 ir inicializacijos vektorius SV = E(K_{ENC}, SSC), t. y. einamoji siuntimo sekos skaitiklio vertė, užšifruota naudojant K_{ENC}.

CSM_187 Pranešimų autentiškumo tikrinimo tikslais CMAC režimu taikant AES algoritmą, kaip nurodyta [SP 800-38B], naudojamas K_{MAC}. MAC ilgis susiejamas su AES seanso raktų ilgiu, nustatytu CSM_50 punkte. Siuntimo sekos skaitiklis į MAC įtraukiamas jį pridedant prieš duomenų paketo autentiškumo tikrinimą.

▼B

10.5.2 *Saugiojo pranešimo struktūra*

CSM_188 Saugiojo keitimosi pranešimais tikslais naudojami tik 5 lentelėje nurodyti saugiojo keitimosi pranešimais duomenų objektai (žr. [ISO 7816-4]). Visuose pranešimuose šie duomenų objektai naudojami šioje lentelėje nurodyta tvarka.

5 lentelė.

Saugiojo keitimosi pranešimais duomenų objektai

Duomenų objekto pavadinimas	Žymena	Privalomas (P), sąlyginis (S), draudžiamas (D)	
		Komandose	Atsakuose
Paprastoji vertė, neužkoduota BER-TLV metodu	‘81’	S	S
Paprastoji vertė, užkoduota BER-TLV metodu, tačiau neįtraukiant SM DO	‘B3’	S	S
Užpildo turinio indikatorius ir kriptograma (paprastoji vertė, neužkoduota BER-TLV metodu)	‘87’	S	S
Apsaugotas Le	‘97’	S	D
Apdorojimo statusas	‘99’	D	P
Kriptografinė kontrolinė suma	‘8E’	P	P

Pastaba. Kaip nurodyta 2 priedėlyje, tachografų kortelės gali būti suderinamos su READ BINARY ir UPDATE BINARY komandomis, naudojant nelyginį INS baitą (atitinkamai ‘B1’ ir ‘D7’). Šie komandų variantai reikalingi 32 768 baitų ir didesnėms rinkmenoms nuskaityti ir atnaujinti. Jei naudojamas toks variantas, vietoje duomenų objekto, kurio žymena ‘B3’, naudojamas duomenų objektas, kurio žymena ‘81’. Daugiau informacijos pateikta 2 priedėlyje.

CSM_189 Visi SM duomenų objektai pagal DER užkoduojami kaip TLV, kaip nurodyta standarte [ISO 8825-1]. Atlikus tokį kodavimą gaunama toliau nurodytos struktūros žymenos ilgio vertė (TLV).

Žymena: žymena užkoduojama vienu arba dviem oktetais, ja nurodomas turinys.

Ilgis: ilgis užkoduojamas vienu, dviem arba trim oktetais kaip nepasirašytas sveikasis skaičius, jo didžiausias galimas ilgis – 65 535 oktetai. Naudojama kuo mažiau oktetų.

Vertė: vertė užkoduojama nuliu arba daugiau oktetų.

CSM_190 Saugiojo keitimosi pranešimais būdu apsaugoti APDU kuriami taip:

— skaičiuojant MAC, įtraukiama komandos antraštė, todėl skaičiuojant klasės baitą CLA naudojama vertė ‘0C’;

▼B

— kaip nurodyta 2 priedėlyje, visi INS baitai turi būti lyginiai, išskyrus komandoms READ BINARY ir UPDATE BINARY skirtus INS baitus – jie gali būti nelyginiai;

— pasinaudojus saugiuoju keitimusi pranešimais, faktinė Lc vertė pakeičiama į Lc';

— duomenų laukas sudaromas iš SM duomenų objektų;

— perduodant apsaugotą komandos APDU, naujam Le baitui suteikiama vertė ‘00’. Jei reikia, pradinei Le vertei perduoti į duomenų lauką įtraukiamas duomenų objektas ‘97’.

CSM_191 Visi užšifruotini duomenų objektai pagal standartą [ISO 7816-4] užpildomi naudojant užpildo turinio indikatorių ‘01’. Skaičiuojant MAC, kiekvienas APDU duomenų objektas pagal standartą [ISO 7816-4] užpildomas atskirai.

Pastaba. Taikant saugųjį keitimąsi pranešimais, užpildymas visada atliekamas saugiojo keitimosi pranešimais lygmeniu, o ne taikant CMAC ar CBC algoritmus.

Santrauka ir pavyzdžiai

Taikant saugųjį keitimąsi pranešimais naudojamo komandos APDU struktūra turi būti tokia, kaip nurodyta toliau, atsižvelgiant į atitinkamos neapsaugotos komandos atvejį (DO – duomenų objektas).

1 atvejis:	CLA INS P1 P2 || Lc' || DO ‘8E’ || Le
2 atvejis:	CLA INS P1 P2 || Lc' || DO ‘97’ || DO‘8E’ || Le
3 atvejis (lyginis INS baitas):	CLA INS P1 P2 || Lc' || DO ‘81’ || DO‘8E’ || Le
3 atvejis (nelyginis INS baitas):	CLA INS P1 P2 || Lc' || DO ‘B3’ || DO‘8E’ || Le
4 atvejis (lyginis INS baitas):	CLA INS P1 P2 || Lc' || DO ‘81’ || DO‘97’ || DO‘8E’ || Le
4 atvejis (nelyginis INS baitas):	CLA INS P1 P2 || Lc' || DO ‘B3’ || DO‘97’ || DO‘8E’ || Le

Čia Le = ‘00’ arba ‘00 00’, atsižvelgiant į tai, ar naudojami trumpieji, ar didesnio ilgio laukai; žr. standartą [ISO 7816-4].

Taikant saugųjį keitimąsi pranešimais atsako APDU struktūra turi būti tokia, kaip nurodyta toliau, atsižvelgiant į atitinkamo neapsaugoto atsako atvejį.

1 arba 3 atvejis:	DO ‘99’ || DO ‘8E’ || SW1SW2
2 arba 4 atvejis (lyginis INS baitas) taikant šifravimą:	DO ‘81’ || DO ‘99’ || DO ‘8E’ || SW1SW2
2 arba 4 atvejis (lyginis INS baitas) netaikant šifravimo:	DO ‘87’ || DO ‘99’ || DO ‘8E’ || SW1SW2
2 arba 4 atvejis (nelyginis INS baitas) netaikant šifravimo:	DO ‘B3’ || DO ‘99’ || DO ‘8E’ || SW1SW2

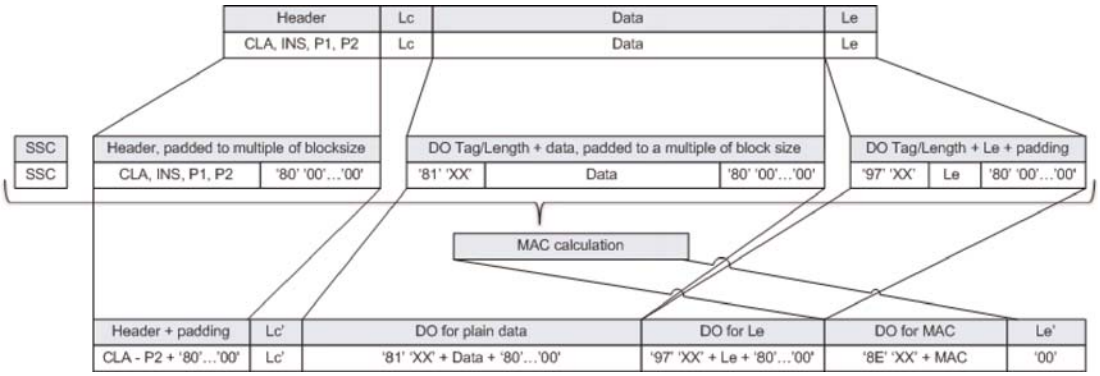
Pastaba. 2 arba 4 atvejis (nelyginis INS baitas) taikant šifravimą niekada nenaudojamas transporto priemonės bloko ir kortelės ryšiui.

▼B

Toliau pateikti trys APDU transformacijos pavyzdžiai, susiję su komandomis, kurioms naudojamas lyginis INS kodas. 8 paveiksle parodytas patvirtintas su 4 atveju susijęs komandos APDU, 9 paveiksle – patvirtintas su 2 arba 4 atveju susijęs atsako APDU, 10 paveiksle – užšifruotas ir patvirtintas su 2 arba 4 atveju susijęs atsako APDU.

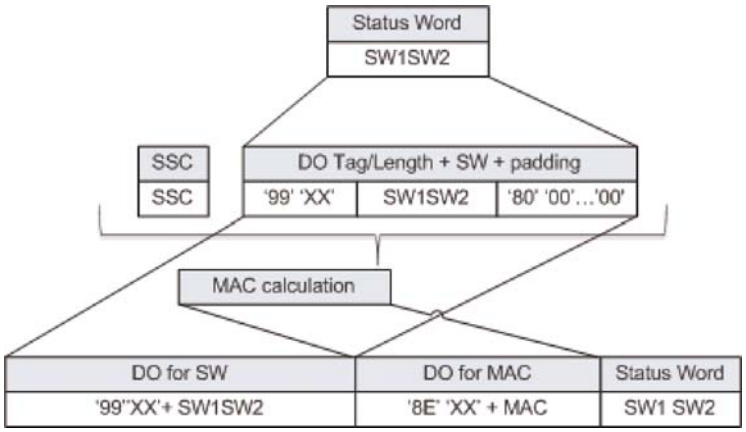
8 pav.

Patvirtinto su 4 atveju susijusio komandos APDU transformacija



9 pav.

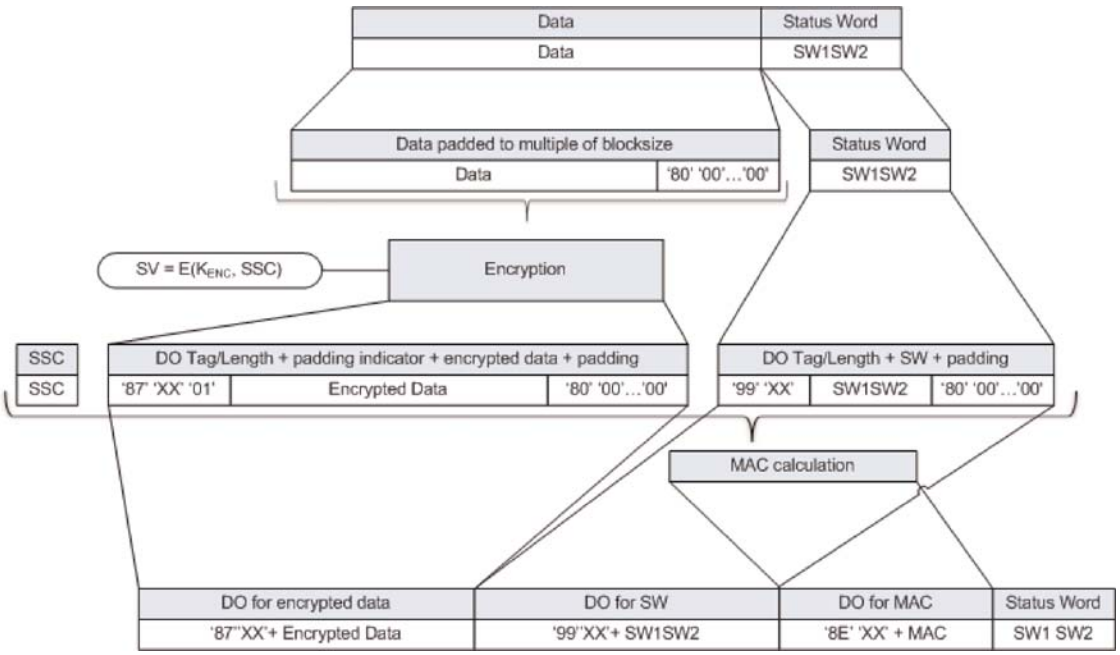
Patvirtinto su 1 arba 3 atveju susijusio atsako APDU transformacija



▼B

10 pav.

Užšifruoto ir patvirtinto su 2 arba 4 atveju susijusio atsako APDU transformacija



10.5.3 *Saugiojo keitimosi pranešimais seanso nutraukimas*

CSM_192 Transporto priemonės blokas vykstantį saugiojo keitimosi pranešimais seansą nutraukia tik susidarius vienai iš šių sąlygų:

— Transporto priemonės blokas gauna paprastąjį atsako APDU;

— Transporto priemonės blokas nustato saugiojo keitimosi pranešimais klaidą, susijusią su atsako APDU:

  — trūksta numatyto saugiojo keitimosi pranešimais duomenų objekto, duomenų objektai išdėstyti netinkama tvarka arba įtrauktas nežinomas duomenų objektas;

  — saugiojo keitimosi pranešimais duomenų objektas yra neteisingas, pvz., nurodoma neteisinga MAC vertė, TLV struktūra yra netinkama arba žymenoje ‘87’ pateikta užpildo indikatoriaus vertė yra ne ‘01’;

— kortelė perduoda būsenos baitą, kuriuo nurodoma, kad nustatyta SM klaida (žr. CSM_194 punktą);

— vykstančiame seanse pasiekiama komandų ir susijusių atsakų skaičiaus riba. Konkrečiam transporto priemonės blokui šią ribą nustato jo gamintojas, atsižvelgdamas į naudojamos aparatinės įrangos saugumo reikalavimus; didžiausia galima vertė yra 240 SM komandų ir susijusių atsakų per vieną seansą.

▼B

CSM_193 Tachografo kortelė vykstantį saugiojo keitimosi pranešimais seansą nutraukia tik susidarius vienai iš šių sąlygų:

— tachografo kortelė gauna paprastąjį atsako APDU;

— tachografo kortelė nustato saugiojo keitimosi pranešimais klaidą, susijusią su komandos APDU:

— trūksta numatyto saugiojo keitimosi pranešimais duomenų objekto, duomenų objektai išdėstyti netinkama tvarka arba įtrauktas nežinomas duomenų objektas;

— saugiojo keitimosi pranešimais duomenų objektas yra neteisingas, pvz., nurodoma neteisinga MAC vertė, arba TLV struktūra yra netinkama;

— nutrūksta tachografo kortelės maitinimas arba atkuriama jos pradinė būsena;

— transporto priemonės blokas parenka kortelės taikomąją programą;

— transporto priemonės blokas pradeda savo autentiškumo tikrinimo procesą;

— vykstančiame seanse pasiekiama komandų ir susijusių atsakų skaičiaus riba. Konkrečiai kortelei šią ribą nustato jo gamintojas, atsižvelgdamas į naudojamos aparatinės įrangos saugumo reikalavimus; didžiausia galima vertė yra 240 SM komandų ir susijusių atsakų per vieną seansą.

CSM_194 Tachografo kortelės atliekamas SM klaidų tvarkymas:

— jei komandos APDU trūksta kai kurių numatytų saugiojo keitimosi pranešimais duomenų objektų, duomenų objektų išdėstymo tvarka yra netinkama arba įtraukti nežinomi duomenų objektai, tachografo kortelė atsako būsenos baitais ‘69 87’.

— jei komandos APDU saugiojo keitimosi pranešimais duomenų objektas yra neteisingas, tachografo kortelė atsako būsenos baitais ‘69 88’.

Tokiu atveju statuso baitai pateikiami netaikant SM.

CSM_195 Jei nutraukiamas transporto priemonės bloko ir tachografo kortelės saugiojo keitimosi pranešimais seansas, transporto priemonės blokas ir tachografo kortelė:

— saugiai sunaikina išsaugotus seanso raktus;

— nedelsdami pradeda naują saugiojo keitimosi pranešimais seansą, kaip aprašyta 10.2–10.5 skirsniuose.

CSM_196 Jei dėl kokių nors priežasčių transporto priemonės blokas nusprendžia iš naujo pradėti abipusį autentiškumo tikrinimą įdėtos kortelės atžvilgiu, procesas iš naujo pradedamas nuo kortelės pažymėjimų sekos tikrinimo, kaip aprašyta 10.2 skirsnyje, ir tęsiamas taip, kaip aprašyta 10.2–10.5 skirsniuose.

▼B

11. TRANSPORTO PRIEMONĖS BLOKO IR IŠORINIO GNSS ĮRENGINIO SUJUNGIMAS, ABIPUSIS AUTENTIŠKUMO TIKRINIMAS IR SAUGUSIS KEITIMASIS PRANEŠIMAIS

11.1. **Bendrosios nuostatos**

CSM_197 GNSS įrenginys, kurį transporto priemonės blokas naudoja savo buvimo vietai nustatyti, gali būti vidinis (t. y. sumontuotas transporto priemonės bloko korpuse ir neišimamas) arba tai gali būti išorinis modulis. Pirmuoju atveju GNSS įrenginio ir transporto priemonės bloko vidinio ryšio standartizuoti nereikia, šiame skyriuje nustatyti reikalavimai netaikomi. Antruoju atveju transporto priemonės bloko ir išorinio GNSS įrenginio ryšį būtina standartizuoti ir apsaugoti, kaip aprašyta šiame skyriuje.

CSM_198 Saugus transporto priemonės bloko ir išorinio GNSS įrenginio ryšys užtikrinamas taip pat, kaip saugus transporto priemonės bloko ir tachografo kortelės ryšys, tik šiuo atveju vietoj kortelės omenyje turimas išorinis GNSS įrenginys (EGF). EGF turi atitikti visus 10 skyriuje nurodytus tachografo kortelėms keliamus reikalavimus, atsižvelgiant į šiame skyriuje nurodytus nukrypimus, paaiškinimus ir papildymus. Pirmiausia atliekamas abipusis pažymėjimų sekos tikrinimas, transporto priemonės bloko autentiškumo tikrinimas ir lusto autentiškumo tikrinimas, kaip aprašyta 11.3 ir 11.4 skirsniuose.

CSM_199 Transporto priemonės bloko ir EGF ryšys nuo transporto priemonės bloko ir kortelės ryšio skiriasi tuo, kad tam, jog transporto priemonės blokas ir EGF įprastu veikimo režimu galėtų keistis GNSS pagrįstais duomenimis, transporto priemonės blokas ir EGF turi būti sujungti dirbtuvėse. Sujungimo procesas aprašytas 11.2 skirsnyje.

CSM_200 Transporto priemonės bloko ir EGF ryšiui užtikrinti naudojamos APDU komandos ir atsakai, nustatyti standartuose [ISO 7816-4] ir [ISO 7816-8]. Tiksli šių APDU struktūra nustatyta šio priedo 2 priedėlyje.

11.2. **Transporto priemonės bloko ir išorinio GNSS įrenginio sujungimas**

CSM_201 Transporto priemonės blokas ir EGF transporto priemonėje sujungiami dirbtuvėse. Tik sujungti transporto priemonės blokas ir EGF galės palaikyti ryšį įprastu veikimo režimu.

CSM_202 Sujungti transporto priemonės bloką ir EGF turi būti galima tik kai transporto priemonės blokas veikia kalibravimo režimu. Sujungimo procedūrą pradeda transporto priemonės blokas.

CSM_203 Dirbtuvėse transporto priemonės blokas bet kada gali būti iš naujo sujungiamas su kitu EGF arba vėl sujungiamas su tuo pačiu EGF. Atliekant naują sujungimą, transporto priemonės blokas saugiai sunaikina savo atmintyje saugomą EGF_MA pažymėjimą ir išsaugo EGF, su kuriuo jis sujungiamas, EGF_MA pažymėjimą.

CSM_204 Dirbtuvėse išorinis GNSS įrenginys bet kada gali būti gali būti iš naujo sujungiamas su kitu transporto priemonės bloku arba vėl sujungiamas su tuo pačiu transporto priemonės bloku. Iš naujo atliekant sujungimą, EGF saugiai sunaikina savo atmintyje saugomą VU_MA pažymėjimą ir išsaugo transporto priemonės bloko, su kuriuo jis sujungiama, VU_MA pažymėjimą.

▼B

11.3. **Abipusis pažymėjimų sekos tikrinimas**

11.3.1 *Bendrosios nuostatos*

CSM_205 Abipusis transporto priemonės bloko ir EGF pažymėjimų sekos tikrinimas atliekamas tik dirbtuvėse sujungiant transporto priemonės bloką ir EGF. Sujungtiems transporto priemonės blokui ir EGF veikiant įprastu režimu, pažymėjimai netikrinami. Transporto priemonės blokas ir EGF, patikrinę pažymėjimų, kurie juose buvo išsaugoti atliekant sujungimą, galiojimo laiką, turi jais pasikliauti. Kad būtų apsaugotas įprastu veikimo režimu veikiančių transporto priemonės bloko ir EGF ryšys, transporto priemonės blokas ir EGF nepasikliauna jokiais kitais pažymėjimais.

11.3.2 *Transporto priemonės bloko ir EGF sujungimas*

CSM_206 Transporto priemonės bloką sujungiant su EGF taikomas 4 paveiksle (10.2.1 skirsnis) pavaizduotas išorinio GNSS įrenginio pažymėjimų sekos tikrinimo protokolas.

Susijusios pastabos dėl 4 paveikslo

— Ryšio kontrolė šiuo priedėliu nereglamentuojama. Tačiau EGF nėra išmanioji kortelė, todėl transporto priemonės blokas veikiausiai neperduos komandos *Reset*, kad užmegztų ryšį, ir negaus ATR.

— Paveiksle nurodyti kortelės pažymėjimai ir viešieji raktai turi būti suprantami kaip abipusiam autentiškumo tikrinimui skirti EGF pažymėjimai ir viešieji raktai. 9.1.6 skirsnyje jie žymimi EGF_MA.

— Paveiksle nurodyti Card.CA pažymėjimai ir viešieji raktai turi būti suprantami kaip EGF pažymėjimams pasirašyti skirti MSCA pažymėjimai ir viešieji raktai. 9.1.3 skirsnyje jie žymimi MSCA_VU-EGF.

— Paveiksle nurodytas Card.CA.EUR pažymėjimas turi būti suprantamas kaip MSCA_VU-EGF pažymėjimo CAR nurodytas Europos pagrindinis pažymėjimas.

— Paveiksle nurodytas Card.Link pažymėjimas turi būti suprantamas kaip EGF sąsajos pažymėjimas, jei toks yra. Kaip nurodyta 9.1.2 skirsnyje, tai sąsajos pažymėjimas, skirtas ERCA sukurtai ir naudojant ankstesnį Europos privatųjį raktą pasirašytai naujai Europos pagrindinei raktų porai.

— Card.Link.EUR pažymėjimas yra Card.Link pažymėjimo CAR nurodytas Europos pagrindinis pažymėjimas.

— Vietoje `cardExtendedSerialNumber`, transporto priemonės blokas iš EF ICC nuskaito `sensorGNSSserialNumber`.

— Transporto priemonės blokas pasirenka ne tachografo AID, o EGF AID.

— „Ignore Card“ turi būti suprantama kaip „Ignore EGF“.

▼B

CSM_207 Patikrinęs EGF_MA pažymėjimą, transporto priemonės blokas šį pažymėjimą išsaugo naudojimui įprastu veikimo režimu; žr. 11.3.3 skirsnį.

CSM_208 Išorinį GNSS įrenginį sujungiant su transporto priemonės bloku taikomas 5 paveiksle (10.2.2 skirsnis) pavaizduotas transporto priemonės bloko pažymėjimų sekos tikrinimo protokolas.

Susijusios pastabos dėl 5 paveikslo

— Transporto priemonės blokas, remdamasis EGF pažymėjime nurodytais domeno parametrais, sugeneruoja naują trumpalaikių raktų porą.

— Paveiksle nurodyti transporto priemonės bloko pažymėjimai ir viešieji raktai yra skirti abipusiam autentiškumo tikrinimui. 9.1.4 skirsnyje jie žymimi VU_MA.

— Paveiksle nurodyti VU.CA pažymėjimai ir viešieji raktai yra skirti transporto priemonės bloko ir išorinio GNSS įrenginio pažymėjimams pasirašyti. 9.1.3 skirsnyje jie žymimi MSCA_VU-EGF;

— Paveiksle nurodytas VU.CA.EUR pažymėjimas yra VU.CA pažymėjimo CAR nurodytas Europos pagrindinis pažymėjimas.

— paveiksle nurodytas VU.Link pažymėjimas yra transporto priemonės bloko sąsajos pažymėjimas, jei toks yra. Kaip nurodyta 9.1.2 skirsnyje, tai sąsajos pažymėjimas, skirtas ERCA sukurtai ir naudojant ankstesnį Europos privatųjį raktą pasirašytai naujai Europos pagrindinei raktų porai.

— VU.Link.EUR pažymėjimas yra VU.Link pažymėjimo CAR nurodytas Europos pagrindinis pažymėjimas.

CSM_209 Nukrypstant nuo CSM_167 reikalavimo, kiekvieno pateikto pažymėjimo galiojimo laiką EGF tikrina remdamasis GNSS laiku.

CSM_210 Patikrinęs VU_MA pažymėjimą, išorinis GNSS įrenginys šį pažymėjimą išsaugo naudojimui įprastu veikimo režimu; žr. 11.3.3 skirsnį.

11.3.3 *Įprastas veikimo režimas*

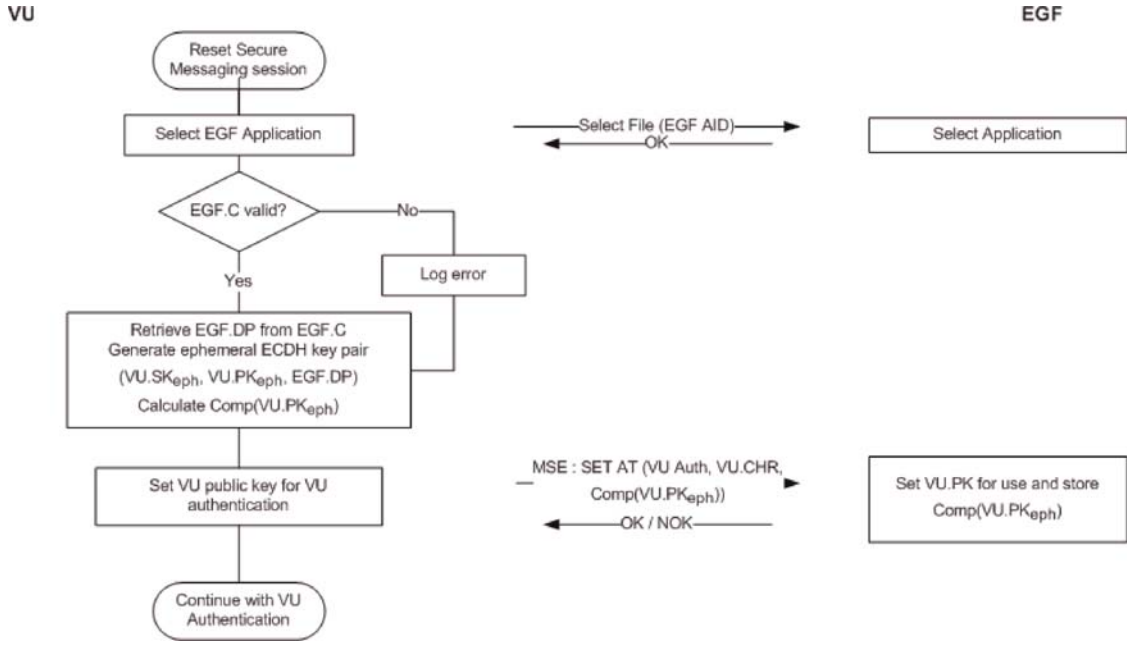
CSM_211 Įprastu veikimo režimu transporto priemonės blokas ir EGF taiko 11 paveiksle pavaizduotą protokolą, pagal kuri tikrinamas išsaugotų EGF_MA ir VU_MA pažymėjimų galiojimo laikas ir nustatomas VU_MA viešasis raktas, kas vėliau būtų galima patvirtinti transporto priemonės bloko autentiškumą. Įprastu veikimo režimu neatliekama jokio kito abipusio pažymėjimų sekų tikrinimo.

Atkreipkite dėmesį, kad 11 paveiksle iš esmės pavaizduoti pirmieji 4 ir 5 paveiksluose nurodyti etapai. Taip pat atkreipkite dėmesį, kad EGF nėra išmanioji kortelė, todėl transporto priemonės blokas veikiausiai neperduos komandos *Reset*, kad užmegztų ryšį, ir negaus ATR. Bet kokiu atveju tai šiuo priedėliu nereglamentuojama.

▼B

11 pav.

Abipusis pažymėjimų galiojimo laiko tikrinimas įprastu transporto priemonės bloko ir EGF veikimo režimu



CSM_212 Kaip parodyta 11 paveiksle, jei EGF_MA pažymėjimas nebegalioja, transporto priemonės blokas registruoja klaidą. Tačiau abipusis autentiškumo tikrinimas, raktų derinimas ir tolesnis informacijos perdavimas taikant saugųjį keitimąsi pranešimais vykdomi įprasta tvarka.

11.4. **Transporto priemonės bloko autentiškumo tikrinimas, lusto autentiškumo tikrinimas ir seanso raktų derinimas**

CSM_213 Transporto priemonės bloko autentiškumas patikrinamas, lusto autentiškumas patikrinamas ir seanso raktai tarp transporto priemonės bloko ir EGF derinami sujungimo metu ir kaskart, kai įprastu veikimo režimu pradedamas saugiojo keitimosi pranešimais seansas. Transporto priemonės blokas ir EGF vykdo 10.3 ir 10.4 skirsniuose aprašytus procesus. Taikomi visi šiuose skirsniuose nustatyti reikalavimai.

11.5. **Saugusis keitimasis pranešimais**

CSM_214 Visos komandos ir atsakai, kuriais transporto priemonės blokas ir išorinis GNSS įrenginys iki seanso pabaigos apsikeitė sėkmingai patvirtinus lusto autentiškumą, apsaugomi taikant saugųjį keitimąsi pranešimais tik autentiškumo tikrinimo režimu. Taikomi visi 10.5 skirsnyje nustatyti reikalavimai.

CSM_215 Jei transporto priemonės bloko ir EGF saugiojo keitimosi pranešimais seansas nutraukiamas, transporto priemonės blokas nedelsdamas pradeda naują saugiojo keitimosi pranešimais seansą, kaip aprašyta 11.3.3 ir 11.4 skirsniuose.

12. TRANSPORTO PRIEMONĖS BLOKO IR JUDESIO JUTIKLIO SIEJIMAS IR RYŠYS

12.1. **Bendrosios nuostatos**

CSM_216 Siejimo metu ir įprasto veikimo režimu transporto priemonės bloko ir judesio jutiklio ryšys užtikrinamas taikant standarte [ISO 16844-3] nustatytą sąsajos protokolą su pakeitimais, aprašytais šiame ir 9.2.1 skirsnyje.

▼B

Pastaba. Šio skirsnio skaitytojai turėtų būti susipažinę su standarto [ISO 16844-3] turiniu.

12.2. **Transporto priemonės bloko ir judesio jutiklio siejimas naudojant skirtingų kartų raktus**

Kaip paaiškinta 9.2.1 skirsnyje, judesio jutiklio pagrindinis raktas ir visi susiję raktai reguliariai keičiami. Dėl to dirbtuvių kortelėse gali būti net trijų skirtingų kartų su judesio jutikliais susiję AES raktai $K_{M\text{-}WC}$ (nuoseklių kartų). Judesio jutikliuose atitinkamai gali būti net trys skirtingi AES algoritmu pagrįsti duomenų šifravimo variantai (pagrįsti nuosekliomis judesio jutiklio pagrindinio rakto K_M kartomis). Transporto priemonės bloke yra tik vienas su judesio jutikliu susijęs raktas $K_{M\text{-}VU}$.

CSM_217 Antrosios kartos transporto priemonės blokas ir antrosios kartos judesio jutiklis siejami taip, kaip nurodyta toliau (plg. standarte [ISO 16844-3] pateiktą 6 lentelę).

1. Į transporto priemonės bloką įdedama antrosios kartos dirbtuvių kortelė ir jis prijungiamas prie judesio jutiklio.

2. Transporto priemonės blokas nuskaito visus dirbtuvių kortelėje esančius raktus $K_{M\text{-}WC}$, patikrina jų versijos numerius ir pasirenka raktą, kurio versijos numeris atitinka transporto priemonės bloko rakto $K_{M\text{-}VU}$ versijos numerį. Jei dirbtuvių kortelėje atitinkamo rakto $K_{M\text{-}WC}$ nėra, transporto priemonės blokas nutraukia siejimo procesą ir dirbtuvių kortelės turėtojui parodo atitinkamą pranešimą apie klaidą.

3. Transporto priemonės blokas, remdamasis $K_{M\text{-}VU}$ ir $K_{M\text{-}WC}$, apskaičiuoja judesio jutiklio pagrindinį raktą K_M, o remdamasi K_M – identifikavimo raktą K_{ID}, kaip nurodyta 9.2.1 skirsnyje.

4. Transporto priemonės blokas perduoda komandą pradėti siejimą su judesio jutikliu, kaip aprašyta standarte [ISO 16844-3], ir, naudodamas identifikavimo raktą K_{ID}, užšifruoja iš judesio jutiklio gautą serijos numerį. Užšifruotą serijos numerį transporto priemonės blokas perduoda atgal judesio jutikliui.

5. Judesio jutiklis šį užšifruotą serijos numerį paeiliui palygina su kiekvienu jame saugomu užšifruotu serijos numeriu. Jei randamas atitikmuo, patvirtinamas transporto priemonės bloko autentiškumas. Judesio jutiklis užregistruoja transporto priemonės bloko naudojamo rakto K_{ID} kartą ir pateikia atitinkamos versijos užšifruotą savo siejimo raktą, t. y. užšifruotą raktą, sukurtą naudojant tos pačios kartos K_M.

6. Transporto priemonės blokas, naudodamas K_M, iššifruoja siejimo raktą, sugeneruoja seanso raktą K_S, jį užšifruoja naudodamas siejimo raktą ir rezultatą perduoda judesio jutikliui. Judesio jutiklis iššifruoja K_S.

7. Transporto priemonės blokas surenka siejimo informaciją, kaip nustatyta standarte [ISO 16844-3], užšifruoja šią informaciją naudodamas siejimo raktą ir rezultatą perduoda judesio jutikliui. Judesio jutiklis iššifruoja siejimo informaciją.

8. Judesio jutiklis, naudodamas gautą K_S, užšifruoja gautą siejimo informaciją ir ją pateikia transporto priemonės blokui. Transporto priemonės blokas patikrina, ar ši siejimo informacija yra ta pati informacija, kurią transporto priemonės blokas pirmiau perdavė judesio jutikliui.

▼B

Jeigu taip, tai patvirtina, kad judesio jutiklis naudojo tą patį K_S, kaip ir transporto priemonės blokas, vadinasi, 5 etape perdavė savo siejimo raktą, užšifruotą naudojant tinkamos kartos raktą K_M. Taigi laikoma, kad judesio jutiklio autentiškumas patvirtintas.

Atkreipkite dėmesį, kad 2 ir 5 etapai skiriasi nuo standarte [ISO 16844-3] nustatyto standartinio proceso; kiti etapai yra standartiniai.

Pavyzdys. Tarkime, siejimas atliekamas pirmaisiais ERCA (3) pažymėjimo galiojimo metais; žr. 9.2.1.2 skirsnyje pateiktą 2 paveikslą. Be to:

— tarkime, kad judesio jutiklis buvo išduotas paskutiniaisiais ERCA (1) pažymėjimo galiojimo metais. Taigi jame bus tokie raktai ir duomenys:

  — $N_s[1]$: jo serijos numeris, užšifruotas naudojant 1 kartos K_{ID};

  — $N_s[2]$: jo serijos numeris, užšifruotas naudojant 2 kartos K_{ID};

  — $N_s[3]$: jo serijos numeris, užšifruotas naudojant 3 kartos K_{ID};

  — $K_P[1]$: jo 1 kartos siejimo raktas ([1]), užšifruotas naudojant 1 kartos K_M;

  — $K_P[2]$: jo 2 kartos siejimo raktas, užšifruotas naudojant 2 kartos K_M;

  — $K_P[3]$: jo 3 kartos siejimo raktas, užšifruotas naudojant 3 kartos K_M;

— tarkime, kad dirbtuvių kortelė buvo išduota pirmaisiais ERCA (3) pažymėjimo galiojimo metais. Taigi joje bus 2 ir 3 kartos raktai $K_{M\text{-}WC}$;

— tarkime, transporto priemonės blokas yra 2 kartos, jame yra 2 kartos $K_{M\text{-}VU}$.

Tokiu atveju 2–5 etapuose bus atlikti tokie veiksmai:

— 2 etapas. Transporto priemonės blokas iš dirbtuvių kortelės nuskaito 2 ir 3 kartos $K_{M\text{-}WC}$ ir patikrina jų versijos numerius;

— 3 etapas. Transporto priemonės blokas, naudodamas 2 kartos $K_{M\text{-}WC}$ ir savo $K_{M\text{-}VU}$, apskaičiuoja K_M ir K_{ID};

— 4 etapas. Transporto priemonės blokas, naudodamas K_{ID}, užšifruoja iš judesio jutiklio gautą serijos numerį;

— 5 etapas. Judesio jutiklis gautus duomenis palygina su $N_s[1]$ ir neranda atitikmens. Tada jis šiuos duomenis palygina su $N_s[2]$ ir randa atitikmenį. Judesio jutiklis padaro išvadą, kad transporto priemonės blokas yra 2 kartos, todėl atgal perduoda $K_P[2]$.

([1]) Įstačius kortelę, suaktyvinamos reikiamos teisės atlikti duomenų perkėlimą ir gauti prieigą prie jų. Vis dėlto turi būti įmanoma duomenis iš vairuotojo kortelės, įstatytos į vieną iš transporto priemonės bloko lizdų, perkelti net jei į kitą lizdą neįstatyta jokia kito tipo kortelė.

▼B

12.3. **Transporto priemonės bloko ir judesio jutiklio siejimas ir ryšys taikant AES**

CSM_218 Kaip nurodyta 9.2.1 skirsnyje pateiktoje 3 lentelėje, visi siejant transporto priemonės bloką ir judesio jutiklį ir vėliau palaikant ryšį naudojami raktai turi būti AES raktai, o ne dvigubo ilgio TDES raktai, kaip nustatyta standarte [ISO 16844-3]. Šie AES raktai gali būti 128, 192 arba 256 bitų ilgio. Kadangi AES bloko dydis yra 16 baitų, užšifruoto pranešimo ilgis turi būti 16 baitų – o ne 8 baitų, kaip TDES atveju – kartotinis. Be to, kai kurie iš šių pranešimų bus naudojami AES raktams, kurių ilgis gali būti 128, 192 arba 256 bitai, perduoti. Todėl standarto [ISO 16844-3] 5 lentelėje nurodytas komandos baitų skaičius pakeičiamas taip, kaip nurodyta 6 lentelėje:

6 lentelė.

Standarte [ISO 16844-3] nustatytas vienai komandai naudojamas grynojo teksto ir užšifruotų duomenų baitų skaičius

Komanda	Užklausa / atsakas	Duomenų aprašas	Grynojo teksto duomenų baitų kiekis pagal [ISO 16844-3]	Grynojo teksto duomenų baitų kiekis naudojant AES raktus	Užšifruotų duomenų baitų kiekis naudojant AES raktus, kurių ilgis bitais yra:		
					128	192	256
10	Užklausa	Autentiškumo tikrinimo duomenys ir rinkmenos numeris	8	8	16	16	16
11	Atsakas	Autentiškumo tikrinimo duomenys ir rinkmenos turinys	16 arba 32, atsižvelgiant į rinkmeną	16 arba 32, atsižvelgiant į rinkmeną	16 arba 32	16 arba 32	16 arba 32
41	Užklausa	Judesio jutiklio serijos numeris	8	8	16	16	16
41	Atsakas	Siejimo raktas	16	16 arba 24, arba 32	16	32	32
42	Užklausa	Seanso raktas	16	16 arba 24, arba 32	16	32	32
43	Užklausa	Siejimo informacija	24	24	32	32	32
50	Atsakas	Siejimo informacija	24	24	32	32	32
70	Užklausa	Autentiškumo tikrinimo duomenys	8	8	16	16	16
80	Atsakas	Judesio jutiklio skaitiklio vertė ir autentiškumo tikrinimo duomenys	8	8	16	16	16

CSM_219 Siejimo informacija, perduodama 43 komanda (transporto priemonės bloko užklausa) ir 50 komanda (judesio jutiklio atsakas), surenkama taip, kaip nurodyta standarto [ISO 16844-3] 7.6.10 skirsnyje, išskyrus tai, kad pagal siejimo duomenų šifravimo schemą vietoj TDES algoritmo naudojamas AES algoritmas, todėl gaunami du AES algoritmu užšifruotų duomenų rinkiniai ir, siekiant užtikrinti atitiktį AES bloko dydžiui, taikomas CSM_220 nustatytas užpildymas. Šio šifravimo tikslais naudojamas raktas K'_P sugeneruojamas taip:

— jei siejimo raktas K_P yra 16 baitų ilgio: $K'_P = K_P$ XOR $(N_s||N_s)$;

▼B

— jei siejimo raktas K_P yra 24 baitų ilgio: $K'_p = K_P$ XOR $(N_s||N_s||N_s)$;

— jei siejimo raktas K_P yra 32 baitų ilgio: $K'_p = K_P$ XOR $(N_s||N_s||N_s||N_s)$;

čia N_s – judesio jutiklio 8 baitų serijos numeris.

CSM_220 Jei grynojo teksto duomenų ilgis (naudojant AES raktus) nėra 16 baitų kartotinis, taikomas standarte [ISO 9797-1] nustatytas 2 užpildymo metodas.

Pastaba. Pagal standartą [ISO 16844-3] grynojo teksto baitų skaičius visada yra aštuonių kartotinis, todėl, taikant TDES, užpildymas nebūtinas. Standarte [ISO 16844-3] pateikta duomenų ir pranešimų apibrėžtis šioje priedėlio dalyje nekeičiama, todėl būtina taikyti užpildymą.

CSM_221 Jei taikoma 11 komanda ir jei būtina užšifruoti daugiau daugiau kaip vieną duomenų bloką, taikomas standarte [ISO 10116] nustatytas nuosekliojo blokinio šifravimo režimas, naudojant kaitaliojimo parametrą *m* = 1. Naudojamas toks IV:

— taikant 11 komandą: standarto [ISO 16844-3] 7.6.3.3 skirsnyje nustatytas 8 baitų autentiškumo tikrinimo blokas, užpildytas standarte [ISO 9797-1] nustatytu 2 užpildymo metodu; taip pat žr. standarto [ISO 16844-3] 7.6.5 ir 7.6.6 skirsnius;

— visų kitų komandų atveju, kai perduodama daugiau kaip 16 baitų, kaip nurodyta 6 lentelėje: ‘00’ {16}, t. y. šešiolika baitų, kurių dvejetainė vertė lygi 0.

Pastaba. Kaip nurodyta standarto [ISO 16844-3] 7.6.5 ir 7.6.6 skirsniuose, kai judesio jutiklis užšifruoja duomenų rinkmenas, skirtas įtraukti į 11 komandą, autentiškumo tikrinimo blokas:

— naudojamas kaip duomenų rinkmenų šifravimo CBC režimu inicializacijos vektorius ir

— užšifruojamas ir įtraukiamas kaip pirmasis duomenų, kurie perduodami transporto priemonės blokui, blokas.

12.4. **Transporto priemonės bloko ir judesio jutiklio siejimas naudojant skirtingų kartų įrangą**

CSM_222 Kaip paaiškinta 9.2.1 skirsnyje, antrosios kartos judesio jutiklyje gali būti pagal TDES algoritmą užšifruotų siejimo duomenų (kaip nustatyta šio priedėlio A dalyje), suteikiančių galimybę judesio jutiklį susieti su pirmosios kartos transporto priemonės bloku. Tokiu atveju pirmosios kartos transporto priemonės blokas ir antrosios kartos judesio jutiklis siejami taip, kaip aprašyta šio priedėlio A dalyje ir standarte [ISO 16844-3]. Jiems susieti gali būti naudojama pirmosios arba antrosios kartos dirbtuvių kortelė.

Pastabos

— Antrosios kartos transporto priemonės bloko negalima sieti su pirmosios kartos judesio jutikliu.

▼B

— Antrosios kartos transporto priemonės blokui su judesio jutikliu sujungti negalima naudoti pirmosios kartos dirbtuvių kortelės.

13. DSRC PAGRĮSTO NUOTOLINIO RYŠIO SAUGUMAS

13.1. **Bendrosios nuostatos**

Kaip nustatyta 14 priedėlyje, transporto priemonės blokas reguliariai sugeneruoja nuotolinės tachografo kontrolės (RTM) duomenis ir juos persiunčia (vidiniam arba išoriniam) nuotolinio ryšio įrenginiui (RCF). Nuotolinio ryšio įrenginio paskirtis – naudojant 14 priedėlyje aprašytą DSRC sąsają persiųsti šiuos duomenis nuotoliniam užklausikliui. 1 priedėlyje nustatyta, kad RTM duomenis sudaro šie sujungti duomenys:

užšifruotas informacinis tachografo turinys, t. y. užšifruotas tachografo grynojo teksto turinys,

DSRC apsaugos duomeny, aprašyti toliau.

Tachografo grynojo teksto turinio duomenų formatas nustatytas 1 priedėlyje ir išsamiau aprašytas 14 priedėlyje. Šiame skirsnyje aprašoma DSRC apsaugos duomenų struktūra; oficiali specifikacija pateikta 1 priedėlyje.

CSM_223 Grynojo teksto `tachographPayload`duomenys, kuriuos transporto priemonės blokas perduoda nuotolinio ryšio įrenginiui (jei transporto priemonės bloko atžvilgiu RCF yra išorinis) arba kuriuos transporto priemonės blokas per DSRC sąsają perduoda nuotoliniam užklausikliui (jei transporto priemonės bloko atžvilgiu RCF yra vidinis), apsaugomi taikant užšifravimo ir autentiškumo tikrinimo režimą, t. y. pirma užšifruojami tachografo informacinio turinio duomenys, kad būtų užtikrintas pranešimo konfidencialumas, o tada apskaičiuojamas MAC, kad būtų užtikrintas duomenų autentiškumas ir nepažeistumas.

CSM_224 DSRC apsaugos duomenis sudaro toliau nurodyta tvarka sujungti tokie duomenų elementai (taip pat žr. 12 paveikslą):

dabartinė data ir laikas:	transporto priemonės bloko rodoma data ir laikas (duomenų tipas – `TimeReal`);
skaitiklis:	3 baitų skaitiklis, žr. CSM_225 punktą;
transporto priemonės bloko serijos numeris:	transporto priemonės bloko serijos numeris (duomenų tipas – VuSerialNumber `VuSerialNumber`);
DSRC pagrindinio rakto versijos numeris:	1 baito DSRC pagrindinio rakto, kuriuo remiantis buvo apskaičiuoti konkrečiam transporto priemonės blokui skirti DSRC raktai, versijos numeris, žr. 9.2.2 skirsnį;
MAC:	MAC, apskaičiuotas remiantis visais ankstesniais RTM duomenų baitais.

CSM_225 3 baitų DSRC apsaugos duomenų skaitiklio formatas turi būti „MSB-first“. Transporto priemonės blokas, pirmą kartą skaičiuodamas RTM duomenų rinkinį, kai jis buvo pradėtas naudoti, nustato skaitiklio vertę, lygią 0. Prieš pradėdamas skaičiuoti kitą RTM duomenų rinkinį, transporto priemonės blokas skaitiklio duomenų vertę kaskart padidina vienetu.

▼B

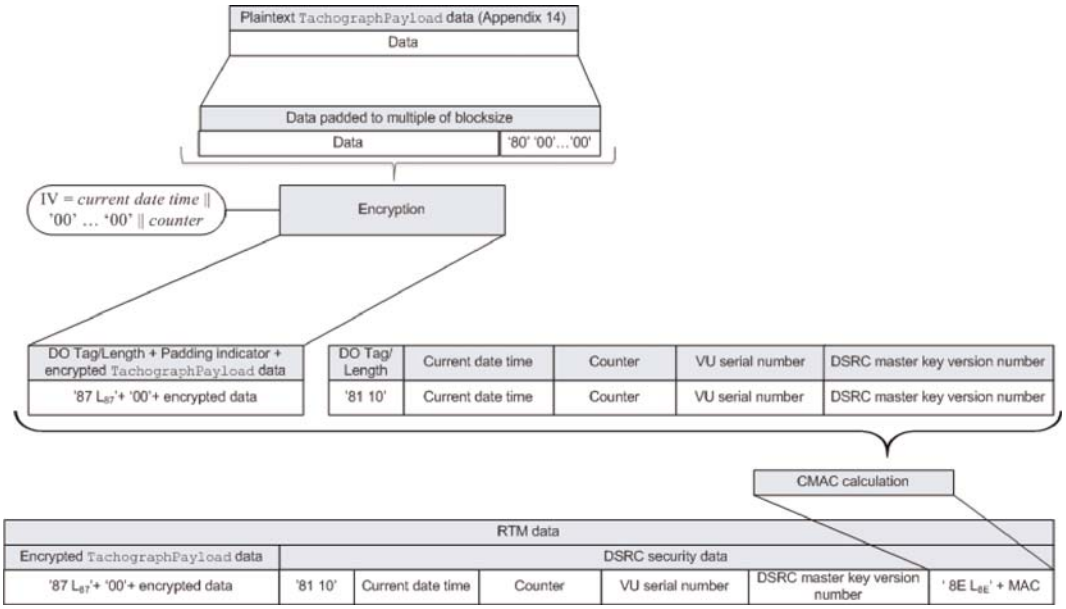
13.2. **Tachografo informacinio turinio užšifravimas ir MAC generavimas**

CSM_226 Gavęs grynojo teksto duomenų elementą, kurio duomenų tipas – `TachographPayload`, kaip aprašyta 14 priedėlyje, transporto priemonės blokas užšifruoja šiuos duomenis, kaip parodyta 12 paveiksle: nuosekliojo blokinio šifravimo (CBC) režimu taikant AES algoritmą, kaip apibrėžta standarte [ISO 10116], ir naudojant kaitaliojimo parametrą m = 1, raktui $K_VU_{DSRC}_ENC$ užšifruoti (žr. 9.2.2 skirsnį) naudojamas transporto priemonės bloko DSRC raktas. Inicializacijos vektorius turi būti lygus *IV = dabartinė data ir laikas* || *'00 00 00 00 00 00 00 00'* || *skaitiklis*; čia *dabartinė data ir laikas* ir *skaitiklis* yra tokie, kaip nustatyta CSM_224 punkte. Užšifruotini duomenys užpildomi standarte [ISO 9797-1] nustatytu 2 užpildymo metodu.

CSM_227 Transporto priemonės blokas apskaičiuoja DSRC apsaugos duomenų MAC, kaip parodyta 12 paveiksle: MAC apskaičiuojamas remiantis visais pirmesniais RTM duomenų baitais iki DSRC pagrindinio rakto versijos numerio (imtinai), taip pat įtraukiant duomenų objektų žymenas ir ilgius. Autentiškumo tikrinimo raktui $K_VU_{DSRC}_MAC$ (žr. 9.2.2 skirsnį) apskaičiuoti transporto priemonės blokas naudoja savo DSRC raktą, CMAC režimu taikydamas AES algoritmą, kaip nustatyta [SP 800-38B]. MAC ilgis susiejamas su konkrečiam transporto priemonės blokui skirtų DSRC raktų ilgiu, nustatytu CSM_50 punkte.

12 pav.

Tachografo informacinio turinio užšifravimas ir MAC generavimas



13.3. **Tachografo informacinio turinio tikrinimas ir iššifravimas**

CSM_228 Nuotolinis užklausiklis, iš transporto priemonės bloko gavęs RTM duomenis, visus juos perduoda kontrolės kortelei komandos PROCESS DSRC MESSAGE duomenų lauke, kaip aprašyta 2 priedėlyje. Tada:

▼B

1. kontrolės kortelė patikrina DRSC apsaugos duomenyse nurodytą DSRC pagrindinio rakto versijos numerį. Jei kontrolės kortelė neatpažįsta nurodyto DRSC pagrindinio rakto, ji praneša apie 2 priedėlyje nurodytą klaidą ir nutraukia procesą;

2. kontrolės kortelė, naudodama nurodytąjį DSRC pagrindinį raktą ir DSRC apsaugos duomenyse nurodytą transporto priemonės bloko serijos numerį, apskaičiuoja konkrečiam transporto priemonės blokui skirtus DSRC raktus $K_VU_{DSRC}_ENC$ ir $K_VU_{DSRC}_MAC$, kaip nurodyta CSM_124 punkte;

3. kontrolės kortelė, naudodama K_VUDSRC_MAC, patikrina DRSC apsaugos duomenyse nurodytą MAC, kaip nurodyta CSM_227 punkte. Jei MAC neteisingas, kontrolės kortelė praneša apie 2 priedėlyje nurodytą klaidą ir nutraukia procesą;

4. kontrolės kortelė, naudodama $K_VU_{DSRC}_ENC$, iššifruoja užšifruotą tachografo informacinį turinį, kaip nurodyta CSM_226 punkte. Kontrolės kortelė pašalina užpildą ir iššifruotus tachografo informacinio turinio duomenis pateikia nuotoliniam užklausikliui.

CSM_229 Siekdamas išvengti pakartojimo atakų, nuotolinis užklausiklis patikrina RTM duomenų aktualumą patikrindamas, ar DSRC apsaugos duomenyse nurodyta *dabartinė data ir laikas* pernelyg nesiskiria nuo nuotolinio užklausiklio dabartinio laiko.

Pastabos

— Tam reikia, kad nuotolinis užklausiklis turėtų tikslų ir patikimą laiko šaltinį.

— Kadangi 14 priedėlyje reikalaujama, kad transporto priemonės blokas kas 60 sekundžių apskaičiuotų naują RTM duomenų rinkinį, ir leidžiama, kad transporto priemonės bloko laikrodis viena minute nukryptų nuo tikrojo laiko, apatinė RTM laiko duomenų naujumo riba yra dvi minutės. Faktiškai reikalaujamas naujumas priklauso nuo nuotolinio užklausiklio laikrodžio tikslumo.

CSM_230 Dirbtuvėse patikrinus, ar tinkamai veikia transporto priemonės bloko DSRC funkcija, visi iš transporto priemonės bloko gauti RTM duomenys komandos PROCESS DSRC MESSAGE duomenų lauke perduodami į dirbtuvių kortelę, kaip aprašyta 2 priedėlyje. Dirbtuvių kortelė atlieka visas patikras ir veiksmus, nurodytus CSM_228 punkte.

14. PERKELIAMŲ DUOMENŲ PASIRAŠYMAS IR PARAŠŲ TIKRINIMAS

14.1. **Bendrosios nuostatos**

CSM_231 Specializuota įranga su mikroprocesoriumi (IDE) vieno duomenų perkėlimo seanso metu iš transporto priemonės bloko arba kortelės gautus duomenis išsaugo vienoje fizinėje duomenų rinkmenoje. Duomenys gali būti saugomi išorinėje laikmenoje (ESM). Šioje rinkmenoje yra skaitmeniniai duomenų blokų parašai, nustatyti 7 priedėlyje. Be to, šioje rinkmenoje yra tokie pažymėjimai (žr. 9.1 skirsnį):

▼B

— jei perkeliami transporto priemonės bloko duomenys:

— VU_Sign pažymėjimas;

— MSCA_VU-EGF pažymėjimas su viešuoju raktu, skirtu VU_Sign pažymėjimui patikrinti;

— jei perkeliami kortelės duomenys:

— Card_Sign pažymėjimas;

— MSCA_Card pažymėjimas su viešuoju raktu, skirtu Card_Sign pažymėjimui patikrinti;

CSM_232 Specializuotoje įrangoje su mikroprocesoriumi taip pat turi būti:

— jei parašui patikrinti naudojama kontrolės kortelė, kaip nurodyta 13 paveiksle: sąsajos pažymėjimas, kuriuo naujausias EUR pažymėjimas susiejamas su EUR pažymėjimu, kurio galiojimo laikotarpis yra prieš pat naujausio EUR pažymėjimo galiojimo laikotarpį, jei toks pažymėjimas yra;

— jei ji tikrina parašą pati: visi galiojantys Europos pagrindiniai pažymėjimai.

Pastaba. Metodas, kurį IDE taiko šiems pažymėjimams išrinkti, šiame priedėlyje nenurodomas.

14.2. **Parašo generavimas**

CSM_233 Perkeltų duomenų skaitmeniniams parašams kurti taikomas ECDSA pasirašymo algoritmas, nurodytas [DSS], naudojant maišos algoritmą, susietą su transporto priemonės bloko arba kortelės rakto dydžiu, nustatytu CSM_50 punkte. Parašo formatas turi būti paprastas, kaip nurodyta [TR-03111].

14.3. **Parašo tikrinimas**

CSM_234 Perkeltų duomenų parašą tikrinimą IDE gali atlikti pati arba naudodama kontrolės kortelę. Jei IDE naudoja kontrolės kortelę, parašas tikrinamas taip, kaip nurodyta 13 paveiksle. Jei IDE parašą tikrina pati, patikrinamas visų duomenų rinkmenos pažymėjimų sekai priklausančių pažymėjimų autentiškumas ir galiojimas ir pagal [DSS] nustatytą schemą patikrinamas duomenų parašas.

Pastabos dėl 13 paveikslo

— Duomenims, kurie bus analizuojami, pasirašyti naudota įranga žymima EQT.

— Paveiksle nurodyti EQT pažymėjimai ir viešieji raktai, pvz., VU_Sign arba Card_Sign, yra skirti pasirašyti.

— Paveiksle nurodyti EQT.CA pažymėjimai ir viešieji raktai yra skirti transporto priemonės bloko ir kortelės pažymėjimams pasirašyti, jei taikytina.

— Paveiksle nurodytas EQT.CA.EUR pažymėjimas yra EQT.CA pažymėjimo CAR nurodytas Europos pagrindinis pažymėjimas.

▼B

— Paveiksle nurodytas EQT.Link pažymėjimas yra EQT sąsajos pažymėjimas, jei toks yra. Kaip nurodyta 9.1.2 skirsnyje, tai sąsajos pažymėjimas, skirtas ERCA sukurtai ir naudojant ankstesnį Europos privatųjį raktą pasirašytai naujai Europos pagrindinei raktų porai.

— EQT.Link.EUR pažymėjimas yra EQT.Link pažymėjimo CAR nurodytas Europos pagrindinis pažymėjimas.

CSM_235 Maišos vertei M, kuri perduodama kontrolės kortelei taikant komandą *PSO:Hash*, apskaičiuoti IDE taiko maišos algoritmą, susietą su transporto priemonės bloko arba kortelės, iš kurių perkeliami duomenys, raktų dydžiu, nustatytu CSM_50 punkte.

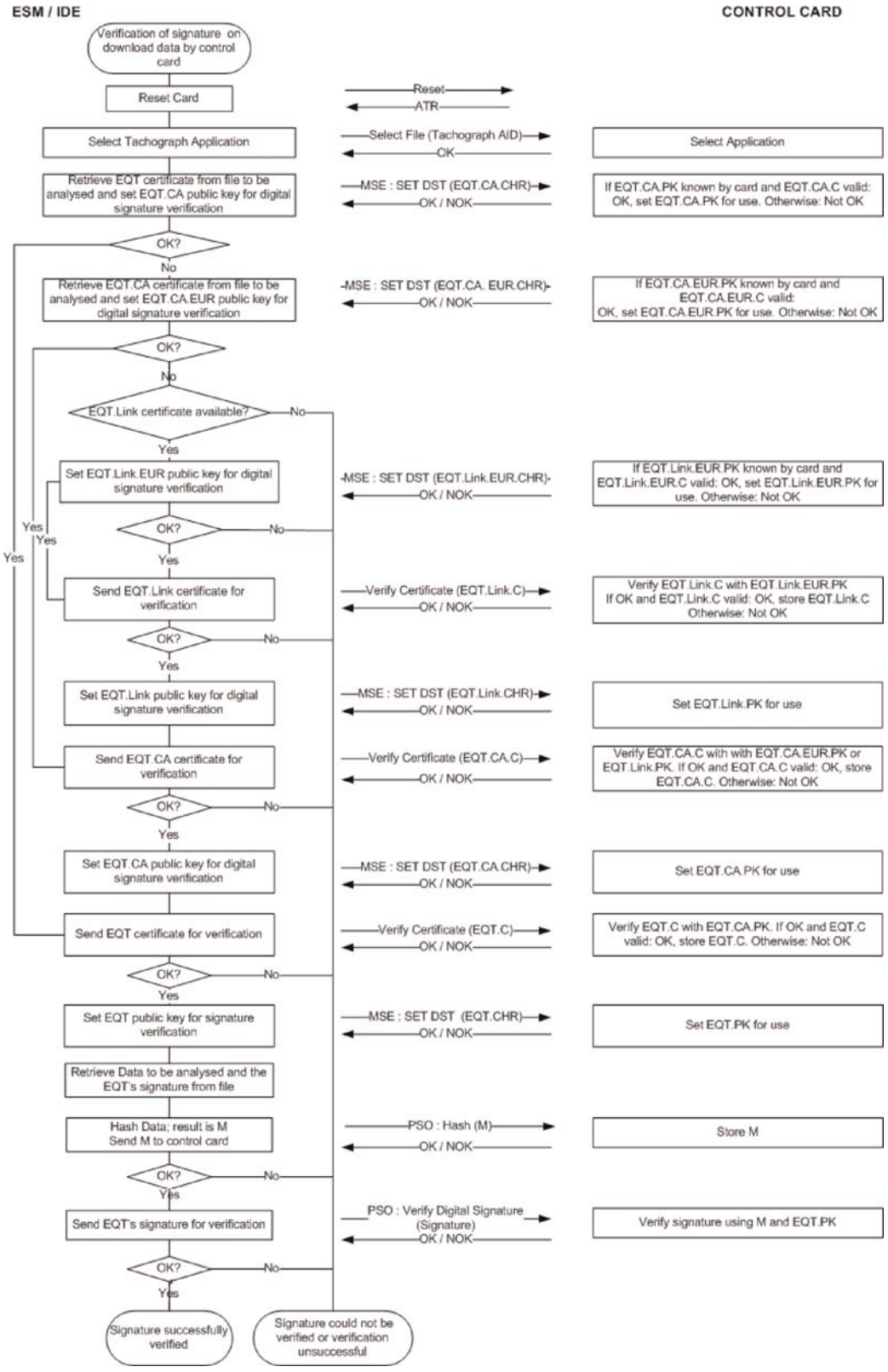
CSM_236 EQT parašą kontrolės kortelė tikrina pagal [DSS] nustatytą parašo schemą.

Pastaba. Šiame dokumente nenustatoma jokių veiksmų, kurių turėtų būti imamasi, kai negalima patikrinti perkeltų duomenų parašo arba kai patikrinimas yra nesėkmingas.

▼B

13 pav.

Perkeltų duomenų rinkmenos parašo tikrinimo protokolas



▼B

12 priedėlis

BUVIMO VIETOS NUSTATYMAS NAUDOJANTIS PASAULINE PALYDOVINĖS NAVIGACIJOS SISTEMA (GNSS)

TURINYS

1. ĮVADAS

1.1. Taikymo sritis

1.2. Santrumpos ir žymenys

2. GNSS IMTUVO SPECIFIKACIJA

3. NMEA SAKINIAI

4. TRANSPORTO PRIEMONĖS BLOKAS SU IŠORINIU GNSS ĮRENGINIU

4.1. Konfigūracija

4.1.1 Pagrindiniai komponentai ir sąsajos

4.1.2 Baigto gaminti išorinio GNSS įrenginio būklė

4.2. Išorinio GNSS įrenginio ir transporto priemonės bloko ryšys

4.2.1 Ryšio protokolas

4.2.2 Saugus GNSS duomenų perdavimas

4.2.3 Įrašo nuskaitymo komandos struktūra

4.3. GNSS įrenginio ir transporto priemonės bloko sujungimas, abipusis autentiškumo tikrinimas ir seanso raktų derinimas

4.4. Klaidų valdymas

4.4.1 Ryšio su išoriniu GNSS įrenginiu klaida

4.4.2 Išorinio GNSS įrenginio fizinio vientisumo pažeidimas

4.4.3 Iš GNSS imtuvo negaunama buvimo vietos nustatymo informacijos

4.4.4 Baigėsi išorinio GNSS įrenginio pažymėjimo galiojimas

5. TRANSPORTO PRIEMONĖS BLOKAS BE IŠORINIO GNSS ĮRENGINIO

5.1. Konfigūracija

5.2. Klaidų valdymas

5.2.1 Iš GNSS imtuvo negaunama buvimo vietos nustatymo informacijos

6. SU GNSS LAIKU NESUDERINTAS LAIKAS

7. TRANSPORTO PRIEMONĖS JUDĖJIMO NESUDERINAMUMAS

1. ĮVADAS

Šiame priedėlyje nustatomi transporto priemonės bloko naudojamiems GNSS duomenims keliami techniniai reikalavimai, įskaitant protokolus, kurie turi būti įdiegti siekiant užtikrinti saugų ir tinkamą buvimo vietos nustatymo informacijos perdavimą.

Pagrindiniai Reglamento (ES) Nr. 165/2014 straipsniai, kuriais remiantis nustatomi šie reikalavimai, yra: 8 straipsnis „Transporto priemonės pozicijos tam tikruose taškuose registravimas kasdienio darbo laiko metu“, 10 straipsnis „Sąsaja su intelektinėmis transporto sistemomis“ ir 11 straipsnis „Išsamios nuostatos, susijusios su išmaniaisiais tachografais“.

▼B

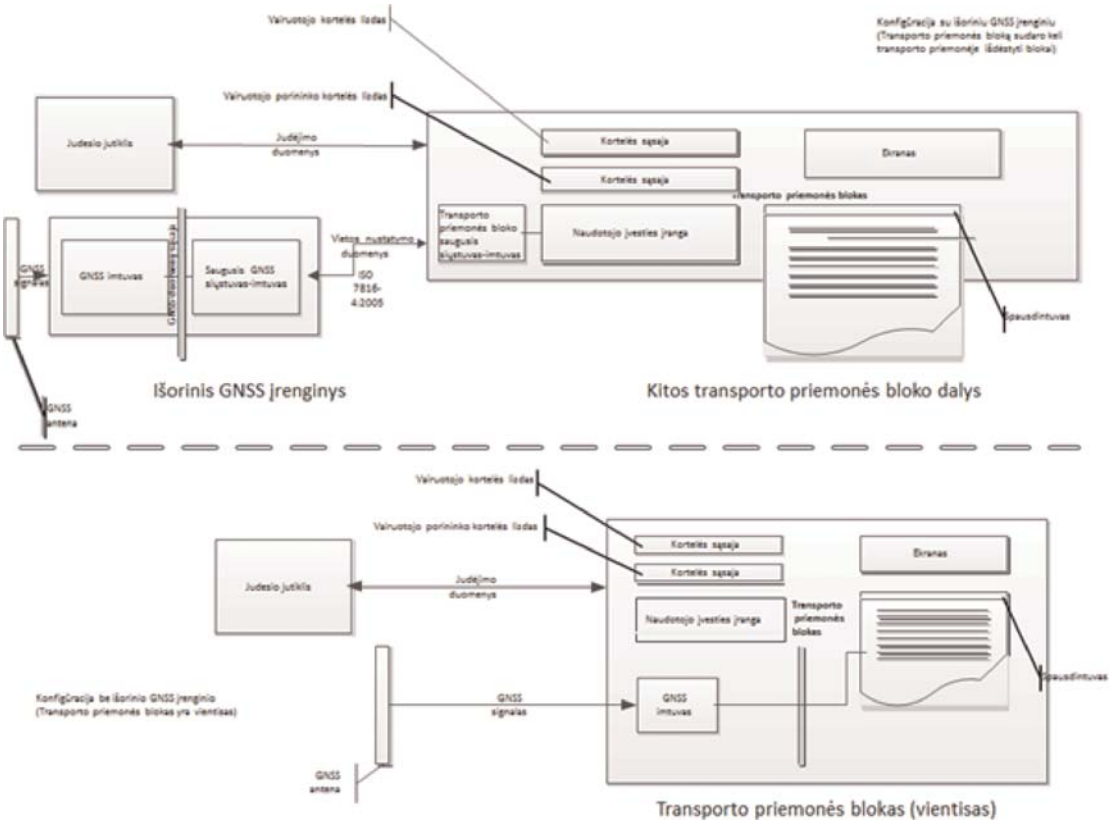
1.1. **Taikymo sritis**

GNS_1 Siekiant padėti įgyvendinti 8 straipsnį, transporto priemonės bloke bent iš vienos GNSS renkami vietos nustatymo duomenys.

Išorinis GNSS įrenginys gali būti sumontuotas transporto priemonės bloke arba jo gali nebūti, kaip parodyta 1 paveiksle.

1 pav

Įvairios GNSS imtuvo konfigūracijos



1.2. **Santrumpos ir žymenys**

Šiame priedėlyje vartojamos santrumpos

DOP tikslumo paklaida

EGF elementariojo failo GNSS įrenginys

EGNOS Europos geostacionarinė navigacinė tinklo sistema

GNSS Pasaulinė palydovinės navigacijos sistema

GSA GPS DOP ir veikiantys palydovai

HDOP horizontaliojo tikslumo paklaida

ICD sąsajos kontrolės dokumentas

NMEA Nacionalinė laivų elektroninės įrangos asociacija

▼B

PDOP buvimo vietos tikslumo paklaida

RMC rekomenduojamas mažiausias specifinis

SIS signalas erdvėje

VDOP vertikaliojo tikslumo paklaida

VU transporto priemonės blokas

2. GNSS IMTUVO SPECIFIKACIJA

Kad ir kokia būtų išmaniojo tachografo konfigūracija – su išoriniu GNSS įrenginiu ar be jo, tikslios ir patikimos buvimo vietos nustatymo informacijos teikimas yra labai svarbus išmaniojo tachografo veiksmingo veikimo aspektas. Todėl tikslinga reikalauti, kad ši įranga būtų suderinama su paslaugomis, kurias teikia GALILEO ir Europos geostacionarinė navigacinė tinklo sistema (EGNOS), kaip nustatyta Europos Parlamento ir Tarybos reglamente (ES) Nr. 1285/2013 ([1]). Pagal programą GALILEO sukurta sistema – tai autonominė pasaulinės palydovinės navigacijos sistema, o pagal programą EGNOS sukurta sistema – tai regioninės palydovinės navigacijos sistema, kurią naudojant pagerinama globalinės padėties nustatymo sistemos signalo kokybė.

GNS_2 Gamintojai užtikrina, kad išmaniuosiuose tachografuose montuojami GNSS imtuvai būtų suderinami su buvimo vietos nustatymo paslaugomis, kurias teikia GALILEO ir EGNOS sistemos. Gamintojai taip pat gali nuspręsti papildomai užtikrinti suderinamumą su kitomis palydovinės navigacijos sistemomis.

GNS_3 GNSS imtuvas turi būti suderinamas su autentiškumo tikrinimu naudojantis GALILEO atvirąja paslauga, jei tokią paslaugą teiks GALILEO sistema ir palaikys GNSS imtuvų gamintojai. Tačiau nebus reikalaujama modernizuoti išmaniųjų tachografų, kurie rinkoje bus pasiūlyti anksčiau, nei bus įvykdytos minėtos salygos, ir nebus suderinami su autentiškumo tikrinimu naudojantis GALILEO atvirąja paslauga.

3. NMEA SAKINIAI

Šiame skirsnyje aprašyti NMEA sakiniai, naudojami išmaniojo tachografo veikimui užtikrinti. Šis skirsnis taikytinas ir išmaniesiems tachografams su išoriniu GNSS įrenginiu, ir išmaniesiems tachografams be tokio įrenginio.

GNS_4 Vietos nustatymo duomenys gaunami naudojant NMEA sakinį *Recommended Minimum Specific (RMC) GNSS Data*, juos sudaro buvimo vietos informacija (platuma, ilguma), suderintasis pasaulinis laikas (hhmmss.ss), mazgais išreikštas greitis ant žemės ir papildomos reikšmės.

RMC sakinio formatas yra toks (nuo tada, kai buvo patvirtinta NMEA standarto 4.1 versija):

([1]) 2013 m. gruodžio 11 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1285/2013 dėl Europos palydovinės navigacijos sistemų įdiegimo ir eksploatavimo, kuriuo panaikinamas Tarybos reglamentas (EB) Nr. 876/2002 ir Europos Parlamento ir Tarybos reglamentas (EB) Nr. 683/2008 (OL L 347, 2013 12 20, p. 1).

▼B

2 pav

RMC sakinio struktūra



1) Laikas (UTC)
2) Būsena, A = patvirtinta buvimo vieta, V = perspėjimas
3) Platuma
4) Š arba P
5) Ilguma
6) R arba V
7) Greitis ant žemės mazgais
8) Tikrasis kursas, laipsniai
9) Data, ddmmyy
10) Magnetinė deklinacija, laipsniai
11) R arba V
12) Kontrolinė suma

Būsena rodo, ar gaunamas GNSS signalas. Kol nenustatoma būsenos vertė A, gaunami duomenys (pvz., apie laiką arba ilgumą ir platumą) negali būti naudojami transporto priemonės buvimo vietai registruoti transporto priemonės bloke.

Buvimo vietos tikslumas priklauso nuo pirmiau aprašyto RMC sakinio formato 3 ir 5 laukelių pirmoji dalis (pirmieji du skaitmenys) skirta laipsniams nurodyti. Likusioji dalis skirta minutėms nurodyti tūkstantųjų tikslumu. Taigi tikslumas yra 1/1 000 minutės arba 1/60 000 laipsnio (nes viena minutė yra 1/60 laipsnio).

GNS_5 Transporto priemonės blokas transporto priemonės bloko duomenų bazėje buvimo vietos nustatymo informaciją – ilgumą ir platumą – išsaugo 1/10 minutės arba 1/600 laipsnio tikslumu, kaip aprašyta 1 priedėlyje, skirtame tipui *GeoCoordinates*.

Signalo buvimui ir tikslumui nustatyti transporto priemonės blokas gali naudoti komandą *GPS DOP and active satellites (GSA)*. Pirmiausia, norint nurodyti užregistruotų vietos nustatymo duomenų tikslumą, gali būti naudojama HDOP (žr. 4.2.2 punktą). Transporto priemonės blokas išsaugos horizontaliojo tikslumo paklaidos (HDOP) vertę, kuri apskaičiuojama kaip mažiausioji HDOP vertė iš verčių, gautų iš pasiekiamų GNSS sistemų.

Laukelyje *GNSS System Id* nurodoma GPS, GLONASS, GALILEO, „BeiDou“ arba palydovinė signalų tikslinimo sistema (angl. *Satellite-Based Augmentation System*, SBAS).

3 pav

GSA sakinio struktūra



1) Parinkties režimas
2) Režimas
3) 1-ojo palydovo, naudojamo buvimo vietai nustatyti, identifikatorius
4) 2-ojo palydovo, naudojamo buvimo vietai nustatyti, identifikatorius
...
14) 12-ojo palydovo, naudojamo buvimo vietai nustatyti, identifikatorius
15) PDOP metrais
16) HDOP metrais
17) VDOP metrais
18) GNSS sistemos identifikatorius
19) Kontrolinė suma

▼B

Šiuo atveju režimas (2) rodo, kad buvimo vietos nustatyti negalima (Mode=1) arba kad galimas 2D (Mode=2) arba 3D (Mode=3) nustatymas.

GNS_6 *GSA* sakinys išsaugomas įrašo numeriu 06.

GNS_7 Didžiausias galimas NMEA sakinių (pvz., RMC, GSA arba kitų) ilgis, kurį galima naudoti įrašo nuskaitymo komandos tikslais, yra 85 baitai (žr. 1 lentelę).

4. TRANSPORTO PRIEMONĖS BLOKAS SU IŠORINIU GNSS ĮRENGINIU

4.1. **Konfigūracija**

4.1.1 *Pagrindiniai komponentai ir sąsajos*

Tokioje konfigūracijoje GNSS imtuvas yra išorinio GNSS įrenginio dalis.

GNS_8 Išorinis GNSS įrenginys turi būti maitinamas naudojant specialią transporto priemonės sąsają.

GNS_9 Išorinį GNSS įrenginį turi sudaryti tokie komponentai (žr. 4 paveikslą):

a) Rinkoje parduodamas GNSS imtuvas, skirtas buvimo vietos nustatymo duomenims teikti per GNSS duomenų sąsają. Pavyzdžiui, GNSS duomenų sąsaja gali būti įrengta pagal NMEA standarto 4.10 versiją: GNSS imtuvas veikia kaip pranešimų šaltinis ir 1 Hz dažniu saugiajam GNSS siųstuvui-imtuvui perduoda NMEA sakinius iš parengto NMEA sakinių rinkinio, kuriame turi būti bent RMC ir GSA sakiniai. Kokią GNSS duomenų sąsają įrengti, sprendžia išorinių GNSS įrenginių gamintojai.

b) Siuntimo ir priėmimo blokas (saugusis GNSS siųstuvas-imtuvas), suderinamas su standartu ISO/IEC 7816-4:2013 (žr. 4.2.1 punktą), skirtas ryšiui su transporto priemonės bloku palaikyti ir GNSS duomenų sąsajai su GNSS imtuvu užtikrinti. Šiame bloke yra sumontuota atmintinė, skirta GNSS imtuvo ir išorinio GNSS įrenginio identifikavimo duomenims saugoti.

c) Korpuso sistema su neteisėto keitimo nustatymo funkcija, gaubianti GNSS imtuvą ir saugųjį GNSS siųstuvą-imtuvą. Diegiant neteisėto keitimo funkciją, įdiegiamos saugumo užtikrinimo priemonės, kaip reikalaujama išmaniojo tachografo apsaugos apraše.

d) Ant transporto priemonės sumontuota ir prie GNSS imtuvo per korpuso sistemą prijungta GNSS antena.

GNS_10 Išoriniame GNSS įrenginyje turi būti įrengtos bent šios išorinės sąsajos:

a) sąsaja su GNSS antena, sumontuota ant transporto priemonės arba sunkvežimio, jeigu naudojama išorinė antena;

b) sąsaja su transporto priemonės bloku.

GNS_11 Transporto priemonės bloke sumontuotas transporto priemonės bloko saugusis siųstuvas-imtuvas yra kitas saugaus ryšio su GNSS saugiuoju siųstuvu-imtuvu galinis įrenginys, kuris turi būti suderinamas su standartu ISO/IEC 7816-4:2013, kad jį būtų galima prijungti prie išorinio GNSS įrenginio.

▼B

GNS_12 Kalbant apie fizinį ryšio su išoriniu GNSS įrenginiu lygmenį, transporto priemonės blokas turi būti suderinamas su standartu ISO/IEC 7816-12:2005 arba kitu standartu, kuriuo galima užtikrinti suderinamumą su standartu ISO/IEC 7816-4:2013. (Žr. 4.2.1 punktą).

4.1.2 *Baigto gaminti išorinio GNSS įrenginio būklė*

GNS_13 Iš gamyklos išvežamo išorinio GNSS įrenginio saugiojo GNSS siųstuvo-imtuvo liekamojoje atmintinėje turi būti įrašytos tokios vertės:

— EGF_MA raktų pora ir atitinkamas pažymėjimas;

— MSCA_VU-EGF pažymėjimas su viešuoju raktu MSCA_VU-EGF.PK, skirtu EGF_MA pažymėjimui patikrinti;

— EUR pažymėjimas su viešuoju raktu EUR.PK, skirtu MSCA_VU-EGF pažymėjimui patikrinti;

— EUR pažymėjimas, kurio galiojimo laikotarpis yra prieš pat EUR pažymėjimo, skirto MSCA_VU-EGF pažymėjimui patikrinti, galiojimo laikotarpį, jei toks pažymėjimas yra;

— sąsajos pažymėjimas, kuriuo susiejami šie du EUR pažymėjimai, jeigu tokie yra;

— pailgintas išorinio GNSS įrenginio serijos numeris;

— GNSS įrenginio operacinės sistemos identifikatorius;

— išorinio GNSS įrenginio tipo patvirtinimo numeris;

— išorinio GNSS modulio apsaugos komponento identifikatorius.

4.2. **Išorinio GNSS įrenginio ir transporto priemonės bloko ryšys**

4.2.1 *Ryšio protokolas*

GNS_14 Taikant išorinio GNSS įrenginio ir transporto priemonės bloko ryšio protokolą turi būti galima atlikti šias tris funkcijas:

1. rinkti ir platinti GNSS duomenis (pvz., duomenis apie buvimo vietą, laiką, greitį);

2. rinkti išorinio GNSS įrenginio konfigūracijos duomenis;

3. naudoti valdymo protokolą siekiant užtikrinti išorinio GNSS įrenginio ir transporto priemonės bloko sujungimą, abipusį autentiškumo tikrinimą ir seanso raktų derinimą.

GNS_15 Ryšio protokolas grindžiamas standartu ISO/IEC 7816-4:2013, transporto priemonės bloko saugiajam siųstuvui-imtuvui suteikiant pagrindinį statusą, o GNSS saugiajam siųstuvui-imtuvui – pavaldųjį statusą. Fizinis išorinio GNSS įrenginio ir transporto priemonės bloko sujungimas užtikrinamas pagal standartą ISO/IEC 7816-12:2005 arba kitą standartą, kuriuo galima užtikrinti suderinamumą su standartu ISO/IEC 7816-4:2013.

▼B

GNS_16 Pagal ryšio protokolą neturi būti palaikomi didesnio ilgio laukai.

GNS_17 Standartais ISO 7816 (*-4:2013 ir *-12:2005) pagrįsto ryšio protokolo, kuriuo užtikrinamas išorinio GNSS įrenginio ryšys su transporto priemonės bloku, vertė T turi būti 1.

GNS_18 Atliekant 1) GNSS duomenų rinkimo ir platinimo 2) išorinio GNSS įrenginio konfigūracijos duomenų rinkimo ir 3) valdymo protokolo funkcijas, saugusis GNSS siųstuvas-imtuvas turi imituoti išmaniąją kortelę, kurios rinkmenų sistemos architektūra būtų sudaryta iš pagrindinės rinkmenos (MF), kataloginės rinkmenos(DF) su taikomosios programos identifikatoriumi, nurodytu 1 priedėlio 6.2skirsnyje (‘FF 44 54 45 47 4D’), ir trim elementariosiomis rinkmenomis(EF), kuriose laikomi trys pažymėjimai, ir vienos elementariosios rinkmenos (EF.EGF), kurios identifikatorius yra ‘2F2F’, kaip aprašyta 1 lentelėje.

GNS_19 Saugusis GNSS siųstuvas-imtuvas rinkmenoje EF.EGF turi išsaugoti informaciją, gaunamą iš GNSS imtuvo, ir konfigūraciją. Tai tiesinė kintamo ilgio įrašo rinkmena, kurios identifikatorius šešioliktainiu formatu yra ‘2F2F’.

GNS_20 Saugiojo GNSS siųstuvo-imtuvo atmintyje išsaugomi duomenys, kuriuos naudojant būtų galima atlikti ne mažiau kaip 20 mln. įrašymo ir nuskaitymo ciklų. Išskyrus šį aspektą, saugiojo GNSS siųstuvo-imtuvo vidaus konstrukcija ir įdiegimas paliekamas gamintojo nuožiūrai.

Įrašų numerių ir duomenų išdėstymas aprašytas 1 lentelėje. Pažymėtina, kad yra keturi GSA sakiniai, skirti keturioms palydovinėms sistemoms ir palydovinei signalų tikslinimo sistemai (SBAS).

GNS_21 Rinkmenų struktūra nurodyta 1 lentelėje. Prieigos sąlygos (ALW, NEV, SM-MAC) aprašytos 2 priedėlio 3.5 skirsnyje.

1 lentelė

Rinkmenų struktūra

		Prieigos sąlygos		
Rinkmena	Rinkmenos identifikatorius	Nuskaitymas	Atnaujinimas	Šifruota
MF	3F00			
EF.ICC	0002	ALW	NEV (transporto priemonės blokas)	Ne
DF, GNSS įrenginys	0501	ALW	NEV	Ne
EF EGF_MACertificate	C100	ALW	NEV	Ne
EF CA_Certificate	C108	ALW	NEV	Ne
EF Link_Certificate	C109	ALW	NEV	Ne
EF.EGF	2F2F	SM-MAC	NEV (transporto priemonės blokas)	Ne

▼B

Rinkmena / duomenų elementas	Įrašo Nr.	Dydis (baitais)		Numatytosios vertės
		Min.	Maks.	
MF		552	1 031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
DF, GNSS įrenginys		*612*	*1 023*	
EF EGF_MACertificate		*204*	*341*	
EGFCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF.EGF				
RMC NMEA sakinys	‘01’	85	85	
Pirmasis GSA NMEA sakinys	‘02’	85	85	
Antrasis GSA NMEA sakinys	‘03’	85	85	
Trečiasis GSA NMEA sakinys	‘04’	85	85	
Ketvirtasis GSA NMEA sakinys	‘05’	85	85	
Penktasis GSA NMEA sakinys	‘06’	85	85	
Išorinio GNSS įrenginio pailgintas serijos numeris, 1 priedėlyje apibrėžt as kaip „SensorGNSSSerialNumber“.	‘07’	8	8	
Saugiojo GNSS siųstuvo-imtuvo operacinės sistemos identifikatorius, 1 priedėlyje apibrėžtas kaip „SensorOSIdentifier“.	‘08’	2	2	
Išorinio GNSS įrenginio tipo patvirtinimo numeris, 1 priedėlyje apibrėžtas kaip „SensorExternalGNSSApprovalNumber“.	‘09’	16	16	
Išorinio GNSS įrenginio apsaugos komponento identifikatorius, 1 priedėlyje apibrėžtas kaip „SensorExternalGNSSSCIdentifier“.	‘10’	8	8	
Rezervuota panaudoti vėliau	Nuo ‘11’ iki ‘FD’			

4.2.2 *Saugus GNSS duomenų perdavimas*

GNS_22 Saugus GNSS nustatytos buvimo vietos duomenų perdavimas leidžiamas tik įvykdžius šias sąlygas:

1. Baigtas sujungimo procesas, kaip aprašyta 11 priedėlyje „Bendrieji apsaugos mechanizmai“.

▼B

2. Nurodytu dažnumu atliktas transporto priemonės bloko ir išorinio GNSS įrenginio periodinis abipusis autentiškumo tikrinimas ir seanso raktų derinimas, kaip aprašyta 11 priedėlyje „Bendrieji apsaugos mechanizmai“.

GNS_23 Kas T sekundžių (T vertė ne didesnė kaip 10), išskyrus atvejus, kai atliekamas sujungimas arba abipusis autentiškumo tikrinimas ir seanso raktų derinimas, transporto priemonės blokas išoriniam GNSS įrenginiui toliau išdėstyta seka pateikia buvimo vietos nustatymo informacijos užklausą.

1. Transporto priemonės blokas išoriniam GNSS įrenginiui pateikia vietos nustatymo duomenų ir tikslumo paklaidos duomenų užklausą (GSA NMEA sakinio pagrindu). Transporto priemonės bloko saugusis siųstuvas-imtuvas 11 priedėlio 11.5 skirsnyje aprašytu tik autentiškumo tikrinimo režimu, taikomu vykdant saugiojo keitimosi pranešimais procesą, perduoda standarte ISO/IEC 7816-4:2013 nustatytas komandas SELECT ir READ RECORD(S), nurodydamas rinkmenos identifikatorių ‘2F2F’ ir, jei tai RMC NMEA sakinys, įrašo (RECORD) numerį ‘01’, arba, jei tai GSA NMEA sakinys, įrašo numerius ‘02’, ‘03’, ‘04’, ‘05’, ‘06’.

2. Gauti naujausi vietos nustatymo duomenys išsaugomi EF, priskiriant identifikatorių ‘2F2F’ ir įtraukiant 1 lentelėje apibūdintus įrašus, kuriuos saugusis GNSS siųstuvas-imtuvas įrašo, kai iš GNSS imtuvo per GNSS duomenų sąsają ne mažesniu kaip 1 Hz dažniu gauna NMEA duomenis.

3. Saugusis GNSS siųstuvas-imtuvas, naudodamas APDU atsakymo pranešimą, 11 priedėlio 11.5 skirsnyje aprašytu tik autentiškumo tikrinimo režimu, taikomu vykdant saugiojo keitimosi pranešimais procesą, perduoda atsakymą transporto priemonės bloko saugiajam siųstuvui-imtuvui.

4. Transporto priemonės bloko saugusis siųstuvas-imtuvas patikrina gauto atsakymo autentiškumą ir vientisumą. Jei rezultatas teigiamas, vietos nustatymo duomenys per GNSS duomenų sąsają perduodami transporto priemonės bloko procesoriui.

5. Transporto priemonės bloko procesorius patikrina gautus duomenis, informaciją (pvz., apie platumą, ilgumą, laiką) paimdamas iš RMC NMEA sakinio. RMC NMEA sakinyje taip pat pateikiama informacija, ar buvimo vietos duomenys galioja. Jei jie negalioja, laikoma, kad vietos nustatymo duomenys dar neparengti ir negali būti naudojami transporto priemonės buvimo vietai registruoti. Jei buvimo vietos duomenys galioja, transporto priemonės bloko procesorius iš GSA NMEA sakinių taip pat paima HDOP vertes ir apskaičiuoja vidutinę pasiekiamų palydovinių sistemų pateikiamą vertę (t. y. kai galima nustatyti buvimo vietą).

6. Gautą ir apdorotą informaciją, pvz., informaciją apie platumą, ilgumą, laiką ir greitį, kartu su HDOP verte, apskaičiuota kaip mažiausioji iš HDOP verčių, gautų iš pasiekiamų GNSS sistemų, transporto priemonės bloko procesorius 1 priedėlyje pateiktame duomenų žinyne nustatytu formatu išsaugo transporto priemonės bloke kaip geografines koordinates (*GeoCoordinates*).

▼B

4.2.3 *Įrašo nuskaitymo komandos struktūra*

Šiame skirsnyje išsamiai aprašyta komandos *Read Record* struktūra. Pagal 11 priedėlį „Bendrieji apsaugos mechanizmai“ taip pat užtikrinamas saugusis keitimasis pranešimais (tik autentiškumo tikrinimo režimu).

GNS_24 Ši komanda turi būti suderinama su saugiajam keitimusi pranešimais taikomu tik autentiškumo tikrinimo režimu, žr. 11 priedėlį.

GNS_25 Komandos pranešimas

Baitas	Ilgis	Vertė	Aprašas
CLA	1	‘0Ch’	Prašoma saugaus keitimosi pranešimais.
INS	1	‘B2h’	Nuskaityti įrašą
P1	1	‘XXh’	Įrašo numeris (‘00’ – einamasis įrašas)
P2	1	‘04h’	Nuskaityti įrašą, kurio įrašo numeris nurodytas P1 baite
Le	1	‘XXh’	Laukiamų duomenų ilgis. Nuskaitytinų baitų skaičius

GNS_26 P1 baite nurodytas įrašas tampa einamuoju įrašu.

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

— Sėkmingai įvykdžius komandą, saugusis GNSS siųstuvas-imtuvas pateikia vertę ‘**9000**’.

— Jei einamoji rinkmena nėra susijusi su įrašu, saugusis GNSS siųstuvas-imtuvas pateikia vertę **‘6981’**.

— Jei duodant komandą nurodoma, kad P1 vertė yra ‘00’, bet einamosios EF nėra, saugusis GNSS siųstuvas-imtuvas pateikia vertę **‘6986’** (komanda neleidžiama).

— Jei nerandama įrašo, saugusis GNSS siųstuvas-imtuvas pateikia vertę **‘6A 83’**.

— Jei išorinis GNSS įrenginys nustatė, kad buvo daromas neteisėtas keitimas, jis pateikia būsenos žodžius **‘66 90’**.

GNS_27 Saugusis GNSS siųstuvas-imtuvas turi būti suderinamas su 2 priedėlyje nurodytomis 2 kartos tachografų komandomis:

Komanda	Nuoroda
Select	2 priedėlio 3.5.1 punktas
Read Binary	2 priedėlio 3.5.2 punktas
Get Challenge	2 priedėlio 3.5.4 punktas
PSO: Verify Certificate	2 priedėlio 3.5.7 punktas
External Authenticate	2 priedėlio 3.5.9 punktas
General Authenticate	2 priedėlio 3.5.10 punktas
MSE:SET	2 priedėlio 3.5.11 punktas

▼B

4.3. **GNSS įrenginio ir transporto priemonės bloko sujungimas, abipusis autentiškumo tikrinimas ir seanso raktų derinimas**

GNSS įrenginio ir transporto priemonės bloko sujungimas, abipusis autentiškumo tikrinimas ir seanso raktų derinimas aprašytas 11 priedėlio „Bendrieji apsaugos mechanizmai“ 11 skyriuje.

4.4. **Klaidų valdymas**

Šiame skirsnyje aprašyta, kaip šalinamos ir į transporto priemonės bloką įrašomos galimos išorinio GNSS įrenginio klaidos.

4.4.1 *Ryšio su išoriniu GNSS įrenginiu klaida*

GNS_28 Jei transporto priemonės blokui ilgiau kaip 20 minučių (be pertrūkio) nepavyksta užmegzti ryšio su prijungtu išoriniu GNSS įrenginiu, transporto priemonės blokas sukuria ir savo atmintyje užregistruoja *EventFaultType* tipo įvykį, priskirdamas įvykio numerį ‘53’H *External GNSS communication fault* ir dabartinio laiko žymą. Įvykis sukuriamas tik tuo atveju, jei įvykdomos šios dvi sąlygos: a) išmanusis tachografas veikia ne kalibravimo režimu ir b) transporto priemonė juda. Tokiomis aplinkybėmis ryšio klaida fiksuojama tada, kai transporto priemonės bloko saugusis siųstuvas-imtuvas negauna atsakymo pranešimo į pateiktą užklausos pranešimą, kaip aprašyta 4.2 skirsnyje.

4.4.2 *Išorinio GNSS įrenginio fizinio vientisumo pažeidimas*

GNS_29 Jei pažeidžiamas išorinis GNSS įrenginys, saugusis GNSS siųstuvas-imtuvas ištrina visus jo atmintinėje saugomus duomenis, įskaitant šifruotą informaciją. Kaip aprašyta GNS_25 ir GNS_26, transporto priemonės blokas nustato neteisėtą keitimą, jei atsako būsena yra ‘6690’. Tada transporto priemonės blokas sukuria *EventFaultType* tipo įvykį, priskirdamas įvykio numerį *‘55’H Tamper detection of GNSS*.

4.4.3 *Iš GNSS imtuvo negaunama buvimo vietos nustatymo informacijos*

GNS_30 Jei saugusis GNSS siųstuvas-imtuvas ilgiau kaip 3 valandas (be pertrūkio) negauna duomenų iš GNSS imtuvo, jis parengia atsakymo pranešimą į komandą READ RECORD, suteikdamas įrašo (RECORD) numerį ‘01’ ir sukurdamas 12 baitų duomenų lauką su vertėmis, lygiomis 0xFF. Gavęs atsakymo pranešimą su tokios vertės duomenų lauku, transporto priemonės blokas sukuria ir užregistruoja *EventFaultType* tipo įvykį, priskirdamas įvykio numerį ‘52’H *external GNSS receiver fault* ir laiko žymą, bet tik tuo atveju, jei įvykdomos šios dvi sąlygos: a) išmanusis tachografas veikia ne kalibravimo režimu ir b) transporto priemonė juda.

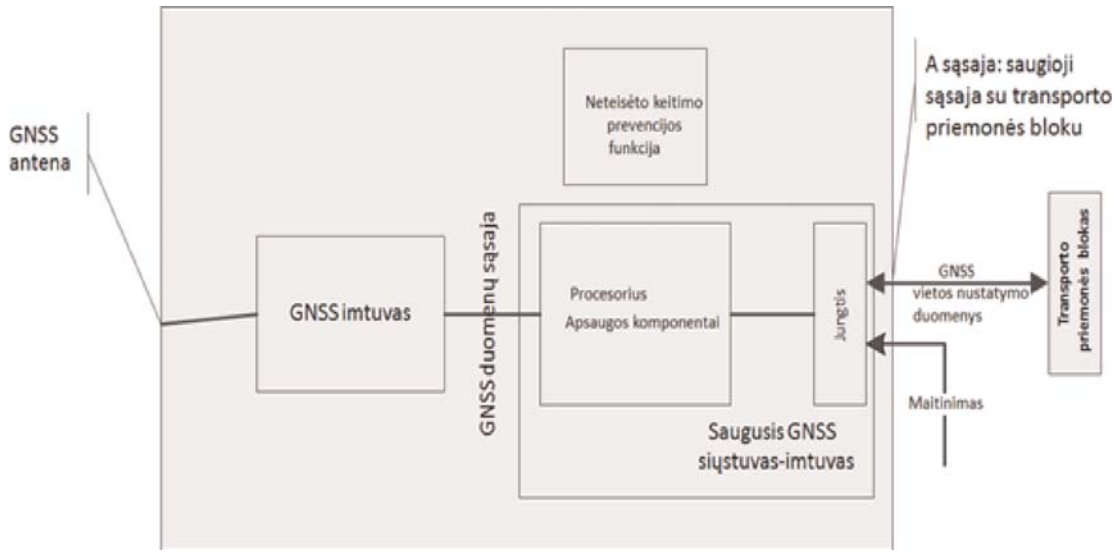
4.4.4 *Baigėsi išorinio GNSS įrenginio pažymėjimo galiojimas*

GNS_31 Jei transporto priemonės blokas nustato, kad abipusiam autentiškumo tikrinimui skirtas EGF pažymėjimas nebegalioja, jis sukuria ir užregistruoja *EventFaultType* tipo tachografo triktį, priskirdamas įvykio numerį *‘56’H External GNSS facility certificate expired* ir laiko žymą. Transporto priemonės blokas vis vien naudoja iš GNSS gautus buvimo vietos nustatymo duomenis.

▼B

4 pav

Išorinio GNSS įrenginio schema



5. TRANSPORTO PRIEMONĖS BLOKAS BE IŠORINIO GNSS ĮRENGINIO

5.1. **Konfigūracija**

Tokioje konfigūracijoje GNSS imtuvas yra transporto priemonės bloko viduje, kaip pavaizduota1 paveiksle.

GNS_32 GNSS imtuvas veikia kaip pranešimų šaltinis ir 1/10 Hz arba aukštesniu dažniu perduoda transporto priemonės bloko procesoriui (šis veikia kaip priėmimo įrenginys) NMEA sakinius iš parengto NMEA sakinių rinkinio, sudaryto bent iš RMC ir GSA sakinių.

GNS_33 Prie transporto priemonės bloko turi būti prijungta ant transporto priemonės sumontuota išorinė GNSS antena arba vidinė GNSS antena.

5.2. **Klaidų valdymas**

5.2.1 *Iš GNSS imtuvo negaunama buvimo vietos nustatymo informacijos*

GNS_34 Jei transporto priemonės blokas ilgiau kaip 3 valandas (be pertrūkio) negauna duomenų iš GNSS imtuvo, jis sukuria ir užregistruoja *EventFaultType* tipo įvykį, priskirdamas įvykio numerį ‘51’H *Internal GNSS receiver fault* ir laiko žymą, bet tik tuo atveju, jei įvykdomos šios dvi sąlygos: a) išmanusis tachografas veikia ne kalibravimo režimu ir b) transporto priemonė juda.

6. SU GNSS LAIKU NESUDERINTAS LAIKAS

Jei transporto priemonės blokas nustato, kad jo rodomas laikas daugiau kaip 1 minute skiriasi nuo GNSS imtuvo laiko, transporto priemonės blokas užregistruoja *EventFaultType* tipo įvykį, priskirdamas įvykio numerį *‘0B’H Time conflict (GNSS versus VU internal clock)*. Šis įvykis užregistruojamas kartu su transporto priemonės bloko vidinio laikrodžio rodmeniu ir atliekamas automatinis laiko koregavimas. Nustatęs, kad laikas nesuderintas, transporto priemonės blokas laiko neatitikimo netikrina 12 valandų. Tokio įvykio nefiksuojama, jei GNSS imtuvas per pastarąsias 30 dienų negavo tinkamo GNSS signalo. Tačiau, iš GNSS imtuvo vėl pradėjus gauti buvimo vietos nustatymo informaciją, turi būti atliekamas automatinis laiko koregavimas.

▼B

7. TRANSPORTO PRIEMONĖS JUDĖJIMO NESUDERINAMUMAS

GNS_35 Jei remiantis judesio jutikliu apskaičiuota informacija apie judėjimą neatitinka judėjimo informacijos, apskaičiuotos remiantis vidinio GNSS imtuvo arba išorinio GNSS įrenginio pateikta informacija, transporto priemonės blokas fiksuoja ir registruoja transporto priemonės judėjimo nesuderinamą (žr. šio priedo 84 reikalavimą), jam priskirdamas laiko žymą. Tokioms neatitiktims nustatyti naudojama šių šaltinių nurodomo greičio skirtumų medianos vertė, kaip nurodyta toliau:

— ne rečiau kaip kas 10 sekundžių apskaičiuojama transporto priemonės greičio, nustatyto remiantis GNSS informacija, ir greičio, apskaičiuoto remiantis judesio jutiklio informacija, skirtumo absoliuti vertė;

— medianos vertė apskaičiuojama iš visų verčių, apskaičiuotų per paskutines penkias judėjimo minutes;

— medianos vertė apskaičiuojama kaip 80 % verčių, likusių pašalinus didžiausias absoliučias vertes, vidurkis.

Transporto priemonės judėjimo nesuderinamumas fiksuojamas, jei per penkias transporto priemonės judėjimo minutes (be pertrūkio) medianos vertė yra didesnė kaip 10 km/h. Taip pat gali būti naudojami kiti autonominiai transporto priemonės judėjimo nustatymo šaltiniai, jei jais remiantis patikimiau nustatomas manipuliavimas tachografu. (Pastaba: per paskutiniąsias penkias minutes apskaičiuota mediana taikoma siekiant sumažinti neįprastų ir trumpalaikių verčių išmatavimo riziką.) Tokio įvyko nefiksuojama šiomis sąlygomis: a) kai keliamasi keltu arba pervežama traukiniu, b) kai iš GNSS imtuvo negaunama buvimo vietos nustatymo informacijos ir c) kai įjungtas kalibravimo režimas.

▼B

13 priedėlis

ITS SĄSAJA

TURINYS

1. ĮVADAS

2. TAIKYMO SRITIS

2.1. Santrumpos, apibrėžtys ir žymenys

3. NURODYTIEJI REGLAMENTAI IR STANDARTAI

4. SĄSAJOS VEIKIMO PRINCIPAI

4.1. Išankstinės duomenų perdavimo per ITS sąsają sąlygos

4.1.1 Duomenų perdavimas per ITS sąsają

4.1.2 Duomenų turinys

4.1.3 ITS taikomosios programos

4.2. Ryšio technologija

4.3. PIN patvirtinimas

4.4. Pranešimo formatas

4.5. Vairuotojo sutikimas

4.6. Standartinių duomenų nuskaitymas

4.7. Asmeninių duomenų nuskaitymas

4.8. Įvykių ir trikčių duomenų nuskaitymas

1. ĮVADAS

Šiame priedėlyje apibrėžiamas projektavimas ir procedūros, taikytinos diegiant sąsają su intelektinėmis transporto sistemomis (ITS) pagal Reglamento (ES) Nr. 165/2014 (toliau – *reglamentas*) 10 straipsnį.

Reglamente nustatoma, kad transporto priemonių tachografuose galima įdiegti standartines sąsajas, sudarančias galimybę tachografu užregistruotus ar sugeneruotus duomenis naudoti veikimo režimu naudojant išorinį įrenginį, jeigu laikomasi šių sąlygų:

a) sąsaja nedaro poveikio tachografo duomenų autentiškumui ir nepažeistumui;

b) sąsaja atitinka reglamento 11 straipsnyje nurodytas išsamias nuostatas;

c) su sąsaja sujungtam išoriniam įrenginiui prieiga prie asmens duomenų, įskaitant vietos nustatymo duomenis, suteikiama tik įsitikinus, kad vairuotojas, su kuriuo susiję tie duomenys, yra davęs sutikimą.

2. TAIKYMO SRITIS

Šiame priedėlyje nustatoma, kaip per „Bluetooth®“ jungtį išorinių įrenginių taikomosioms programoms galima iš tachografo perduoti duomenis (toliau – *duomenys*).

Per šią sąsają gaunami *duomenys* aprašyti šio dokumento 1 priede. Nustačius šią sąsają neužkertamas kelias įdiegti kitas sąsajas (pvz., CAN magistralę), per kurias transporto priemonės bloko duomenys būtų perduodami į kitus transporto priemonės procesorius.

▼B

Šiame priedėlyje nustatoma:

— per ITS sąsają prieinami *duomenys,*

— „Bluetooth®“ profilis, taikomas duomenims perduoti,

— užklausos bei duomenų perkėlimo procedūros ir operacijų eiliškumas,

— tachografo ir išorinio įrenginio susiejimo mechanizmas,

— sutikimo mechanizmas, kuriuo gali naudotis vairuotojas.

Pažymėtina, kad šiame priede nėra nustatoma:

— *duomenų* rinkimas ir tvarkymas transporto priemonės bloke (tai turi būti nustatoma kitoje *reglamento* vietoje arba kitu atveju tai turi būti projektuojant gaminį numatyta funkcija),

— surinktų duomenų pateikimo išorinio įrenginio taikomajai programai forma,

— duomenų saugumo nuostatos, kuriomis užtikrinamas didesnis saugumas, palyginti su „Bluetooth®“ (pvz., užšifravimas), ir kurios yra susijusios su *duomenų* turiniu (jos pateikiamos kitoje *reglamento* vietoje [10 priedėlis. Bendrieji apsaugos mechanizmai]),

— su ITS sąsaja naudojami „Bluetooth®“ protokolai.

2.1. **Santrumpos, apibrėžtys ir žymenys**

Šiame priedėlyje vartojamos santrumpos ir sąvokų apibrėžtys

Ryšys	duomenų ir (arba) informacijos mainai tarp pagrindinio įrenginio (t. y. tachografų) ir išorinio įrenginio naudojant ITS sąsają ir „Bluetooth®“ ryšio technologiją
Duomenys	1 priedėlyje apibrėžti duomenų rinkiniai
Reglamentas	2014 m. vasario 4 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 165/2014 dėl kelių transporto priemonėse naudojamų tachografų, kuriuo panaikinamas Tarybos reglamentas (EEB) Nr. 3821/85 dėl kelių transporto priemonėse naudojamų tachografų ir iš dalies keičiamas Europos Parlamento ir Tarybos reglamentas (EB) Nr. 561/2006 dėl tam tikrų su kelių transportu susijusių socialinių teisės aktų suderinimo
BR	pagrindinė sparta
EDR	didesnė duomenų perdavimo sparta
GNSS	pasaulinė palydovinės navigacijos sistema
IRK	tapatybės nustatymo raktas
ITS	intelektinė transporto sistema
LE	mažas energijos kiekis
PIN	asmeninis identifikavimo kodas
PUC	asmeninis blokavimo panaikinimo kodas
SID	perdavimo identifikatorius
SPP	nuosekliosios jungties profilis

▼B

SSP	saugus paprastas susiejimas
TRTP	perdavimo užklausos parametras
TREP	perdavimo atsako parametras
VU	transporto priemonės blokas

3. NURODYTIEJI REGLAMENTAI IR STANDARTAI

Šiame priedėlyje nustatyta specifikacija grindžiama visais toliau nurodytais reglamentais ir standartais ir susijusi su jais arba jų dalimis. Šio priedėlio punktuose nurodomi atitinkami standartai arba tam tikri jų punktai. Jeigu nustatomas koks nors prieštaravimas, pirmenybė teikiama šio priedėlio punktams.

Šiame priedėlyje nurodyti šie reglamentai ir standartai:

— 2014 m. vasario 4 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 165/2014 dėl kelių transporto priemonėse naudojamų tachografų, kuriuo panaikinamas Tarybos reglamentas (EEB) Nr. 3821/85 dėl kelių transporto priemonėse naudojamų tachografų ir iš dalies keičiamas Europos Parlamento ir Tarybos reglamentas (EB) Nr. 561/2006 dėl tam tikrų su kelių transportu susijusių socialinių teisės aktų suderinimo

— 2006 m. kovo 15 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 561/2006 dėl tam tikrų su kelių transportu susijusių socialinių teisės aktų suderinimo ir iš dalies keičiantis Tarybos reglamentus (EEB) Nr. 3821/85 ir (EB) Nr. 2135/98 bei panaikinantis Tarybos reglamentą (EEB) Nr. 3820/85

— ISO 16844-4. Kelių transporto priemonės. Tachografų sistemos. 4 dalis. CAN sąsaja

— ISO 16844-7. Kelių transporto priemonės. Tachografų sistemos. 7 dalis. Parametrai

— Bluetooth®. Nuosekliosios jungties profilis. V1.2

— Bluetooth®. Pagrindinė versija 4.2

— NMEA 0183 V4.1 protokolas

4. SĄSAJOS VEIKIMO PRINCIPAI

4.1. **Išankstinės duomenų perdavimo per ITS sąsają sąlygos**

Transporto priemonės blokas turi nuolat atnaujinti duomenis ir tvarkyti jame išsaugotinus duomenis nenaudojant ITS sąsajos. Priemonės, kuriomis tai užtikrinama, yra pačiame transporto priemonės bloke ir nustatomos kitoje reglamento vietoje, o ne šiame priedėlyje.

4.1.1 *Duomenų perdavimas per ITS sąsają*

Transporto priemonės blokas turi atnaujinti duomenis, prieinamus per ITS sąsają, o atnaujinimo dažnumas nustatomas pagal transporto priemonės bloko procedūras – nepriklausomai nuo ITS sąsajos. Transporto priemonės bloko duomenys naudojami *duomenims* rinkti ir atnaujinti, o priemonės, kuriomis tai užtikrinama, nurodomos kitoje reglamento vietoje arba, jeigu tokios specifikacijos nėra, yra produkto konstrukcijos funkcija ir šiame priedėlyje nenustatomos.

▼B

4.1.2 *Duomenų turinys*

Duomenų turinys turi atitikti nustatytąjį šio priedėlio 1 priede.

4.1.3 *ITS taikomosios programos*

ITS taikomosios programos naudoja per ITS sąsają gautus duomenis, pvz., vairuotojo veiklos valdymui optimizuoti atsižvelgiant į reglamento nuostatas, galimoms tachografo triktims nustatyti arba GNSS duomenims naudoti. Taikomųjų programų specifikacija šiame priedėlyje nenustatoma.

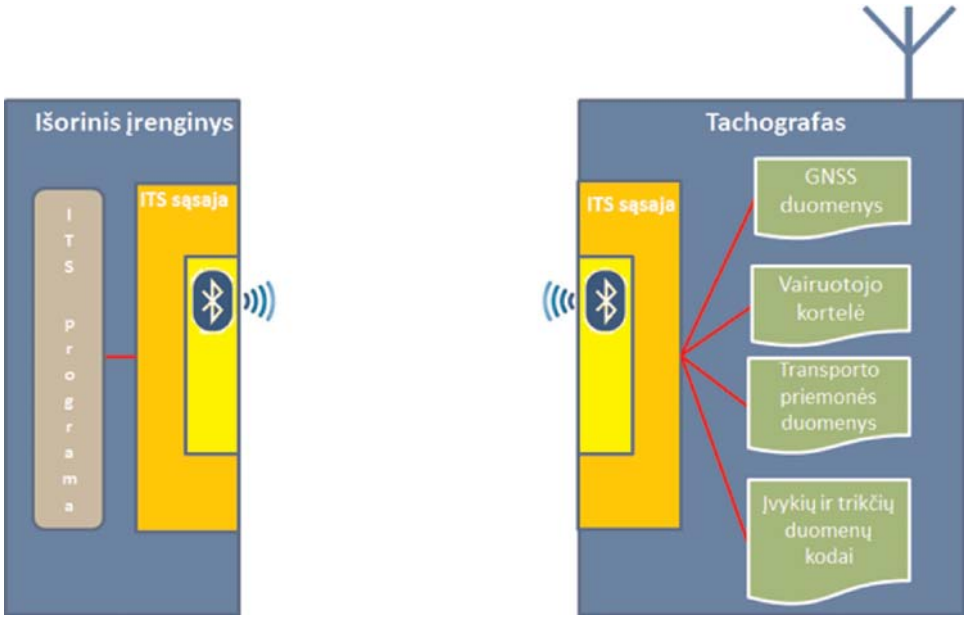
4.2. **Ryšio technologija**

Duomenų perdavimas per ITS sąsają turi būti atliekamas per „Bluetooth®“ sąsają, suderinamą su 4.2 ar naujesne versija. „Bluetooth®“ veikia nelicencijuotoje pramonės, mokslo ir medicinos (ISM) 2,4–2,485 GHz dažnių juostoje. 4.2 versijos „Bluetooth®“ geriau apsaugomas privatumas, užtikrinami patikimesni saugumo mechanizmai, didesnė duomenų perdavimo sparta ir patikimumas. Šioje specifikacijoje naudojama 2 radijo klasės „Bluetooth®“, kurios ryšio zona ne didesnė kaip 10 metrų. Išsami informacija apie 4.2 versijos „Bluetooth®“ pateikta adresu www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676).

Ryšys užmezgamas naudojant ryšio įrangą po to, kai patvirtintasis įtaisas užbaigia susiejimo procesą. „Bluetooth®“ ryšio technologija naudoja pagrindinio įtaiso ir pavaldžiojo įtaiso modelį, kad būtų kontroliuojama, kada ir kur įtaisai gali perduoti duomenis, šiuo atveju tachografas yra pagrindinis įtaisas, o išorinis įrenginys – pavaldusis įtaisas.

Kai išorinis įrenginys pirmą kartą patenka į transporto priemonės bloko veikimo zoną, gali būti pradedamas „Bluetooth®“ susiejimo procesas (taip pat žr. 2 priedą). Įtaisai keičiasi savo adresais, pavadinimais, profiliais ir bendruoju slaptu raktu, kuris suteikia jiems galimybę ateityje užmegzti ryšį, kai jie yra kartu. Užbaigus šį etapą išorinis įrenginys yra patvirtinamas ir gali inicijuoti duomenų perkėlimo iš tachografo užklausas. Be „Bluetooth®“ užtikrinamų priemonių, galimybė įtraukti šifravimo mechanizmus nėra numatyta. Tačiau, jeigu būtini papildomi apsaugos mechanizmai, jie taikomi pagal 10 priedėlį „Bendrieji apsaugos mechanizmai“.

Bendrasis ryšio užmezgimo principas pavaizduotas toliau pateiktame paveikslėlyje.



▼B

„Bluetooth®“ technologijos SPP (nuosekliosios jungties profilis) turi būti naudojamas duomenims iš transporto priemonės bloko perduoti į išorinį įrenginį.

4.3. **PIN patvirtinimas**

Siekiant užtikrinti saugumą transporto priemonės blokas turi naudoti PIN kodo patvirtinimo sistemą, kuri turi būti atskirta nuo „Bluetooth“ susiejimo. Kiekvienas transporto priemonės blokas turi galėti generuoti iš ne mažiau kaip 4 skaitmenų sudarytus PIN kodus, skirtus autentiškumui patikrinti. Kiekvieną kartą, kai išorinis įrenginys susiejamas su transporto priemonės bloku, prieš gaudamas duomenis jis turi pateikti teisingą PIN kodą.

Jeigu PIN kodas patvirtinamas, įrenginys įtraukiamas į baltąjį sąrašą. Baltajame sąraše turi būti galima išsaugoti ne mažiau kaip 64 įrenginius, susietus su konkrečiu transporto priemonės bloku.

Jeigu tris kartus paeiliui pateikiamas neteisingas PIN kodas, įrenginys laikinai įtraukiamas į juodąjį sąrašą. Kol jis nepašalinamas iš juodojo sąrašo, bet kuris jo mėginimas yra atmetamas. Jeigu neteisingas PIN kodas vėl pateikiamas dar tris kartus iš eilės, tada taikoma gerokai ilgesnė draudimo trukmė (žr. 1 lentelę). Pateikus teisingą PIN kodą atkuriama pradinė draudimo trukmės ir mėginimų skaičiaus vertė. 2 priedo 1 pav. nurodyta PIN patvirtinimo mėginimų sekos schema.

Lentelė 1

Draudimo trukmė, priklausanti nuo to, kiek kartų iš eilės pateikiamas neteisingas PIN kodas

Nesėkmingų mėginimų iš eilės skaičius	Draudimo trukmė
3	30 sekundžių
6	5 minutės
9	1 valanda
12	24 valandos
15	Nuolatinis draudimas

Jeigu neteisingas PIN kodas pateikiamas penkiolika kartų (5x3) iš eilės, tada ITS blokas visam laikui įtraukiamas į juodąjį sąrašą. Šį nuolatinį draudimą galima panaikinti tik įvedus teisingą PUC kodą.

PUC kodas turi būti sudarytas iš 8 skaitmenų ir jį pateikia gamintojas kartu su transporto priemonės bloku. Jeigu neteisingas PUC kodas pateikiamas dešimt kartų iš eilės, ITS blokas visam laikui (neatšaukiamai) įtraukiamas į juodąjį sąrašą.

Gamintojas gali pasiūlyti galimybę keisti PIN kodą pačiame transporto priemonės bloke, tačiau pakeisti PUC neturėtų būti įmanoma. Keičiant PIN kodą, jeigu įmanoma, privalo būti reikalaujama, kad esamas PIN kodas būtų įvedamas tiesiogiai į transporto priemonės bloką.

Be to, visi į baltąjį sąrašą įtraukti įrenginiai turi būti jame laikomi tol, kol naudotojas juos pašalins rankiniu būdu (pvz., per transporto priemonės bloko žmogaus ir mašinos sąsają ar kitu būdu). Taip iš baltojo sąrašo galima pašalinti prarastus ar pavogtus ITS blokus. Taip pat jeigu ITS blokas iš „Bluetooth“ ryšio zonos pašalinamas ilgesniam kaip 24 val. laikotarpiui, jis turi būti savaime šalinamas iš transporto priemonės bloko baltojo sąrašo, o vėl užmezgant ryšį privaloma pateikti teisingą PIN kodą.

▼B

Iš transporto priemonės bloko sąsajos į transporto priemonės bloką ir atvirkščiai perduodamų pranešimų formatas nėra numatytas ir jį savo nuožiūra parenka gamintojas. Tačiau tas gamintojas turi užtikrinti, kad būtų atsižvelgiama į pranešimų formatą tarp ITS bloko ir transporto priemonės bloko sąsajos (žr. ASN.1 specifikacijas).

Vadinasi, prieš pradedant apdoroti bet kurią duomenų užklausą turi būti tinkamai patikrinamas siųstuvo saugumo požymis. 2 priedo 2 pav. pateikiama šios procedūros sekos schema. Visi į juodąjį sąrašą įtraukti įrenginiai turi būti savaime atmetami, visiems į juodąjį sąrašą ir į baltąjį sąrašą neįtrauktiems įrenginiams turi būti pateikiama PIN užklausa, kurią privaloma įvykdyti prieš pakartotinai siunčiant savo duomenų užklausą.

4.4. **Pranešimo formatas**

Visų pranešimų, kuriuos ITS blokas siunčia transporto priemonės bloko sąsajai ir atvirkščiai, formatas yra struktūra, kuria sudaro trys dalys: antraštė, sudaryta iš tikslinio baito (TGT), šaltinio baito (SRC) ir ilgio baito (LEN).

Duomenų laukas, kurį sudaro paslaugos identifikatoriaus baitas (SID) ir įvairus duomenų baitų skaičius (ne daugiau kaip 255).

Kontrolinės sumos baitas yra 1 baito modulio 256 visų pranešimo baitų, išskyrus pačią CS, sumos serija.

Pranešimas turi būti „Big Endian“.

2 lentelė

Bendrasis pranešimo formatas

Antraštė			Duomenų laukas					Kontrolinė suma
TGT	SRC	LEN	SID	TRTP	CC	CM	DUOMENYS	CS
3 baitai			Ne daugiau kaip 255 baitai					1 baitas

Antraštė

TGT ir SRC: pranešimo paskirties įrenginio (TGT) ir šaltinio (SRC) identifikatoriai. Numatytasis transporto priemonės bloko sąsajos identifikatorius turi būti EE. Keisti šio identifikatoriaus neleidžiama. ITS blokas turi naudoti numatytąjį ryšio seanso pirmojo pranešimo identifikatorių A0. Tada transporto priemonės bloko sąsaja ITS blokui priskiria unikalųjį identifikatorių ir šiam blokui siunčia pranešimą apie minėtą identifikatorių, kuris naudojamas su kitais per seansą perduodamais pranešimais.

LEN baitas turi atsižvelgti tik į duomenų lauko dalį DUOMENYS (žr. 2 lentelę), 4 pirmi baitai yra numanomi.

Transporto priemonės bloko sąsaja turi patvirtinti pranešimo siųstuvo autentiškumą: šiuo tikslu ji savąjį identifikatorių sąrašą sutikrina su „Bluetooth“ duomenimis ir pagal pateiktą identifikatorių patikrina ITS bloką, kuris tuo metu yra „Bluetooth“ ryšio zonoje.

Duomenų laukas

Į duomenų lauką, be SID, taip pat įtraukiami kiti parametrai: perdavimo užklausos parametras (TRTP) ir skaitiklio baitai.

▼B

Jeigu perduotini duomenys yra pernelyg ilgi, kad tilptų į pranešimą, pranešimas skaidomas į kelias dalis. Kiekvienos pranešimo dalies antraštė ir SID yra tie patys, tačiau joje turi būti 2 baitų skaitiklis, „Counterr Current“ (CC) ir „Counter Max“ (CM), kad būtų pateikiamas pranešimo dalies numeris. Kad būtų tikrinamos klaidos ir atliekamas atmetimas, imtuvas patvirtina kiekvieną pranešimo dalį. Imtuvas gali priimti pranešimo dalį, siųsti užklausą, kad pranešimo dalis būtų perduota dar kartą, siųsti siųstuvui užklausą vėl pradėti perdavimą ar jį nutraukti.

Jeigu nenaudojama, tada CC ir CM priskiriama vertė 0xFF.

Pvz., šis pranešimas

ANTRAŠTĖ	SID	TRTP	CC	CM	DUOMENYS	CS
3 baitai	Ilgesnis kaip 255 baitai					1 baitas

turi būti perduodamas taip:

ANTRAŠTĖ	SID	TRTP	01	n	DUOMENYS	CS
3 baitai	255 baitai					1 baitas

ANTRAŠTĖ	SID	TRTP	02	n	DUOMENYS	CS
3 baitai	255 baitai					1 baitas

…

ANTRAŠTĖ	SID	TRTP	N	N	DUOMENYS	CS
3 baitai	Ne daugiau kaip 255 baitai					1 baitas

3 lentelėje pateikti pranešimai, kuriais keistis turi galėti transporto priemonės blokas ir ITS blokas. Kiekvieno parametro turinys nurodomas šešioliktaine verte. Jeigu dėl aiškumo lentelėje nėra pateikti CC ir CM, žr. pirmiau nurodytą išsamų formatą.

3 lentelė

Išsamus pranešimo turinys

Pranešimas	Antraštė			DUOMENYS			Kontrolinė suma
	TGT	SRC	LEN	SID	TRTP	DUOMENYS	
RequestPIN	*ITSID*	EE	00	01	FP		
SendITSID	*ITSID*	EE	01	02	FP	*ITSID*	
SendPIN	EE	*ITSID*	04	03	FP	4*INTEGER (0..9)	
PairingResult	*ITSID*	EE	01	04	FP	BOOLEAN (T/F)	
SendPUC	EE	*ITSID*	08	05	FP	8*INTEGER (0..9)	

▼B

Pranešimas	Antraštė			DUOMENYS			Kontrolinė suma
	TGT	SRC	LEN	SID	TRTP	DUOMENYS	
BanLiftingResult	*ITSID*	EE	01	06	FP	BOOLEAN (T/F)	
RequestRejected	*ITSID*	EE	08	07	FP	Laikas	
RequestData							
standardTachData	EE	*ITSID*	01	08	01		
personalTachData	EE	*ITSID*	01	08	02		
gnssData	EE	*ITSID*	01	08	03		
standardEventData	EE	*ITSID*	01	08	04		
personalEventData	EE	*ITSID*	01	08	05		
standardFaultData	EE	*ITSID*	01	08	06		
manufacturerData	EE	*ITSID*	01	08	07		
ResquestAccepted	*ITSID*	EE	Len	09	TREP	Duomenys	
DataUnavailable							
Nėra duomenų	*ITSID*	EE	02	0 A	TREP	10	
Asmens duomenys nepateikiami	*ITSID*	EE	02	0 A	TREP	11	
NegativeAnswer							
Bendrasis atmetimas	*ITSID*	EE	02	0B	SID Req	10	
Paslauga netinkama	*ITSID*	EE	02	0B	SID Req	11	
Subfunkcija netinkama	*ITSID*	EE	02	0B	SID Req	12	
Neteisingas pranešimo ilgis	*ITSID*	EE	02	0B	SID Req	13	
Netinkamos sąlygos arba užklausos sekos klaida	*ITSID*	EE	02	0B	SID Req	22	
Užklausa nepriimtina	*ITSID*	EE	02	0B	SID Req	31	
Laukiama atsakymo	*ITSID*	EE	02	0B	SID Req	78	
ITSID neatitiktis	*ITSID*	EE	02	0B	SID Req	FC	
ITSID nerasta	*ITSID*	EE	02	0B	SID Req	FB	

RequestPIN (SID 01)

Šį pranešimą išsiunčia transporto priemonės bloko sąsaja, jeigu duomenų užklausą atsiunčia į juodąjį sąrašą neįtrauktas ir į baltąjį sąrašą neįtrauktas ITS blokas.

▼B

SendITSID (SID 02)

Šį pranešimą išsiunčia transporto priemonės bloko sąsaja kiekvieną kartą, kai užklausą atsiunčia naujas įrenginys. Šis įrenginys, prieš jam priskiriant ryšio seansui skirtą unikalųjį identifikatorių, turi naudoti numatytąjį identifikatorių A0.

SendPIN (SID 03)

Šį pranešimą išsiunčia ITS blokas, kad transporto priemonės bloko sąsaja jį įtrauktų į baltąjį sąrašą. Šio pranešimo turinys yra kodas, kurį sudaro 4 sveikieji skaičiai nuo 0 iki 9.

PairingResult (SID 04)

Šį pranešimą išsiunčia transporto priemonės bloko sąsaja, kad į ITS bloką būtų perduota informacija, ar jo atsiųstas kodas buvo teisingas. Šio pranešimo turinys turi būti loginė (BOOLEAN) reikšmė „True“, jeigu PIN kodas buvo teisingas, ir „False“, jeigu jis buvo neteisingas.

SendPUC (SID 05)

Šį pranešimą išsiunčia ITS blokas, kad būtų išbrauktas iš transporto priemonės bloko sąsajos juodojo sąrašo. Šio pranešimo turinys yra kodas, kurį sudaro 8 sveikieji skaičiai nuo 0 iki 9.

BanLiftingResult (SID 06)

Šį pranešimą išsiunčia transporto priemonės bloko sąsaja, kad į ITS bloką būtų perduota informacija, ar jo atsiųstas PUC kodas buvo teisingas. Šio pranešimo turinys turi būti loginė (BOOLEAN) reikšmė „True“, jeigu PUC kodas buvo teisingas, ir „False“, jeigu jis buvo neteisingas.

RequestRejected (SID 07)

Šį pranešimą išsiunčia transporto priemonės bloko sąsaja, pateikdama atsakymą į bet kokį pranešimą, kurį atsiuntė į juodąjį sąrašą įtrauktas ITS blokas, išskyrus „SendPUC“. Pranešime nurodoma likusi ITS bloko įtraukimo į juodąjį sąrašą trukmė, po kurios pateikiamas 3 priede apibrėžtas „Laiko“ sekos formatas.

RequestData (SID 08)

Šį duomenų prieigos pranešimą išsiunčia ITS blokas. Vieno baito perdavimo užklausos parametru (TRTP) nurodomas prašomų duomenų tipas. Naudojami kelių tipų duomenys:

— standardTachData (TRTP 01): iš tachografo gaunami duomenys, laikomi ne asmeniniais duomenimis;

— personalTachData (TRTP 02): iš tachografo gaunami duomenys, laikomi asmeniniais duomenimis;

— gnssData (TRTP 03): GNSS duomenys, jie visada yra asmeniniai;

— standardEventData (TRTP 04): užregistruoti įvykio duomenys, laikomi ne asmeniniais;

— personalEventData (TRTP 05): užregistruoti įvykio duomenys, laikomi asmeniniais;

— standardFaultData (TRTP 06): užregistruotos triktys, laikomos neasmeninėmis;

— manufacturerData (TRTP 07): gamintojo pateikiami duomenys.

▼B

Žr. šio priedėlio 3 priedą, kuriame pateikta išsami informacija apie kiekvieno tipo duomenų turinį.

Žr. 12 priedėlį, kuriame pateikta išsami informacija apie GNSS duomenų formatą ir turinį.

Žr. IB ir IC priedus, kuriuose pateikta išsami informacija apie įvykio duomenų kodą ir triktis.

ResquestAccepted (SID 09)

Šį pranešimą išsiunčia transporto priemonės bloko sąsaja, jeigu ITS bloko pranešimas „RequestData“ buvo priimtas. Šiame pranešime pateikiamas 1 baito TREP, kuris yra susijusio „RequestData“ pranešimo TRTP baitas, ir visi prašyto tipo duomenys.

DataUnavailable (SID 0A)

Šį pranešimą išsiunčia transporto priemonės bloko sąsaja, jeigu dėl tam tikrų priežasčių prašomų duomenų neįmanoma nusiųsti į ITS bloką, įtrauktą į baltąjį sąrašą. Šiame pranešime pateikiamas 1 baito TREP, kuris yra prašomų duomenų TRTP, ir 3 lentelėje nurodytas 1 baito klaidos kodas. Galimi šie kodai:

— nėra duomenų (10): transporto priemonės bloko sąsaja dėl nenurodytų priežasčių neturi prieigos prie transporto priemonės bloko duomenų.

— asmeniniais duomenimis nesikeičiama (11): ITS blokas mėgina nuskaityti asmeninius duomenis, nors jais nesikeičiama.

NegativeAnswer (SID 0B)

Šiuos pranešimus išsiunčia transporto priemonės bloko sąsaja, jeigu užklausos neįmanoma užbaigti dėl kokios nors kitos priežasties, išskyrus duomenų neprieinamumą. Šie pranešimai paprastai išsiunčiami dėl reikalavimų neatitinkančio užklausos formato (ilgis, SID, ITSID...), tačiau ne vien dėl šios priežasties. Į duomenų lauke pateikiamą TRTP įtraukiama užklausos SID. Į duomenų lauką įtraukiamas kodas, kuriuo apibūdinama neigiamo atsakymo priežastis. Galimi šie kodai:

— Bendrasis atmetimas (kodas 10)

— Veiksmo negalima atlikti dėl priežasties, kuri nėra nurodoma toliau ir skirsnyje (įveskite *DataUnavailable* skirsnio numerį)

— Paslauga netinkama (kodas 11)

— Užklausos SID nesuprantamas.

— Subfunkcija netinkama (kodas 12)

— Užklausos TRTP nesuprantamas Pavyzdžiui, jo gali nebūti arba jo vertė neatitinka priimtinų verčių

— Netinkamas pranešimo ilgis (kodas 13)

— Gauto pranešimo ilgis nėra tinkamas (LEN baitas neatitinka pranešimo tikrojo ilgio)

— Netinkamos sąlygos arba užklausos sekos klaida (kodas 22)

— Pareikalauta paslauga neaktyvi arba užklausos pranešimų seka yra neteisinga

— Užklausa nepriimtina (kodas: 33)

▼B

— Užklausos parametro įrašas (duomenų laukas) negalioja

— Laukiama atsakymo (kodas: 78)

— Pareikalauto veiksmo negalima užbaigti laiku ir transporto priemonės blokas nepasirengęs priimti kitos užklausos

— *ITSID* neatitiktis (kodas FB)

— Atlikus palyginimą su „Bluetooth“, informacija SRC *ITSID* neatitinka susietojo įrenginio

— *ITSID* nerastas (kodas FC)

— SRC *ITSID* nesusietas su jokiu prietaisu

3 priede nurodyto ASN.1 kodo 1–72 eilutės (**FormatMessageModule**) apibrėžia pranešimų formatą taip, apibūdintą 3 lentelėje. Išsami informacija apie pranešimų turinį pateikta toliau.

4.5. **Vairuotojo sutikimas**

Visi prieinami duomenys laikomi standartiniais arba asmeniniais. Asmeniniai duomenys prieinami tik tuo atveju, jeigu vairuotojas davė sutikimą ir neprieštarauja, kad jo asmeniniai duomenys iš tachografo per informacinį transporto priemonės tinklą būtų perduodami trečiosios šalies taikomosioms programoms.

Vairuotojas duoda sutikimą, kai pirmą kartą įstatant vairuotojo kortelę arba dirbtuvių kortelę, kuri transporto priemonės blokui dar nežinoma, kortelės turėtojo prašoma patvirtinti savo sutikimą dėl su tachografu susijusių asmeninių duomenų išvesties per pasirenkamąją ITS sąsają (taip pat žr. I C priedo 3.6.2 skirsnį).

Į tachografo atmintį įrašomas sutikimo statusas (aktyvintas ir (arba) atšauktas).

Jeigu yra daugiau vairuotojų, su ITS sąsaja dalijamasi tik tų vairuotojų asmeniniais duomenimis, kurie yra davę sutikimą. Pvz., jeigu transporto priemonėje yra du vairuotojai ir tik pirmasis vairuotojas sutinka dalytis savo asmeniniais duomenimis, antrojo vairuotojo asmeniniais duomenimis neturi būti dalijamasi.

4.6. **Standartinių duomenų nuskaitymas**

2 priedo 3 pav. pateikiama ITS bloko siunčiamos galiojančios užklausos dėl prieigos prie standartinių duomenų sekos schema. Jeigu ITS blokas yra įtrauktas į baltąjį sąrašą pagal reikalavimus ir nesiunčia užklausos dėl asmeninių duomenų, jokio kito patikrinimo atlikti nebūtina. Schemose atsižvelgta į 2 priedo 2 pav. nurodytą tinkamą procedūrą, kuri jau buvo taikyta. Jas galima prilyginti pilkam langeliui *REQUEST TREATMENT* (*UŽKLAUSOS APDOROJIMAS*) iš 2 pav.

Iš turimų duomenų standartiniais laikomi šie duomenys:

— standardTachData (TRTP 01)

— StandardEventData (TRTP 04)

— standardFaultData (TRTP 06)

4.7. **Asmeninių duomenų nuskaitymas**

2 priedo 4 pav. pateikiama asmeninių duomenų užklausos apdorojimo sekos schema. Transporto priemonės bloko sąsaja, kaip jau nurodyta pirmiau, asmeninius duomenis siunčia tik tuo atveju, jeigu vairuotojas yra davęs aiškų sutikimą (taip pat žr. 4.5 punktą). Kitu atveju užklausa turi būti savaime atmetama.

▼B

Iš turimų duomenų asmeniniais laikomi šie duomenys:

— personalTachData (TRTP 02)

— gnssData (TRTP 03)

— personalEventData (TRTP 05)

— manufacturerData (TRTP 07)

4.8. **Įvykių ir trikčių duomenų nuskaitymas**

Iš ITS blokų turi būti įmanoma nusiųsti užklausą dėl įvykių duomenų, apimančių visų nenumatytų įvykių sąrašą. Šie duomenys laikomi standartiniais arba asmeniniais, žr. 3 priedą. Kiekvieno įvykio turinys apibrėžiamas dokumentuose, pateiktuose šio priedėlio 1 priede.

▼B

1 PRIEDAS

PER ITS SĄSAJĄ PRIEINAMŲ DUOMENŲ SĄRAŠAS

Duomenys	Šaltinis	Duomenų klasifikavimas (asmeniniai ir neasmeniniai duomenys)
VehicleIdentificationNumber	Transporto priemonės blokas	**neasmeniniai**
CalibrationDate	Transporto priemonės blokas	**neasmeniniai**
TachographVehicleSpeed speed instant t	Transporto priemonės blokas	asmeniniai
Driver1WorkingState Selector driver	Transporto priemonės blokas	asmeniniai
Driver2WorkingState	Transporto priemonės blokas	asmeniniai
DriveRecognize Speed Threshold detected	Transporto priemonės blokas	**neasmeniniai**
Driver1TimeRelatedStates Weekly day time	Vairuotojo kortelė	asmeniniai
Driver2TimeRelatedStates	Vairuotojo kortelė	asmeniniai
DriverCardDriver1	Transporto priemonės blokas	**neasmeniniai**
DriverCardDriver2	Transporto priemonės blokas	**neasmeniniai**
OverSpeed	Transporto priemonės blokas	asmeniniai
TimeDate	Transporto priemonės blokas	**neasmeniniai**
HighResolutionTotalVehicleDistance	Transporto priemonės blokas	**neasmeniniai**
ServiceComponentIdentification	Transporto priemonės blokas	**neasmeniniai**
ServiceDelayCalendarTimeBased	Transporto priemonės blokas	**neasmeniniai**
Driver1Identification	Vairuotojo kortelė	asmeniniai
Driver2Identification	Vairuotojo kortelė	asmeniniai
NextCalibrationDate	Transporto priemonės blokas	**neasmeniniai**
Driver1ContinuousDrivingTime	Vairuotojo kortelė	asmeniniai
Driver2ContinuousDrivingTime	Vairuotojo kortelė	asmeniniai
Driver1CumulativeBreakTime	Vairuotojo kortelė	asmeniniai
Driver2CumulativeBreakTime	Vairuotojo kortelė	asmeniniai
Driver1CurrentDurationOfSelectedActivity	Vairuotojo kortelė	asmeniniai
Driver2CurrentDurationOfSelectedActivity	Vairuotojo kortelė	asmeniniai
SpeedAuthorised	Transporto priemonės blokas	**neasmeniniai**
TachographCardSlot1	Vairuotojo kortelė	**neasmeniniai**
TachographCardSlot2	Vairuotojo kortelė	**neasmeniniai**
Driver1Name	Vairuotojo kortelė	asmeniniai
Driver2Name	Vairuotojo kortelė	asmeniniai

▼B

Duomenys	Šaltinis	Duomenų klasifikavimas (asmeniniai ir neasmeniniai duomenys)
OutOfScopeCondition	Transporto priemonės blokas	**neasmeniniai**
ModeOfOperation	Transporto priemonės blokas	**neasmeniniai**
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	Vairuotojo kortelė	asmeniniai
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	Vairuotojo kortelė	asmeniniai
EngineSpeed	Transporto priemonės blokas	asmeniniai
RegisteringMemberState	Transporto priemonės blokas	**neasmeniniai**
VehicleRegistrationNumber	Transporto priemonės blokas	**neasmeniniai**
Driver1EndOfLastDailyRestPeriod	Vairuotojo kortelė	asmeniniai
Driver2EndOfLastDailyRestPeriod	Vairuotojo kortelė	asmeniniai
Driver1EndOfLastWeeklyRestPeriod	Vairuotojo kortelė	asmeniniai
Driver2EndOfLastWeeklyRestPeriod	Vairuotojo kortelė	asmeniniai
Driver1EndOfSecondLastWeeklyRestPeriod	Vairuotojo kortelė	asmeniniai
Driver2EndOfSecondLastWeeklyRestPeriod	Vairuotojo kortelė	asmeniniai
Driver1CurrentDailyDrivingTime	Vairuotojo kortelė	asmeniniai
Driver2CurrentDailyDrivingTime	Vairuotojo kortelė	asmeniniai
Driver1CurrentWeeklyDrivingTime	Vairuotojo kortelė	asmeniniai
Driver2CurrentWeeklyDrivingTime	Vairuotojo kortelė	asmeniniai
Driver1TimeLeftUntilNewDailyRestPeriod	Vairuotojo kortelė	asmeniniai
Driver2TimeLeftUntilNewDailyRestPeriod	Vairuotojo kortelė	asmeniniai
Driver1CardExpiryDate	Vairuotojo kortelė	asmeniniai
Driver2CardExpiryDate	Vairuotojo kortelė	asmeniniai
Driver1CardNextMandatoryDownloadDate	Vairuotojo kortelė	asmeniniai
Driver2CardNextMandatoryDownloadDate	Vairuotojo kortelė	asmeniniai
TachographNextMandatoryDownloadDate	Transporto priemonės blokas	**neasmeniniai**
Driver1TimeLeftUntilNewWeeklyRestPeriod	Vairuotojo kortelė	asmeniniai
Driver2TimeLeftUntilNewWeeklyRestPeriod	Vairuotojo kortelė	asmeniniai
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	Vairuotojo kortelė	asmeniniai
Driver2NumberOfTimes9hDailyDrivingTimesExceeced	Vairuotojo kortelė	asmeniniai

▼B

Duomenys	Šaltinis	Duomenų klasifikavimas (asmeniniai ir neasmeniniai duomenys)
Driver1CumulativeUninterruptedRestTime	Vairuotojo kortelė	asmeniniai
Driver2CumulativeUninterruptedRestTime	Vairuotojo kortelė	asmeniniai
Driver1MinimumDailyRest	Vairuotojo kortelė	asmeniniai
Driver2MinimumDailyRest	Vairuotojo kortelė	asmeniniai
Driver1MinimumWeeklyRest	Vairuotojo kortelė	asmeniniai
Driver2MinimumWeeklyRest	Vairuotojo kortelė	asmeniniai
Driver1MaximumDailyPeriod	Vairuotojo kortelė	asmeniniai
Driver2MaximumDailyPeriod	Vairuotojo kortelė	asmeniniai
Driver1MaximumDailyDrivingTime	Vairuotojo kortelė	asmeniniai
Driver2MaximumDailyDrivingTime	Vairuotojo kortelė	asmeniniai
Driver1NumberOfUsedReducedDailyRestPeriods	Vairuotojo kortelė	asmeniniai
Driver2NumberOfUsedReducedDailyRestPeriods	Vairuotojo kortelė	asmeniniai
Driver1RemainingCurrentDrivingTime	Vairuotojo kortelė	asmeniniai
Driver2RemainingCurrentDrivingTime	Vairuotojo kortelė	asmeniniai
GNSS position	Transporto priemonės blokas	asmeniniai

2) GAVUS VAIRUOTOJO SUTIKIMĄ PRIEINAMI TOLYDIEJI GNSS DUOMENYS

Žr. 12 priedėlį. GNSS.

3) BE VAIRUOTOJO SUTIKIMO PRIEINAMI ĮVYKIŲ KODAI

Įvykis	Duomenų laikymo taisyklės	Registruojami duomenys apie kiekvieną įvykį
Įstatyta negaliojanti kortelė	— 10 paskutinių įvykių	— Įvykio data ir laikas — Įvykį sukėlusios kortelės rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Panašių įvykių tą dieną skaičius
Kortelių nesuderinamumas	— 10 paskutinių įvykių	— Įvykio pradžios data ir laikas — Įvykio pabaigos data ir laikas — Abiejų nesuderinamų kortelių rūšis, numeriai, jas išdavusi valstybė narė ir kortelės karta
Netinkamai užbaigtas paskutinis kortelės naudojimo seansas	— 10 paskutinių įvykių	— Kortelės įstatymo data ir laikas — Kortelės rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Paskutiniai iš kortelės nuskaityti seanso duomenys: — Kortelės įstatymo data ir laikas — Transporto priemonės registracijos numeris, registracijos valstybė narė ir transporto priemonės bloko karta

▼B

Įvykis	Duomenų laikymo taisyklės	Registruojami duomenys apie kiekvieną įvykį
Maitinimo nutrūkimas (2)	— Ilgiausiai trukęs įvykis per kiekvieną iš paskutinių 10 dienų, kuriomis jis įvyko — Penki ilgiausiai trukę įvykiai per paskutines 365 dienas	— Įvykio pradžios data ir laikas — Įvykio pabaigos data ir laikas — Kortelės, kuri buvo kortelės lizde įvykio pradžioje ir (arba) pabaigoje, rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Panašių įvykių tą dieną skaičius
Ryšio su nuotolinio ryšio įrenginiu klaida	— Ilgiausiai trukęs įvykis per kiekvieną iš paskutinių 10 dienų, kuriomis jis įvyko — Penki ilgiausiai trukę įvykiai per paskutines 365 dienas	— Įvykio pradžios data ir laikas — Įvykio pabaigos data ir laikas — Kortelės, kuri buvo kortelės lizde įvykio pradžioje ir (arba) pabaigoje, rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Panašių įvykių tą dieną skaičius
Iš GNSS imtuvo negauta informacijos apie buvimo vietą	— Ilgiausiai trukęs įvykis per kiekvieną iš paskutinių 10 dienų, kuriomis jis įvyko — Penki ilgiausiai trukę įvykiai per paskutines 365 dienas	— Įvykio pradžios data ir laikas — Įvykio pabaigos data ir laikas — Kortelės, kuri buvo kortelės lizde įvykio pradžioje ir (arba) pabaigoje, rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Panašių įvykių tą dieną skaičius
Duomenų apie judėjimą klaida	— Ilgiausiai trukęs įvykis per kiekvieną iš paskutinių 10 dienų, kuriomis jis įvyko — Penki ilgiausiai trukę įvykiai per paskutines 365 dienas	— Įvykio pradžios data ir laikas — Įvykio pabaigos data ir laikas — Kortelės, kuri buvo kortelės lizde įvykio pradžioje ir (arba) pabaigoje, rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Panašių įvykių tą dieną skaičius
Transporto priemonės judėjimo nesuderinamumas	— Ilgiausiai trukęs įvykis per kiekvieną iš paskutinių 10 dienų, kuriomis jis įvyko — Penki ilgiausiai trukę įvykiai per paskutines 365 dienas	— Įvykio pradžios data ir laikas — Įvykio pabaigos data ir laikas — Kortelės, kuri buvo kortelės lizde įvykio pradžioje ir (arba) pabaigoje, rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — 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), — Kortelės, kuri buvo kortelės lizde įvykio pradžioje ir (arba) pabaigoje, rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Įvykio rūšis

▼B

Įvykis	Duomenų laikymo taisyklės	Registruojami duomenys apie kiekvieną įvykį
Nesuderintas laikas	— Ilgiausiai trukęs įvykis per kiekvieną iš paskutinių 10 dienų, kuriomis jis įvyko — Penki ilgiausiai trukę įvykiai per paskutines 365 dienas	— Tachografo data ir laikas — GNSS data ir laikas — Kortelės, kuri buvo kortelės lizde įvykio pradžioje ir (arba) pabaigoje, rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Panašių įvykių tą dieną skaičius

4) GAVUS VAIRUOTOJO SUTIKIMĄ PRIEINAMI ĮVYKIŲ KODAI

Įvykis	Duomenų laikymo taisyklės	Registruojami duomenys apie kiekvieną įvykį
Važiavimas be reikiamos kortelės	— Ilgiausiai trukęs įvykis per kiekvieną iš paskutinių 10 dienų, kuriomis jis įvyko — Penki ilgiausiai trukę įvykiai per paskutines 365 dienas	— Įvykio pradžios data ir laikas — Įvykio pabaigos data ir laikas — Kortelės, kuri buvo kortelės lizde įvykio pradžioje ir (arba) pabaigoje, rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Panašių įvykių tą dieną skaičius
Kortelė įstatyta važiuojant	— Paskutinis įvykis per kiekvieną iš paskutinių 10 dienų, kuriomis jis įvyko	— Įvykio data ir laikas — Kortelės rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta — Panašių įvykių tą dieną skaičius
Greičio viršijimas (1)	— Svarbiausias įvykis per kiekvieną iš paskutinių 10 dienų kuriomis jis įvyko (t. y. tas įvykis, kai greitis viršytas daugiausiai) — Penki svarbiausi įvykiai per paskutines 365 dienas — Pirmasis po paskutinio kalibravimo įvykęs įvykis	— Įvykio pradžios data ir laikas — Įvykio pabaigos data ir laikas — Didžiausias įvykio metu išmatuotas greitis — Įvykio metu išmatuoto greičio aritmetinis vidurkis — Vairuotojo kortelės rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta (kai tinkama) — Panašių įvykių tą dieną skaičius

5) BE VAIRUOTOJO SUTIKIMO PRIEINAMI TRIKČIŲ DUOMENŲ KODAI

Triktis	Duomenų laikymo taisyklės	Registruojami duomenys apie kiekvieną triktį
Kortelės triktis	— 10 paskutinių vairuotojo kortelės trikčių	— Trikties pradžios data ir laikas — Trikties pabaigos data ir laikas — Kortelės rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta
Tachografo triktys	— 10 paskutinių kiekvienos rūšies trikčių — Pirmoji triktis po paskutinio kalibravimo	— Trikties pradžios data ir laikas — Trikties pabaigos data ir laikas — Trikties rūšis — Kortelės, kuri buvo kortelės lizde, kai įvyko ir (arba) baigėsi triktis, rūšis, numeris, ją išdavusi valstybė narė ir kortelės karta

▼B

Šią triktį gali sukelti bet kuris iš toliau nurodytų gedimų, jeigu nėra įjungtas kalibravimo režimas:

— Transporto priemonės bloko vidinė triktis

— Spausdintuvo triktis

— Ekrano triktis

— Duomenų perkėlimo triktis

— Jutiklio triktis

— GNSS imtuvo arba išorinio GNSS įrenginio triktis

— Nuotolinio ryšio įrenginio triktis

6) BE VAIRUOTOJO SUTIKIMO PRIEINAMI DUOMENYS APIE SU GAMINTOJU SUSIJUSIUS ĮVYKIUS IR TRIKTIS

Įvykis arba triktis	Duomenų laikymo taisyklės	Registruojami duomenys apie kiekvieną įvykį
Nustato gamintojas	Nustato gamintojas	Nustato gamintojas

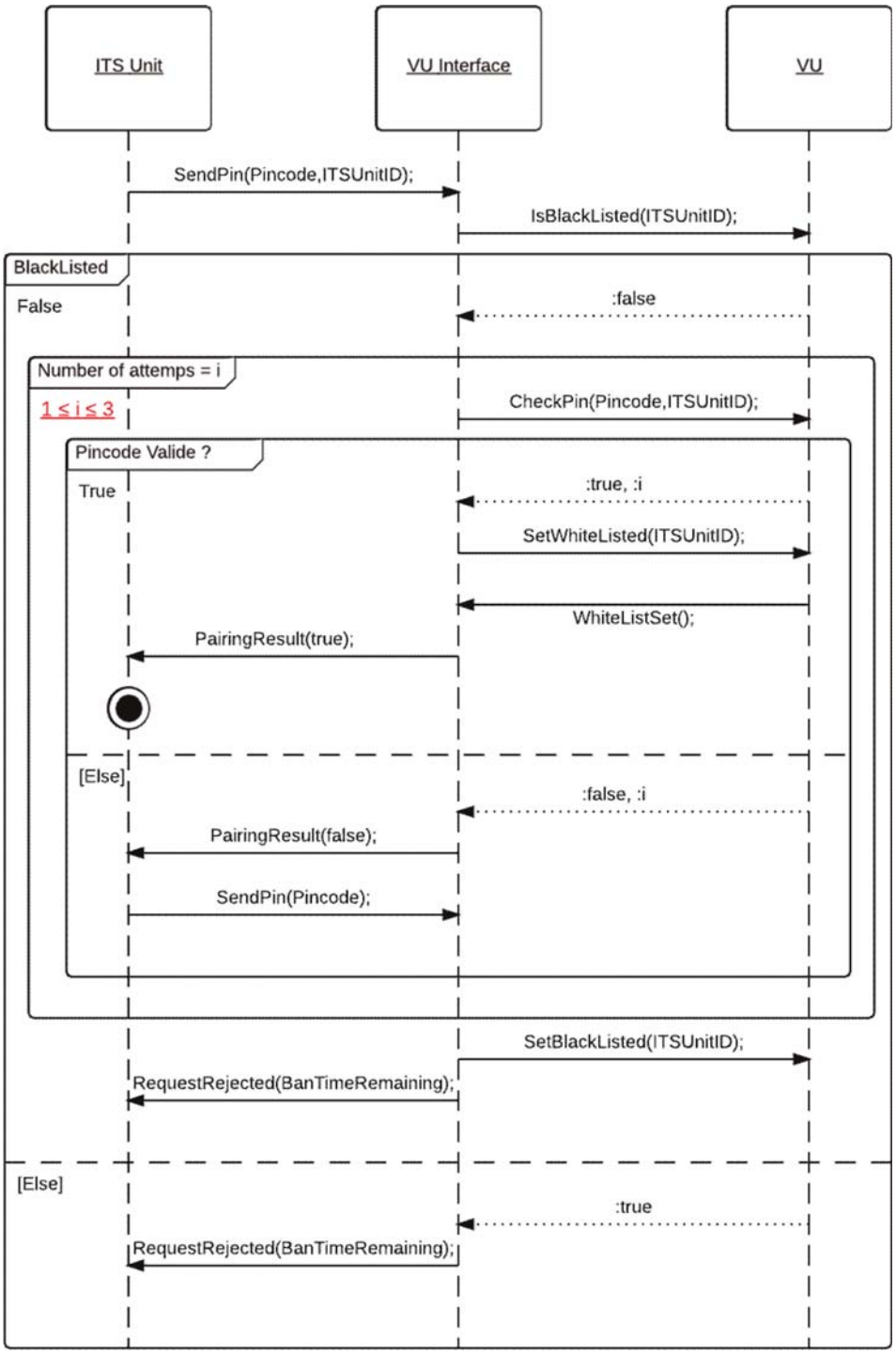
▼B

2 PRIEDAS

PRANEŠIMŲ, KURIAIS KEIČIAMASI SU ITS BLOKU, SEKOS SCHEMOS

1 pav

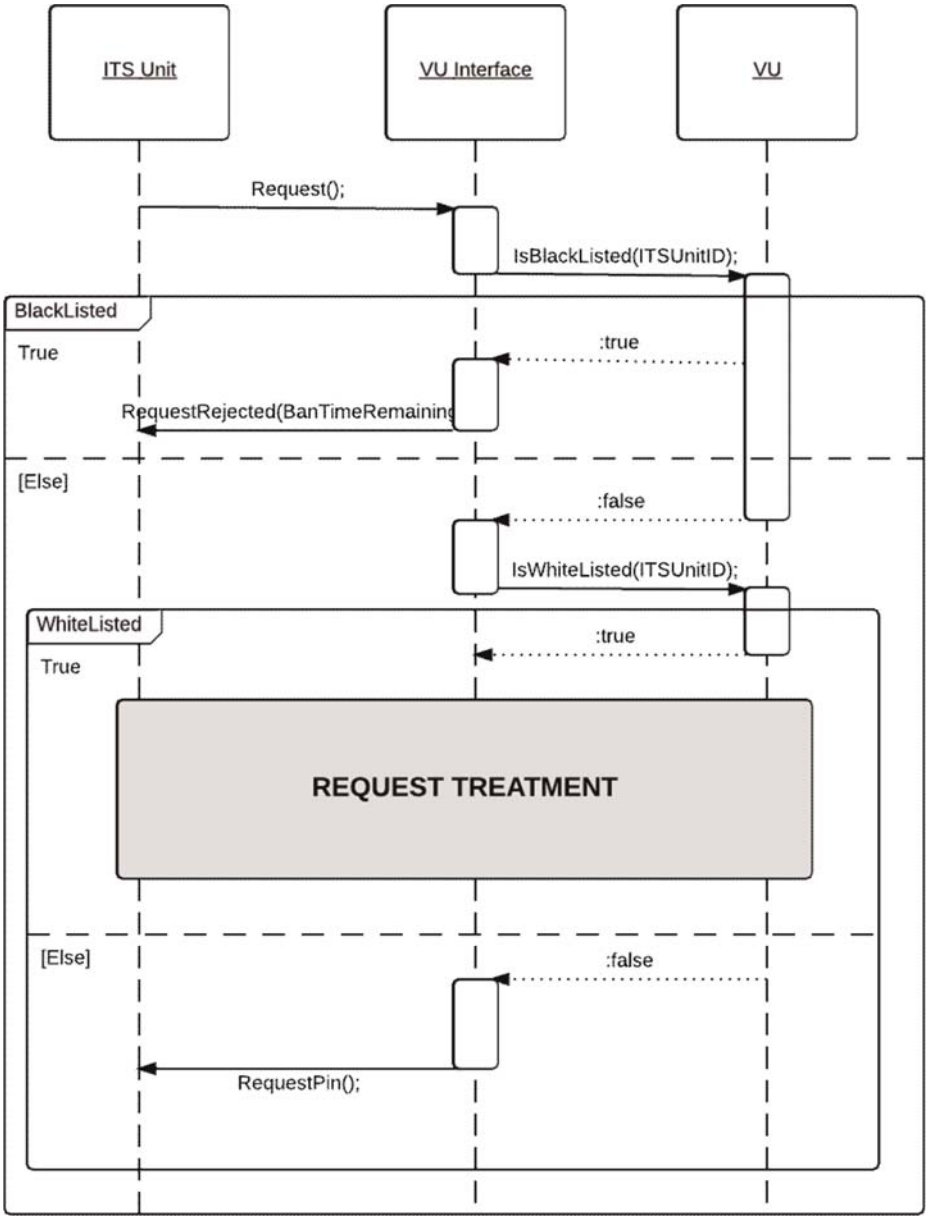
Mėginimo patvirtinti PIN sekos schema



▼B

2 pav

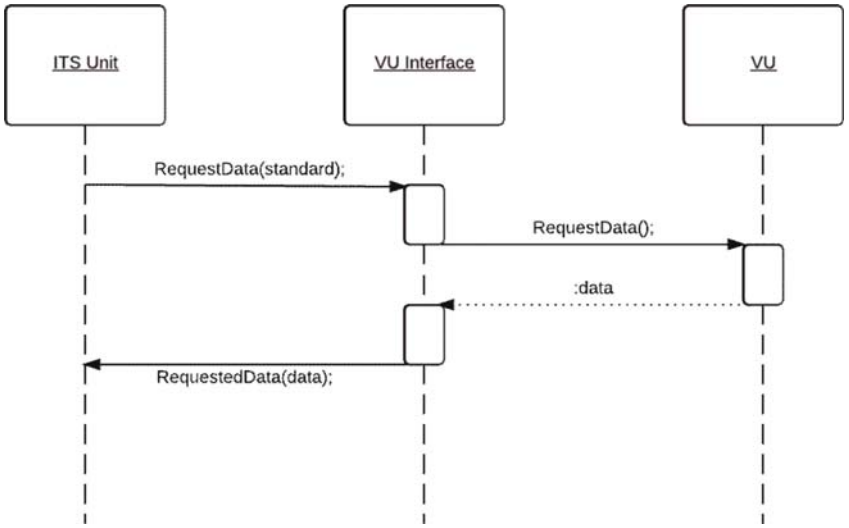
ITS bloko patvirtinimo tikrinimo sekos schema



▼B

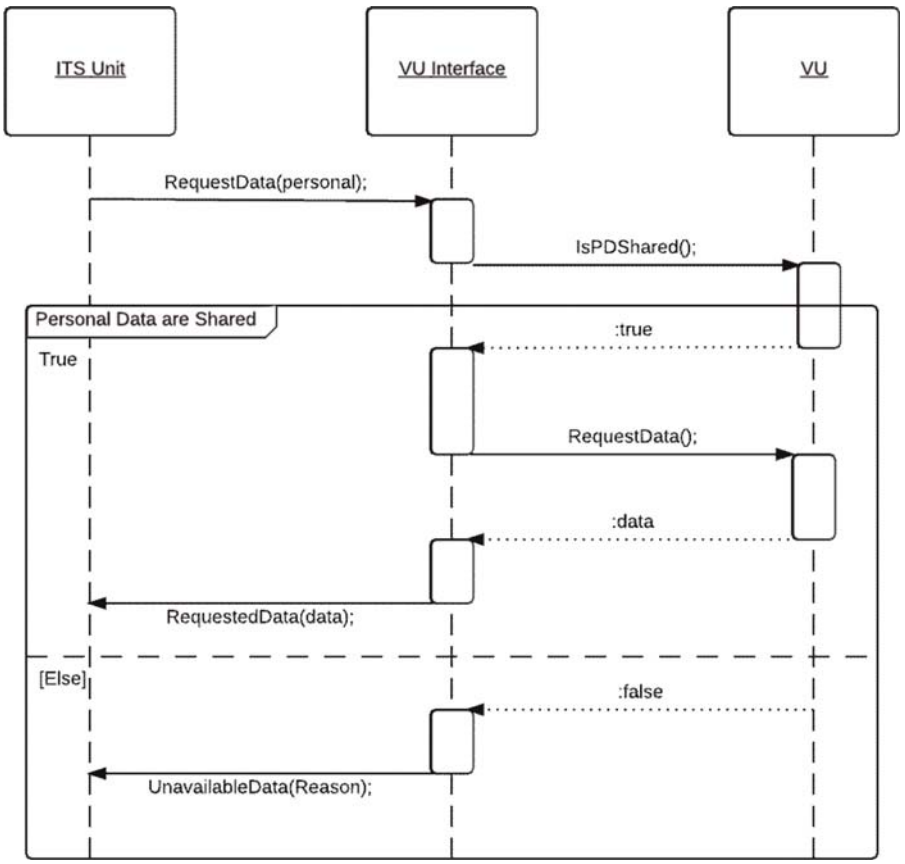
3 pav

Duomenų, laikomų ne asmeniniais duomenimis, užklausos apdorojimo sekos schema (įvedus teisingą PIN)



4 pav

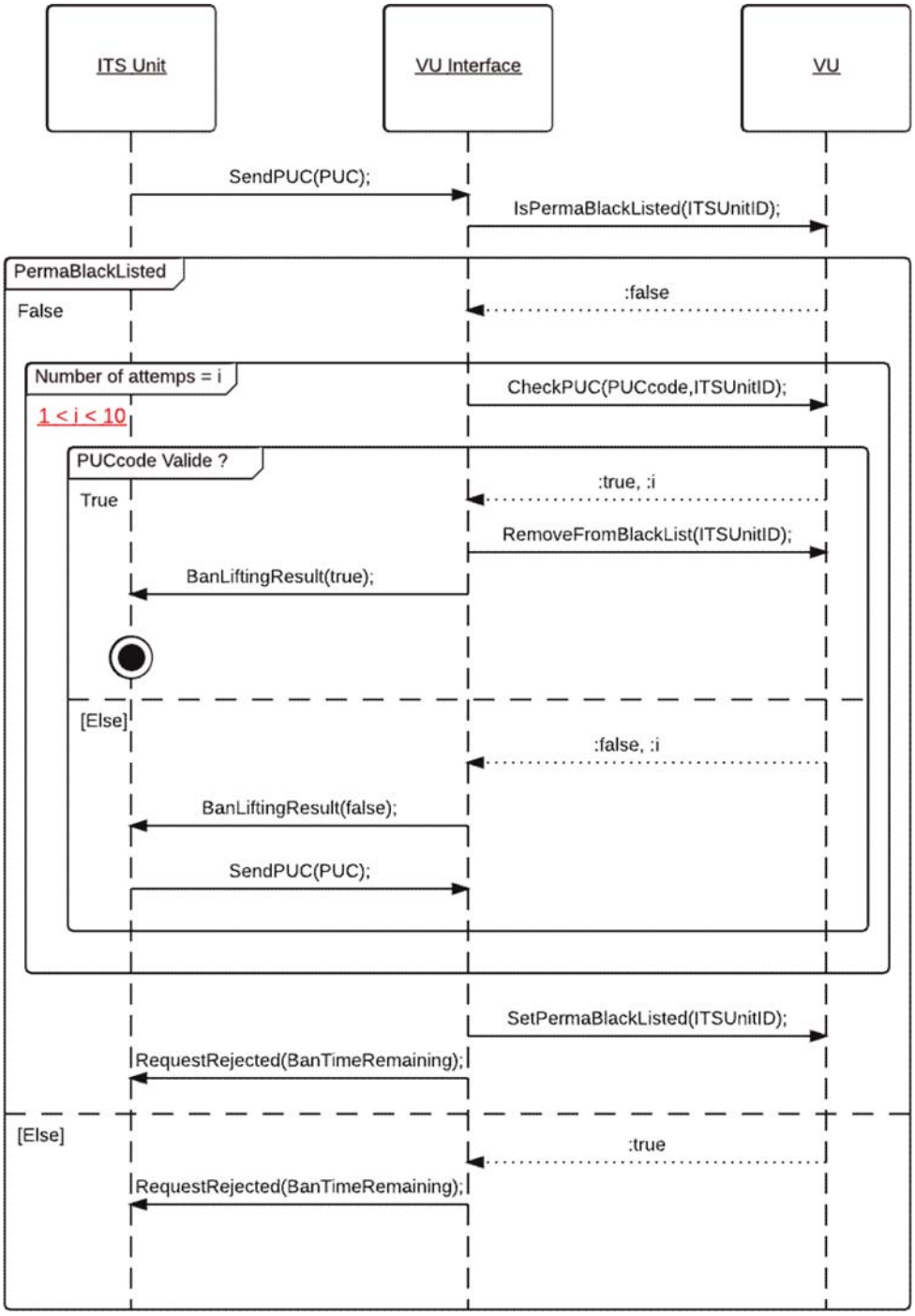
Duomenų, laikomų asmeniniais duomenimis, užklausos apdorojimo sekos schema (įvedus teisingą PIN)



▼B

5 pav

Mėginimo patvirtinti PUC sekos schema



▼B

3 PRIEDAS

ASN.1 SPECIFIKACIJOS

```
FormatMessageModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS ;
IMPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
        BanLiftingResult FROM PINPUCDataFieldsModule
        RequestAccepted,RequestData, DataUnavailable FROM
        RequestDataFieldsModule
        SendITSID, NegativeAnswer FROM OtherDataFieldsModule;

       CompleteMessage ::=SEQUENCE{
             header Header,
             data DataField,
             checksum Checksum
       }

       ----------------
       --HEADER TYPES--
       ----------------


       Header::=SEQUENCE{
             tgt IDList,
             src IDList,
             len BIT STRING (1..255)
       }

       vuID BIT STRING ::= 'EE'H
       IDList ::=CHOICE{
             vu BIT STRING (vuID),
             itsUnits SEQUENCE OF BIT STRING,
                   --Default hex Value:A0, redefined after first message exchange--
                   --Each ID will be linked to the Bluetooth ID of the device--
             ...
       }

       --------------------
       --DATAFIELDS TYPES--
       --------------------
       DataField ::=SEQUENCE{
             sid BIT STRING,
             trtp BIT STRING,
             subMBytes SubMessageBytes,
             dataField Content,
             ...
       }

       SubMessageBytes ::= SEQUENCE{
             currentSubM BIT STRING,
             totalSubM BIT STRING
       }

       Content ::= CHOICE{
             requestPIN RequestPIN,
             sendITSID SendITSID,
             sendPin SendPIN,
```

▼B

```
55                pairRslt PairingResult,
56                sendPUC SendPUC,
57                banlift BanLiftingResult,
58                requestRejected RequestRejected,
59                requestData RequestData,
60                requestOK RequestAccepted,
61                dataUnavailable DataUnavailable,
62                negAns NegativeAnswer
63          }
64
65          ------------------
66          --CHECKSUM TYPES--
67          ------------------
68
69          Checksum ::= SEQUENCE{
70                --SHA2 checksum
71          }
72    END
73
```

▼B

```
PINPUCDataFieldsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
BanLiftingResult;
IMPORTS ;

      ----------
      ---Utils--
      ----------

      PUC ::= SEQUENCE (SIZE(8)) OF
      INTEGER (SIZE(0..9))

      PIN ::=      SEQUENCE (SIZE(4)) OF
            INTEGER (SIZE(0..9))

      -------------------------
      --Messages From ITS Unit--
      -------------------------

      SendPIN {PIN:pin} ::= SEQUENCE {
            sid BIT STRING ('03'H),
            pin PIN (pin)
      }

      SendPUC {PUC:puc} ::= SEQUENCE {
            sid BIT STRING ('05'H),
            puc PUC (puc)
      }
      --------------------
      --Messages From VU--
      --------------------

      PairingResult ::= SEQUENCE{
            sid BIT STRING ('04'H),
            result BOOLEAN
      }

      RequestPIN {MType:receivedRequest}::= SEQUENCE{
            sid BIT STRING ('01'H)
      }

      RequestRejected ::= SEQUENCE{
            sid BIT STRING ('07'H),
            banTimeRemaining GeneralizedTime, --PermaBan == 1k years-- }

      BanLiftingResult ::= SEQUENCE{
            sid BIT STRING ('06'H),
            result BOOLEAN
      }
END
```

▼B

```
RequestDataFields DEFINITIONS AUTOMATIC TAGS ::= BEGIN
	EXPORTS RequestAccepted,RequestData, DataUnavailable ;
	IMPORTS StandardEvent, PersonalEvent, StandardFault FROM EventsModule;

	------------------
	---From ITS Unit--
	------------------
	RequestData ::= SEQUENCE{
		sid BIT STRING ('08'H),
		requestedData DataTypeCode,
		...
	}

	-----------
	--From VU--
	-----------
	RequestAccepted ::=SEQUENCE{
		sid BIT STRING ('09'H),
		trtp DataTypeCode,
		dataSheet CHOICE{
			standardData StandardTachDataContent,
			personalData PersonalTachDataContent,
			gnss GNSSDataContent,
			standardEvent StandardEventContent,
			personalEvent PersonalEventContent,
			standardFault StandardFaultContent,
			manufacturerdata ManufacturerDataContent,
			...
		}
	}

	DataTypeCode ::=CHOICE{
		standardTachData BIT STRING ('01'H),
		personalTachData BIT STRING ('02'H),
		gnssData BIT STRING ('03'H),
		standardEventData BIT STRING ('04'H),
		personalEventData BIT STRING ('05'H),
		standardFaultData BIT STRING ('06'H),
		manufacturerData BIT STRING ('07'H),
		...
	}

	DataUnavailable ::=SEQUENCE{
		sid BIT STRING ('0A'H),
		trtp DataTypeCode,
		reason UnavailableDataCodes
	}

	UnavailableDataCodes ::= CHOICE{
		noDataAvailable BIT STRING ('10'H),
		personalDataNotShared BIT STRING ('11'H),
		...
	}
	---------------------------
	--Complete Tachograph Data--
	---------------------------
	--The format of the data was taken from the ISO16844-7 norm, more information
available in this ISO document—

```

▼B

```
Time ::= SEQUENCE{
       seconds INTEGER (0..59.75), --increment: 0.25s--
       minutes INTEGER (0..59), --increment: 1min--
       hours INTEGER (0..23), --increment: 1h--
       day INTEGER (0.25.. 31.75), --increment: 0.25d--
       month INTEGER (1..12), --increment: 1month--
       year INTEGER (1985..2235), --increment: 1year--
       locMinOffset INTEGER (-59..59), --increment: 1min--
       locHouroffset INTEGER (-23..23)--increment: 1h--
}

Date ::= SEQUENCE{
       month INTEGER (1..12), --increment: 1month--
       day INTEGER (0.25.. 31.75), --increment: 0.25d--
       year INTEGER (1985..2235) --increment: 1year--
}

DriverName ::=SEQUENCE{
       codePageSurname UTF8String, --See ISO/IEC 8859--
       surname UTF8String,
       codePageFirstname UTF8String, --See ISO/IEC 8859--
       firstname UTF8String,
}

-------------------
--Message Content--
-------------------

StandardTachDataContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&standardTachData),
       personal BOOLEAN (FALSE),
       data StandardTachyDataSheet,
}

PersonalTachDataContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&personalTachData),
       personal BOOLEAN (TRUE),
       data PersonalTachyDataSheet
}

GNSSDataContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&gnssData),
       personal BOOLEAN (TRUE),
       data GNSSDataSheet
}

StandardEventContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&standardEventData),
       personal BOOLEAN (FALSE),
       data StandardEventDataSheet
}

PersonalEventContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&personalEventData),
       personal BOOLEAN (TRUE),
       data PersonalEventDataSheet
}

StandardFaultContent ::= SEQUENCE{
```

▼B

```
243                trtp DataTypeCode (DataTypeCode.&standardFaultData),
244                personal BOOLEAN (FALSE),
245                data StandardFault
246          }
247
248          ManufacturerDataContent ::= SEQUENCE{
249                trtp DataTypeCode (DataTypeCode.&manufacturerData),
250                personal BOOLEAN (TRUE),
251                ...
252          }
253
254          ---------------
255          --DATA SHEETS--
256          ---------------
257
258          --Data sheet format follows ISO 16844-7.--
259          StandardTachyDataSheet ::= SEQUENCE{
260                vin UTF8String (SIZE(17)),
261                calibrationDate Date,
262                driveRecognize INTEGER (2 UNION 12),
263                driverCardDriver1 INTEGER (2 UNION 12),
264                driverCardDriver2 INTEGER (2 UNION 12),
265                timeDate Time,
266                highResolutionTotalVehicleDistance INTEGER (0..21055406), --increment:
267    5m--
268                serviceComponentIdentification INTEGER (0..255),
269                serviceDelayCalendarTimeBased INTEGER (-125..125), --increment: 1week-
270    -
271                nextCalibrationDate Date,
272                speedAuthorised INTEGER (0..250.996), --increment 1/256km/h--
273                tachographCardSlot1 INTEGER (0..4...), --Maximum 250--
274                tachographCardSlot2 INTEGER (0..4...), --Maximum 250--
275                outOfScopeCondition INTEGER(2 UNION 12),
276                modeOfOperation INTEGER (0..4...), --Maximum 250--
277                registeringMemberState UTF8String,
278          vehicleRegistrationNumber SEQUENCE {
279                      codePageVRN INTEGER (0..255),
280                      vrn OCTET STRING (SIZE(13)),
281                },
282                tachographNextMandatoryDownloadDate Date,
283                ...
284          }
285
286          PersonalTachyDataSheet ::= SEQUENCE{
287                tachographVehicleSpeed INTEGER (0..250.996), --increment 1/256km/h--
288                driver1WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
289    UNION 1012...),
290                driver2WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
291    UNION 1012...),
292
293                driver1TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
294    1002 UNION
295                                                 1012 UNION 1102 UNION 1112 UNION
296    10002 UNION 10012 UNION
297                                                 10102 UNION 10112 UNION 11002 UNION
298    11012...),
299                driver2TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
300    1002 UNION
```

▼B

```
                                                    1012 UNION 1102 UNION 1112 UNION
10002 UNION 10012 UNION
                                                    10102 UNION 10112 UNION 11002 UNION
11012...),

              overSpeed INTEGER (2 UNION 12),
              driver1Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
              driver2Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
              driver1ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
              driver2ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
              driver1CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
              driver2CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
              driver1Name DriverName,
              driver2Name DriverName,
              driver1CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
              driver2CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
              engineSpeed INTEGER(0..8031.875), --increment: 0,125r/min--
              driver1EndOfLastDailyRestPeriod Time,
              driver2EndOfLastDailyRestPeriod Time,
              driver1EndOfLastWeeklyRestPeriod Time,
              driver2EndOfLastWeeklyRestPeriod Time,
              driver1EndOfSecondLastWeeklyRestPeriod Time,
              driver2EndOfSecondLastWeeklyRestPeriod Time,
              driver1CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
              driver2CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
              driver1CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
              driver2CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
              driver1TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
              driver2TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
              driver1CardExpiryDate Date,
              driver2CardExpiryDate Date,
              driver1CardNextMandatoryDownloadDate Date,
              driver2CardNextMandatoryDownloadDate Date,
              driver1TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
              driver2TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
              driver1NumberOfTimes9hDailyDrivingTimesExceeded INTEGER (0..13),
              driver2NumberOfTimes9hDailyDrivingTimesExceeced INTEGER (0..13),
              driver1CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
              driver2CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
              driver1MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
              driver2MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
              driver1MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
              driver2MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
```

▼B

```
360                driver1MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
361                driver2MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
362                driver1MaximumDailyDrivingTime INTEGER (910 UNION 1010),
363                driver2MaximumDailyDrivingTime INTEGER (910 UNION 1010),
364                driver1NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
365                driver2NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
366                driver1RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
367    1min--
368                driver2RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
369    1min--
370                ...
371          }
372
373          GNSSDataSheet ::=  SEQUENCE {
374          gnssPosition GeoCoordinates
375                --See Appendix 1 for definition of GeoCoordinates--
376          }
377
378          StandardEventDataSheet ::= SEQUENCE{
379                events SEQUENCE OF StandardEvent
380          }
381
382          PersonalEventDataSheet ::= SEQUENCE{
383                events SEQUENCE OF PersonalEvent
384          }
385    END
386
387    EventsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
388          EXPORTS ALL;
389          IMPORTS NationAlpha FROM Appendix1; --See Appendix 1 for more information
390    about NationAlpha--
391
392                SecurityBreachEvent ::=SEQUENCE{
393                      --See Annex 1B for more information--
394                }
395
396                RecordingEquipmentFaultType ::= SEQUENCE{
397                      --See Annex 1B for more information--
398                }
399
400                StandardEvent::= CHOICE{
401                      insertionInvalidCard InsertionOfANonValidCard,
402                      cardConflict CardConflict,
403                      timeOverlap TimeOverlap,
404                      previousSessionNotClosed LastCardSessionNotCorrectlyClosed,
405                      overSpeeding OverSpeeding,
406                      powerSupplyInterruption PowerSupplyInterruption,
407                      comErrorWithRemoteFacility
408    CommunicationErrorWithTheRemoteCommunicationFacility,
409                      absenceGNSSPosition
410    AbsenceOfPositionInformationFromGNSSReceiver,
411                      positionDataError PositionDataError,
412                      motionDataError MotionDataError,
413                      vehicleMotionConflict VehicleMotionConflict,
414                      securityBreachAttempt SecurityBreachAttempt,
415                      timeConflict TimeConflict,
416                      ...
417                }
418
```

▼B

```
PersonalEvent ::= CHOICE{
      lackOfAppropriateCard DrivingWithoutAnAppropriateCard,
      cardInsertionWhileDriving CardInsertionWhileDriving,
      overSpeeding OverSpeeding,
      ...
}

StandardFault ::= CHOICE{
      cardFault CardFault,
      recordingEquipementFault RecordingEquipmentFault,
...
}

---------------
--EVENTS LIST--
---------------

InsertionOfANonValidCard::=SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER
}

CardConflict ::= SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER
}

TimeOverlap ::=SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER,
      numberSimilarEvent INTEGER
}

DrivingWithoutAnAppropriateCard ::= SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER,
      numberOfSimilarEvent INTEGER
}

CardInsertionWhileDriving ::= SEQUENCE{
      date GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
```

▼B

```
478                     issuingMemberState SEQUENCE OF NationAlpha,
479                     numberOfSimilarEvents INTEGER
480             }
481
482             LastCardSessionNotCorrectlyClosed ::=SEQUENCE{
483                     beginDate GeneralizedTime,
484                     endDate GeneralizedTime,
485                     carsdType SEQUENCE OF UTF8String,
486                     cardsNumber SEQUENCE OF INTEGER,
487                     issuingMemberState SEQUENCE OF NationAlpha,
488                     cardsGeneration SEQUENCE OF INTEGER,
489                     oldSession SEQUENCE{
490                             beginDate GeneralizedTime,
491                             endDate GeneralizedTime,
492                             vrn UTF8String,
493                             issuingMemberState NationAlpha,
494                             cardsGeneration INTEGER,
495                     }
496             }
497
498             OverSpeeding ::=SEQUENCE{
499                     beginDate GeneralizedTime,
500                     endDate GeneralizedTime,
501                     maximumSpeed INTEGER,
502                     averageSpeed INTEGER,
503                     cardType UTF8String,
504                     cardNumber INTEGER,
505                     issuingMemberState NationAlpha,
506                     cardGeneration INTEGER,
507                     numberOfSimilarEvents INTEGER
508             }
509
510             PowerSupplyInterruption ::=SEQUENCE{
511                     beginDate GeneralizedTime,
512                     endDate GeneralizedTime,
513                     carsdType SEQUENCE OF UTF8String,
514                     cardsNumber SEQUENCE OF INTEGER,
515                     issuingMemberState SEQUENCE OF NationAlpha,
516                     cardsGeneration SEQUENCE OF INTEGER,
517                     numberOfSimilarEvent INTEGER
518             }
519
520             CommunicationErrorWithTheRemoteCommunicationFacility ::=SEQUENCE{
521                     beginDate GeneralizedTime,
522                     endDate GeneralizedTime,
523                     carsdType SEQUENCE OF UTF8String,
524                     cardsNumber SEQUENCE OF INTEGER,
525                     issuingMemberState SEQUENCE OF NationAlpha,
526                     cardsGeneration SEQUENCE OF INTEGER,
527                     numberOfSimilarEvent INTEGER
528             }
529
530             AbsenceOfPositionInformationFromGNSSReceiver ::= SEQUENCE{
531                     beginDate GeneralizedTime,
532                     endDate GeneralizedTime,
533                     carsdType SEQUENCE OF UTF8String,
534                     cardsNumber SEQUENCE OF INTEGER,
535                     issuingMemberState SEQUENCE OF NationAlpha,
536                     cardsGeneration SEQUENCE OF INTEGER,
```

▼B

```
537                     numberOfSimilarEvent INTEGER
538             }
539
540             PositionDataError ::= SEQUENCE{
541                     beginDate GeneralizedTime,
542                     endDate GeneralizedTime,
543                     carsdType SEQUENCE OF UTF8String,
544                     cardsNumber SEQUENCE OF INTEGER,
545                     issuingMemberState SEQUENCE OF NationAlpha,
546                     cardsGeneration SEQUENCE OF INTEGER,
547                     numberOfSimilarEvent INTEGER
548             }
549
550             MotionDataError ::= SEQUENCE{
551                     beginDate GeneralizedTime,
552                     endDate GeneralizedTime,
553                     carsdType SEQUENCE OF UTF8String,
554                     cardsNumber SEQUENCE OF INTEGER,
555                     issuingMemberState SEQUENCE OF NationAlpha,
556                     cardsGeneration SEQUENCE OF INTEGER,
557                     numberOfSimilarEvent INTEGER
558             }
559
560             VehicleMotionConflict ::= SEQUENCE{
561                     beginDate GeneralizedTime,
562                     endDate GeneralizedTime,
563                     carsdType SEQUENCE OF UTF8String,
564                     cardsNumber SEQUENCE OF INTEGER,
565                     issuingMemberState SEQUENCE OF NationAlpha,
566                     cardsGeneration SEQUENCE OF INTEGER,
567                     numberOfSimilarEvent INTEGER
568             }
569
570             SecurityBreachAttempt ::= SEQUENCE{
571                     beginDate GeneralizedTime,
572                     endDate GeneralizedTime OPTIONAL,
573                     carsdType SEQUENCE OF UTF8String,
574                     cardsNumber SEQUENCE OF INTEGER,
575                     issuingMemberState SEQUENCE OF NationAlpha,
576                     numberOfSimilarEvent INTEGER,
577                     typeOfEvent SecurityBreachEvent
578             }
579
580
581             TimeConflict ::= SEQUENCE{
582                     beginDate GeneralizedTime,
583                     endDate GeneralizedTime,
584                     carsdType SEQUENCE OF UTF8String,
585                     cardsNumber SEQUENCE OF INTEGER,
586                     issuingMemberState SEQUENCE OF NationAlpha,
587                     cardsGeneration SEQUENCE OF INTEGER,
588                     numberOfSimilarEvent INTEGER
589             }
590
591             ---------------
592             --FAULTS LIST--
593             ---------------
594
595             CardFault ::= SEQUENCE{
```

▼B

```
596                     beginDate GeneralizedTime,
597                     endDate GeneralizedTime,
598                     carsdType SEQUENCE OF UTF8String,
599                     cardsNumber SEQUENCE OF INTEGER,
600                     issuingMemberState SEQUENCE OF NationAlpha,
601                     cardsGeneration SEQUENCE OF INTEGER,
602             }
603
604             RecordingEquipmentFault ::= SEQUENCE{
605                     beginDate GeneralizedTime,
606                     endDate GeneralizedTime,
607                     faultType RecordingEquipmentFaultType,
608                     carsdType SEQUENCE OF UTF8String,
609                     cardsNumber SEQUENCE OF INTEGER,
610                     issuingMemberState SEQUENCE OF NationAlpha,
611                     cardsGeneration SEQUENCE OF INTEGER,
612             }
613 END
```

▼B

14 priedėlis.

NUOTOLINIO RYŠIO FUNKCIJA

TURINYS

1 ĮVADAS

2 TAIKYMO SRITIS

3 SANTRUMPOS, APIBRĖŽTYS IR ŽYMENYS

4 NAUDOJIMO MODELIAI

4.1 Apžvalga

4.1.1 Išankstinės duomenų perdavimo per 5,8 GHz DSRC sąsają sąlygos

4.1.2 1a profilis. Nutaikomas ranka arba laikinai pritvirtinamas pakelėje ir nutaikomas nuotolinio ankstyvo nustatymo ryšio skaitytuvas

4.1.3 1b profilis. Transporto priemonėje įmontuotas ir nukreipiamas nuotolinio ankstyvo nustatymo ryšio skaitytuvas

4.2 Saugumas ir (arba) nepažeistumas

5 NUOTOLINIO RYŠIO TECHNOLOGIJA IR PROTOKOLAI

5.1 Technologija

5.2 Operacijų seka

5.2.1 Operacijos

5.2.2 Naudojant DSRC ryšį gautų duomenų aiškinimas

5.3 Nuotolinio ryšio DSRC fizinės sąsajos parametrai

5.3.1 Su vieta susiję apribojimai

5.3.2 Žemynkryptės ryšio linijos ir aukštynkryptės ryšio linijos parametrai

5.3.3 Antenos konstrukcija

5.4 RTM taikomi DSRC protokolo reikalavimai

5.4.1 Apžvalga

5.4.2 Komandos

5.4.3 Užklausos komandos seka

5.4.4 Duomenų struktūros

5.4.5 RtmData elementai, atliekami veiksmai ir apibrėžtys

5.4.6 Duomenų perdavimo mechanizmas

5.4.7 Išsamus DSCR transakcijos aprašymas

5.4.8 DSRC transakcijos bandymo aprašymas

5.5 Direktyvos 2015/71/EB įgyvendinimo stiprinimas

5.5.1 Apžvalga

5.5.2 Komandos

▼B

5.5.3 Užklausos komandos seka

5.5.4 Duomenų struktūros

5.5.5 OWS DSRC transakcijai taikomas ASN.1 modulis

5.5.6 OwsData elementai, atliekami veiksmai ir apibrėžtys

5.5.7 Duomenų perdavimo mechanizmai

5.6 Duomenų perdavimas tarp DSRC-VU ir transporto priemonės bloko

5.6.1 Fizinė jungtis ir sąsajos

5.6.2 Taikomosios programos protokolas

5.7 Klaidų valdymas

5.7.1 Duomenų įrašymas į DSRC-VU ir jų perdavimas

5.7.2 Belaidžio ryšio klaidos

6 NUOTOLINIO RYŠIO FUNKCIJOS NAUDOJIMO PRADŽIAIR PERIODINIO PATIKRINIMO BANDYMAI

6.1 Bendrosios nuostatos

6.2 ECHO GD

6.3 Saugių duomenų turinio patvirtinimo bandymai

1 ĮVADAS

Šiame priedėlyje apibrėžiamas projektavimas ir procedūros, taikytinos užtikrinant nuotolinio ryšio funkciją (toliau – ryšys), kaip nustatyta Reglamento (ES) Nr. 165/2014 (toliau – reglamentas) 9 straipsnyje.

DSC_1 Reglamentu (ES) Nr. 165/2014 nustatyta, kad tachografe turi būti įdiegta nuotolinio ryšio funkcija, kurią naudodamiesi kompetentingos kontrolės institucijos pareigūnai galėtų nuskaityti tachografo informaciją iš pravažiuojančių transporto priemonių nuotoline užklausos įranga (nuotolinio ankstyvo nustatymo ryšio skaitytuvu [REDCR], tiksliau sakant, užklausos įranga, užmezgančia belaidį ryšį per CEN 5.8 GHz skirtojo trumpojo nuotolio ryšio (DSRC) sąsajas.

Svarbu suvokti, kad šią funkciją numatoma naudoti tik transporto priemonėms, kurios bus tikrinamos nuodugniau, atrinkti ir ji neatstoja Reglamento (ES) Nr. 165/2014 nuostatomis apibrėžto oficialaus patikros proceso. Žr. šio reglamento preambulės 9 konstatuojamąją dalį, kurioje nurodoma, kad nuotolinis ryšys tarp tachografo ir kontrolės institucijų užmezgamas norint atlikti kontrolę kelyje ir taip palengvinamas tikslinių patikrinimų kelyje vykdymas.

DSC_2 *Duomenys* perduodami naudojant *ryšį*, kuris turi būti belaidis ryšys, pagrįstas šio priedėlio nuostatas atitinkančiais 5.8 GHz DSRC belaidžiais ryšiais ir išbandytas taikant atitinkamus parametrus, nustatytus standarte EN 300 674-1 {Elektromagnetinis suderinamumas ir radijo dažnių spektro dalykai; Informacijos apie kelių transportą ir eismą apdorojimo bei perdavimo priemonės; Skirtoji trumpojo nuotolio ryšių perdavimo

▼B

įranga (500 kbit/s ir (arba) 250 kbit/s spartos), veikianti pramonės, mokslo ir medicinos (PMM) diapazono 5,8 GHz dažniu. 1 dalis. Keliuose ir transporto priemonėse įrengtų įtaisų bendrosios charakteristikos ir bandymo metodai}.

DSC_3 *Ryšys* su ryšių įranga turi būti užmezgamas tik jeigu tokią užklausą atsiunčia kontrolės institucijų įranga, naudojanti reikalavimus atitinkančias radijo ryšio priemones (*nuotolinio ankstyvo nustatymo skaitytuvas (REDCR)*).

DSC_4 *Duomenys* turi būti apsaugomi siekiant užtikrinti jų nepažeistumą.

DSC_5 Prieiga prie perduodamų *duomenų* suteikiama kompetentingoms kontrolės institucijoms, įgaliotoms tikrinti, ar nepažeidžiamas Reglamentas (EB) Nr. 561/2006 ir Reglamentas (ES) Nr. 165/2014, ir dirbtuvėms, jeigu būtina patikrinti, ar tachografas veikia tinkamai.

DSC_6 Užmezgus *ryšį* keičiamasi tik tais *duomenimis*, kurie yra būtini transporto priemonių, kurių tachografų duomenys gali būti klastojami arba netinkamai naudojami, tikslinėms patikroms kelyje atlikti.

DSC_7 Duomenų nepažeistumas ir saugumas užtikrinamas apsaugant transporto priemonės bloke laikomus *duomenis* ir perduodant tik apsaugotus informacinio turinio duomenis bei su saugumu susijusius duomenis (žr. 5.4.4) naudojant 5,8 GHz DSRC nuotolinio ryšio kanalą, t. y. užtikrinant, kad tik įgaliotieji kompetentingos kontrolės institucijos pareigūnai turi priemones, leidžiančias suprasti naudojant *ryšį* perduodamus duomenis ir patikrinti jų autentiškumą. Žr. 11 priedėlį „Bendrieji apsaugos mechanizmai“.

DSC_8 *Duomenys* turi būti pažymėti laiko žyma, rodančia, kada jie atnaujinti paskutinį kartą.

DSC_9 Saugumo duomenų turinys turi būti žinomas tik kompetentingoms kontrolės institucijoms ir jų tvarkomas bei prieinamas toms šalims, su kuriomis kontrolės institucijos dalijasi šia informacija, o turiniui netaikomos nuostatos ryšio, kuriam galioja šio priedėlio reikalavimai, išskyrus tuo atveju, jeigu ryšio nuostatomis numatoma saugumo duomenų paketą perduoti su kiekvienu informacinio turinio duomenų rinkiniu.

DSC_10 Ta pati architektūra ir įranga turi būti tinkama pritaikyti prie kitų duomenų struktūrų (pvz., transporto priemonėje įrengta svėrimo įranga) naudojant šiame priedėlyje nurodytą architektūrą.

DSC_11 Paaiškiname, kad pagal Reglamento (ES) Nr. 165/2014 (7 straipsnio) nuostatas vairuotojo tapatybės duomenys neturi būti perduodami naudojant *ryšį*.

2 TAIKYMO SRITIS

Šiame priedėlyje nustatoma, kaip kompetentingų kontrolės institucijų pareigūnai naudoja 5,8 GHz DSRC belaidį ryšį, kad užmezgus nuotolinį ryšį iš pasirinktų transporto priemonių būtų gaunami duomenys

▼B

(*duomenys*), kuriais remiantis būtų įmanoma daryti prielaidą, jog pasirinktoji transporto priemonė pažeidžia Reglamentą (ES) Nr. 165/2014, ir todėl ją reikėtų sustabdyti ir nuodugniai patikrinti.x

Reglamente (ES) Nr. 165/2014 nurodoma, kad turi būti renkami tik tie duomenys, kuriais remiantis nustatomas galimas pažeidimas ar su juo susiję duomenys, kaip apibrėžta Reglamento (ES) Nr. 165/2014 9 straipsnyje.

Pagal šį scenarijų perdavimui skiriamas ribotas laikas, nes *ryšys* yra tikslinis ir veikia tik trumpuoju atstumu. Be to, tas pačias tachografo nuotolinės kontrolės (RTM) ryšio priemones kompetentingos kontrolės institucijos taip pat gali rinktis kitiems tikslams (pvz., Direktyvoje 2015/719/EB nustatytai didžiausiai leidžiamai sunkiasvorių krovinių transporto priemonių masei ir matmenims kontroliuoti) ir kompetentingų kontrolės institucijų nuožiūra šios operacijos gali būti atliekamos atskirai arba paeiliui.

Šiame priedėlyje nustatoma:

— ryšio įranga, taikytinos *ryšio* procedūros ir protokolai;

— standartai ir taisyklės, kuriuos turi atitikti radijo ryšio įranga;

— *duomenų* perdavimas *ryšio* įrangai;

— užklausos ir duomenų atsisiuntimo procedūros ir operacijų eiliškumas;

— perduotini *duomenys;*

— galimas *duomenų,* perduotų naudojant *ryšį*, aiškinimas;

— su *ryšiu* susijusių saugumo duomenų nuostatos;

— *duomenų* prieinamumas kompetentingoms kontrolės institucijoms;

— kaip *nuotolinio ankstyvo nustatymo ryšio skaitytuvas* gali siųsti užklausą dėl skirtingos struktūros duomenų apie krovinį ir automobilių parką.

Pažymėtina, kad šiame priedėlyje nėra nustatoma:

— *duomenų* rinkimas ir tvarkymas transporto priemonės bloke (tai turi būti projektuojant produktą numatyta funkcija, jeigu tai nenurodyta kurioje nors kitoje Reglamento (ES) Nr. 165/2014) vietoje;

— nei surinktų duomenų pateikimo kompetentingos kontrolės institucijos pareigūnui forma, nei kriterijai, kuriais remdamosi kompetentingos kontrolės institucijos spręstų, kurią transporto priemonę būtina sustabdyti (tai turi būti numatyta projektuojant produktą, jeigu kitaip nenustatyta nors kitoje Reglamento (ES) Nr. 165/2014 vietoje arba jeigu kompetentingos kontrolės institucijos nėra priėmusios politinio sprendimo). Atkreipiame dėmesį, kad: *duomenys* naudojant *ryšį* tik perduodami kompetentingoms kontrolės institucijoms, kad jos galėtų priimti pagrįstus sprendimus;

▼B

— duomenų saugumo nuostatos (pvz., užšifravimo) dėl *duomenų* turinio (jos nustatomos 11 priedėlyje „Bendrieji apsaugos mechanizmai“);

— išsami informacija apie visas duomenų struktūras, išskyrus RTM, kurią galima gauti naudojant tą pačią architektūrą ir įrangą;

— išsami informacija apie veikimą ir transporto priemonės bloko bei DSRC-VU derinimą ir DSRC-VU veikimas (išskyrus *duomenų* pateikimą, kai gaunama REDCR užklausa).

3 SANTRUMPOS, APIBRĖŽTYS IR ŽYMENYS

Šiame priedėlyje vartojamos santrumpos ir sąvokų apibrėžtys

Antena	kartu su radijo siųstuvu arba radijo imtuvu naudojamas elektros prietaisas, elektros energiją verčiantis radijo bangomis ir atvirkščiai. Veikiantis radijo siųstuvas aukštojo dažnio virpesius elektros grandinėje perduoda į antenos įvadus ir ji išspinduliuoja elektros srovės energiją elektromagnetinėmis bangomis (radijo bangomis). Priimamoji antena tam tikrą elektromagnetinių bangų energiją paverčia silpna elektros įtampa antenos įvaduose, ir ši įtampa perduodama į imtuvą, kur ji yra sustiprinama.
Ryšys	informacijos ir (arba) duomenų mainai tarp DSRC-REDCR ir DSRC-VU pagal 5 skirsnį užtikrinant pagrindinio ir pavaldžiojo įrenginio ryšį, kad būtų gaunami duomenys.
Duomenys	apibrėžto formato apsaugotieji duomenys (žr. 5.4.4), dėl kurių užklausą pateikia *DSRC-REDCR* ir kuriuos *DSRC-VU* pateikia *DSRC-REDCR* naudodamas 5 punkte apibrėžtą 5,8 GHz DSRC ryšio kanalą.
Reglamentas (ES) Nr. 165/2014	2014 m. vasario 4 d. Europos Parlamento ir Tarybos Reglamentas Nr. 165/2014 dėl kelių transporto priemonėse naudojamų tachografų, kuriuo panaikinamas Tarybos reglamentas (EEB) Nr. 3821/85 dėl kelių

▼B

	transporto priemonėse naudojamų tachografų ir iš dalies keičiamas Europos Parlamento ir Tarybos reglamentas (EB) Nr. 561/2006 dėl tam tikrų su kelių transportu susijusių socialinių teisės aktų suderinimo.
AID	taikomosios programos identifikatorius
BLE	mažai energijos naudojanti „Bluetooth“ technologija
BST	tikrinimo kelyje įrangos parengti ir perduoti duomenys
CIWD	kortelė įstatyta važiuojant
CRC	ciklinė perteklinė kontrolė
DSC (n)	tam tikram DSRC priedėliui taikomo reikalavimo identifikatorius
DSRC	skirtasis trumpojo nuotolio ryšys
DSRC-REDCR	DSRC nuotolinio ankstyvo nustatymo ryšio skaitytuvas
DSRC-VU	DSRC transporto priemonės blokas. Tai 1C priede apibrėžtas nuotolinio ankstyvo nustatymo įrenginys
DWVC	važiavimas be galiojančios kortelės
EID	elemento identifikatorius
LLC	loginio ryšio valdymas
LPDU	LLC protokolo duomenų vienetas
OWS	transporto priemonėje įrengta svėrimo sistema
PDU	protokolo duomenų vienetas
REDCR	nuotolinio ankstyvo nustatymo ryšio skaitytuvas. Tai 1C priede apibrėžtas nuotolinio ankstyvo nustatymo ryšio skaitytuvas
RTM	nuotolinė tachografo kontrolė
SM-REDCR	saugumo modulis – nuotolinio ankstyvo nustatymo ryšio skaitytuvas
TARV	telematikos priemonių taikymas reglamentuojamoms transporto priemonėms (ISO 15638 serijos standartai)

▼B

VU	transporto priemonės blokas
VUPM	naudingoji transporto priemonės bloko atmintis
VUSM	transporto priemonės bloko saugumo modulis
VST	transporto priemonės informacijos blokas
WIM	važiuojančių transporto priemonių masės nustatymo sistema
WOB	transporto priemonės įranga duomenims apie jos masę perduoti

Šiame priedėlyje nustatyta specifikacija grindžiama visais toliau nurodytais reglamentais ir standartais ir susijusi su jais arba jų dalimis. Šio priedėlio punktuose nurodomi atitinkami standartai arba tam tikri jų punktai. Jeigu nustatomas koks nors prieštaravimas, pirmenybė teikiama šio priedėlio punktams. Jeigu iškyla koks nors prieštaravimas, o šiame priedėlyje nėra aiškiai nustatyta specifikacija, naudojimui taikant ERC 70-03 (ir atlikus bandymą pagal atitinkamus standarte EN 300 674-1 nustatytus parametrus) teikiama pirmenybė ir galioja (mažėjančia svarbumo eile) EN 12795, EN 12253, EN 12834 ir EN 13372, 6.2, 6.3, 6.4 ir 7.1.

Šiame priedėlyje nurodyti šie reglamentai ir standartai:

[1] 2014 m. vasario 4 d. Europos Parlamento ir Tarybos Reglamentas Nr. 165/2014 dėl kelių transporto priemonėse naudojamų tachografų, kuriuo panaikinamas Tarybos reglamentas (EEB) Nr. 3821/85 dėl kelių transporto priemonėse naudojamų tachografų ir iš dalies keičiamas Europos Parlamento ir Tarybos reglamentas (EB) Nr. 561/2006 dėl tam tikrų su kelių transportu susijusių socialinių teisės aktų suderinimo;

[2] 2006 m. kovo 15 d. Europos Parlamento ir Tarybos reglamentas Nr. 561/2006 dėl tam tikrų su kelių transportu susijusių socialinių teisės aktų suderinimo ir iš dalies keičiantis Tarybos reglamentus (EEB) Nr. 3821/85 ir (EB) Nr. 2135/98 bei panaikinantis Tarybos reglamentą (EEB) Nr. 3820/85 (tekstas svarbus EEE);

[3] ERC 70-03 CEPT. ECC rekomendacija Nr. 70-03, susijusi su trumpojo nuotolio įrangos (SRD) naudojimu;

[4] ISO 15638. Intelektinės transporto sistemos. Reglamentuojamoms komercinėms krovininėms transporto priemonėms taikoma bendradarbiavimo telematikos priemonių sistema (TARV);

[5] EN 300 674-1. Elektromagnetinio suderinamumo ir radijo dažnių spektro dalykai; Informacijos apie kelių transportą ir eismą apdorojimo bei perdavimo priemonės; Skirtoji trumpojo nuotolio ryšių perdavimo įranga (500 kbit/s ir (arba) 250 kbit/s spartos), veikianti pramonės, mokslo ir medicinos (PMM) diapazono 5,8 GHz dažniu. 1 dalis. Keliuose ir transporto priemonėse įrengtų įtaisų bendrosios charakteristikos ir bandymo metodai.

[6] EN 12253. Informacijos apie kelių transportą ir eismą apdorojimo bei perdavimo priemonės. Skirtoji trumpojo nuotolio ryšio sistema. Fizinis lygmuo, naudojant 5,8 GHz dažnį;

▼B

[7] EN 12795. Informacijos apie kelių transportą ir eismą apdorojimo bei perdavimo priemonės. Skirtoji trumpojo nuotolio ryšio sistema. Duomenų ryšio lygmuo. Prieiga prie laikmenos ir loginio kanalo valdymas.

[8] EN 12834. Informacijos apie kelių transportą ir eismą apdorojimo bei perdavimo priemonės. Skirtoji trumpojo nuotolio ryšio sistema. Taikomasis lygmuo;

[9] EN 13372 Informacijos apie kelių transportą ir eismą apdorojimo bei perdavimo priemonės. Skirtoji trumpojo nuotolio ryšio sistema. Šios sistemos profilių taikymas informacijos apie kelių transportą ir eismą apdorojimui bei perdavimui;

[10] ISO 14906 Elektroninis mokesčių rinkimas. Skirtosios trumpojo nuotolio ryšio sistemos sietuvo apibrėžtis.

4 NAUDOJIMO MODELIAI

4.1 **Apžvalga**

Reglamentu (ES) Nr. 165/2014 nustatyti specialūs ir reglamentuojami naudotini *ryšio* modeliai.

Užtikrinamas šių modelių naudojimas:

1 ryšio profilis. Patikrinimas keliuose naudojant trumpojo nuotolio belaidį nuotolinio ankstyvo nustatymo ryšio skaitytuvą siekiant atlikti fizinį patikrinimą kelyje (pagrindinis įrenginys ir pavaldusis įrenginys);

1a skaitytuvo profilis. Nutaikomas ranka arba laikinai pritvirtinamas pakelėje ir nutaikomas nuotolinio ankstyvo nustatymo ryšio skaitytuvas.

1b skaitytuvo profilis. Transporto priemonėje įmontuotas ir nukreipiamas nuotolinio ankstyvo nustatymo ryšio skaitytuvas.

4.1.1 *Išankstinės duomenų perdavimo per 5,8 GHz DSRC sąsają sąlygos*

PASTABA. Kad būtų lengviau suprasti išankstinių sąlygų kontekstą, siūloma peržiūrėti toliau pateiktą 14.3 pav.

4.1.1.1 Transporto priemonės bloke laikomi duomenys

DSC_12 Transporto priemonės blokas turi atnaujinti savo atmintyje saugomus duomenis kas 60 sekundžių ir juos tvarkyti – nepriklausomai nuo DSRC ryšio funkcijos. Priemonės, kuriomis tai užtikrinama, yra pačiame transporto priemonės bloke, jos nustatomos Reglamento (ES) Nr. 165/2014 1 C priedo 3.19 skirsnyje „Nuotolinis ryšys tikslinėms patikroms kelyje atlikti“, o ne šiame priedėlyje.

4.1.1.2 Į DSRC-VU įrenginį perduodami duomenys

DSC_13 Transporto priemonės blokas turi atnaujinti DSRC tachografo duomenis (*duomenis*) kaskart, kai transporto priemonės bloke laikomi duomenys atnaujinami 4.1.1.1 punkte (DSC_12) nustatytu intervalu – nepriklausomai nuo DSRC ryšio funkcijos.

DSC_14 Transporto priemonės bloko duomenys naudojami *duomenims* rinkti ir atnaujinti, o priemonės, kuriomis tai užtikrinama, nurodomos 1 C priedo 3.19 skirsnyje „Nuotolinis ryšys tikslinėms patikroms kelyje atlikti“ arba, jeigu tokios specifikacijos nėra, yra produkto konstrukcijos funkcija ir šiame priedėlyje nenustatomos. DSRC-VU įrenginio jungties su transporto priemonės bloku konstrukcija apibūdinta 5.6 skirsnyje.

▼B

4.1.1.3 Duomenų turinys

DSC_15 *Duomenų* turinys ir forma turi būti tokia, kad juos iššifravus turinio bei formos struktūra ir jų pateikimas atitiktų šio priedėlio 5.4.5 skirsnyje nustatytą formą ir formatą (duomenų struktūros).

4.1.1.4 Duomenų pateikimas

DSC_16 *Duomenys*, kurie periodiškai atnaujinami pagal 4.1.1.1 punkte apibrėžtas procedūras, turi būti apsaugomi prieš juos perduodant į *DSRC-VU* ir pateikiami taikant apsaugotų duomenų struktūros vertę laikinajam laikymui *DSRC-VU* kaip dabartinė *duomenų* versija. Šie duomenys iš *VUSM* perduodami DSRC funkcijai *VUPM*. *VUSM* ir *VUPM* yra funkcijos ir nebūtinai fiziniai objektai. Fizinė šių funkcijų vykdymo priemonės turi būti numatomos projektuojant produktą, jeigu jos nenurodytos kurioje nors kitoje Reglamento (ES) Nr. 165/2014 vietoje.

4.1.1.5 Saugumo duomenys

DSC_17 Saugumo duomenys (*securityData)*, kurie yra būtini, kad REDCR galėtų iššifruoti *duomenis*, turi būti perduodami taip, kaip apibrėžta 11 priedėlyje „Bendrieji apsaugos mechanizmai“, ir pateikiami kaip duomenų struktūros vertė laikinajam laikymui *DSRC-VU* kaip dabartinė *securityData* versija šio priedėlio 5.4.4 punkte apibrėžta forma.

4.1.1.6 Per DSRC sąsają perduodami VUPM duomenys

DSC_18 Duomenų struktūra, kuri visada turi būti prieinama naudojant DSRC funkciją neatidėliotinam VUPM perdavimui, kai siunčiama užklausa iš *REDCR*, apibrėžiama išsamiomis ASN.1 Modulio specifikacijomis 5.4.4 punkte.

Bendroji 1 ryšio profilio apžvalga

Šis profilis apima naudojimo modelį, kai siekdamas nuotoliniu būdu nustatyti transporto priemonę, kuri galbūt pažeidžia Reglamentą (ES) Nr. 165/2014, kompetentingų kontrolės institucijų pareigūnas naudoja trumpojo nuotolio nuotolinio ryšio nuotolinio ankstyvo nustatymo ryšio skaitytuvą (pagal ERC 70-03 nuostatas naudojamos 5,8 GHz DSRC sąsajos, išbandytos pagal atitinkamus standarto EN 300 674-1 parametrus, kaip nustatyta 5skirsnyje). Užbaigęs identifikavimą, tyrimą atliekantis kompetentingų kontrolės institucijų pareigūnas sprendžia, ar transporto priemonę reikėtų sustabdyti.

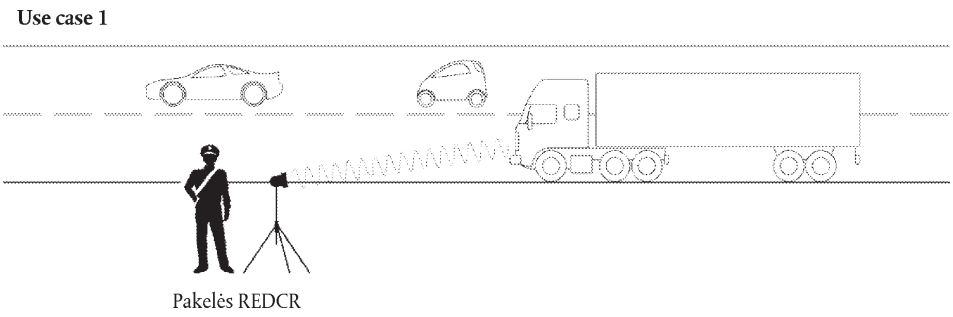
4.1.2 *1a profilis. Nutaikomas ranka arba laikinai pritvirtinamas pakelėje ir nutaikomas nuotolinio ankstyvo nustatymo ryšio skaitytuvas*

Jeigu pasirenkamas šis naudojimo modelis, kompetentingų kontrolės institucijų pareigūnas stovi pakelėje ir rankinį, arba pritvirtintą prie trikojo, arba panašų nešiojamąjį *REDCR* nukreipia į pasirinktos transporto priemonės priekinio stiklo vidurį. Užklausai atlikti naudojamos 5,8 GHz DSRC sąsajos, taikomos pagal ERC 70-03 nuostatas, ir išbandytos pagal atitinkamus standarte EN 300 674-1 nustatytus parametrus, kaip aprašyta 5 skirsnyje. Žr. 14.1 pav. (1 naudojimo modelis).

▼B

14.1 pav.

Belaidė užklausa tikrinimo kelyje įranga naudojant 5,8 GHz DSRC

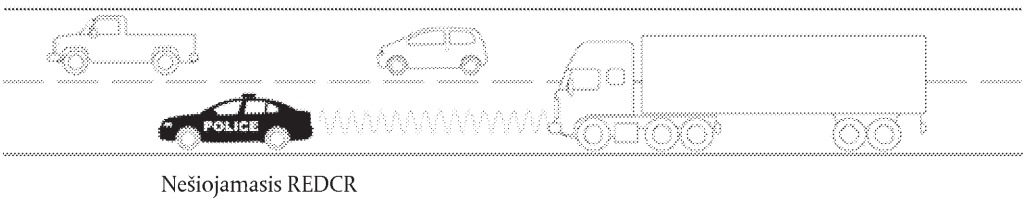


4.1.3 *1b profilis. Transporto priemonėje įmontuotas ir nukreipiamas nuotolinio ankstyvo nustatymo ryšio skaitytuvas*

Jeigu pasirenkamas šis naudojimo modelis, kompetentingų kontrolės institucijų pareigūnas būna važiuojančioje transporto priemonėje ir rankinį nešiojamąjį *REDCR* nukreipia į pasirinktos transporto priemonės priekinio stiklo vidurį, arba *REDCR* yra įmontuotas transporto priemonėje arba sumontuotas ant jos taip, kad būtų nukreiptas į pasirinktos transporto priemonės priekinio stiklo vidurį, kai transporto priemonė su nuotolinio ankstyvo nustatymo ryšio skaitytuvu pasirinktosios transporto priemonės atžvilgiu yra tam tikroje padėtyje (pvz., eismo sraute važiuoja tiesiai prieš ją). Atliekant užklausą naudojamos 5,8 GHz DSRC sąsajos, taikomos pagal ERC 70-03 nuostatas, ir išbandytos taikant atitinkamus standarte EN 300 674-1 nustatytus parametrus, kaip aprašyta 5 skirsnyje. Žr. 14.2 pav. (2 naudojimo modelis).

14.2.

Užklausa transporto priemonėje esančia įranga naudojant 5,8 GHz DSRC



4.2 **Saugumas ir (arba) nepažeistumas**

Kad būtų galima patikrinti nuotoliniu ryšiu atsisiunčiamų duomenų autentiškumą ir nepažeistumą apsaugotieji *duomenys* yra tikrinami ir iššifruojami pagal 11 priedėlio „Bendrieji apsaugos mechanizmai“ nuostatas.

5 NUOTOLINIO RYŠIO TECHNOLOGIJA IR PROTOKOLAI

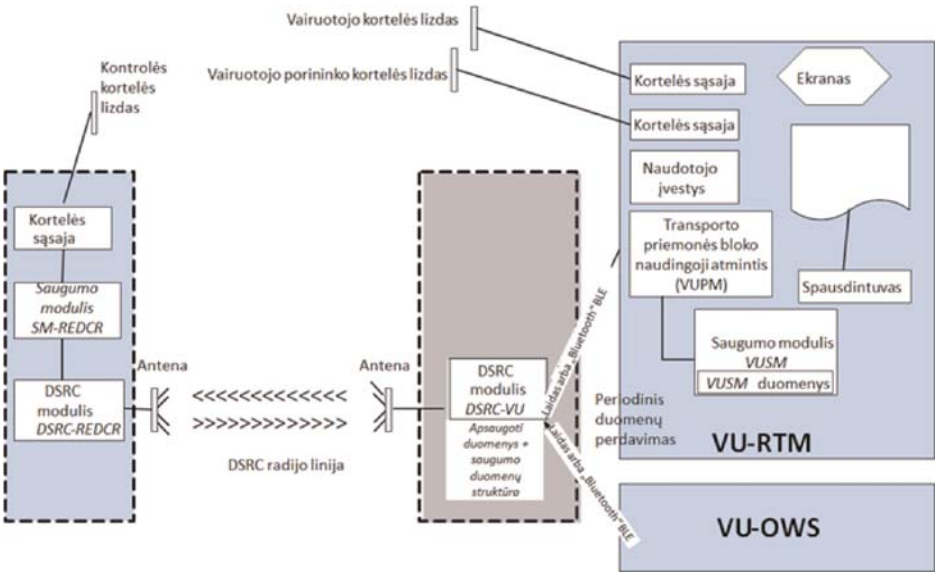
5.1 **Technologija**

Išmaniuosiuose tachografuose taikoma nuotolinio ryšio technologija pavaizduota 14.3 pav.

▼B

14.3 pav.

Nuotolinio ryšio technologija



DSC_19 Transporto priemonės bloke yra šios funkcijos:

— Saugumo modulis (*VUSM*). Taikant šią transporto priemonės bloko funkciją užtikrinamas kompetentingų kontrolės institucijų pareigūnui iš *DSRC-VU* nuotoliniu ryšiu perduotinų *duomenų* saugumas.

— Apsaugotieji duomenys laikomi VUSM atmintyje. 4.1.1.1 punkte (DSC_12) nustatytais intervalais transporto priemonės blokas užšifruoja ir papildo DSRC-VU atmintyje laikomą RTM duomenų struktūrą (ji apima šiame priedėlyje nustatytas informacinio turinio duomenų ir saugumo duomenų struktūros vertes). Saugumo modulio veikimas apibrėžtas 11 priedėlyje „Bendrieji apsaugos mechanizmai“ ir jam šio priedėlio nuostatos netaikomos, išskyrus šiam moduliui nustatytą reikalavimą, kad jis turi pateikti atnaujintus duomenis VU ryšio įrenginiui kaskart, kai pakeičiami VUSM duomenys.

— VU ryšys su DSRC-VU gali būti laidinis ryšys arba mažai energijos naudojanti „Bluetooth“ (BLE) ryšio technologija, o fizinė DSRC-VU buvimo vieta gali būti prie transporto priemonės priekinio stiklo pritvirtinta antena, DSRC-VU gali būti transporto priemonės bloko viduje arba kokioje nors kitoje vietoje.

— DSRC-VU turi būti sujungtas su patikimu nenutrūkstamą maitinimą užtikrinančiu energijos šaltiniu. Priemonės, kuriomis užtikrinamas nenutrūkstamas maitinimas, numatomos projektuojant gaminį.

— DSRC-VU atmintis turi būti ilgalaikė, kad DSRC-VU sukaupti duomenys būtų išlaikyti ir tada, kai išjungiamas transporto priemonės uždegimo jungiklis.

— Jeigu ryšys tarp VU ir DSRC-VU užtikrinamas naudojant BLE technologiją, o energijos šaltinis yra neįkraunamoji baterija, DSRC-VU energijos šaltinis turi būti keičiamas kaskart, kai atliekama periodinė patikra, o už tai, kad

▼B

maitinimo užtikrinimas nuo vienos periodinės patikros iki kitos periodinės patikros būtų adekvatus ir visą tą laikotarpį REDCR turėtų įprastą prieigą prie duomenų be trikčių arba pertrūkių, yra atsakingas DSRC-VU įrangos gamintojas.

— VU RTM naudingoji atmintis (*VUPM*). Ši transporto priemonės bloko funkcija yra skirta *duomenims* pateikti ir atnaujinti. *Duomenų* turinys. („TachographPayload“) apibrėžiama tolesniuose 5.4.4/5.4.5 punktuose ir atnaujinama 4.1.1.1 punkte (DSC_12) nustatytais intervalais.

— DSRC-VU. Ši funkcija, įdiegta antenoje arba su ja susieta, naudojant laidinę ar belaidę (BLE) technologiją užtikrina ryšį su transporto priemonės bloku, kuriame laikomi esami duomenys (*VUPM duomenys*), ir garantuoja atsaką į užklausą, pateiktą naudojant 5,8 GHz DSRC ryšį. DSRC įrenginio atjungimas arba jo veikimo trukdžiai įprastu būdu eksploatuojant transporto priemonę turi būti laikomi Reglamento (ES) Nr. 165/2014 pažeidimu.

— Saugumo modulis (REDCR) (*SM-REDCR*) naudojamas iš transporto priemonės bloko perduodamiems duomenims iššifruoti ir jų nepažeistumui patikrinti. Priemonės, kuriomis tai užtikrinama, nustatomos 11 priedėlyje „Bendrieji saugumo mechanizmai“, o ne šiame priedėlyje.

— DSRC įrenginyje (REDCR) (*DSRC-REDCR*) numatyta funkcija apima 5,8 GHz siųstuvą-imtuvą ir susijusią aparatinę bei programinę įrangą, pagal šį priedėlį užtikrinančią *ryšį* su *DSRC-VU*.

— Naudodamas DSCR kanalą *DSRC-REDCR* užmezga ryšį su pasirinktos transporto priemonės *DSRC-VU* ir gauna *duomenis* (pasirinktosios transporto priemonės esamus *VUPM duomenis*) ir gautus duomenis apdoroja bei laiko DSCR *SM-REDCR*.

— *DSRC-VU* antena montuojama tokioje vietoje, kad DSRC ryšys tarp transporto priemonės ir tikrinimo kelyje įrangos antenos būtų optimalus (paprastai transporto priemonės priekinio stiklo centre arba arti jo). Jeigu tai yra lengvosios transporto priemonės, anteną galima montuoti viršutinėje priekinio stiklo dalyje.

— Priešais anteną arba greta jos neturi būti ryšį galinčių trikdyti metalinių objektų (pvz., pavadinimo plokštelių, lipdukų, neatspindžiosios folijos juostelių (spalvotų juostelių), nuo saulės spindulių apsaugančių skydelių, priekinio lango valytuvo, kai jis nenaudojamas).

— Antena turi būti tvirtinama taip, kad jos didžiausio spinduliavimo ašis būtų apytikriai lygiagreti su kelio paviršiumi.

▼B

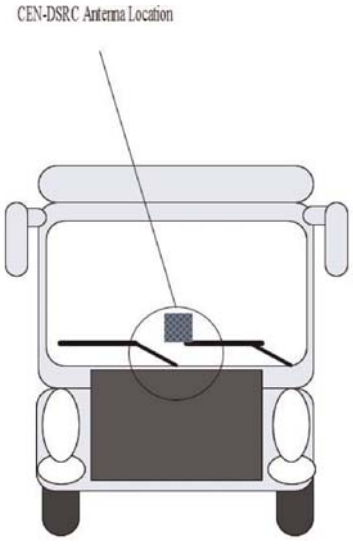
DSC_20 Antena ir ryšys naudojamas taip, kaip nustatyta ERC 70-03, išbandytas pagal atitinkamus standarto EN 300 674-1 parametrus, kaip aprašyta 5 skirsnyje. Naudojant anteną ir užmezgant ryšį galima taikyti belaidžių trukdžių rizikos mažinimo priemones, aprašytas Europos ryšių komiteto (ECC) atskaitoje Nr. 228, pvz., CEN DSRC 5,8 GHz ryšio filtrus.

DSC_21 DSRC antena su DSRC-VU įrenginiu sujungiama pritvirtintame modulyje tiesiogiai ar greta priekinio stiklo arba naudojant specialų laidą, kurio konstrukcija tokia, kad jį būtų sunku neteisėtai atjungti. Antenos atjungimas arba jos veikimo trikdymas laikomas Reglamento (ES) Nr. 165/2014 pažeidimu. Tyčinis antenos veikimo apribojimas ar jos eksploatacines charakteristikas bloginantis kitoks poveikis laikomas Reglamento (ES) Nr. 165/2014 pažeidimu.

DSC_22 Antenos formos faktorius nėra apibrėžtas ir jo pasirinkimas yra komercinis sprendimas, jeigu įtaisytas DSRC-VU atitinka 5 skirsnyje apibrėžtus atitikties reikalavimus. Antenos įtaisymo vieta parenkama, kaip nurodyta DSC_19 punkte ir pavaizduota 14.4 pav. (ovalo formos linija), ji turi būti tinkama naudoti su 4.1.2 ir 4.1.3 aprašytais naudojimo būdais.

14.4 pav.

5,8 GHz DSRC antenos įtaisymo vietos ant reglamentuojamos transporto priemonės priekinio stiklo pavyzdys



REDCR ir jo antenos formos faktorius gali skirtis atsižvelgiant į skaitytuvo pobūdį (tvirtinamas prie trikojo, rankinis, tvirtinamas ant transporto priemonės) ir kompetentingos kontrolės institucijos pareigūno pasirinktą naudojimo būdą.

Rodymo ir (arba) pranešimo funkcijos paskirtis yra pateikti nuotolinio ryšio funkcijos rezultatus kompetentingos kontrolės institucijos pareigūnui. Rodymas gali būti rodinys ekrane, spaudinys, garsinis signalas arba šių pranešimų derinys. Šio rodymo ir (arba) pranešimo formos reikalavimus nustato kompetentingos kontrolės institucijos pareigūnai ir šie reikalavimai priklauso nuo įrangos konstrukcijos, todėl šiame priedėlyje jie nenustatomi.

▼B

DSC_23 *REDCR* konstrukcija ir formos faktorius turi būti komercinės konstrukcijos, taikomos pagal ERC 70-30 nuostatas, funkcija ir šiame priedėlyje (5.3.2 punkte) nustatytų konstrukcijos ir eksploatavimo specifikacijų funkcija siekiant užtikrinti didžiausią rinkos lankstumą projektuojant ir tiekiant įrangą, kad būtų įmanoma patenkinti konkrečius bet kurios kompetentingos kontrolės institucijos pasirinktus užklausos modelius.

DSC_24 *DSRC-VU* konstrukcija ir formos faktorius bei jo vieta transporto priemonės bloko viduje ar už jo ribų turi būti komercinės konstrukcijos, taikomos pagal ERC 70-30 nuostatas, funkcija ir šiame priedėlyje (5.3.2 punkte) ir šiame punkte (5.1) nustatytų konstrukcijos ir eksploatavimo specifikacijų funkcija.

DSC_25 Tačiau *DSRC-VU* turi būti tinkamai pritaikytas naudojant atvirojo pramonės standarto jungtį ir protokolus iš kitos išmaniosios transporto priemonės įrangos priimti duomenų struktūros vertes. (Pvz., iš transporto priemonėje įrengtos svėrimo įrangos) tol, kol šias duomenų struktūras įmanoma identifikuoti unikaliais ir žinomais programos identifikatoriais ir (arba) rinkmenų pavadinimais, o nurodymai naudoti šiuos protokolus turi būti pateikiami Europos Komisijai ir nemokamai prieinami atitinkamos įrangos gamintojams.

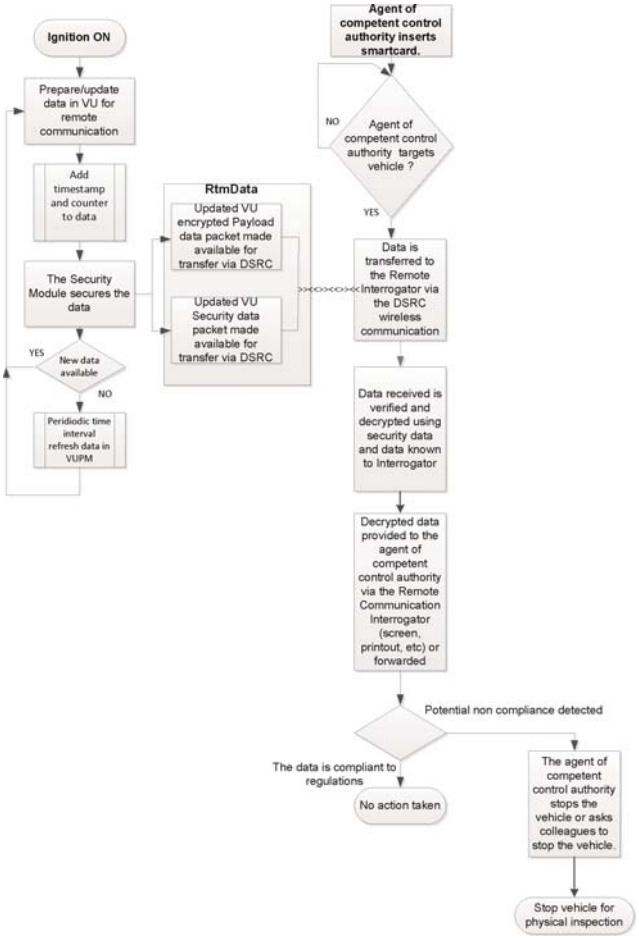
5.2 **Operacijų seka**

5.2.1 *Operacijos*

Operacijų seka pavaizduota 14.5 pav.

14.5 pav.

Nuotolinio ryšio funkcijos operacijų seka



▼B

Etapai aprašyti toliau.

a. Jeigu transporto priemonė yra eksploatuojama (ĮJUNGTAS degimas), tachografas perduoda duomenis transporto priemonės bloko funkcijai. Transporto priemonės bloko funkcija parengia *duomenis* nuotolinio ryšio funkcijai (užšifruoja) ir atnaujina *DSRC-VU* atmintyje laikomą *VUPM* (kaip apibrėžta 4.1.1.1–4.1.1.2 punktuose). Surinkti duomenys formatuojami pagal toliau 5.4.4–5.4.5 punktuose pateiktas nuostatas.

b. Kiekvieną kartą atnaujinant *duomenis* saugumo duomenų struktūroje apibrėžta laiko žyma turi būti atnaujinama.

c. Naudojant *VUSM* funkciją duomenys apsaugomi taikant 11 priedėlyje apibrėžtas procedūras.

d. Kiekvieną kartą atnaujinant *duomenis* (žr. 4.1.1.1–4.1.1.2 punktus) jie turi būti perduodami į *DSRC-VU*, kur jie pakeičia visus ankstesnius duomenis siekiant užtikrinti, kad atnaujinti esami duomenys (*duomenys*) visada būtų prieinami, jeigu *REDCT* pateiktų užklausą. Kai *duomenys* iš transporto priemonės bloko perduodami į DSRC-VU, jie turi būti identifikuojami rinkmenos pavadinimu *RTMData* arba ApplicationID ir požymio identifikatoriais.

e. Jeigu kompetentingų kontrolės institucijų pareigūnas ketina patikrinti transporto priemonę ir iš pasirinktosios transporto priemonės atsisiųsti *duomenis*, jis pirmiausia į *REDCR* turi įkišti savo lustinę kortelę, kad būtų užmezgamas *ryšys*, ir palaukti, kol *SM-REDCR* patikrins jos autentiškumą ir iššifruos duomenis.

f. Tada kompetentingų kontrolės institucijų pareigūnas pasirenka transporto priemonę ir pateikia užklausą nuotoliniu ryšiu atsiųsti duomenis. *REDCR* pradeda 5,8 GHz DSRC sąsajos seansą su pasirinktosios transporto priemonės *DSRC-VU* ir siunčia *duomenų* užklausą. *Duomenys* į *REDCR* perduodami belaidžio ryšio sistema kaip DSRC požymis, naudojant 5.4 punkte apibrėžtą taikomąją paslaugą GET. Į požymį yra įtrauktos iššifruotų informacinio turinio duomenų vertės ir DSCR saugumo duomenys.

g. Duomenis analizuoja *REDCR* įranga ir tada jie pateikiami kompetentingų kontrolės institucijų pareigūnui.

h. Kompetentingų kontrolės institucijų pareigūnas remiasi duomenimis nuspręsdamas, ar transporto priemonę stabdyti ir ją nuodugniai patikrinti ar jos nestabdyti arba prašyti kito kompetentingų kontrolės institucijų pareigūno, kad jis sustabdytų transporto priemonę.

5.2.2 *Naudojant DSRC ryšį gautų duomenų aiškinimas*

DSC_26 Per 5,8 GHz sąsają gautuose duomenyse turi būti nurodoma toliau 5.4.4 ir 5.4.5 punktuose apibrėžta reikšmė ir importas bei tik ši reikšmė ir importas ir jie turi būti suprantami atsižvelgiant į tuose punktuose nustatytus tikslus. Pagal Reglamento (ES) Nr. 165/2014 nuostatas *duomenys* turi būti naudojami tik atitinkamai informacijai pateikti kompetentingai kontrolės institucijai siekiant jai padėti nustatyti, kuri transporto

▼B

priemonė turėtų būtų stabdoma fizinei patikrai, ir šie duomenys vėliau turi būti sunaikinami pagal Reglamento (ES) Nr. 165/2014 9 straipsnį.

5.3 **Nuotolinio ryšio DSRC fizinės sąsajos parametrai**

5.3.1 *Su vieta susiję apribojimai*

DSC_27 Nuotolinės užklausos siuntimas transporto priemonėms taikant 5,8 GHz DSRC sąsają neturėtų būti vykdomas 200 metrų atstumu nuo naudojamos 5,8 GHz DSRC santvaros.

5.3.2 *Žemynkryptės ryšio linijos ir aukštynkryptės ryšio linijos parametrai*

DSC_28 Nuotolinės tachografo kontrolės įranga turi atitikti ERC70-03 nuostatas ir būti eksploatuojama pagal jas bei atitikti toliau 14.1 ir 14.2 lentelėse nustatytus parametrus.

DSC_29 Be to, siekiant užtikrinti suderinamumą su kitų standartinių 5,8 GHz DSRC sistemų veikimo parametrais, nuotolinės tachografo kontrolės įranga turi atitikti EN 12253 ir EN 13372 standartuose nustatytus parametrus.

Nustatyti parametrai

14.1 lentelė.

Žemynkryptės ryšio linijos parametrai

Objekto Nr.	Parametras	Vertė (-ės)	Pastaba
D1	Žemynkryptės ryšio linijos nešlio dažniai	Naudojant REDCR galima rinktis keturias galimybes: 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	Pagal ERC 70-03 Nešlio dažnius gali rinktis tikrinimo kelyje sistemos įgyvendintojas ir jie neturi būti žinomi DSCR-VU (Atitinka standartus EN 12253, EN 13372)
D1a (*)	Leidžiamoji nešlio dažnių nuokrypa	± 5 ppm	(Atitinka standartą EN 12253)
D2 (*)	RSU (REDCR) siųstuvo spektro kaukė	Pagal ERC 70-03. REDCR turi atitikti standarte EN 12253 apibrėžtą B, C klasę. Šiame priede nėra kitų konkrečių reikalavimų	Parametras naudojamas gretimų užklausiklių trukdžiams kontroliuoti (kaip apibrėžta standartuose EN 12253 ir EN 13372).
D3	OBU(DSRC-VU) mažiausias dažnio intervalas	5,795–5,815 GHz	(Atitinka standartą EN 12253)
D4 (*)	Didžiausia E.I.R.P. (efektyvioji izotropinės spinduliuotės galia)	Pagal ERC 70-03 (nelicencijuojama) ir laikantis nacionalinių taisyklių Ne daugiau kaip + 33 dBm	(Atitinka standartą EN 12253)

▼B

Objekto Nr.	Parametras	Vertė (-ės)	Pastaba
D4a	Kampinė E.I.R.P. kaukė	Pagal užklausiklio projektuotojo deklaruotą ir paskelbtą specifikaciją	(Atitinka standartą EN 12253)
D5	Poliarizacija	Kairinė apskritiminė	(Atitinka standartą EN 12253)
D5a	Kryžminė poliarizacija	XPD: Išilgai didžiausio antenos spinduliavimo ašies: (REDCR) RSU t ≥ 15 δB (DSRC-VU) OBU r ≥ 10 δB – 3 dB zonoje: (REDCR) RSU t ≥ 10 δB (DSRC-VU) OBU r ≥ 6 δB	(Atitinka standartą EN 12253)
D6 (*)	Moduliavimas	Dviejų lygių amplitudės moduliavimas	(Atitinka standartą EN 12253)
D6a (*)	Moduliacijos rodiklis	0,5 ... 0,9	(Atitinka standartą EN 12253)
D6b	Akies diagrama	≥ 90 proc. (laikas) / ≥ 85 proc. (amplitudė)	
D7 (*)	Duomenų kodavimas	FM0 „1“ bitas perėjimus turi tik bitų intervalo pradžioje ir pabaigoje. „0“ bitas turi papildomą perėjimą bito intervalo viduryje, palyginti su 1 bitu.	(Atitinka standartą EN 12253)
D8 (*)	Sparta bitais	500 kBit/sek.	(Atitinka standartą EN 12253)
D8a	Bitų taktų signalo leidžiamoji paklaida	Geresnė kaip ± 100 ppm	(Atitinka standartą EN 12253)
D9 (*)	Bitų klaidų dažnis (B.E.R.) užmezgant ryšį	≤ 10^{-6}, jeigu krintančioji galia OBU (DSRC-VU) atitinka intervalą, nustatytą [D11a–D11b].	(Atitinka standartą EN 12253)
D10	OBU (DSRC-VU) aktyvinimo trigeris	OBU (DSRC-VU) aktyvinamas, kai jam perduodamas bet koks kadras su 11 arba daugiau oktetų (įskaitant preambulę)	Nėra būtinas joks specialus aktyvinimo trigeris. DSRC-VU galima aktyvinti jam perdavus kadrą, sudarytą iš mažiau kaip 11 oktetų (Atitinka standartą EN 12253)
D10a	Ilgiausia paleidimo trukmė	≤ 5 ms	(Atitinka standartą EN 12253)
D11	Ryšio zona	Erdvės sritis, kurioje pagal D9a užtikrinamas B.E.R.	(Atitinka standartą EN 12253)
D11a (*)	Ryšio galios apribojimas (didžiausia vertė).	– 24dBm	(Atitinka standartą EN 12253)

▼B

Objekto Nr.	Parametras	Vertė (-ės)	Pastaba
D11b (*)	Ryšio galios apribojimas (mažiausia vertė).	Krintančioji galia: – 43 dBm (didžiausio antenos spinduliavimo ašis) – 41 dBm (neviršijant – 45° – + 45° ir atsižvelgiant į plokštumą, lygiagrečią su kelio paviršiumi, kai DSRC-VU vėliau įmontuojamas į transporto priemonę (azimutas)	(Atitinka standartą EN 12253) Papildomas reikalavimas dėl ne didesnių kaip ± 45° horizontaliųjų kampų atsižvelgiant į šiame priede apibrėžtus naudojimo modelius
D12 (*)	Galios atkirtimo lygis (DSRC-VU)	– 60 dBm	(Atitinka standartą EN 12253)
D13	Preambulė	Preambulė yra privaloma	(Atitinka standartą EN 12253)
D13a	Preambulės ilgis ir šablonas	►C2 16 bitų ± 1 FM0 bitas, koduotas „1“ bitais ◄	(Atitinka standartą EN 12253)
D13b	Preambulės bangos forma	Kintanti žemo lygio ir aukšto lygio seka 2 µs pulso trukme. Leidžiamoji nuokrypa nurodyta D8a	(Atitinka standartą EN 12253)
D13c	Pabaigos bitai	Leidžiama, kad RSU (REDCR) perduotų ne daugiau kaip 8 bitus po galinės žymos. Nereikalaujama, kad OBU (DSRC-VU) atsižvelgtų į šiuos papildomus bitus.	(Atitinka standartą EN 12253)

(*) Žemynkryptės ryšio linijos parametrams taikomas atitikties bandymas pagal standarte EN 300 674-1 nustatytus atitinkamus parametrus.

▼C2

14.2 lentelė.

Aukštynkryptės ryšio linijos parametrai

▼B

Objekto Nr.	Parametras	Vertė (-ės)	Pastaba
U1 (*)	Ponešlio dažniai	OBU (DSRC-VU) turi būti pritaikytas naudoti 1,5 MHz ir 2,0 MHz RSU (REDCR) turi būti pritaikytas naudoti 1,5 MHz arba 2,0 MHz, arba abu dažnius. U1-0: 1,5 MHz U1-1: 2,0 MHz	Ponešlio dažnio pasirinkimas (1,5 MHz arba 2,0 MHz) priklauso nuo pasirinkto standarte EN 13372 nustatyto profilio.
U1a (*)	Leidžiamosios ponešlio dažnių nuokrypos	± 0,1 proc.	(Atitinka standartą EN 12253)
U1b	Šalutinės juostos naudojimas	Tie patys abiejų pusių duomenys	(Atitinka standartą EN 12253)
U2 (*)	OBU (DSRC-VU) siųstuvo spektro kaukė	Pagal standartą EN 12253 1) Su dažnių juosta nesusijusi galia: žr. ETSI EN 300674-1	(Atitinka standartą EN 12253)

▼B

Objekto Nr.	Parametras	Vertė (-ės)	Pastaba
		2) Dažnių juostos galia: [U4a] dBm naudojant 500 kHz 3) Spinduliavimas į bet kokią kitą aukštynkryptę ryšio liniją Kanalas: U2(3)-1 = -35 dBm naudojant 500 kHz	
U4a (*)	Didžiausia šalutinės juostos E.I.R.P. (didžiausio antenos spinduliavimo ašis)	Dvi parinktys: U4a-0: – 14 dBm U4a-1: – 21 dBm	Pagal įrangos projektuotojo deklaruotą ir paskelbtą specifikaciją
U4b (*)	Didžiausia šalutinės juostos E.I.R.P. (35°)	Dvi parinktys: — Netaikoma — – 17dBm	Pagal įrangos projektuotojo deklaruotą ir paskelbtą specifikaciją
U5	Poliarizacija	Kairinė apskritiminė	(Atitinka standartą EN 12253)
U5a	Kryžminė poliarizacija	XPD: Išilgai didžiausio antenos spinduliavimo ašies: (REDCR) RSU r ≥ 15 δB (DSRC-VU) OBU t ≥ 10 δB Naudojant -3 dB: (REDCR) RSU r ≥ 10 δB (DSRC-VU) OBU t ≥ 6 δB	(Atitinka standartą EN 12253)
U6	Ponešlio moduliavimas	2-PSK Koduoti duomenys sinchronizuoti su ponešliu: koduotų duomenų perėjimai sutampa su ponešlio perėjimais	(Atitinka standartą EN 12253)
U6b	Aukšto ar žemo dažnio impulsų ilgio santykis su visa ciklo trukme	Aukšto ar žemo dažnio impulsų ilgio santykis su visa ciklo trukme: 50 proc. ± α, α ≤ 5 proc.	(Atitinka standartą EN 12253)
U6c	Nešlio moduliavimas	Moduliuoto ponešlio daugininimas iš nešlio	(Atitinka standartą EN 12253)
U7 (*)	Duomenų kodavimas	NRZI (Perėjimo „1“ bito pradžioje nėra, perėjimas „0“ bito pradžioje, perėjimo bite nėra)	(Atitinka standartą EN 12253)
U8 (*)	Sparta bitais	250 kbit/sek.	(Atitinka standartą EN 12253)
U8a	Bitų taktų signalo leidžiamoji paklaida	± 1 000 ππμ	(Atitinka standartą EN 12253)
U9	Bitų klaidų dažnis (B.E.R.) užtikrinant ryšį	$\leq 10^{-6}$	(Atitinka standartą EN 12253)

▼B

Objekto Nr.	Parametras	Vertė (-ės)	Pastaba
U11	Ryšio zona	Erdvės sritis, kurioje DSRC-VU padėtis yra tokia, kad DSRC-VU siunčiamus duomenis priima REDCR, kurio B.E.R. (bitų klaidų dažnis) yra mažesnis už nustatytą U9a	(Atitinka standartą EN 12253)
U12a (*)	Atgaminimo našumas (apatinė riba)	1 dB kiekvienai šalutinei juostai Kampo intervalas: Tolydus apskritimas tarp didžiausio antenos spinduliavimo ašies ir ± 35° ir	
		neviršijant – 45° – + 45° bei atsižvelgiant į plokštumą, lygiagrečią su kelio paviršiumi, kai DSRC-VU vėliau įmontuojamas į transporto priemonę (azimutas)	Didesnė už nurodytą horizontaliųjų kampų vertės intervalą neviršijant ± 45° vertės ir atsižvelgiant į šiame priede apibrėžtus naudojimo modelius.
U12b (*)	Atgaminimo našumas (viršutinė riba)	10 dB kiekvienai šalutinei juostai	Mažesnis už nustatytą vertės intervalą kiekvienai šalutinei juostai apskritajame kūgyje aplink didžiausio antenos spinduliavimo ašį ± 45° skėsties kampu
U13	Preambulė	Preambulė yra privaloma	(Atitinka standartą EN 12253)
U13a	Preambulė Ilgis ir šablonas	32–36 μs moduliavimas naudojant tik ponešlį, tada taikant NRZI, kuris koduotas „0“ bitais, 8 bitus.	(Atitinka standartą EN 12253)
U13b	Pabaigos bitai	Leidžiama, kad DSRC-VU perduotų ne daugiau kaip 8 bitus po galinės žymos. Reikalavimas, kad RSU (REDCR) atsižvelgtų į šiuos papildomus bitus, nėra taikomas.	(Atitinka standartą EN 12253)

(*) Aukštynkryptės ryšio linijos parametrams taikomas atitikties bandymas pagal standarte EN 300 674-1 nustatytus atitinkamus parametrus.

5.3.3 *Antenos konstrukcija*

5.3.3.1 REDCR antena

DSC_30 *REDCR* antenos konstrukcija – tai komercinės konstrukcijos funkcija, taikoma laikantis 5.3.2 punkte nustatytų apribojimų ir pritaikyta optimizuoti *DSRC-REDCR* nuskaitymo gebėjimą konkrečioms reikmėms ir skaitymo aplinkybėms, kuriomis *REDCR* buvo suprojektuotas eksploatuoti.

5.3.3.2 Transporto priemonės bloko antena

DSC_31 *DSRC-VU* antenos konstrukcija – tai komercinės konstrukcijos funkcija, taikoma laikantis 5.3.3 punkte nustatytų apribojimų ir pritaikyta optimizuoti *DSRC-REDCR* nuskaitymo gebėjimą konkrečioms reikmėms ir skaitymo aplinkybėms, kuriomis *REDCR* buvo suprojektuotas eksploatuoti.

▼B

DSC_32 VU antena turi būti tvirtinama prie priekinio transporto priemonės stiklo arba greta jo, kaip pirmiau nurodyta 5.1 punkte.

DSC_33 Bandymo atlikimo sąlygomis dirbtuvėse (žr. 6.3 skirsnį) pagal pirmiau 5.1 punkte nurodytas nuostatas pritvirtinta DSRC-VU antena turi užmegzti standartinį bandomąjį ryšį ir pagal šiame priedėlyje pateiktą apibrėžtį sėkmingai įvykdyti RTM transakciją 2–10 metrų atstumu, per trumpesnę kaip 99 proc. laiko vertę, vidurkintą per 1 000 nuskaitymo užklausų.

5.4 **RTM taikomi DSRC protokolo reikalavimai**

5.4.1 *Apžvalga*

DSC_34 Transakcijos protokolas siekiant atsisiųsti *duomenis* per 5,8 GHz DSRC sąsają turi būti taikomas toliau nurodytais etapais. Šiame skirsnyje aprašomas transakcijos srautas idealiomis sąlygomis be kartotinio perdavimo arba ryšio pertrūkių.

PASTABA. Taikant inicijavimo etapą (1 etapas) siekiama užmegzti ryšį tarp *REDCR* ir DSRC-VU, kurie yra 5,8 GHz DSRC (pagrindinio įtaiso –pavaldžiojo įtaiso) transakcijos zonoje, tačiau kuris kol kas nėra užmezgęs ryšio su *REDCR*, ir pateikti pranešimą apie taikymo procesą.

— **1 etapas.** Inicijavimas. *REDCR* siunčia kadrą su tikrinimo kelyje įrangos parengtais ir perduotais duomenimis (BST), į kuriuos įtraukiami suderinamų taikomųjų programų identifikatoriai (AID), nurodyti paslaugų sąraše. RTM taikomoje programoje tai bus tiesiog perdavimas naudojant AID vertę = 2 (Freight&Fleet). *DSRC-VU* įvertina gautus BST ir perduoda atsakymą (žr. toliau) nurodydamas suderinamų programų sąrašą su „Freight&Fleet“ sritimi arba nepateikia atsakymo, jeigu suderinamų programų nėra. Jeigu *REDCR* neužtikrina AID=2, DSRC-VU neturi perduoti atsakymo REDCR.

— **2 etapas.** *DSRC-VU* siunčia kadrą, į kurį įtraukta užklausa suteikti atskirą langą.

— **3 etapas.** *REDCR* siunčia kadrą, į kurį įtrauktas atskiro lango suteikimas.

— **4 etapas.** *DSRC-VU* naudoja paskirtąjį atskirą langą, kad nusiųstų kadrą, į kurį įtrauktas transporto priemonės informacijos blokas (VST). Į šį VST įtrauktas visų skirtingų programos, su kuria šis *DSCR-VU* pritaikytas naudoti AID=2 sistemoje, konkretizavimų sąrašas. Skirtingi konkretizavimai turi būti identifikuojami EID generuojamomis unikaliomis priemonėmis, iš kurių kiekviena susieta su taikomos programos konteksto žymos parametro verte, nurodančia taikomą programą ir palaikomą standartą.

— **5 etapas.** Po to *REDCR* analizuoja pateiktą VST ir arba nutraukia ryšį (RELEASE), nes niekas nėra reikalinga REDCR, kas yra pateikiama VST (t. y. REDCR gauna VST iš *DSRC-VU*, kuris nesuderinamas su RTM transakcija), arba, jeigu REDCR gauna atitinkamą VST, tada REDCR pradeda taikomos programos konkretizavimą.

▼B

— **6 etapas.** Norint atlikti šią operaciją REDCR turi siųsti kadrą, į kurį įtraukta komanda nuskaityti RTM duomenis, identifikuojančius RTM taikomos programos konkretizavimą ir šiuo tikslu nurodant identifikatorių, atitinkantį RTM taikomos programos konkretizavimą (kaip nurodoma naudojant VST pateiktą DSRC-VU), ir priskirti atskirą langą.

— **7 etapas.** *DSRC-VU* naudoja naujai sukurtą atskirą langą ir nusiunčia kadrą, į kurį įtrauktas adresavimo identifikatorius, atitinkantis RTM taikomos programos konkretizavimą, kaip numatyta VST, ir po kurio pateikiamas požymis *RtmData* (informacinio turinio elementas + saugumo elementas).

— **8 etapas.** Jeigu pateikiama užklausa dėl daugybinių paslaugų, vertė ‘n’ pakeičiama kitos paslaugos identifikavimo numeriu ir procesas pakartojamas.

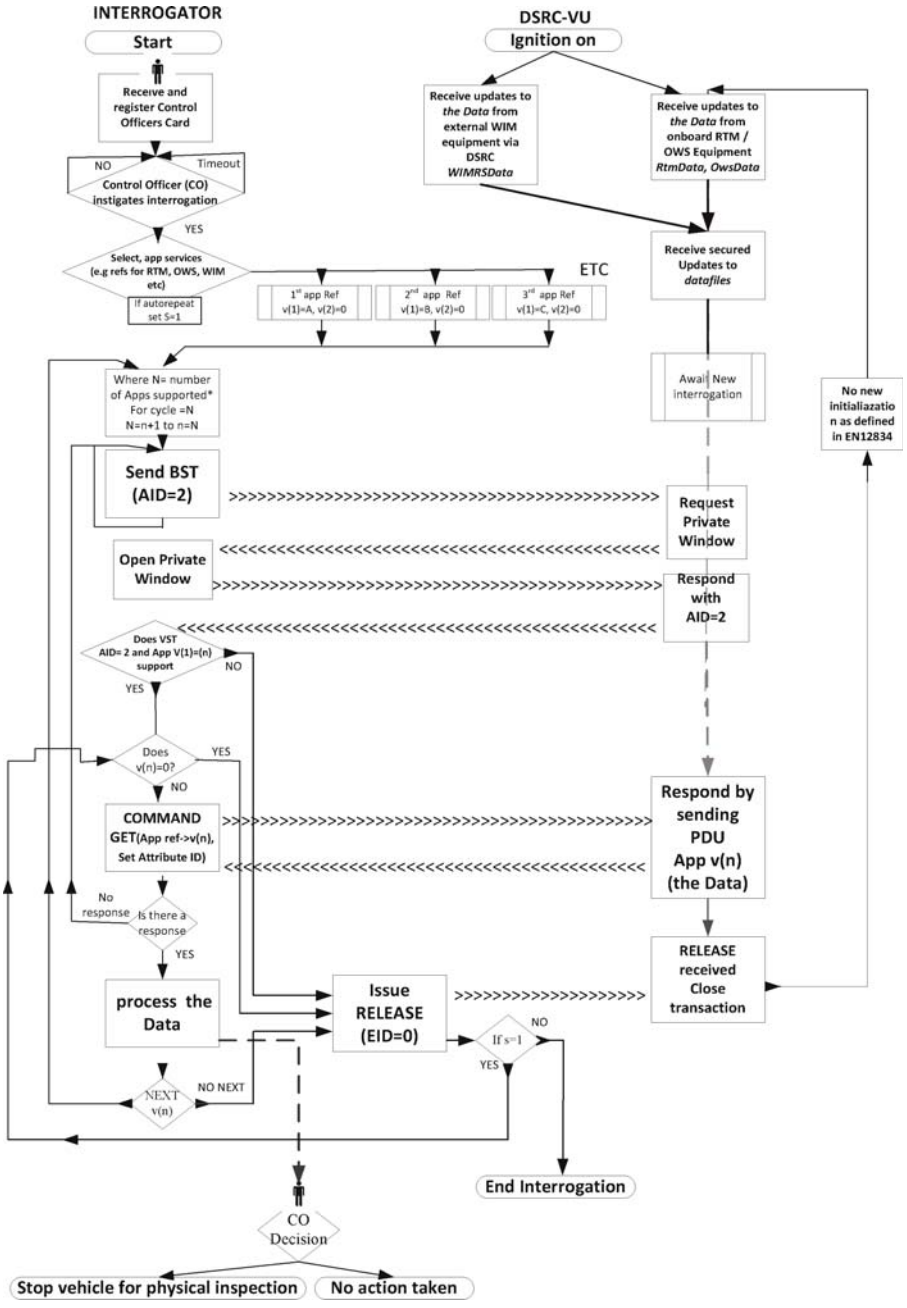
— **9 etapas.** Duomenų gavimą *REDCR* patvirtina nusiųsdamas *DSRC-VU* kadrą, į kurį įtraukta komanda RELEASE, kad būtų nutraukiamas seansas ARBA, jeigu *REDCR* nepavyko patvirtinti, jog buvo sėkmingai gautas LDPU, tada *REDCR* persijungia į 6 etapą.

Žr. 14.6 pav., kuriame pateikta transakcijos protokolo iliustracija.

▼B

14.6 pav.

RTM operacijų seka naudojant 5,8 GHz DSRC



5.4.2 *Komandos*

DSC_35 Toliau nurodytos komandos – tai tik funkcijos, naudojamos RTM transakcijos etape.

— **INITIALISATION.request**: REDCR perduodama komanda (pranešimas), kurioje apibrėžiamos su READCR suderinamos taikomosios programos.

— **INITIALISATION.response**: DSRC-VU atsakymas, kuriuo patvirtinamas ryšys ir į kurį įtrauktas suderinamų taikomųjų programų sąrašas su charakteristikomis ir informacija apie jų iškvietą (EID).

▼B

— **GET.request**: iš *REDCR* į *DSRC-VU* nusiųsta komanda, kuria nurodoma, kad taikomos programos konkretizavimas turi būti iškviečiamas pasirenkant kartu su VST gautą apibrėžtą EID, ir kuria siunčiamas reikalavimas *DSRC-VU* jog pasirinktas (-i) požymis (-iai) būtų siunčiamas (-i) su *duomenimis*. GET komandą siunčiant į *REDCR* siekiama gauti *duomenis* iš *DSRC-VU*.

— **GET.response**: iš DSRC-VU gautas atsakymas, į kurį įtraukta *duomenų* užklausa.

— **ACTION.request ECHO**: komanda, kuria *DSRC-VU* perduodamas nurodymas siųsti duomenis iš *DSRC-VU į REDCR*. Siunčiant ECHO komandą siekiama dirbtuvėms ar tipo patvirtinimo bandymą atliekančioms įstaigoms suteikti galimybę patikrinti, ar DSRC ryšio kanalas veikia nereikalaujant prieigos prie saugumo požymių.

— **ACTION**.response ECHO: DSRC VU pateikiamas atsakymas gavus ECHO komandą.

— **EVENT_REPORT.request** RELEASE: komanda, kuria *DSRC-VU* nurodoma, kad transakcija yra užbaigta. Siunčiant RELEASE komandą siekiant užbaigti seansą su *DSRC-VU*. Jeigu *DSRC-VU* gauna RELEASE komandą, *DSRC-VU* neturi atsakyti į jokią kitą užklausą, perduodamą naudojant esamą ryšį. Atkreipiame dėmesį, kad pagal standartą EN 12834 DSRC-VU nebus du kartus sujungiamas su tuo pačiu užklausikliu, jeigu jis nebuvo 255 sekundes ne ryšio zonoje arba jeigu užklausiklio Beacon ID nebuvo pakeistas.

5.4.3 *Užklausos komandos seka*

DSC_36 Atsižvelgiant į komandų ir atsakymų eiliškumą transakcija apibrėžiama taip:

Seka	Siųstuvas		Imtuvas	Aprašymas	Veiksmas
1	REDCR	>	DSRC-VU	Ryšio inicijavimas. Užklausa	REDCR siunčia BST
2	*DSRC-VU*	>	*REDCR*	*Ryšio inicijavimas. Atsakas*	*Jeigu BST tinkami AID=2, tada DSRC-VU pateikia atskiro lango užklausą*
3	REDCR	>	DSRC-VU	Suteikia atskirą langą	Siunčia kadrą su atskiro lango priskyrimu
4	*DSRC-VU*	>	*REDCR*	*Siunčia VST*	*Siunčia kadrą su VST*
5	REDCR	>	DSRC-VU	Siunčia GET.request konkrečiam EID dėl duomenų su požymiu	
6	*DSRC-VU*	>	*REDCR*	*Siunčia GET.request konkrečiam EID su užklausiamu požymiu*	*Siunčia požymį (RTMData, OWSData….) su konkrečiam EID skirtais duomenimis*

▼B

Seka	Siųstuvas		Imtuvas	Aprašymas	Veiksmas
7	REDCR	>	DSRC-VU	Siunčia GET.request dėl duomenų, išskyrus požymį (jeigu būtina)	
8	*DSRC-VU*	>	*REDCR*	*Siunčia GET.response su užklausa dėl požymio*	*Siunčia požymį su konkrečiam EID skirtais duomenimis*
9	REDCR	>	DSRC-VU	Patvirtina sėkmingą duomenų gavimą	Siunčia RELEASE komandą, kuria nutraukiama transakcija
10	*DSRC-VU*			*Nutraukia transakciją*	

Transakcijos sekos pavyzdys ir kadrų, kuriais buvo keičiamasi, turinys apibrėžiamas 5.4.7 ir 5.4.8 punktuose.

5.4.4 *Duomenų struktūros*

DSC_37 Per 5,8 GHz DSRC sąsają perduodamų *duomenų* semantinė struktūra turi atitikti šiame priedėlyje pateiktas nuostatas. Šių duomenų struktūra nustatyta šiame punkte.

DSC_38 Informacinio turinio duomenis (RTM duomenis) sudaro sujungtos šios dvi eilutės:

1. EncryptedTachographPayload duomenys, kurie gaunami koduojant ASN.1 5.4.5. punkte apibrėžtą TachographPayload. Užšifravimo metodas aprašytas 11 priedėlyje.

2. 11 priedėlyje nurodyti DSRCSecurityData.

DSC_39 RTM duomenys iškviečiami naudojant RTM požymį=1 ir perduodami RTM pakete =10.

DSC_40 RTM konteksto žyma turi nurodyti palaikomą standarto dalį TARV serijos standartų grupėje (RTM atitinka 9 dalį).

RTM taikomojoje programoje DSRC duomenims taikomas ASN.1 modulis apibrėžiamas taip:

▼B

```
TarvRtm {iso(1) standard(0) 15638 part9(9) version1(1)}
DEFINITIONS AUTOMATIC TAGS
::= BEGIN
IMPORTS
-- Imports data attributes and elements from EFC which are used for RTM
LPN
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports function parameters from the EFC Application Interface Definition
SetMMIRq
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports the L7 DSRCData module data from the EFC Application Interface Definition
Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
Attributes,
BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};


-- Definitions of the RTM functions:
RTM-InitialiseComm-Request ::= BST
RTM-InitialiseComm-Response::= VST
RTM-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials ABSENT,iid
ABSENT,  attrIdList})
RTM-DataRetrieval-Response::= Get-Response {RtmContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
RTM-TerminateComm::= Event-Report-Request {RtmContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
eventType (0)})

RTM-TestComm-Request::= Action-Request {RtmContainer} (WITH COMPONENTS {..., eid (0), actionType
(15), accessCredentials ABSENT, iid ABSENT})

RTM-TestComm-Response::= Action-Response {RtmContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
(0), iid ABSENT})

-- Definitions of the RTM attributes:
RtmData ::= SEQUENCE {
      encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calculated encrypting
TachographPayload as per Appendix 11 --}),
      DSRCSecurityData OCTET STRING
      }
TachographPayload ::= SEQUENCE {
            tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
            tp15638SpeedingEvent            BOOLEAN,  -- 1= Irregularities in speed (see Annex 1C)
            tp15638DrivingWithoutValidCard  BOOLEAN,     -- 1= Invalid card usage (see Annex 1C)
            tp15638DriverCard               BOOLEAN,-- 0= Indicates a valid driver card  (see Annex 1C)
            tp15638CardInsertion            BOOLEAN, -- 1= Card insertion while driving (see Annex 1C)
            tp15638MotionDataError          BOOLEAN, -- 1= Motion data error (see Annex 1C)
            tp15638VehicleMotionConflict    BOOLEAN, -- 1= Motion conflict (see Annex 1C)
            tp156382ndDriverCard            BOOLEAN, -- 1= Second driver card inserted (see Annex 1C)
            tp15638CurrentActivityDriving   BOOLEAN, -- 1= other activity selected;
                                                      -- 0= driving selected
            tp15638LastSessionClosed        BOOLEAN, -- 1= improperly, 0= properly, closed
            tp15638PowerSupplyInterruption  INTEGER (0..127), -- Supply interrupts in the last 10 days
            tp15638SensorFault              INTEGER (0..255),-- eventFaultType as per data dictionary
-- All subsequent time related types as defined in Annex 1C.
            tp15638TimeAdjustment           INTEGER(0..4294967295), -- Time of the last time adjustment
            tp15638LatestBreachAttempt      INTEGER(0..4294967295), -- Time of last breach attempt
            tp15638LastCalibrationData      INTEGER(0..4294967295), -- Time of last calibration data
            tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Time of previous calibration data
            tp15638DateTachoConnected       INTEGER(0..4294967295), -- Date tachograph connected
            tp15638CurrentSpeed             INTEGER (0..255), -- Last current recorded speed
            tp15638Timestamp                INTEGER(0..4294967295) -- Timestamp of current record[2]
            }
Rtm-ContextMark ::= SEQUENCE {
 standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version

 RtmCommProfile          INTEGER {
                           C1 (1),
                           C2 (2)
                           } (0..255) DEFAULT 1
 }
RtmTransferAck ::= INTEGER {
                Ok (1),
                NoK (2)
                } SIZE (1..255)
```

▼B

```
StandardIdentifier ::= OBJECT IDENTIFIER
RtmContainer ::= CHOICE {
        integer                     [0]    INTEGER,
        bitstring                   [1]    BIT STRING,
        octetstring                 [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString             [3]    UniversalString,
        beaconId                    [4]    BeaconID,
        t-apdu                      [5]    T-APDUs,
        dsrcApplicationEntityId     [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                 [7]    Dsrc-EID,
        attrIdList                  [8]    AttributeIdList,
        attrList                    [9]    AttributeList{RtmContainer},
        rtmData                     [10]   RtmData,
        rtmContextmark              [11]   Rtm-ContextMark,
        reserved12                  [12]   NULL,
        reserved13                  [13]   NULL,
        reserved14                  [14]   NULL,
        time                        [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

5.4.5 *RtmData elementai, atliekami veiksmai ir apibrėžtys*

DSC_41 Duomenų vertės, kurias apskaičiuoja transporto priemonės blokas ir kurios naudojamos DSRC-VU laikomiems saugumo duomenims atnaujinti, apskaičiuojami laikantis 14.3 lentelėje nustatytų taisyklių.

14.3 lentelė.

RtmData elementai, atliekami veiksmai ir apibrėžtys

1 RTM duomenų elementas	2 Transporto priemonės bloko atliekamas veiksmas		3 ASN.1 duomenų apibrėžimas
RTM1 **Transporto priemonės valstybinio numerio ženklas**	Transporto priemonės blokas turi nustatyti *tp15638VehicleRegistrationPlate* duomenų elemento RTM1 vertę atsižvelgdamas į užregistruotą duomenų tipo vertę *VehicleRegistrationIdentification*, kuri apibrėžta 1 priedėlyje *VehicleRegistrationIdentification*	Transporto priemonės valstybinio numerio ženklas apibrėžiamas simbolių seka	tp15638VehicleRegstrationPlate LPN, -- Transporto priemonės valstybinio numerio ženklas, importuotas iš ISO 14906 taikant standarte EN 15509 nustatytą apribojimą– tai SEKA, sudaryta iš šalies kodo, raidinio indikatoriaus, po kurio pateikiamas transporto priemonės valstybinio numerio ženklas, visada sudarytas iš 14 oktetų (užpildytas „0“), todėl standarte EN 15509 LPN tipo ilgis visada yra 17 oktetų, iš kurių 14 yra „tikrasis“ transporto priemonės valstybinio numerio ženklas.
RTM2 **Greičio viršijimo įvykis**	Transporto priemonės blokas generuoja loginę reikšmę duomenų elementui RTM2 tp15638SpeedingEvent. tp15638SpeedingEvent vertę transporto priemonės blokas apskaičiuoja atsižvelgdamas į tam tikrą greičio viršijimo įvykių skaičių, kurį transporto priemonės blokas yra užregistravęs per pastarąsias 10 dienų, kai toks įvykis įvyko, kaip nustatyta 1C priede.	1 (TRUE) rodo greičio ribojimo pažeidimus per pastarąsias 10 dienų, kai greitis buvo viršytas	tp15638speedingEvent BOOLEAN,

▼B

1 RTM duomenų elementas	2 Transporto priemonės bloko atliekamas veiksmas		3 ASN.1 duomenų apibrėžimas
	Jeigu per pastarąsias 10 dienų įvyko bent vienas tp15638SpeedingEvent, tp15638SpeedingEvent turi būti nustatoma reikšmė TRUE. Jeigu per pastarąsias 10 dienų įvyko bent vienas tp15638SpeedingEvent, tp15638SpeedingEvent turi būti nustatoma reikšmė TRUE.		
RTM3 **Važiavimas be galiojančios kortelės**	Transporto priemonės blokas generuoja loginę reikšmę duomenų elementui RTM3 tp15638DrivingWithoutValidCard. Transporto priemonės blokas kintamajam tp15638DrivingWithoutValidCard turi priskirti reikšmę TRUE, jeigu jis per pastarąsias 10 dienų užregistravo bent vieną įvykį „Važiavimas be reikiamos kortelės“, apibrėžtą 1C priede. Priešingu atveju, jeigu per pastarąsias 10 dienų nenustatyta jokių įvykių, kintamajam tp15638DrivingWithoutValidCard turi būti nustatoma reikšmė FALSE.	1 (TRUE) rodo, kad panaudota negaliojanti kortelė	`tp15638DrivingWithoutValidCard` `BOOLEAN,`
RTM4 **Galiojanti vairuotojo kortelė**	Transporto priemonės blokas generuoja loginę reikšmę duomenų elementui RTM4 tp15638DriverCard atsižvelgdamas į transporto priemonės bloke laikomus duomenis, apibrėžtus 1 priedėlyje. Jeigu galiojanti vairuotojo kortelė nėra naudojama, transporto priemonės blokas kintamajam turi nustatyti reikšmę TRUE. Priešingu atveju, jeigu galiojanti vairuotojo kortelė yra naudojama, transporto priemonės blokas kintamajam turi nustatyti reikšmę FALSE.	0 (FALSE) rodo galiojančią vairuotojo kortelę	`tp15638DriverCard` `BOOLEAN,`
RTM5 **Kortelė įstatyta važiuojant**	Transporto priemonės blokas generuoja loginę reikšmę duomenų elementui RTM5. Transporto priemonės blokas kintamajam tp15638CardInsertion turi priskirti reikšmę TRUE, jeigu jis per pastarąsias 10 dienų užregistravo bent vieną įvykį „Kortelė įstatyta važiuojant“, apibrėžtą 1C priede. Priešingu atveju, jeigu per pastarąsias 10 dienų nenustatyta tokių įvykių, kintamajam tp15638CardInsertion turi būti nustatoma reikšmė FALSE.	1 (TRUE) rodo, kad per pastarąsias 10 dienų kortelė buvo įstatyta važiuojant	`tp15638CardInsertion` `BOOLEAN,`
RTM6 **Duomenų apie judėjimą klaida**	Transporto priemonės blokas generuoja loginę reikšmę duomenų elementui RTM6. Transporto priemonės blokas kintamajam tp15638MotionDataError turi priskirti reikšmę TRUE, jeigu jis per pastarąsias 10 dienų užregistravo bent vieną įvykį „Duomenų apie judėjimą klaida“, apibrėžtą 1C priede. Priešingu atveju, jeigu per pastarąsias 10 dienų nenustatyta tokių įvykių, kintamajam tp15638MotionDataError turi būti nustatoma reikšmė FALSE.	1 (TRUE) rodo duomenų apie judėjimo klaidą per pastarąsias 10 dienų	`tp15638motionDataError` `BOOLEAN,`

▼B

1 RTM duomenų elementas	2 Transporto priemonės bloko atliekamas veiksmas		3 ASN.1 duomenų apibrėžimas
RTM7 **Transporto priemonės judėjimo nesuderinamumas**	Transporto priemonės blokas generuoja loginę reikšmę duomenų elementui RTM7. Transporto priemonės blokas kintamajam tp15638vehicleMotionConflict turi priskirti reikšmę TRUE, jeigu jeigu jis per pastarąsias 10 dienų užregistravo bent vieną įvykį „Transporto priemonės judėjimo nesuderinamumas“ (vertė ‘0A’H). Priešingu atveju, jeigu per pastarąsias 10 dienų nenustatyta jokių įvykių, kintamajam tp15638vehicleMotionConflict turi būti nustatoma reikšmė FALSE.	1 (TRUE) rodo judėjimo duomenų nesuderinamumą per pastarąsias 10 dienų	`tp15638vehicleMotionConflict` `BOOLEAN,`
RTM8 **Antroji vairuotojo kortelė**	Transporto priemonės blokas generuoja loginę reikšmę duomenų elementui RTM8 pagal 1C priedo nuostatas („Vairuotojo veiklos duomenys“ ĮGULA ir VAIRUOTOJO PORININKAS). Jeigu naudojama antroji vairuotojo kortelė, transporto priemonės blokas kintamajam turi nustatyti reikšmę TRUE. Priešingu atveju, jeigu antroji vairuotojo kortelė nenaudojama, transporto priemonės blokas kintamajam turi nustatyti reikšmę FALSE.	1 (TRUE) rodo, kad buvo įstatyta antra vairuotojo kortelė	`tp156382ndDriverCard BOOLEAN,`
RTM9 **Vykdoma veikla**	Transporto priemonės blokas generuoja loginę reikšmę duomenų elementui RTM9. Jeigu transporto priemonės blokas užregistruoja bet kokią kitą vykdomą veiklą, išskyrus veiklos rūšį VAIRAVIMAS, apibrėžtą 1C priede, jis kintamajam nustato reikšmę TRUE. Priešingu atveju, jeigu transporto priemonės blokas kaip vykdomą veiklą užregistravo veiklos rūšį VAIRAVIMAS, jis kintamajam turi nustatyti reikšmę FALSE.	1 (TRUE) – pasirinkta kita veikla 0 (FALSE) – pasirinktas vairavimas	`tp15638currentActivityDriving` `BOOLEAN`
RTM10 **Paskutinis seansas užbaigtas netinkamai**	Transporto priemonės blokas generuoja loginę reikšmę duomenų elementui RTM10. Jeigu paskutinis kortelės naudojimo seansas užbaigtas netinkamai, kaip nustatyta 1C priede, transporto priemonės blokas kintamajam turi nustatyti reikšmę TRUE. Priešingu atveju, jeigu paskutinis kortelės naudojimo seansas buvo užbaigtas tinkamai, transporto priemonės blokas kintamajam turi nustatyti reikšmę FALSE.	1 (TRUE) – užbaigtas netinkamai 0 (FALSE) – užbaigtas tinkamai	`tp15638lastSessionClosed` `BOOLEAN`
RTM11 **Maitinimo nutrūkimas**	Transporto priemonės blokas generuoja sveikojo skaičiaus vertę duomenų elementui RTM11. Transporto priemonės blokas priskiria kintamajam tp15638PowerSupplyInterruption vertę, lygią ilgiausiam maitinimo pertrūkiui pagal Reglamento (ES) Nr. 165/2014 9 straipsnį, jeigu šis pertrūkis priskiriamas 1C priede apibrėžtam maitinimo nutrūkimo tipui.	— Maitinimo pertrūkių skaičius per pastarąsias 10 dienų	`tp15638powerSupplyInterruption` `INTEGER (0..127),`

▼B

1 RTM duomenų elementas	2 Transporto priemonės bloko atliekamas veiksmas		3 ASN.1 duomenų apibrėžimas
	Priešingu atveju, jeigu per pastarąsias 10 dienų maitinimo nutrūkimo įvykių nebuvo, nustatoma sveikojo skaičiaus vertė 0.		
RTM12 **Jutiklio triktis**	Transporto priemonės blokas generuoja sveikojo skaičiaus vertę duomenų elementui RTM12. Transporto priemonės blokas kintamajam sensorFault priskiria vertę: — 1, jeigu per pastarąsias 10 dienų buvo užregistruotas įvykis ‘35’H jutiklio triktis; — 2, jeigu per pastarąsias 10 dienų užregistruotas įvykis GNSS imtuvo triktis (vidinio ar išorinio, vertė ‘51’H arba ‘52’H); — 3, jeigu per pastarąsias 10 dienų registruotas įvykis ‘53’H išorinio GNSS ryšio triktis; — 4, jeigu per pastarąsias 10 dienų registruota jutiklio triktis ir GNSS imtuvo triktis; — 5, jeigu per pastarąsias 10 dienų registruota jutiklio triktis ir išorinio GNSS ryšio triktis; — 6, jeigu per pastarąsias 10 dienų registruota GNSS imtuvo triktis ir išorinio GNSS ryšio triktis; — 7, jeigu per pastarąsias 10 dienų registruotos visos trys jutiklio triktys. Priešingu atveju, transporto priemonės blokas priskiria vertę 0, jeigu per pastarąsias 10 dienų nebuvo registruota jokių įvykių.	— Jutiklio triktis vienas oktetas duomenų žinyne	`tp15638SensorFault INTEGER (0..255),`
RTM13 **Laiko koregavimas**	Transporto priemonės blokas generuoja sveikojo skaičiaus vertę (timeReal 1 priedėlyje) duomenų elementui RTM13, remdamasis užregistruotais 1C priede apibrėžtais laiko koregavimo duomenimis. Transporto priemonės blokas priskiria laiko, kai paskutinį kartą atliktas laiko koregavimas, vertę. Priešingu atveju, jeigu transporto priemonės blokas nėra užregistravęs 1C priede apibrėžto laiko koregavimo įvykio, nustatoma vertė 0.	Paskutinio laiko koregavimo laikas	`tp15638TimeAdjustment INTEGER(0..4294967295),`
RTM14 **Mėginimas pažeisti apsaugą**	Transporto priemonės blokas generuoja sveikojo skaičiaus vertę (timeReal 1 priedėlyje) duomenų elementui RTM14, remdamasis užregistruotu 1C priede apibrėžtu mėginimo pažeisti apsaugą įvykiu. Transporto priemonės blokas nustato paskutinio jo užregistruoto mėginimo pažeisti apsaugą laiko vertę.	Paskutinio mėginimo pažeisti apsaugą laikas — Numatytoji vertė 0x00FF	`tp15638LatestBreachAttempt INTEGER(0..4294967295),`

▼B

1 RTM duomenų elementas	2 Transporto priemonės bloko atliekamas veiksmas		3 ASN.1 duomenų apibrėžimas
	Priešingu atveju, jeigu transporto priemonės blokas nėra užregistravęs 1C priede apibrėžto mėginimo pažeisti apsaugą įvykio, nustatoma vertė 0x00FF.		
RTM15 **Paskutinis kalibravimas**	Transporto priemonės blokas generuoja sveikojo skaičiaus vertę (timeReal 1 priedėlyje) duomenų elementui RTM15, remdamasis užregistruotais 1C priede apibrėžtais kalibravimo duomenimis. Transporto priemonės blokas nustato laiko vertę paskutiniams dviem kalibravimo atvejams (RTM15 ir RTM16), kurie nustatyti 1 priedėlyje apibrėžtuose VuCalibrationData. Transporto priemonės blokas RTM15 nustato paskutinio kalibravimo įrašo timeReal vertę.	Paskutinio kalibravimo duomenų laikas	`tp15638LastCalibrationData` `INTEGER(0..4294967295),`
RTM16 **Ankstesnis kalibravimas**	Transporto priemonės blokas generuoja sveikojo skaičiaus vertę (timeReal 1 priedėlyje) duomenų elementui RTM16 – prieš paskutinįjį kalibravimą padarytam kalibravimo įrašui. Priešingu atveju, jeigu neužregistruota ankstesnio kalibravimo, transporto priemonės blokas nustato, kad RTM16 vertė yra 0.	Ankstesniojo kalibravimo duomenų laikas	`tp15638PrevCalibrationData` `INTEGER(0..4294967295),`
RTM17 **Tachografo prijungimo data**	Transporto priemonės blokas duomenų elementui RTM17 generuoja sveikojo skaičiaus vertę (timeReal 1 priedėlyje). Transporto priemonės blokas nustato laiko, kai jis buvo įdiegtas pirmą kartą, vertę Šiuos duomenis transporto priemonės blokas nuskaito iš VuCalibrationData (1 priedėlis), iš vuCalibrationRecords, kai kalibravimo tikslas yra lygus ‘03’H.	Tachografo prijungimo data	`tp15638DateTachoConnected` `INTEGER(0..4294967295),`
RTM18 **Rodomas greitis**	Transporto priemonės blokas generuoja sveikojo skaičiaus vertę duomenų elementui RTM18. Transporto priemonės blokas RTM16 nustato paskutinę užregistruotą rodomo greičio vertę, kai paskutinį kartą buvo atnaujinti RtmData.	Paskutinis registruotas rodomas greitis	`tp15638CurrentSpeed` `INTEGER (0..255),`
RTM19 **Laiko žyma**	Transporto priemonės blokas duomenų elementui RTM19 generuoja sveikojo skaičiaus vertę (timeReal 1 priedėlyje). Transporto priemonės blokas RTM19 nustato paskutinio RtmData atnaujinimo laiko vertę.	Einamojo TachographPayload įrašo laiko žyma	`tp15638Timestamp` `INTEGER(0..4294967295),`

5.4.6 *Duomenų perdavimo mechanizmas*

DSC_42 Pirmiau apibrėžtus informacinio turinio duomenis REDCR nuskaito užbaigus inicijavimo etapą ir vėliau *DSRC-VU* juos siunčia į paskirtą langą. Duomenims nuskaityti REDCR naudoja komandą GET.

▼B

DSC_43 Atliekant visus DSRC mainus duomenys turi būti koduojami naudojant PER (pakuojamojo kodavimo taisykles).

5.4.7 *Išsamus DSCR transakcijos aprašymas*

DSC_44 Inicijavimas atliekamas pagal DSC_44–DSC_48 ir 14.4–14.9 lenteles. Prasidėjus inicijavimo etapui REDCR ima siųsti kadrą, į kurį įtraukti BST (tikrinimo kelyje įrangos parengti ir perduoti duomenys) pagal standartus EN 12834 ir EN 13372, 6.2, 6.3, 6.4 ir 7.1 punktus ir toliau pateiktoje 14.4 lentelėje nurodytus nuostačius.

14.4 lentelė.

Inicijavimas. BST kadro nuostačiai

Laukelis	Nuostačiai
Ryšio linijos identifikatorius	Perdavimo adresas
BeaconId	Kaip nustatyta standarte EN 12834
Laikas	Kaip nustatyta standarte EN 12834
Profilis	Jokio plėtinio, turi būti naudojamas 0 arba 1
MandApplications	Jokio plėtinio, EID nepateikta, parametras nepateiktas, AID = 2 Freight&Fleet
NonMandApplications	Nepateikta
ProfileList	Jokio plėtinio, profilių skaičius sąraše = 0
Fragmentation header	Fragmentavimas netaikomas
2 lygmens nuostačiai	PDU komanda, UI komanda

14.4 lentelėje nurodytų nuostačių praktinis pavyzdys su nurodytais bito kodavimais pateiktas tolesnėje 14.5 lentelėje.

14.5 lentelė.

Inicijavimas. BST kadro turinio pavyzdys

Oktetas #	Požymis ir (arba) laukelis	Bitų skaičius oktete	Aprašymas
1	FLAG	0111 1110	Pradinė žyma
2	Broadcast ID	1111 1111	Perdavimo adresas
3	MAC Control Field	1010 0000	PDU komanda
4	LLC Control field	0000 0011	UI komanda

▼B

Oktetas #	Požymis ir (arba) laukelis	Bitų skaičius oktete	Aprašymas
5	Fragmentation header	1xxx x001	Fragmentavimas netaikomas
6	BST	1000	Inicijavimo užklausa
	SEQUENCE {		
	OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	NonMand taikomos programos nepateiktos
		xxx	Gamintojo tapatybės identifikatorius
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727)	xxx	Gamintojui prieinama 27 bitų ID
9		xxxx xxxx	
10		xxxx xxxx	
11	}	xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	32 bitų UNIX tikrasis laikas
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127,...)	0000 0000	Jokio plėtinio. Pavyzdinis profilis 0
17	MandApplications SEQUENCE (SIZE(0..127,...)) OF {	0000 0001	Jokio plėtinio, mandApplications skaičius = 1
18	SEQUENCE {		
	OPTION indicator	0	EID nepateiktas
	OPTION indicator	0	Parametras nepateiktas
	AID DSRCApplicationEntityID } }	00 0010	Jokio plėtinio. AID = 2 Freight&Fleet

▼B

Oktetas #	Požymis ir (arba) laukelis	Bitų skaičius oktete	Aprašymas
19	ProfileList SEQUENCE (0..127,...) OF Profile }	0000 0000	Jokio plėtinio, profilių skaičius sąraše = 0
20	FCS	xxxx xxxx	Kadro patikros seka
21		xxxx xxxx	
22	Flag	0111 1110	Galinė žyma

DSC_45 *DSRC-VU*, kai jam siunčiami BST, turi būti skiriamas standartuose EN 12795 ir EN 13372, 7.1.1 punkte apibrėžtas atskiras langas be jokių konkrečių RTM nuostačių. 14.6 lentelėje pateiktas bito kodavimo pavyzdys.

14.6 lentelė.

Inicijavimas. Atskiro lango skyrimo užklausos kadro turinys

Oktetas #	Požymis ir (arba) laukelis	Bitų skaičius oktete	Aprašymas
1	FLAG	0111 1110	Pradinė žyma
2	Private LID	xxxx xxxx	Konkretaus DSCR-VU ryšio linijos adresas
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control Field	0110 0000	Atskiro lango užklausa
7	FCS	xxxx xxxx	Kadro patikros seka
8		xxxx xxxx	
9	Flag	0111 1110	Galinė žyma

DSC_46 Tada REDCR siunčia atsakymą ir priskiria standartuose EN 12795 ir EN 13372, 7.1.1 punkte apibrėžtą atskirą langą be jokių konkrečių RTM nuostačių.

14.7 lentelėje pateiktas bito kodavimo pavyzdys.

14.7 lentelė.

Inicijavimas. Atskiro lango priskyrimo kadro turinys

Oktetas #	Požymis ir (arba) laukelis	Bitų skaičius oktete	Aprašymas
1	FLAG	0111 1110	Pradinė žyma
2	Private LID	xxxx xxxx	Konkretaus DSCR-VU ryšio linijos adresas
3		xxxx xxxx	

▼B

Oktetas #	Požymis ir (arba) laukelis	Bitų skaičius oktete	Aprašymas
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control Field	0010 s000	Atskiro lango priskyrimas
7	FCS	xxxx xxxx	Kadro patikros seka
8		xxxx xxxx	
9	Flag	0111 1110	Galinė žyma

DSC_47 *DSRC-VU* gauna atskiro lango priskyrimą ir siunčia standartuose EN 12834 ir EN 13372, 6.2, 6.3, 6.4 bei 7.1 punkte apibrėžtą savo VST (transporto priemonės informacijos bloką), su 14.8 lentelėje nurodytais nuostačiais, naudodamas priskirtą perdavimo langą.

14.8 lentelė.

Inicijavimas. VST lango nuostačiai

Laukelis	Nuostačiai
Private LID	Kaip nustatyta standarte EN 12834
VST parametrai.	Fill=0, tada kiekvienai suderinamai taikomajai programai: EID pateiktas, parametras pateiktas, AID=2, EID, kurį sugeneravo OBU
Parametras	Jokio plėtinio, įtraukta RTM konteksto žyma
ObeConfiguration	Galima pateikti pasirenkamąjį ObeStatus lauką, tačiau REDCR neturi naudoti šio lauko
Fragmentation header	Fragmentavimas netaikomas
2 lygmens nuostačiai	PDU komanda, UI komanda

DSC_48 *DSRC-VU* turi būti suderinamas su programa „Freight and Fleet“, identifikuota programos identifikatoriumi ‘2’. Kitus programos identifikatorius galima naudoti, tačiau jų nebūtina įtraukti į šį VST, nes BST pakanka AID=2. Programų lauke pateiktas suderinamų programų pavyzdžių, naudojamų *DSCR-VU*, sąrašas. Kiekvieno suderinamos programos konkretizavimo atveju pateikiama nuoroda į atitinkamą standartą ir ši nuoroda sudaroma iš „Rtm Context“ žymos, sudarytos iš OBJEKTO IDENTIFIKATORIAUS, atitinkančio susijusį standartą, jos dalies (9, jeigu tai yra RTM) ir, galimas daiktas, jos versijos bei DSRC-VU sugeneruoto EID ir susieto su taikomosios programos pavyzdžiu.

14.8 lentelėje nurodytų nuostačių praktinis pavyzdys su nurodytais bito kodavimais pateiktas 14.9 lentelėje.

▼B

14.9 lentelė.

Inicijavimas. VST kadro turinio pavyzdys

Oktetas #	Požymis ir (arba) laukelis	Bitų skaičius oktete	Aprašymas
1	FLAG	0111 1110	Pradinė žyma
2	Private LID	xxxx xxxx	Konkretaus DSCR-VU ryšio linijos adresas
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control Field	1100 0000	PDU komanda
7	LLC Control field	0000 0011	UI komanda
8	Fragmentation header	1xxx x001	Fragmentavimas netaikomas
9	VST SEQUENCE {	1001	Inicijavimo atsakas
	Fill BIT STRING (SIZE(4))	0000	Nenaudojama ir nustatyta vertė 0
10	Profile INTEGER (0..127,...) Applications SEQUENCE OF {	0000 0000	Jokio plėtinio. Pavyzdinis profilis 0
11		0000 0001	Jokio plėtinio, 1 programa
12	SEQUENCE {		
	OPTION indicator	1	EID pateiktas
	OPTION indicator	1	Parametras pateiktas
	AID DSRCApplicationEntityID	00 0010	Jokio plėtinio. AID = 2 Freight&Fleet
13	EID Dsrc-EID	xxxx xxxx	Apibrėžta naudojant OBU ir identifikuojantis programos pavyzdį
14	Parameter Container {	0000 0010	Jokio plėtinio, paketo parinktis = 02 Oktetų eilutė
15		0000 1000	Jokio plėtinio, Rtm kontekso žymos ilgis = 8

▼B

Oktetas #	Požymis ir (arba) laukelis	Bitų skaičius oktete	Aprašymas
16	Rtm-ContextMark::= SEQUENCE { StandardIdentifier standardIdentifier	0000 0110	Palaikomo standarto objekto identifikatorius, dalis ir versija. Pavyzdys: ISO (1) Standartas (0) TARV (15638) dalis 9(9) Versija1 (1). Pirmas oktetas – tai 06H, kuris yra objekto identifikatorius, o antras oktetas 06H yra ilgis. Kiti 6 oktetai koduoja pavyzdinį objekto identifikatorių Atkreipkite dėmesį, kad pateikiamas tik vienas sekos elementas (pasirenkamasis RtmCommProfile elementas yra praleistas)
17		0000 0110	
18		0010 1000	
19		1000 0000	
20		1111 1010	
21		0001 0110	
22		0000 1001	
23		0000 0001	
24	ObeConfiguration Sequence {		
	OPTION indicator	0	ObeStatus nepateiktas
	EquipmentClass INTEGER (0..32767)	xxx xxxx	
25		xxxx xxxx	
26	ManufacturerId INTEGER (0..65535)	xxxx xxxx	DSRC-VU gamintojo identifikatorius toks, kaip aprašyta standarto ISO 14816 registre
27		xxxx xxxx	
28	FCS	xxxx xxxx	Kadro patikros seka
29		xxxx xxxx	
30	Flag	0111 1110	Galinė žyma

DCS_49 Tada REDCR nuskaito duomenis nusiųsdamas komandą GET, atitinkančią standarto EN 13372, 6.2, 6.3, 6.4 punktuose ir standarte EN 12834 apibrėžtą GET komandą su 14.10 lentelėje nurodytais nuostačiais.

14.10 lentelė.

Pateikimas. GET užklausos kadro nuostačiai

Laukelis	Nuostačiai
Invoker Identifier (IID)	Nepateikta
Link Identifier (LID)	Konkretaus DSCR-VU ryšio linijos adresas
Chaining	Ne
Element Identifier (EID)	Kaip nurodyta VST Jokio plėtinio

▼B

Laukelis	Nuostačiai
Access Credentials	Ne
AttributeIdList	Jokio plėtinio, 1 požymis, AttributeID = 1 (RtmData)
Fragmentation	Ne
Layer2 settings	PDU komanda, pateikta ACn komanda

14.11 lentelėje pateiktas RTM duomenų nuskaitymo pavyzdys.

14.11 lentelė.

Pateikimas. GET užklausos kadro pavyzdys

Oktetas #	Požymis ir (arba) laukelis	Bitų skaičius oktete	Aprašymas
1	FLAG	0111 1110	Pradinė žyma
2	Private LID	xxxx xxxx	Konkretaus DSCR-VU ryšio linijos adresas
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control Field	1010 s000	PDU komanda
7	LLC Control field	n111 0111	Pateikta ACn komanda, n bitas
8	Fragmentation header	1xxx x001	Fragmentavimas netaikomas
9	Get.request SEQUENCE {	0110	GET užklausa
	OPTION indicator	0	Prieigos saugumo požymiai nepateikti
	OPTION indicator	0	IID nepateiktas
	OPTION indicator	1	AttributeIdList pateiktas
	Fill BIT STRING(SIZE(1))	0	Nustatyta vertė 0
10	EID INTEGER(0..127,…)	xxxx xxxx	Su RTM programos pavyzdžio EID, kaip nustatyta VST. Jokio plėtinio
11	AttributeIdList SEQUENCE OF { AttributeId }}	0000 0001	Jokio plėtinio, požymių skaičius = 1
12		0000 0001	AttributeId=1, RtmData. Jokio plėtinio
13	FCS	xxxx xxxx	Kadro patikros seka
14		xxxx xxxx	
15	Flag	0111 1110	Galinė žyma

▼B

DSC_50 *DSRC-VU*, kai gauna GET užklausą, nusiunčia GET atsaką su prašomais duomenimis, atitinkantį standarto EN 13372, 6.2, 6.3, 6.4 punktuose ir standarte EN 12834 apibrėžtą GET atsaką su 14.12 lentelėje nurodytais nuostačiais.

14.12 lentelė.

Pateikimas. GET atsako kadro pavyzdys

Laukelis	Nuostačiai
Invoker Identifier (IID)	Nepateikta
Link Identifier (LID)	Kaip nustatyta standarte EN 12834
Chaining	Ne
Element Identifier (EID)	Kaip nurodyta VST
Access Credentials	Ne
Fragmentation	Ne
Layer2 settings	PDU atsakas, atsakas prieinamas ir komanda priimta, ACn komanda

14.13 lentelėje pateiktas RTM duomenų nuskaitymo pavyzdys.

14.13 lentelė.

Pateikimas. Atsako kadro turinio pavyzdys

Oktetas #	Požymis ir (arba) laukelis	Bitų skaičius oktete	Aprašymas
1	FLAG	0111 1110	Pradinė žyma
2	Private LID	xxxx xxxx	Konkretaus DSCR-VU ryšio linijos adresas
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control Field	1101 0000	PDU atsakas
7	LLC Control field	n111 0111	Atsakas prieinamas, ACn komandos n bitas
8	LLC Status field	0000 0000	Atsakas prieinamas ir komanda priimta
9	Fragmentation header	1xxx x001	Fragmentavimas netaikomas
10	Get.response SEQUENCE {	0111	Gauti atsakymą

▼B

Oktetas #	Požymis ir (arba) laukelis	Bitų skaičius oktete	Aprašymas
	OPTION indicator	0	IID nepateiktas
	OPTION indicator	1	Požymių sąrašas pateiktas
	OPTION indicator	0	Grįžtamoji būklė nepateikta
	Fill BIT STRING(SIZE(1))	0	Nenaudojama
11	EID INTEGER(0..127,…)	xxxx xxxx	Atsakymas iš RTM programos Pavyzdžio. Jokio plėtinio,
12	AttributeIdList SEQUENCE OF {	0000 0001	Jokio plėtinio, požymių skaičius = 1
13	Attributes SEQUENCE { AttributeId	0000 0001	Jokio plėtinio, AttributeID = 1 (RtmData)
14	AttributeValue CONTAINER {	0000 1010	Jokio plėtinio, paketo parinktis = 10_{10}.
15		kkkk kkkk	RtmData
16		kkkk kkkk	
17		kkkk kkkk	
…		…	
n	}}}}	kkkk kkkk	
n+1	FCS	xxxx xxxx	Kadro patikros seka
n+2		xxxx xxxx	
n+3	Flag	0111 1110	Galinė žyma

DSC_51 Tada REDCR nutraukia ryšį pateikdamas EVENT_REPORT, RELEASE komandą, atitinkančią standarto EN 13372, 6.2, 6.3, 6.4 punktų ir standarto EN12834,7.3.8 punkto nuostatas netaikant jokių konkrečių RTM nuostačių. 14.14 lentelėje pateiktas RELEASE komandos bito kodavimo pavyzdys.

14.14 lentelė.

Nutraukimas. EVENT_REPORT RELEASE kadro turinys

Oktetas #	Požymis ir (arba) laukelis	Bitų skaičius oktete	Aprašymas
1	FLAG	0111 1110	Pradinė žyma
2	Private LID	xxxx xxxx	Konkretaus DSCR-VU ryšio linijos adresas
3		xxxx xxxx	
4		xxxx xxxx	

▼B

Oktetas #	Požymis ir (arba) laukelis	Bitų skaičius oktete	Aprašymas
5		xxxx xxxx	
6	MAC Control Field	1000 s000	Į kadrą įtraukta LPDU komanda
7	LLC Control field	0000 0011	UI komanda
8	Fragmentation header	1xxx x001	Fragmentavimas netaikomas
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Release)
	OPTION indicator	0	Prieigos saugumo požymiai nepateikti
	OPTION indicator	0	Įvykio parametras nepateiktas
	OPTION indicator	0	IID nepateiktas
	Mode BOOLEAN	0	Atsakymo nelaukiama
10	EID INTEGER (0..127,…)	0000 0000	Jokio plėtinio, EID = 0 (sistema)
11	EventType INTEGER (0..127,…) }	0000 0000	Įvykio tipas 0 = nutraukimas
12	FCS	xxxx xxxx	Kadro patikros seka
13		xxxx xxxx	
14	Flag	0111 1110	Galinė žyma

DSC_52 Nenumatyta, kad *DSRC-VU* reaguotų į nutraukimo komandą. Tada ryšys yra nutraukiamas.

5.4.8 *DSRC transakcijos bandymo aprašymas*

DSC_53 Naudodami pirmiau apibrėžtą įprastą GET komandą, prieigą prie saugos procedūrų turintys įgaliotieji asmenys turi atlikti visus 11 priedėlyje „Bendrieji apsaugos mechanizmai“ nustatytus bandymus, įskaitant duomenų saugumo užtikrinimą.

DSC_54 Priimamieji bandymai ir periodiniai tikrinimo bandymai, kuriuos atliekant būtina iššifruoti duomenis ir suprasti iššifruotų duomenų turinį, turi būti vykdomi pagal 11 priedėlio „Bendrieji apsaugos mechanizmai“ ir 9 priedėlio „Tipo patvirtinimas. Būtinųjų bandymų sąrašas“ nuostatas.

Tačiau pagrindinį DSRC ryšį galima bandyti naudojant ECHO komandą. Šiuos bandymus gali būti reikalaujama atlikti atiduodant eksploatuoti, imantis periodinio tikrinimo ar kitais atvejais, jeigu gaunamas kompetentingos kontrolės institucijos prašymas arba pagal Reglamentą (ES) Nr. 165/2014 (žr. 6 dalį).

▼B

DSC_55 Kad būtų atliekamas šis pagrindinis ryšio bandymas, vykstant seansui, t. y. kai sėkmingai užbaigiamas inicijavimo etapas, REDCR siunčia ECHO komandą. Vadinasi, transakcijų seka yra panaši į užklausos seką:

— 1 etapas. *REDCR* siunčia tikrinimo kelyje įrangos sukurtus ir perduotus duomenis (BST), į kuriuos įtraukti suderinamų programų identifikatoriai (AID), nurodyti paslaugų sąraše. RTM taikomoje programoje tai bus tiesiog perdavimas naudojant AID vertę = 2.

DSRC-VU įvertina gautus BST ir jeigu jis nustato, kad BST prašoma „Freight&Fleet“ (AID = 2), tada *DSRC-VU* siunčia atsaką. Jeigu *REDCR* neužtikrina AID=2, *DSRC-VU* turi nutraukti savo transakciją su *REDCR*.

— 2 etapas. *DSRC-VU* siunčia užklausą, kad būtų suteiktas atskiras langas.

— 3 etapas. REDCR siunčia atskiro lango suteikimą.

— 4 etapas. *DSRC-VU* naudoja paskirtąjį atskirą langą, kad nusiųstų transporto priemonės informacijos bloką (VST). Į šį VST įtrauktas visų skirtingų programos, su kuria šis *DSCR-VU* pritaikytas naudoti AID=2 sistemoje, konkretizavimų sąrašas. Skirtingi konkretizavimai turi būti identifikuojami unikaliais EID, iš kurių kiekvienas susiejamas su parametro verte, nurodančia suderinamą programą.

— 5 etapas. Po to *REDCR* analizuoja pateiktą VST ir arba nutraukia ryšį (RELEASE), nes REDCR niekas nėra reikalinga, kas pateikta VST (t. y. REDCR gauna VST iš *DSRC-VU*, kuris nėra RTM VU, arba, jeigu REDCR gauna atitinkamą VST, jis pradeda taikomos programos konkretizavimą.

— 6 etapas. *REDCR* siunčia komandą (ECHO) konkrečiam *DSRC-VU* ir priskiria atskirą langą.

— 7 etapas. *DSRC-VU* naudoja naują paskirtąjį atskirą langą, kad nusiųstų ECHO atsako kadrą.

Toliau pateiktose lentelėse nurodomi praktiniai ECHO mainų seanso pavyzdžiai,

DSC_56 Inicijavimas atliekamas pagal 5.4.7 punktą (DSC_44–DSC_48) ir 14.4–14.9 lenteles.

DSC_57 Tada REDCR siunčia standartą ISO 14906 atitinkančią ACTION, ECHO komandą, sudarytą iš duomenų 100 oktetų ir be jokių konkrečių RTM nuostačių. 14.15 lentelėje pateikiamas REDCR siunčiamo kadro turinys.

▼B

14.15 lentelė.

ACTION, ECHO užklausos kadro pavyzdys

Oktetas #	Požymis ir (arba) laukelis	Bitų skaičius oktete	Aprašymas
1	FLAG	0111 1110	Pradinė žyma
2	Private LID	xxxx xxxx	Konkretaus DSCR-VU ryšio linijos adresas
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control Field	1010 s000	PDU komanda
7	LLC Control field	n111 0111	Pateikta ACn komanda, n bitas
8	Fragmentation header	1xxx x001	Fragmentavimas netaikomas
9	ACTION.request SEQUENCE {	0000	Veiksmo užklausa (ECHO)
	OPTION indicator	0	Prieigos saugumo požymiai nepateikti
	OPTION indicator	1	Veiksmo parametras pateiktas
	OPTION indicator	0	IID nepateiktas
	Mode BOOLEAN	1	Atsako laukiama
10	EID INTEGER (0..127,…)	0000 0000	Jokio plėtinio, EID = 0 (sistema)
11	ActionType INTEGER (0..127,…)	0000 1111	Jokio plėtinio, veiksmo tipas ECHA užklausa
12	ActionParameter CONTAINER {	0000 0010	Jokio plėtinio, paketo parinktis = 2
13		0110 0100	Jokio plėtinio. Eilutės ilgis = 100 oktetų
14		xxxx xxxx	Duomenys turi būti pateikiami ekrane
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Kadro patikros seka
115		xxxx xxxx	
116	Flag	0111 1110	Galinė žyma

▼B

DSC_58 Gavęs ECHO užklausą, atsižvelgdamas į atsiųstą komandą *DSRC-VU* pagal standartą ISO 14906 ir be jokių konkrečių RTM nuostatų siunčia duomenų 100 oktetų ECHO atsaką. 14.16 lentelėje pateikiamas bitų lygmens kodavimo pavyzdys.

14.16 lentelė.

ACTION, ECHO atsako kadro pavyzdys

Oktetas #	Požymis ir (arba) laukelis	Bitų skaičius oktete	Aprašymas
1	FLAG	0111 1110	Pradinė žyma
2	Private LID	xxxx xxxx	Konkretaus transporto priemonės bloko ryšio linijos adresas
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control Field	1101 0000	PDU atsakas
7	LLC Control field	n111 0111	ACn komandos n bitas
8	LLC status field	0000 0000	Atsakas prieinamas
9	Fragmentation header	1xxx x001	Fragmentavimas netaikomas
10	ACTION.response SEQUENCE {	0001	ACTION response (ECHO)
	OPTION indicator	0	IID nepateiktas
	OPTION indicator	1	Atsako parametras pateiktas
	OPTION indicator	0	Grįžtamoji būklė nepateikta
	Fill BIT STRING (SIZE (1))	0	Nenaudojama
11	EID INTEGER (0..127,…)	0000 0000	Jokio plėtinio, EID = 0 (sistema)
12	ResponseParameter CONTAINER {	0000 0010	Jokio plėtinio, paketo parinktis = 2
13		0110 0100	Jokio plėtinio. Eilutės ilgis = 100 oktetų
14		xxxx xxxx	Ekrane pateikiami duomenys
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Kadro patikros seka
115		xxxx xxxx	
116	Flag	0111 1110	Galinė žyma

▼B

5.5 **Direktyvos 2015/71/EB įgyvendinimo stiprinimas**

5.5.1 *Apžvalga*

DSC_59 Siekiant padėti įgyvendinti Direktyvą 2015/719/EB dėl sunkiasvorių transporto priemonių didžiausios leidžiamos masės ir matmenų, transakcijos protokolas, naudojamas OWS duomenims atsisiųsti 5,8 GHz DSRC sąsajos kanalu, bus toks pats, koks naudojamas RTM duomenims (žr. 5.4.1), o vienintelis skirtumas yra tas, kad su TARV standartu siejamas objekto identifikatorius grindžiamas standarto ISO 15638 (TARV) 20 dalimi, susijusia su WOB/OWS.

5.5.2 *Komandos*

DSC_60 Atliekant OWS transakciją naudojamos tokios pačios komandos, kaip atliekant RTM transakciją.

5.5.3 *Užklausos komandos seka*

DSC_61 OWS duomenims taikoma užklausos komandos seka yra tokia pati, kaip taikoma RTM duomenims.

5.5.4 *Duomenų struktūros*

DSC_62 Informacinio turinio duomenis (OWS duomenis) sudaro sujungti

1. EncryptedOwsPayload duomenys, kurie yra ASN.1 skirsnyje 5.5.5 apibrėžti užšifruoti OwsPayload duomenys. Turi būti taikomas toks pats užšifravimo metodas, kaip 11 priedėlyje apibrėžtas RtmData užšifravimo metodas.

2. DSRCSecurityData apskaičiuoti pagal tuos pačius algoritmus, kurie taikomi RtmData ir nustatyti 11 priedėlyje.

▼B

5.5.5 *OWS DSRC transakcijai taikomas ASN.1 modulis*

DSC_63 RTM taikomojoje programoje DSRC duomenims taikomas ASN.1 modulis apibrėžiamas taip:

```
   TarvOws {iso(1) standard(0) 15638 part20(20)
   version1(1)} DEFINITIONS AUTOMATIC TAGS
   ::= BEGIN
   IMPORTS
   -- Imports data attributes and elements from EFC which are used for OWS
   LPN
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports function parameters from the EFC Application Interface Definition
   SetMMIRq
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports the L7 DSRCData module data from the EFC Application Interface Definition
   Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
   Attributes,
   BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
   EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
   ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
   FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};

   -- Definitions of the OWS functions:
   OWS-InitialiseComm-Request ::= BST
   OWS-InitialiseComm-Response::= VST
   OWS-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials
   ABSENT, iid ABSENT, attrIdList})
   OWS-DataRetrieval-Response::= Get-Response {OwsContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
   OWS-TerminateComm::= Event-Report-Request {OwsContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
   eventType (0)})
   OWS-TestComm-Request::= Action-Request {OwsContainer} (WITH COMPONENTS {..., eid (0), actionType
   (15), accessCredentials ABSENT, iid ABSENT})
   OWS-TestComm-Response::= Action-Response {OwsContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
   (0), iid ABSENT})

   -- Definitions of the OWS attributes:
   OwsData :: = SEQUENCE {
        encryptedOwsPayload OCTET STRING (SIZE(51)) (CONSTRAINED BY { -- calculated encrypting
   OwsPayload as per Appendix 11 --}),
        DSRCSecurityData OCTET STRING
        }
   OwsPayload :: = SEQUENCE {
              tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
              recordedWeight INTEGER (0..65535),            -- 0= Total measured weight of the  heavy
   goods vehicle                                                              -- with 10 Kg
   resolution.
              axlesConfiguration OCTET STRING SIZE (3),     -- 0= 20 bits allowed for the number
                                                                    -- of axles for 10 axles.
              axlesRecordedWeight OCTET STRING SIZE (20),   -- 0= Recorded Weight for each axle
                                                                    -- with 10 Kg resolution.
              tp15638Timestamp              INTEGER(0..4294967295)      -- Timestamp of current record
        }

Ows-ContextMark ::= SEQUENCE {
 standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version
        }

StandardIdentifier ::= OBJECT IDENTIFIER
 OwsContainer ::= CHOICE {
        integer                     [0]    INTEGER,
        bitstring                   [1]    BIT STRING,
        octetstring                 [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString             [3]    UniversalString,
        beaconId                    [4]    BeaconID,
        t-apdu                      [5]    T-APDUs,
        dsrcApplicationEntityId     [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                 [7]    Dsrc-EID,
        attrIdList                  [8]    AttributeIdList,
        attrList                    [9]    AttributeList{RtmContainer},
        reserved10                  [10]   NULL,
        OwsContextmark              [11]   Ows-ContextMark,
        OwsData                     [12]   OwsData,
        reserved13                  [13]   NULL,
        reserved14                  [14]   NULL,
        time                        [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

▼B

5.5.6 *OwsData elementai, atliekami veiksmai ir apibrėžtys*

OwsData elementai apibrėžiami siekiant padėti įgyvendinti Direktyvą 2015/719/EC dėl sunkiasvorių transporto priemonių didžiausios leidžiamos masės ir matmenų. Jie apibrėžiami taip:

— recordedWeight – bendroji išmatuota sunkiasvorės transporto priemonės masė (10 kg tikslumu kaip apibrėžta standarte EN ISO 14906). Pvz., vertė 2 500 atitinka 25 tonų masę.

— axlesConfiguration – sunkiasvorės transporto priemonės konfigūracija, t. y. jos ašių skaičius. Konfigūracija apibrėžiama naudojant 20 bitų kaukę (perkelta iš standarto EN ISO 14906).

2 bitų kaukė atitinka ašies konfigūraciją, kurios formatas yra toks:

— Vertė 00B reiškia, kad vertės neturima, nes transporto priemonėje nėra įrangos, leidžiančios gauti duomenis apie ašies apkrovą.

— Vertė 01B reiškia, kad ašies nėra.

— Vertė 10B reiškia, kad ašis yra, masė buvo apskaičiuota, duomenys surinkti ir kad jie pateikti axlesRecordedWeight lauke.

— Vertė 11B rezervuota panaudoti vėliau.

Paskutiniai 4 bitai rezervuoti panaudoti vėliau.

Ašių skaičius										
Vilkiko ašių skaičius			Priekabos ašių skaičius							
00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	RFU (4 bitai)

— axlesRecordedWeight – konkreti masė, užregistruota kiekvienai ašiai 10 kg tikslumu. Kiekvienai ašiai naudojami du oktetai. Pvz., vertė 150 atitinka 1 500 kg masę.

Kiti duomenų tipai apibrėžti 5.4.5.

5.5.7 *Duomenų perdavimo mechanizmai*

DSC_64 OWS duomenims perduoti transporto priemonėje tarp užklausiklio ir DSRC prietaiso turi būti naudojamas toks pats mechanizmas, kuris taikomas RTM duomenims (žr. 5.4.6).

DSC_65 Duomenų perdavimas transporto priemonėje tarp duomenų apie didžiausią leidžiamąją masę rinkimo platformos ir DSRC įrenginio turi būti grindžiamas fizine jungtimi, sąsajomis ir protokolu, apibrėžtais 5.6skirsnyje.

5.6 **Duomenų perdavimas tarp DSRC-VU ir transporto priemonės bloko**

5.6.1 *Fizinė jungtis ir sąsajos*

DSC_66 Ryšys tarp transporto priemonės bloko ir *DSRC-VU* gali būti užtikrinamas naudojant laidą arba taikant „Bluetooth v4.0 BLE“ technologija pagrįstą trumpojo nuotolio belaidį ryšį.

▼B

DSC_67 Nepaisant pasirinktų fizinio ryšio ir sąsajos užtikrinimo priemonių turi būti laikomasi toliau nurodytų reikalavimų.

DSC_68 a) Siekiant užtikrinti, kad su skirtingais tiekėjais galėtų būtų sudaromos sutartys tiekti transporto priemonės blokus ir DSRC-VU bei iš tiesų skirtingas DSRC-VU partijas, transporto priemonės bloko ir DSRC-VU jungtis turi būti standartinė atviroji jungtis. Transporto priemonės blokas su DSRC-VU turi būti sujungiamas kuriuo nors iš šių būdų:

i) ne trumpesniu kaip 2 m stacionariuoju laidu, standarto DIN 41612 H11 reikalavimus atitinkančia tiesiąja jungtimi – DSRC-VU įtaisyta patvirtinta 11 kontaktų kištukinė jungtis įstatoma į panašią pagal standartą DIN/ISO patvirtintą gaubiančiąją jungtį, įmontuotą transporto priemonės bloke,

ii) taikant mažai energijos naudojančią „Bluetooth“ ryšio technologiją,

iii) standartų ISO 11898 arba SAE J1939 nuostatas atitinkančia jungtimi.

DSC_69 b) Transporto priemonės bloko ir DSRC-VU sąsajų ir jungties apibrėžtis turi būti suderinama su 5.6.2 punkte nurodytomis programos protokolo komandomis.

DSC_70 c) Transporto priemonės blokas ir DSRC-VU turi būti pritaikyti užtikrinti duomenų perdavimą per jungtį atsižvelgiant į eksploatacinius parametrus ir maitinimą.

5.6.2 *Taikomosios programos protokolas*

DSC_71 Tarp transporto priemonės bloko nuotolinio ryšio įrenginio ir DSRC-VU užtikrinamas programos protokolas naudojamas duomenims nuotoliniu ryšiu periodiškai perduoti iš transporto priemonės bloko į DSRC.

DSC_72 Taikomos šios pagrindinės komandos:

1. Ryšio linijos inicijavimas – užklausa

2. Ryšio linijos inicijavimas – atsakas

3. Duomenų siuntimas su RTM programos identifikatoriumi ir informacinio turinio duomenimis, apibrėžtais pagal RTM duomenis

4. Duomenų patvirtinimas

5. Ryšio linijos nutraukimas – užklausa

6. Ryšio linijos nutraukimas – atsakas

DSC_73 ASN1.0 taikomas minėtas komandas galima apibrėžti taip:

▼B

```
Remote Communication DT Protocol DEFINITIONS ::= BEGIN

     RCDT-Communication Link Initialization - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

     RCDT-Communication Link Initialization - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

          RCDT- Send Data ::=
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER, RCDTData
          SignedTachographPayload
     }

          RCDT Data Acknowledgment ::
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER,
          answer         BOOLEAN
     }

          RCDT-Communication Link Termination - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

          RCDT-Communication Link Termination - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

End
```

DSC_74 Komandos ir parametrai apibrėžiami taip:

— `RCDT-Communication Link Initialization - Request` naudojama ryšio linijai inicijuoti. Šią komandą transporto priemonės blokas siunčia DSRC-VU. Transporto priemonės blokas nustato identifikatorių LinkIdentifier ir perduoda jį DSRC-VU, kad būtų atsekta konkreti ryšio linija.

(Pastaba. taip siekiama prisitaikyti prie būsimų ryšio linijų ir kitų programų ir (arba) modulių, pvz., transporto priemonėje įrengta svėrimo įrangos).

— `RCDT-Communication Link Initialization - Response` DSRC-VU naudoja atsakui į užklausą inicijuoti ryšio liniją perduoti. Šią komandą DSRC-VU siunčia transporto priemonės blokui. Komanda inicijavimo rezultatą pateikia kaip atsakymą = 1 (įvykdyta) arba = 0 (neįvykdyta).

DSC_75 Ryšio linijos inicijavimas turi būti atliekamas tik po to, kai transporto priemonės blokas įmontuojamas, sukalibruojamas ir užvedamas variklis ir (arba) įjungiamas transporto priemonės blokas.

▼B

— RCDT-Send Data transporto priemonės blokas naudoja pasirašytiems RCDTData (t. y., *nuotolinio ryšio duomenims*) siųsti į DSRC-VU. Duomenys turi būti siunčiami kas 60 sekundžių. Parametras DataTransactionId identifikuoja konkretų duomenų perdavimą. LinkIdentifier taip pat naudojamas siekiant užtikrinti, kad būtų naudojama tinkama ryšio linija.

— RCDT-Data Acknowledgment DSRC-VU siunčia, kad patvirtintų transporto priemonės blokui, jog gavo duomenis, išsiųstus naudojant komandą RCDT-Send Data, identifikuotą DataTransactionId parametru. Atsakymo parametras yra 1 (įvykdyta) arba =0 (neįvykdyta). Jeigu transporto priemonės blokas gauna daugiau negu tris atsakymus, kurių vertė yra 0, arba jeigu transporto priemonės blokas negauna patvirtinimo, kad buvo gauti RCDT duomenys, gauti prieš tai išsiuntus komandą RCDT–Send Data, identifikuotą konkrečiu DataTransactionId, transporto priemonės blokas generuoja įvykio įrašą.

— RCDT-Communication Link Termination request transporto priemonės blokas siunčia DSRC-VU, kad būtų nutraukta ryšio linija, identifikuota tam tikru LinkIdentifier.

DSC_76 Kai DSRC-VU arba transporto priemonės blokas įjungiamas pakartotinai, visos esamos ryšio linijos turėtų būti nutrauktos, nes staigiai išjungus transporto priemonės bloką galėjo atsirasti „pakibusių“ ryšio linijų.

— RCDT-Communication Link Termination – Response DSRC-VU siunčia transporto priemonės blokui, kad patvirtintų transporto priemonės bloko atsiųstą ryšio linijos, identifikuotos tam tikru LinkIdentifier, nutraukimo užklausą.

5.7 **Klaidų valdymas**

5.7.1 *Duomenų įrašymas į DSRC-VU ir jų perdavimas*

DSC_77 Naudojant *VUSM* funkciją į *DSRC-VU* turi būti perduodami jau apsaugoti duomenys. *VUSM* turi patikrinti, ar į *DSRC-VU* įrašomi duomenys buvo įrašyti teisingai. Visoms duomenų perdavimo iš transporto priemonės bloko į *DSRC-VU* atmintį klaidoms užregistruoti ir pranešimams apie jas pateikti turi būti naudojamas duomenų tipas EventFaultType, nurodoma nuotolinio ryšio įrenginio ryšio trikties numeravimo vertė ‘62’H ir laiko žyma.

DSC_78 Transporto priemonės blokas išsaugo unikaliu pavadinimu pažymėtą rinkmeną, kurią tikrintojai galėtų lengvai identifikuoti, jeigu reikėtų užregistruoti transporto vidinio ryšio triktis.

DSC_79 Jeigu VUPM mėgina transporto priemonės bloko duomenis gauti iš saugumo modelio (kad perduotų juos VU-DSRC), tačiau šios operacijos nepavyksta atlikti, šią triktį VUPM registruoja naudodamas duomenų tipą EventFaultType, nurodymas nuotolinio ryšio įrenginio ryšio trikties numeravimo

▼B

vertą *'62'H* ir laiko žymą. Ryšio triktis nustatoma, jeigu daugiau negu tris kartus paeiliui negaunamas pranešimas `RCDT Data Acknowledgment`, kuriuo patvirtinamas susijusio (t. y. Pranešimai `Send Data and Acknowledgment` identifikuojami tuo pačiu DataTransactionId) pranešimo `RCDT Send Data` gavimas.

5.7.2 *Belaidžio ryšio klaidos*

DSC_80 Ryšio klaidos tvarkomos pagal susijusių DSRC standartų nuostatas, t. y. standartų EN 300 674-1, EN 12253, EN 12795, EN 12834 nuostatas ir taikant atitinkamus standarte EN 13372 nurodytus parametrus.

5.7.2.1 *Užšifravimo ir pasirašymo klaidos*

DSC_81 Užšifravimo ir pasirašymo klaidos tvarkomos taip, kaip nustatyta 11 priedėlyje „Bendrieji apsaugos mechanizmai“, ir jų neturi būti jokiuose su DSRC duomenų perdavimu susijusiuose pranešimuose apie klaidas.

5.7.2.2 *Registravimo klaidos*

DSRC terpė – tai dinaminis belaidis ryšys nepastoviomis atmosferos ir trukdžių sąlygomis, visų pirma tada, kai šios programos naudojimas susijęs su nešiojamuoju REDCR ir judančia transporto priemone. Todėl būtina įvertinti, kuo nuskaitymo triktis skiriasi nuo klaidos. Atliekant transakciją per belaidę sąsają, nuskaitymo triktis yra įprastas dalykas ir ją nustačius paprastai dar kartą mėginama perduoti BST ir atkurti seką, šiuo atveju dažniausiai pavyksta užmegzti ryšį ir perduoti duomenis, jeigu pasirinktoji transporto priemonė neišvažiuoja iš sąveikos zonos, kol atliekamas pakartotinis perdavimas. (Sėkmingas nuskaitymo atvejis gali apimti kelis mėginimus ir pakartotinius mėginimus).

Nuskaitymo triktį gali sukelti tai, kad nebuvo tinkamai susietos antenos (nepavyksta nutaikyti); viena iš antenų uždengta – tai gali būti daroma tyčia, tačiau anteną taip pat gali užstoti kita transporto priemonė; radijo trukdžiai, ypač apytikriai 5,8 GHz WIFI arba kiti viešosios prieigos belaidžiai ryšiai, arba radaro trukdžiai ar sudėtingos orų sąlygos (pvz., prasidėjusi perkūnija); arba minėta triktis gali atsirasti pasitraukus iš DSCR ryšio zonos. Pavienių nuskaitymo trikčių, atsižvelgiant į jų pobūdį, neįmanoma užregistruoti, nes tiesiog nepavyksta užmegzti ryšio.

Tačiau jeigu kompetentingos kontrolės institucijos pareigūnas pasirenka transporto priemonę ir mėgina užmegzti ryšį su jos DSRC-VU, bet duomenys nėra perduodami, ši triktis galėjo atsirasti dėl tyčinio įrangos keitimo, todėl kompetentingos kontrolės institucijos pareigūnui yra būtinos priemonės trikčiai užregistruoti ir pranešti kitiems kolegoms apie galimą pažeidimą. Tada kolegos gali sustabdyti transporto priemonę ir atlikti fizinį patikrinimą. Tačiau jeigu ryšio užmegzti nepavyksta, DSRC-VU negali pateikti trikties duomenų. Todėl projektuojant REDCR įrangą turi būti numatoma šio pranešimo teikimo funkcija.

Nuskaitymo triktis techniniu atžvilgiu skiriasi nuo klaidos. Atsižvelgiant į minėtus dalykus, klaida yra neteisingos vertės registravimas.

▼B

Į *DSRC-VU* perduodami jau apsaugoti duomenys, todėl juos turi tikrinti duomenų pateikėjas (žr. 5.4 punktą).

Per belaidę sąsają vėliau perduodami duomenys tikrinami ryšio lygmeniu atliekant ciklinę perteklinę kontrolę (CRC). Jeigu taikant CRC gaunamas patvirtinimas, vadinasi, duomenys yra teisingi. Jeigu taikant CRC patvirtinimas nėra gaunamas, duomenys perduodami dar kartą. Statistinė tikimybė, kad taikant CRC galėtų būti perduodami neteisingi duomenys, yra tokia maža, kad jos galima nepaisyti.

Jeigu taikant CRC nėra gaunamas patvirtinimas ir jeigu nėra laiko pakartotinai perduoti ir gauti teisingus duomenis, rezultatas būtų ne klaida, o tam tikro tipo nuskaitymo trikties atvejis.

Vieninteliai prasmingi trikties duomenys, kuriuos galima registruoti – kiek kartų pavyko inicijuoti transakciją, kuriai vykstant duomenys nebuvo perduoti REDCR.

DSC_82 Todėl *REDCR* turi registruoti ir laiko žyma pažymėti įvykius, kai DSCR užklausos inicijavimo etapas buvo sėkmingai užbaigtas, tačiau transakcija buvo nutraukta pirmiau negu REDCR pavyko nuskaityti *duomenis*. Šie duomenys turi būti prieinami kompetentingos kontrolės institucijos pareigūnui ir laikomi REDCR įrangos atmintyje. Priemonės, kuriomis tai užtikrinama, turi būti numatomos projektuojant produktą arba kompetentingos kontrolės institucijos parengtoje specifikacijoje.

Vieninteliai prasmingi klaidų duomenys, kuriuos galima registruoti – kiek kartų REDCR nepavyksta iššifruoti gautų *duomenų*. Tačiau būtina pabrėžti, kad tai susiję tik su REDCR programinės įrangos veiksmingumu. Duomenis techniškai gali pavykti iššifruoti, tačiau jie gali neturėti semantinės prasmės.

DSC_83 Todėl *REDCR* turi registruoti ir laiko žyma pažymėti įvykius, kai *REDCR* mėgino iššifruoti per DSRC sąsają gautus duomenis, tačiau jam tai nepavyko.

6 NUOTOLINIO RYŠIO FUNKCIJOS NAUDOJIMO PRADŽIA IR PERIODINIO PATIKRINIMO BANDYMAI

6.1 **Bendrosios nuostatos**

DSC_84 Su nuotolinio ryšio funkcija paprastai atliekami dviejų tipų bandymai:

1) ECHO bandymas siekiant patvirtinti *DSRC-REDCR* >>-:-<*DSRC-VU* belaidžio ryšio kanalo patikimumą.

2) Ištisinis saugumo bandymas siekiant užtikrinti, kad naudojantis dirbtuvių kortele būtų galima sužinoti užšifruotų ir pasirašytų duomenų, sukurtų transporto priemonės bloko ir perduotų belaidžio ryšio kanalu, turinį.

6.2 **ECHO GD**

Šiame punkte pateiktos nuostatos, specialiai parengtos tik tam, kad būtų įmanoma išbandyti, ar *DSRC-REDCR* >>-:-<*DSRC-VU* funkcija yra aktyvi.

▼B

Siunčiant ECHO komandą siekiama dirbtuvėms ar tipo patvirtinimo bandymą atliekančioms įstaigoms suteikti galimybę patikrinti, ar DSRC ryšio kanalas veikia nereikalaujant prieigos prie saugumo požymių. Todėl bandytojo įranga turi būti įmanoma tik inicijuoti DSRC ryšį (siųsti BST, AID = 2) ir po to siųsti ECHO komandą, ir, darant prielaidą, kad DSRC veikia, bus gautas ECHO atsakas. Išsami informacija pateikta 5.4.8 punkte. Padarius prielaidą, kad įranga šį atsaką gauna tinkamai, galima laikyti, kad DSRC ryšio linija (*DSRC-REDCR* >>-:-<*DSRC-VU*) veikia tinkamai.

6.3 **Saugių duomenų turinio patvirtinimo bandymai**

DSC_85 Šis bandymas atliekamas siekiant patvirtinti ištisinio duomenų srauto saugumą. Šiam bandymui atlikti privaloma naudoti DSCR bandomąjį skaitytuvą. DSRC bandomasis skaitytuvas atlieka tą pačią funkciją ir atitinka tas pačias specifikacijas, kaip ir skaitytuvai, kuriuos naudoja teisėsaugos institucijos, tačiau skiriasi tuo, kad DSRC bandomojo skaitytuvo naudotojo tapatybei patvirtinti naudojama dirbtuvių kortelė, o ne kontrolės kortelė. Bandymą galima atlikti užbaigus pradinį išmaniojo tachografo aktyvinimą arba kalibravimo procedūros pabaigoje. Aktyvintas transporto priemonės blokas turi generuoti apsaugotus ankstyvo nustatymo duomenis ir juos perduoti DSRC-VU.

DSC_86 Dirbtuvių darbuotojai DSRC bandomąjį skaitytuvą turi padėti 2–10 m atstumu priešais transporto priemonę.

DSC_87 Tada dirbtuvių darbuotojai į DSRC bandomąjį skaitytuvą įstato dirbtuvių kortelę, kad būtų perduodama užklausa iš transporto priemonės bloko nuskaityti ankstyvo nustatymo duomenis. Sėkmingai priėmus užklausą, dirbtuvių darbuotojai gauna prieigą prie atsiųstų duomenų, kad galėtų įsitikinti, kad duomenų nepažeistumas buvo patvirtintas ir jie buvo iššifruoti.

▼B

15 Priedėlis

PERĖJIMAS PRIE NAUJOS ĮRANGOS. SKIRTINGŲ KARTŲ ĮRANGOS VIENALAIKIO NAUDOJIMO ADMINISTRAVIMAS

TURINYS

1. APIBRĖŽTYS

2. BENDROSIOS NUOSTATOS

2.1. Perėjimo apžvalga

2.2. Transporto priemonės bloko ir kortelių sąveikumas

2.3. Transporto priemonės bloko ir judesio jutiklio sąveikumas

2.4. Transporto priemonės blokų, tachografo kortelių ir duomenų perkėlimo įrangos sąveikumas

2.4.1 Tiesioginis duomenų perkėlimas iš kortelės naudojant IDE

2.4.2 Duomenų perkėlimas iš kortelės naudojant transporto priemonės bloką

2.4.3 Duomenų perkėlimas iš transporto priemonės bloko

2.5. Transporto priemonės bloko ir kalibravimo įrangos sąveikumas

3. PAGRINDINIAI VEIKSMAI LAIKOTARPIU IKI ĮDIEGIMO DATOS

4. LAIKOTARPIUI NUO ĮDIEGIMO DATOS TAIKOMOS NUOSTATOS

1. APIBRĖŽTYS

Šiame priedėlyje vartojami šie terminai:

išmaniojo tachografo sistema*:* apibrėžta šiame priede (1 skyrius: bbb apibrėžtis);

pirmosios kartos tachografo sistema*:* apibrėžta šiame reglamente (2 straipsnis: 1 apibrėžtis);

antrosios kartos tachografo sistema*:* apibrėžta šiame reglamente (2 straipsnis: 7 apibrėžtis);

įdiegimo data*:* apibrėžta šiame priede (1 skyrius: ccc apibrėžtis);

specializuota įranga su mikroprocesoriumi (IDE)*:* įranga, skirta duomenims perkelti, kaip apibrėžta šio priedo 7 priedėlyje.

2. BENDROSIOS NUOSTATOS

2.1. **Perėjimo apžvalga**

Šio priedo preambulėje apžvelgiamas perėjimas nuo pirmosios kartos tachografo sistemos prie antrosios kartos tachografo sistemos.

Be to, kas pasakyta preambulėje, taip pat reikia paminėti, kad:

— pirmosios kartos judesio jutikliai nebus suderinami su antrosios kartos transporto priemonės blokais;

— antrosios kartos judesio jutikliai transporto priemonėse bus pradėti montuoti tu pat metu, kaip ir antrosios kartos transporto priemonių blokai;

▼B

— duomenų perkėlimo ir kalibravimo įranga turės būti tobulinama, kad būtų galima naudoti abiejų kartų tachografus ir tachografo korteles.

2.2. **Transporto priemonės bloko ir kortelių sąveikumas**

Suprantama, kad pirmosios kartos tachografo kortelės yra suderinamos su pirmosios kartos transporto priemonių blokais (atitinkančiais šio reglamento 1B priedo reikalavimus), o antrosios kartos tachografo kortelės – su antrosios kartos transporto priemonių blokais (atitinkančiais šio reglamento 1C priedo reikalavimus). Be to, taikomi toliau nustatyti reikalavimai.

MIG_001 Išskyrus atvejus, nustatytus reikalavimais MIG_004 ir MIG_005, pirmosios kartos tachografo kortelės iki jų galiojimo pabaigos gali būti ir toliau naudojamos antrosios kartos transporto priemonės blokuose. Tačiau tokių kortelių turėtojai gali reikalauti jas pakeisti antrosios kartos tachografo kortelėmis, kai jas bus galima įsigyti.

MIG_002 Antrosios kartos transporto priemonės blokuose turi būti galima naudoti bet kokią įdėtą galiojančią pirmosios kartos vairuotojo, kontrolės ir įmonės kortelę.

MIG_003 Dirbtuvės gali visam laikui atsisakyti naudoti šią galimybę tokiuose transporto priemonės blokuose, kad jie nebegalėtų priimti pirmosios kartos tachografo kortelių. Tai gali būti padaryta tik Europos Komisijai pradėjus procedūrą, kuria dirbtuvės paraginamos tai padaryti, pvz., per kiekvieną periodinį tachografo patikrinimą.

MIG_004 Antrosios kartos transporto priemonės blokuose turi būti galima naudoti tik antrosios kartos dirbtuvių korteles.

MIG_005 Siekiant nustatyti veikimo režimą, antrosios kartos transporto priemonės blokuose turi būti paisoma tik to, kurios rūšies galiojanti kortelė įdėta, o ne kurios kartos ji yra.

MIG_006 Bet kokią galiojančią antrosios kartos tachografo kortelę pirmosios kartos transporto priemonės blokuose turi būti galima naudoti lygiai taip pat, kaip tokios pat rūšis pirmosios kartos tachografo kortelę.

2.3. **Transporto priemonės bloko ir judesio jutiklio sąveikumas**

Suprantama, kad pirmosios kartos judesio jutikliai yra suderinami su pirmosios kartos transporto priemonės blokais, o antrosios kartos judesio jutikliai – su antrosios kartos transporto priemonės blokais. Be to, taikomi toliau nustatyti reikalavimai.

MIG_007 Antrosios kartos transporto priemonės blokų nebus galima susieti ir naudoti su pirmosios kartos judesio jutikliais.

MIG_008 Antrosios kartos judesio jutikliai gali būti siejami ir naudojami tik su antrosios kartos transporto priemonės blokais arba su abiejų kartų transporto priemonės blokais.

2.4. **Transporto priemonės blokų, tachografo kortelių ir duomenų perkėlimo įrangos sąveikumas**

MIG_009 Duomenų perkėlimo įranga gali būti naudojama tik su vienos kartos transporto priemonės blokais ir tachografo kortelėmis arba su abiejų kartų transporto priemonės blokais ir tachografo kortelėmis.

▼B

2.4.1 *Tiesioginis duomenų perkėlimas iš kortelės naudojant IDE*

MIG_010 Naudojant IDE, duomenys iš vienos kartos tachografo kortelių, įdėtų į kortelių nuskaitymo įrenginius, perkeliami taikant tos kartos duomenų apsaugos mechanizmus ir duomenų perkėlimo protokolus, o perkelti duomenys turi būti tai kartai nustatyto formato.

MIG_011 Kad ne ES kontrolės institucijos galėtų kontroliuoti vairuotojus, taip pat turi būti galima duomenis iš antrosios kartos vairuotojo (ir dirbtuvių) kortelių perkelti lygiai taip pat, kaip iš pirmosios kartos vairuotojo (ir dirbtuvių) kortelių. Atliekant tokį perkėlimą, turi būti perkelti tokie duomenys:

— nepasirašytos EF `IC`ir `ICC`;

— nepasirašytos EF (pirmosios kartos) `Card_Certificate`ir `CA_Certificate`;

— kitų programos duomenų EF (esančios `TACHO`DF), kurių reikalaujama pagal duomenų perkėlimo iš pirmosios kartos kortelių protokolą. Ši informacija, taikant pirmosios kartos apsaugos mechanizmus, apsaugoma skaitmeniniu parašu.

Atliekant tokį perkėlimą, neperkeliamos programos duomenų EF, kurios yra tik antrosios kartos vairuotojų (ir dirbtuvių) kortelėse (programos duomenų EF, esančios `TACHO_G2`DF).

2.4.2 *Duomenų perkėlimas iš kortelės naudojant transporto priemonės bloką*

MIG_012 Duomenys iš antrosios kartos kortelės, įdėtos į pirmosios kartos transporto priemonės bloką, perkeliami taikant pirmosios kartos duomenų perkėlimo protokolą. Tokia kortelė į transporto priemonės bloko komandas turi atsakyti lygiai taip pat, kaip pirmosios kartos kortelė, perkeltų duomenų formatas turi būti toks pat, kaip duomenų, perkeltų iš pirmosios kartos kortelės.

MIG_013 Duomenys iš pirmosios kartos kortelės, įdėtos į antrosios kartos transporto priemonės bloką, perkeliami taikant šio priedo 7 priedėlyje nustatytą duomenų perkėlimo protokolą. Transporto priemonės blokas komandas kortelei turi perduoti lygiai taip pat, kaip pirmosios kartos transporto priemonės blokas, perkeltų duomenų formatas turi atitikti pirmosios kartos kortelėms nustatytą formatą.

2.4.3 *Duomenų perkėlimas iš transporto priemonės bloko*

MIG_014 Duomenys iš antrosios kartos transporto priemonės blokų perkeliami taikant antrosios kartos apsaugos mechanizmus ir šio priedo 7 priedėlyje nustatytą duomenų perkėlimo protokolą.

MIG_015 Kad ne ES kontrolės institucijos galėtų kontroliuoti vairuotojus, o ne ES dirbtuvės – perkelti duomenis iš transporto priemonės bloko, taip pat galima suteikti galimybę duomenis iš antrosios kartos transporto priemonės blokų perkelti taikant pirmosios kartos apsaugos mechanizmus ir pirmosios kartos duomenų perkėlimo protokolą. Perkeltų duomenų formatas turi būti toks pat, kaip duomenų, perkeltų iš pirmosios kartos transporto priemonės bloko. Ši galimybė gali būti pasirenkama iš komandų meniu.

▼B

2.5. **Transporto priemonės bloko ir kalibravimo įrangos sąveikumas**

MIG_016 Kalibravimo įranga turi galėti atlikti kiekvienos kartos tachografų kalibravimą, taikydama tos kartos kalibravimo protokolą. Kalibravimo įranga gali būti naudojama tik su vienos kartos tachografais arba su abiejų kartų tachografais.

3. PAGRINDINIAI VEIKSMAI LAIKOTARPIU IKI ĮDIEGIMO DATOS

MIG_017 Bandomieji raktai ir pažymėjimai gamintojams turi būti parengti ne vėliau kaip likus **30 mėnesių** iki įdiegimo datos.

MIG_018 Likus ne mažiau kaip **15 mėnesių** iki įdiegimo datos, turi būti pasirengta gamintojų prašymu atlikti sąveikumo bandymus.

MIG_019 Oficialūs raktai ir pažymėjimai gamintojams turi būti parengti ne vėliau kaip likus **12 mėnesių** iki įdiegimo datos.

MIG_020 Valstybės narės turi būti pasirengusios išduoti antrosios kartos dirbtuvių korteles ne vėliau kaip likus **3 mėnesiams** iki įdiegimo datos.

MIG_021 Valstybės narės turi būti pasirengusios išduoti visų rūšių antrosios kartos tachografo korteles ne vėliau kaip likus **1 mėnesiui iki įdiegimo datos**.

4. LAIKOTARPIUI NUO ĮDIEGIMO DATOS TAIKOMOS NUOSTATOS

MIG_022 Nuo įdiegimo datos valstybės narės išduoda tik antrosios kartos tachografo korteles.

MIG_023 Kad būtų galima pakeisti sugedusias dalis, transporto priemonės blokų ir (arba) judesio daviklių gamintojams pirmosios kartos transporto priemonės blokus ir (arba) judesio daviklius leidžiama gaminti tol, kol jie bus naudojami šioje srityje.

MIG_024 Transporto priemonės blokų ir (arba) judesio daviklių gamintojams leidžiama reikalauti palikti galioti jau patvirtintus pirmosios kartos transporto priemonės blokų ir (arba) judesio daviklių tipus ir gauti jų tolesnio galiojimo patvirtinimą.

▼B

16 Priedėlis.

M1 IR N1 KLASIŲ TRANSPORTO PRIEMONIŲ ADAPTERIAI

TURINYS

1. SANTRUMPOS IR SUSIJĘ DOKUMENTAI

1.1. Santrumpos

1.2. Susiję standartai

2. BENDROSIOS ADAPTERIO SAVYBĖS IR FUNKCIJOS

2.1. Bendras adapterio apibūdinimas

2.2. Funkcijos

2.3. Saugumas

3. TACHOGRAFUI KELIAMI REIKALAVIMAI, KAI ĮRENGIAMAS ADAPTERIS

4. ADAPTERIO KONSTRUKCIJOS IR FUNKCIJŲ REIKALAVIMAI

4.1. Gaunamų greičio impulsų siejimas ir priderinimas

4.2. Gaunamų impulsų perdavimas į įtaisytą judesio jutiklį

4.3. Įtaisytas judesio jutiklis

4.4. Saugumo reikalavimai

4.5. Veikimo charakteristikos

4.6. Medžiagos

4.7. Ženklai

5. TACHOGRAFO ĮRENGIMAS, KAI NAUDOJAMAS ADAPTERIS

5.1. Įrengimas

5.2. Plombavimas

6. TIKRINIMAI, PATIKROS IR REMONTAS

6.1. Periodinės patikros

7. TACHOGRAFO TIPO PATVIRTINIMAS, KAI NAUDOJAMAS ADAPTERIS

7.1. Bendrosios nuostatos

7.2. Veikimo sertifikatas

1. SANTRUMPOS IR SUSIJĘ DOKUMENTAI

1.1. **Santrumpos**

TBD turi būti nustatyta

VU transporto priemonės blokas

1.2. **Susiję standartai**

ISO 16844-3 Kelių transporto priemonės. Tachografų sistemos. 3 dalis. Judesio jutiklio sąsaja.

2. BENDROSIOS ADAPTERIO SAVYBĖS IR FUNKCIJOS

2.1. **Bendras adapterio apibūdinimas**

ADA_001 Adapteris nuolat teikia apsaugotus transporto priemonės greičio ir nuvažiuoto atstumo duomenis prijungtam transporto priemonės blokui.

Adapteris skirtas tik toms transporto priemonėms, kuriose pagal šį reglamentą turi būti įrengtas tachografas.

▼B

Jis įrengiamas ir naudojamas tik tose transporto priemonėse, kurių tipas nustatytas IC priedo yy apibrėžtyje „adapteris“, kai mechaniškai neįmanoma įrengti kitos rūšies judesio jutiklio, kuris kitais atžvilgiais atitiktų šio priedo ir jo 1–16 priedėlių reikalavimus.

Adapteris ne mechaniškai susiejamas su judančia transporto priemonės dalimi, o prijungiamas ten, kur gaunami integruotų jutiklių generuojami ar iš kitų sąsajų gaunami greičio ir (arba) atstumo impulsai.

ADA_002 Patvirtinto tipo judesio jutiklis (pagal šio IC priedo 8 skirsnio „Tachografų ir tachografo kortelių tipo patvirtinimas“ nuostatas) įrengiamas adapterio korpuse, kuriame taip pat turi būti impulsų keitiklis, perduodantis gaunamus impulsus į įtaisytą judesio jutiklį. Įtaisytasis judesio jutiklis sujungiamas su transporto priemonės bloku taip, kad transporto priemonės bloko ir adapterio sąsaja atitiktų ISO 16844-3 standarto reikalavimus.

2.2. **Funkcijos**

ADA_003 Adapteris atlieka šias funkcijas:

— susieja ir priderina gaunamus greičio impulsus,

— perduoda gaunamus impulsus į įtaisytą judesio jutiklį,

— visas įtaisyto judesio jutiklio funkcijas ir teikia apsaugotus judėjimo duomenis į transporto priemonės bloką.

2.3. **Saugumas**

ADA_004 Adapteriui neteikiamas apsaugos pažymėjimas pagal judesio jutiklio bendrąjį apsaugos tikslą, nustatytą šio priedo 10 priedėlyje. Vietoj jo taikomi saugumo reikalavimai nustatyti šio priedėlio 4.4 skirsnyje.

3. TACHOGRAFUI KELIAMI REIKALAVIMAI, KAI ĮRENGIAMAS ADAPTERIS

Tolesniuose skyriuose pateikti reikalavimai rodo, kaip turi būti suprantami šio priedo reikalavimai, kai naudojamas adapteris. Skliaustuose įrašyti susijusių IC priedo reikalavimų numeriai.

ADA_005 Bet kokios transporto priemonės, kurioje įrengtas adapteris, tachografas turi atitikti visas šio priedo nuostatas, nebent šiame priedėlyje nurodyta kitaip.

ADA_006 Jei yra įrengtas adapteris, tachografas apima kabelius, adapterį (įskaitant judesio jutiklį) ir transporto priemonės bloką [01].

ADA_007 Įvykių ir (arba) trikčių nustatymo funkcija tachografe pakeičiama taip:

— transporto priemonės blokas, kai jis veikia ne kalibravimo režimu, fiksuoja „maitinimo nutrūkimo“ įvykį, jei įtaisyto judesio jutiklio maitinimas nutrūksta ilgesniam kaip 200 milisekundžių laikotarpiui [79];

▼B

— transporto priemonės blokas fiksuoja „duomenų apie judėjimą klaidos“ įvykį, jei nutrūksta įprastas duomenų srautas tarp įtaisyto judesio jutiklio ir transporto priemonės bloko ir (arba) jiems keičiantis duomenimis įvyksta duomenų nepažeistumo arba autentiškumo klaida [83];

— transporto priemonės blokas, kai jis veikia ne kalibravimo režimu, fiksuoja „bandymo pažeisti apsaugą“ įvykį, jei įvyksta bet koks kitas įvykis, paveikiantis įtaisyto judesio jutiklio saugumą [85];

— transporto priemonės blokas, kai jis veikia ne kalibravimo režimu, fiksuoja „tachografo“ triktį, kai įvyksta bet kokia įtaisyto judesio jutiklio triktis [88].

ADA_008 Tachografo aptinkamos adapterio triktys yra triktys, susijusios su įtaisytu judesio jutikliu [88].

ADA_009 Transporto priemonės bloko kalibravimo funkcija suteikia galimybę automatiškai susieti įtaisytą judesio jutiklį su transporto priemonės bloku [202, 204].

4. ADAPTERIO KONSTRUKCIJOS IR FUNKCIJŲ REIKALAVIMAI

4.1. **Gaunamų greičio impulsų siejimas ir priderinimas**

ADA_011 Adapterio įvesties sietuvas priima dažnio impulsus, rodančius transporto priemonės greitį ir nuvažiuotą atstumą. Gaunamų impulsų elektrinės savybės: *turi nustatyti gamintojas*. Tinkamas adapterio įvesties susiejimas su transporto priemone, jei taikoma, atliekamas reguliavimo priemonėmis, kurios yra prieinamos tik adapterio gamintojui ir patvirtintoms dirbtuvėms, kurios įrengia adapterį.

ADA_012 Adapterio įvesties sietuvas, jei taikoma, turi gebėti dauginti arba dalyti gaunamų greičio impulsų dažnio impulsus iš pastovaus koeficiento, kad priderintų signalą prie šiame priede nustatyto k koeficiento diapazono (4 000–25 000 impulsų/km). Šį pastovų koeficientą gali užprogramuoti tik adapterio gamintojas ir patvirtintos dirbtuvės, kurios įrengia adapterį.

4.2. **Gaunamų impulsų perdavimas į įtaisytą judesio jutiklį**

ADA_013 Gaunami impulsai (prireikus priderinti, kaip nurodyta pirmiau) perduodami į įtaisytą judesio jutiklį taip, kad judesio jutiklis fiksuotų kiekvieną gaunamą impulsą.

4.3. **Įtaisytas judesio jutiklis**

ADA_014 Perduodami impulsai aktyvina įtaisytą judesio jutiklį ir šis generuoja judėjimo duomenis, tiksliai atitinkančius transporto priemonės judėjimą, lyg būtų mechaniškai susietas su judančia transporto priemonės dalimi.

ADA_015 Transporto priemonės blokas pagal įtaisyto judesio jutiklio identifikacijos duomenis identifikuoja adapterį [95].

▼B

ADA_016 Įtaisytame judesio jutiklyje saugomi įrengimo duomenys laikomi adapterio įrengimo duomenimis [122].

4.4. **Saugumo reikalavimai**

ADA_017 Adapterio korpusas turi būti sukonstruotas taip, kad nebūtų galima jo atidaryti. Jis užplombuojamas, kad bandymą jį fiziškai pažeisti būtų lengva aptikti (pvz., apžiūrint, žr. ADA_035). Plombos turi atitikti tuos pačius reikalavimus, kaip judesio jutiklių plombos [398–406].

ADA_018 Turi būti neįmanoma įtaisyto judesio jutiklio išimti iš adapterio nepažeidžiant adapterio korpuso plombos (-ų) ar plombos tarp jutiklio ir adapterio korpuso (žr. ADA_034).

ADA_019 Adapteris užtikrina, kad judėjimo duomenys būtų gaunami ir apdorojami tik iš adapterio gaunamų duomenų.

4.5. **Veikimo charakteristikos**

ADA_020 Adapteris turi tinkamai veikti gamintojo nustatytame temperatūros intervale.

ADA_021 Adapteris turi tinkamai veikti 10–90 % drėgnumo intervale [214].

ADA_022 Adapteris turi būti apsaugotas nuo viršįtampio, maitinimo įtampos poliškumo pasikeitimo ir trumpojo jungimo [216].

ADA_023 Adapteris turi:

— reaguoti į magnetinį lauką, kuris trukdo nustatyti transporto priemonės judėjimo. Tokiomis aplinkybėmis transporto priemonės blokas įrašo ir laiko atmintyje jutiklio triktį [88] arba

— turėti jutiklį, kuris būtų apsaugotas nuo magnetinių laukų arba jiems atsparus [217].

ADA_024 Adapteris turi atitikti tarptautinę JT EEK R10 taisyklę dėl elektromagnetinio suderinamumo ir turi būti apsaugotas nuo elektrostatinių iškrovų ir trumpalaikių pavienių impulsų [218].

4.6. **Medžiagos**

ADA_025 Adapteris turi atitikti apsaugos klasę (*turi nustatyti gamintojas, priklauso nuo įrengimo vietos*) [220, 221].

ADA_026 Adapterio korpusas turi būti geltonos spalvos.

4.7. **Ženklai**

ADA_027 Prie adapterio turi būti pritvirtinta plokštelė su šiais duomenimis:

— adapterio gamintojo pavadinimas ir adresas,

— gamintojo suteiktas komponento šifras ir adapterio pagaminimo metai,

— adapterio arba tachografo su adapteriu tipo patvirtinimo ženklas,

— adapterio įrengimo data,

▼B

— transporto priemonės, kurioje jis įrengtas, identifikavimo numeris.

ADA_028 Informacinėje plokštelėje taip pat turi būti šie duomenys (jei iš išorės jų nematyti ant įtaisyto judesio jutiklio):

— įtaisyto judesio jutiklio gamintojo pavadinimas,

— gamintojo suteiktas dalies numeris ir įtaisyto judesio jutiklio pagaminimo metai,

— įtaisyto judesio jutiklio tipo patvirtinimo ženklas.

5. TACHOGRAFO ĮRENGIMAS, KAI NAUDOJAMAS ADAPTERIS

5.1. **Įrengimas**

ADA_029 Transporto priemonėse įrengiamus adapterius įrengia tik transporto priemonių gamintojai arba patvirtintos dirbtuvės, turinčios teisę įrengti, aktyvinti ir kalibruoti skaitmeninius ir išmaniuosius tachografus.

ADA_030 Tokios patvirtintos dirbtuvės, įrengdamos adapterį, sureguliuoja įvesties sąsają ir nustato įvesties signalo dalijimo koeficientą (jei taikoma).

ADA_031 Tokios patvirtintos dirbtuvės, įdiegdamos adapterį, užplombuoja adapterio korpusą.

ADA_032 Adapteris įrengiamas kuo arčiau tos transporto priemonės dalies, iš kurios gaunami jo įvesties impulsai.

ADA_033 Adapterio maitinimo laidai turi būti raudonas (teigiamo maitinimo poliaus) ir juodas (įžeminimo).

5.2. **Plombavimas**

ADA_034 Taikomi šie plombavimo reikalavimai:

— adapterio korpusas turi būti užplombuotas (žr. ADA_017),

— įtaisyto jutiklio korpuso sujungimas su adapterio korpusu turi būti užplombuotas, nebent būtų neįmanoma išimti jutiklio iš adapterio korpuso nepažeidus adapterio korpuso plombos (-ų) (žr. ADA_018),

— adapterio korpuso sujungimas su transporto priemone turi būti užplombuotas,

— adapterio ir įrangos, iš kurios gaunami jo įvesties impulsai, sujungimas turi būti užplombuotas iš abiejų pusių (kiek įmanoma).

6. TIKRINIMAI, PATIKROS IR REMONTAS

6.1. **Periodinės patikros**

ADA_035 Kai naudojamas adapteris, per kiekvieną tachografo periodinę patikrą (periodinė patikra atitinka 1C priedo [409]–[413] reikalavimus) turi būti tikrinama:

— ar adapteris pažymėtas atitinkamu tipo patvirtinimo ženklu,

— ar nepažeistos adapterio ir jo sujungimų plombos,

▼B

— ar adapteris įrengtas taip, kaip nurodyta įrengimo plokštelėje,

— ar adapteris įrengtas taip, kaip nurodyta adapterio ir (arba) transporto priemonės gamintojo,

— ar tikrinamoje transporto priemonėje leidžiama įrengti adapterį.

ADA_036 Per šias patikras tachografas kalibruojamas ir pakeičiamos plombos, kad ir kokia būtų jų būklė.

7. TACHOGRAFO TIPO PATVIRTINIMAS, KAI NAUDOJAMAS ADAPTERIS

7.1. **Bendrosios nuostatos**

ADA_037 Tipui patvirtinti tachografas pateikiamas visas, kartu su adapteriu [425].

ADA_038 Bet kuris adapteris gali būti pateiktas jo tipui patvirtinti atskirai ar kaip tachografo dalis.

ADA_039 Tipo patvirtinimas apima adapterio veikimo bandymus. Kiekvieno iš šių bandymų teigiamas rezultatas nurodomas atitinkamame sertifikate [426].

7.2. **Veikimo sertifikatas**

ADA_040 Adapterio ar tachografo su adapteriu veikimo sertifikatas išduodamas adapterio gamintojui tik sėkmingai atlikus visus toliau nurodytus būtinuosius veikimo bandymus.

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
1.	**Administracinis patikrinimas**		
1.1.	Dokumentai	Adapterio dokumentų tinkamumas	
2.	**Apžiūra**		
2.1.	Adapterio atitiktis dokumentams		
2.2.	Adapterio identifikavimas ir (arba) ženklinimas		ADA_027, ADA_028
2.3.	Adapterio medžiagos		[219]–[223] ADA_026
2.4.	Plombavimas		ADA_017, ADA_018, ADA_034
3.	**Veikimo bandymai**		
3.1.	Greičio impulsų perdavimas į įtaisytą judesio jutiklį		ADA_013

▼B

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
3.2.	Gaunamų greičio impulsų siejimas ir priderinimas		ADA_011, ADA_012
3.3.	Judėjimo matavimo tikslumas		[30]–[35], [217]
4.	**Aplinkos poveikio bandymai**		
4.1.	Gamintojo atliktų bandymų rezultatai	Gamintojo atliktų aplinkos poveikio bandymų rezultatai	ADA_020, ADA_021, ADA_022, ADA_024
5.	**Elektromagnetinis suderinamumas**		
5.1.	Spinduliavimas ir imlumas	Atitikties Direktyvai 2006/28/EB patikrinimas	ADA_024
5.2.	Gamintojo atliktų bandymų rezultatai	Gamintojo atliktų aplinkos poveikio bandymų rezultatai	ADA_024

▼C1

II PRIEDAS

PATVIRTINIMO ŽENKLAS IR PAŽYMĖJIMAS

I. PATVIRTINIMO ŽENKLAS

1. Patvirtinimo ženklą sudaro:

a) stačiakampis, kuriame yra raidė „e“, po jos nurodomas skiriamasis skaičius ar raidė šalies, išdavusios patvirtinimą, pagal tokius sutartinius ženklus:

Belgija	6,
Bulgarija	34,
Čekija	8,
Danija	18,
Vokietija	1,
Estija	29,
Airija	24,
Graikija	23,
Ispanija	9,
Prancūzija	2,
Kroatija	25,
Italija	3,
Kipras	CY,
Latvija	32,
Lietuva	36,
Liuksemburgas	13,
Vengrija	7,
Malta	MT,
Nyderlandai	4,
Austrija	12,
Lenkija	20,
Portugalija	21,
Rumunija	19,
Slovėnija	26,
Slovakija	27,
Suomija	17,
Švedija	5,
Jungtinė Karalystė	11,

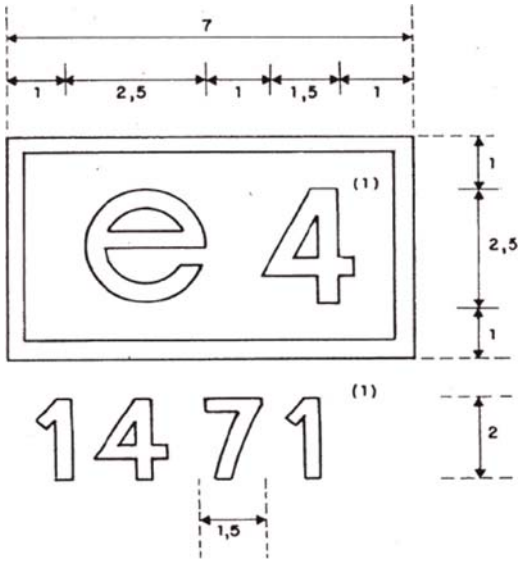
ir

b) patvirtinimo numeris, atitinkantis patvirtinimo pažymėjimo, išduoto tachografo ar registracijos lapo arba tachografo kortelės prototipui, numerį arba tachografo kortelės numerį, įrašomas bet kurioje vietoje, kiek galima arčiau to stačiakampio.

▼C1

2. Patvirtinimo ženklas dedamas ant kiekvieno įrenginio komplekto aprašo plokštelės, ant kiekvieno registracijos lapo ir ant kiekvienos tachografo kortelės. Jis turi būti nenutrinamas ir visada aiškiai įskaitomas.

3. Toliau parodyto patvirtinimo ženklo matmenys ([1]) nurodyti milimetrais, ir tai yra minimalūs stačiakampio matmenys. Būtina išlaikyti matmenų santykį.



([1]) Šie skaičiai pateikiami tik kaip pavyzdys.

▼C1

II. ANALOGINIŲ TACHOGRAFŲ PATVIRTINIMO PAŽYMĖJIMAS

Valstybė narė, kuri patvirtino įrenginį, išduoda pareiškėjui patvirtinimo pažymėjimą, kurio pavyzdys yra pateikiamas toliau. Pranešdama kitoms valstybėms narėms apie suteiktus patvirtinimus arba, jei taip atsitiktų, apie patvirtinimų panaikinimą, valstybė narė naudoja to pažymėjimo kopijas.

PATVIRTINIMO PAŽYMĖJIMAS

Kompetentingos institucijos pavadinimas .....

Pranešimas dėl ([1]):

— tachografo tipo patvirtinimo

— tachografo tipo patvirtinimo panaikinimo

— registracijos lapo pavyzdžio patvirtinimo

— registracijos lapo pavyzdžio patvirtinimo panaikinimo

Patvirtinimo Nr.

.....

1. Prekės ženklas ar pavadinimas .....

2. Tipo ar modelio pavadinimas .....

3. Gamintojo pavadinimas .....

4. Gamintojo adresas .....

5. Pateikimo tvirtinimui data .....

6. Išbandymo vieta .....

7. Bandymo (-ų) data ir numeris .....

8. Patvirtinimo data .....

9. Patvirtinimo panaikinimo data .....

10. Tachografo, kuriame numatyta naudoti registracijos lapą, tipas ar tipai.

11. Vieta .....

12. Data .....

13. Pridėti aprašų dokumentai .....

14. Pastabos (įskaitant plombų vietą, jei taikytina)

(Parašas)

([1]) Išbraukti, kas netinka.

▼C1

III. SKAITMENINIŲ TACHOGRAFŲ PATVIRTINIMO PAŽYMĖJIMAS

Valstybė narė, kuri patvirtino įrenginį, išduoda pareiškėjui patvirtinimo pažymėjimą, kurio pavyzdys yra pateikiamas toliau. Pranešdama kitoms valstybėms narėms apie suteiktus patvirtinimus arba, jei taip atsitiktų, apie patvirtinimų panaikinimą, valstybė narė naudoja to pažymėjimo kopijas.

SKAITMENINIŲ TACHOGRAFŲ PATVIRTINIMO PAŽYMĖJIMAS

Kompetentingos institucijos pavadinimas .....

Pranešimas dėl ([1]):

☐ patvirtinimo: ☐ patvirtinimo panaikinimo:

☐ tachografo modelio

☐ tachografo komponento ([2])

☐ vairuotojo kortelės

☐ dirbtuvių kortelės

☐ įmonės kortelės

☐ kontrolieriaus kortelės

Patvirtinimo Nr.

.....

1. Prekės pavadinimas arba prekės ženklas .....

2. Modelio pavadinimas .....

3. Gamintojo pavadinimas .....

4. Gamintojo adresas .....

5. Pateikimo tvirtinimui data .....

6. Laboratorija (-os) .....

7. Bandymo data ir bandymo ataskaitos numeris .....

8. Patvirtinimo data .....

9. Patvirtinimo panaikinimo data .....

10. Tachografo (-ų), su kuriuo (-iais) numatyta naudoti komponentą, modelis

11. Vieta .....

12. Data .....

13. Pridėti aprašų dokumentai .....

14. Pastabos (įskaitant plombų vietą, jei taikytina)

(Parašas)

([1]) Pažymėkite atitinkamus langelius.
([2]) Nurodykite komponentą, nurodytą pranešime.

▼C1

IV. IŠMANIŲJŲ TACHOGRAFŲ PATVIRTINIMO PAŽYMĖJIMAS

Valstybė narė, kuri patvirtino įrenginį, išduoda pareiškėjui patvirtinimo pažymėjimą, kurio pavyzdys yra pateikiamas toliau. Pranešdama kitoms valstybėms narėms apie suteiktus patvirtinimus arba, jei taip atsitiktų, apie patvirtinimų panaikinimą, valstybė narė naudoja to pažymėjimo kopijas.

IŠMANIŲJŲ TACHOGRAFŲ PATVIRTINIMO PAŽYMĖJIMAS

Kompetentingos institucijos pavadinimas .....

Pranešimas dėl ([1]):

☐ patvirtinimo: ☐ patvirtinimo panaikinimo:

☐ tachografo modelio

☐ tachografo komponento ([2])

☐ vairuotojo kortelės

☐ dirbtuvių kortelės

☐ įmonės kortelės

☐ kontrolieriaus kortelės

Patvirtinimo Nr.

.....

1. Prekės pavadinimas arba prekės ženklas .....
2. Modelio pavadinimas .....
3. Gamintojo pavadinimas .....
4. Gamintojo adresas .....
5. Pateikimo tvirtinimui data .....
6. a) Bandymo laboratorija, išduodanti veikimo sertifikatą .....
   b) Bandymo laboratorija, išduodanti saugumo sertifikatą .....
   c) Bandymo laboratorija, išduodanti sąveikumo sertifikatą .....
7. a) Veikimo sertifikato numeris ir išdavimo data .....
   b) Saugumo sertifikato numeris ir išdavimo data .....
   c) Sąveikumo sertifikato numeris ir išdavimo data .....
8. Patvirtinimo data .....
9. Patvirtinimo panaikinimo data .....
10. Tachografo (-ų), su kuriuo (-iais) numatyta naudoti komponentą, modelis
11. Vieta .....
12. Data .....
13. Pridėti aprašų dokumentai .....
14. Pastabos (įskaitant plombų vietą, jei taikytina)

(Parašas)

([1]) Pažymėkite atitinkamus langelius.
([2]) Nurodykite komponentą, nurodytą pranešime.