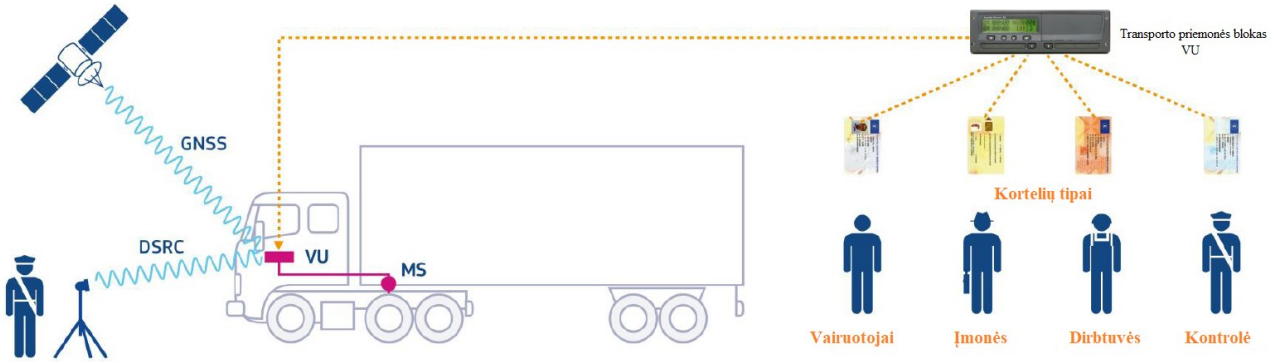
LIETUVOS IŠMANIŲJŲ TACHOGRAFŲ SISTEMOS SERTIFIKAVIMO POLITIKA

pagal 2014 m. vasario 4 d. Europos Parlamento ir Tarybos reglamentą (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, su pakeitimais, padarytais 2020 m. liepos 15 d. Europos Parlamento ir Tarybos reglamentu (ES) 2020/1054



Metrika

Išleido	Lietuvos transporto saugos administracija Švitrigailos g. 42, LT-03209 Vilnius
Informacija	Telefonai: +370 5 278 5602 Faksas +370 5 213 2270 El. paštai: ltsa@ltsa.lrv.lt
Autoriai	Virginijus Čiškauskas
Versija	1.2 versija
Data	2023 m. gruodžio 21 d.

Lietuvos nacionalinės sertifikavimo politikos projekto versijų istorija

Versija 0.1	2019-05-09	Pradinis variantas
Versija 0.2	2019-05-28	Pakeitimai po pirmųjų ERCA pastabų
Versija 0.3	2019-05-29	Versija išsiųsta ERCA patvirtinimui
Versija 0.4	2019-06-10	Pakeitimai po antrųjų ERCA pastabų
Versija 0.4	2019-06-11	ERCA patvirtinta versija, Ares(2019)3717619 – 11/06/2019
Versija 1.0	2019-07-25	Oficiali versija naudojimui
Versija 1.1	2023-10-18	1.5.3, 9 ir 9.11 punktų pakeitimai. Smulkūs redakciniai pakeitimai.
Versija 1.2	2023-12-21	Redakcinio pobūdžio pasikeitimai 1.5.3, 4.2.1, 4.2.2, 4.2.2.1, 4.2.2.2, 4.2.5, 4.2.6, 4.2.8-4.2.13, 4.7, 6.1.1.3 punktuose.

TURINYS

1. Įžanga

1.1. Apžvalga

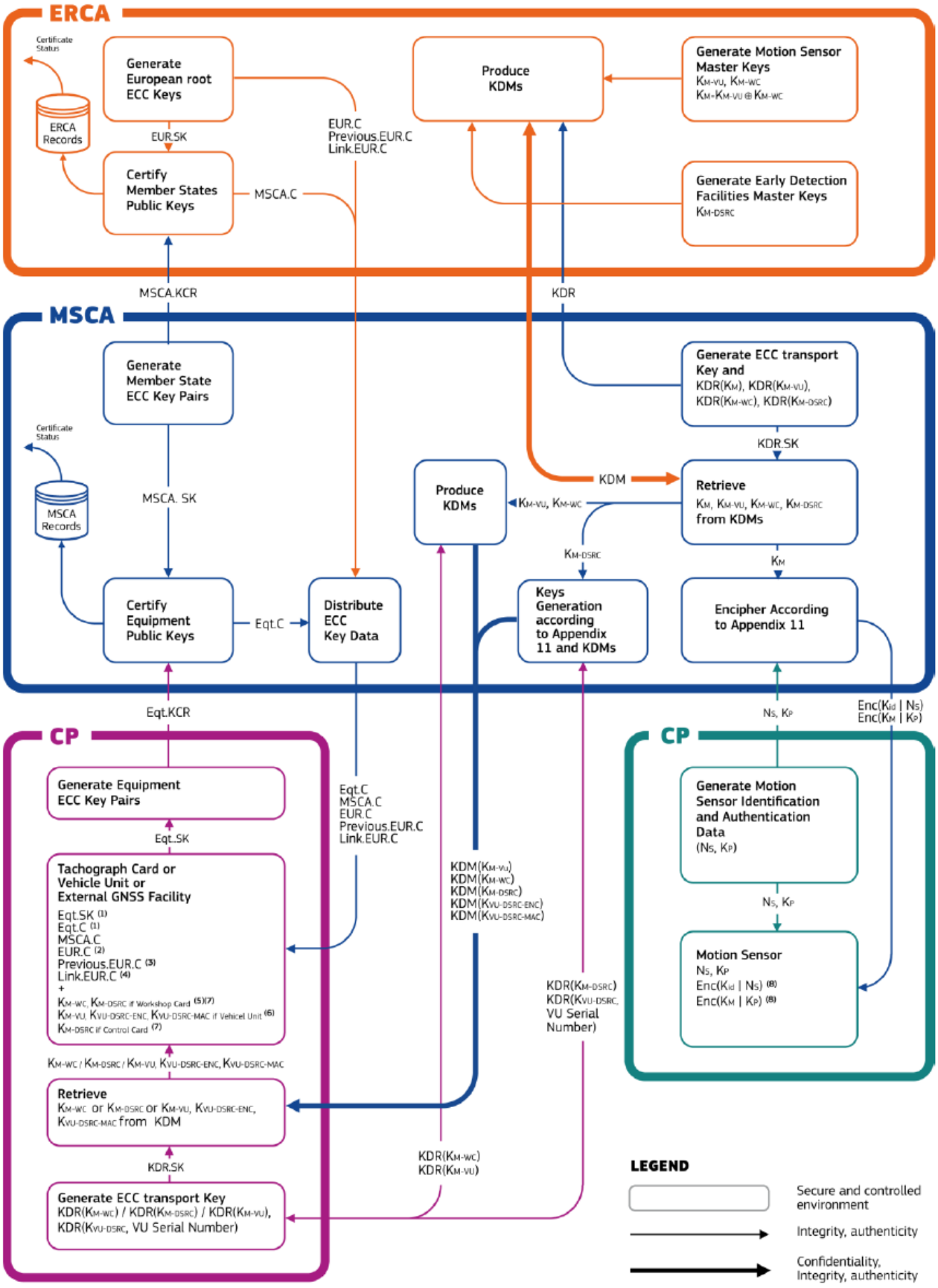
Šiame dokumente aprašoma Lietuvos Respublikos nacionalinė sertifikavimo politika, taikoma išmaniųjų tachografų sistemai.
Antrosios kartos skaitmeninio tachografo sistema, vadinama pažangiuoju tachografu, buvo įvesta Reglamentu (ES) Nr. 165/2014. Tachografų ir jų komponentų konstrukcijos, bandymo, įrengimo, naudojimo ir remonto reikalavimai nustatyti 2016 m. kovo 18 d. Komisijos įgyvendinimo reglamentu (ES) 2016/799, kuriuo įgyvendinamas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 165/2014 ir nustatomi tachografų ir jų komponentų konstrukcijos, bandymo, įrengimo, naudojimo ir remonto reikalavimai, su visais pakeitimais .
Viešojo rakto infrastruktūra (PKI) sukurta remti viešojo rakto sistemas, o simetrinės kriptografinės sistemos remiasi pagrindiniais raktais, kurie turi būti pristatyti suinteresuotiems asmenims. Sukurta trijų sluoksnių infrastruktūra. Europos lygmeniu Europos šakninė sertifikavimo institucija (ERCA) yra atsakinga už šakninių viešojo ir privačiojo rakto porų kūrimą ir valdymą, atitinkamus sertifikatus ir simetriškus pagrindinius raktus.
Šio dokumento struktūra atitinka Sertifikato politikos ir sertifikavimo praktikos gaires RFC 3647.
Skaitmeninis tachografas (pirmosios kartos sistema) ir išmanusis tachografas (antrosios kartos sistema) yra dvi skirtingos sistemos, kurios turi būti naudojamos lygiagrečiai ir nepriklausomai. Dėl šios priežasties, siekiant išvengti problemų, reikia išlaikyti atskiras MSA politikos kryptis, kai ateityje ateis laikas nutraukti skaitmeninį tachografą ir atitinkamą ERCA (*Gen 1*) politiką, todėl Skaitmeninių tachografų sistemos Lietuvos nacionalinė sertifikavimo politika lieka galioti.

1.2. Dokumento pavadinimas ir rodyklė

Dokumento pavadinimas – Lietuvos išmaniųjų tachografų sistemos sertifikavimo politika (toliau – Politika).
Šiame dokumente netaikomos ASN.1 kodavimo taisyklės. Toks identifikatorius nereikalingas, nes išmaniųjų tachografų sistemoje naudojami sertifikatai neturi nuorodos į Politiką.

1.3. PKI dalyviai

Išmaniojo tachografo PKI ir simetriškos raktų infrastruktūros dalyviai aprašyti ir pateikti 1 pav.



pav. 1 Išmaniojo tachografo PKI ir simetriškos raktų infrastruktūros dalyviai

Daugiau informacijos apie simetrinius ir asimetrinius raktus, paminėtus šiame skyriuje, rasite Įgyvendinimo reglamento (ES) 2016/799 1C priedo 11 priedėlio B dalyje.

1.3.1. Sertifikavimo institucijos

Sertifikavime dalyvaujančios institucijos nurodytos Politikos 9.6 ir Politikos 9.8 skyriuje.

1.3.1.1. Europos šakninė sertifikavimo institucija (ERCA)

ERCA yra šakninio sertifikavimo institucija (CA), kuri pasirašo viešojo rakto MSCA sertifikatus. Ji teikia šias komponentines paslaugas: registravimo paslaugą, sertifikato generavimo paslaugą, sklaidos paslaugą.
ERCA generuoja PKI šakninių raktų poras ir atitinkamus sertifikatus kartu su nuorodų sertifikatais, kad sukurtų pasitikėjimo grandinę tarp skirtingų šakninių sertifikatų.
ERCA taip pat yra subjektas, generuojantis, valdantis ir platinantis pagal pageidavimą simetrinius pagrindinius raktus, t. y. judesio jutiklio pagrindinį raktą – VU dalį (K_{M-VU}), judesio jutiklio pagrindinio rakto – dirbtuvės kortelės dalį (K_{M-WC}) ir DSRC pagrindinį raktą (K_{DSRC}).

1.3.1.2. Valstybės narės sertifikavimo institucija (MSCA)

MSCA veikia kaip ERCA subrangovas. Jie pasirašo viešuosius raktų sertifikatus įrangai. Tam jie naudojasi registracijos paslauga, sertifikato generavimo paslauga ir sklaidos paslauga. MSCA gauna sertifikatų užklausas iš komponentų personalizuotojų ir platina sertifikatus šioms šalims. Yra dviejų tipų MSCA raktų pora (-os) ir atitinkamas MSCA sertifikatas (-ai): vienas VU ir EGF sertifikatams išduoti ir vienas Kortelių sertifikatams išduoti. MSCA gali prašyti iš ERCA vieno ar abiejų tipų MSCA sertifikatų, priklausomai nuo jų atsakomybės dėl įrangos išdavimo.
MSCA taip pat yra subjektas, prašantis simetrinių pagrindinių raktų iš ERCA. MSCA platina K_{M-VU} VU gamintojams, K_{M-WC} ir K_{DSRC} kortelių personalizuotojams. MSCA taip pat gali naudoti judesio jutiklio pagrindinį raktą (K_M) judesio jutiklių poravimo raktų (K_P) užšifravimui judesio jutiklio gamintojo prašymu ir gauti judesio jutiklio identifikavimo raktą (K_{ID}) iš K_M, kurį judesio jutiklio gamintojo prašymu jie vėliau naudoja šifruoti jutiklio serijos numerius. Taip pat MSCA gali naudoti K_{DSRC} tam, kad būtų galima nustatyti VU specifinius raktus VU gamintojo prašymu pagal VU serijos numerį.

1.3.1.3. Lietuvos sertifikavimo institucija (LT-MSCA)

Lietuvos MSCA (LT-MSCA) veikia kaip ERCA subrangovas, kaip aprašyta ankstesniame skyriuje. Kadangi Lietuvoje nėra susijusių įrenginių gamintojų, nėra numatyta funkcionalumo, skirto išmaniųjų tachografų sertifikatų pristatymui transporto priemonių įrenginiams (VU), judesio jutikliams (MoS) ir išorinėms GNSS infrastruktūroms (EGF).
LT-MSCA tvarko MSCA raktų porą ir atitinkamą MSCA sertifikatą išduodant kortelių sertifikatus, vadinamus LT-MSCA raktų pora.
LT-MSCA pateikia prašymus dėl simetriškų pagrindinių raktų K_{DSRC} ir K_{M-WC} ERCA ir perduoda gautus raktus į LT-CP – Lietuvos kortelės personalizuotojui naudojant apsaugotą tinklą.
LT-MSCA gauna sertifikatų prašymus iš LT-CP ir platina sertifikatus jai. Be to, vairuotojo kortelių ir dirbtuvės kortelių atveju LT-MSCA užtikrina, kad Card_MA ir Card_Sign sertifikatai turėtų tą pačią sertifikato galiojimo datą.
Dėl savo pareigų LT-MSCA disponuoja šiais kriptografiniais raktais ir sertifikatais bet kuriuo metu:

- dabartine MSCA_Card raktų pora ir atitinkamu sertifikatu;
- visais ankstesniais MSCA_Card sertifikatais, naudojamais tikrinant tachografo kortelių, kurios vis dar galioja, sertifikatus;
- dabartiniu EUR sertifikatu, reikalingu dabartiniam MSCA sertifikatui patikrinti;
- visais ankstesniais EUR sertifikatais, reikalingais visiems galiojantiems MSCA sertifikatams patikrinti.

1.3.2. Registravimo institucijos

Išmaniųjų tachografų PKI registracijos institucijos yra sertifikavimo institucijų, aprašytų ankstesniame skyriuje, dalis. Todėl šiame dokumente nėra jokių specialiųjų reikalavimų registracijos institucijoms.

1.3.3. Prenumeratoriai

Vieninteliai ERCA viešojo rakto sertifikavimo paslaugos prenumeratoriai yra MSCA.
Vieninteliai LT-MSCA viešojo rakto sertifikavimo paslaugos prenumeratoriai yra tachografo kortelių (LT-CP) komponentų personalizuotojai. Tachografo kortelių komponentų personalizuotojai yra atsakingi už keturių skirtingų tipų tachografo kortelių personalizavimą: vairuotojo korteles, įmonės korteles, dirbtuvės korteles ir kontrolės korteles.
Tachografo kortelėse yra kriptografiniai raktai ir sertifikatai.
Vairuotojo kortelėse ir dirbtuvės kortelėse yra du pagrindiniai poros ir atitinkami sertifikatai, išduoti LT-MSCA, t. y.:

- raktų pora ir abipusio autentifikavimo sertifikatas, vadinamas Card_MA;
- raktų pora ir pasirašymo sertifikatas, vadinamas Card_Sign.

Įmonės ir kontrolės kortelės turi raktų porą ir atitinkamą sertifikatą, išduotą LT-MSCA abipusiam autentiškumui patvirtinti.
Kontrolės kortelėse taip pat yra K_{DSRC}.
Komponentų personalizuotojai yra atsakingi už tai, kad įranga būtų aprūpinta atitinkamais raktais ir sertifikatais.
Vairuotojo ir dirbtuvės kortelių personalizuotojas:

- užtikrina dviejų kortelių raktų porų kūrimą abipusiam autentiškumui patikrinti ir pasirašyti;
- atlieka sertifikavimo paraiškų teikimo procesą į LT-MSCA;
- teikia paraišką $K_{M\text{-}WC}$ ir K_{DSRC} (tik dirbtuvės kortelėms);
- užtikrina, kad kortelėje būtų prieinami abipusio autentiškumo patvirtinimo ir pasirašymo raktai ir sertifikatai (turintys identišką sertifikato galiojimo datą), MoS-VU poravimas ir DSRC ryšio atšifravimas ir duomenų autentiškumo tikrinimas (tik dirbtuvės kortelėse).

Kortelės personalizuotojas įmonės ir kontrolės kortelėms:

- užtikrina kortelių raktų poros generavimą abipusiam autentiškumui patvirtinti;
- atlieka sertifikavimo paraiškų teikimo procesą į LT-MSCA;
- teikia paraišką K_{DSRC} (tik kontrolės kortelių);
- užtikrina, kad kortelėje būtų prieinami raktai ir sertifikatai abipusiam autentiškumui ir DSRC ryšiams iššifruoti ir duomenų autentiškumui tikrinti (tik kontrolės kortelės).

Atitinkamų kortelių tipo būtinų raktų apžvalga pateikiama šioje lentelėje:

Kortelės tipas	**Card_MA**	**Card_Sign**	**$K_{M\text{-}WC}$***	**K_{DSRC}***
Vairuotojo	√	√		
Įmonės	√			
Dirbtuvės	√	√	√	√
Kontrolės	√			√

* *Dirbtuvės kortelėje atitinkamai yra iki trijų $K_{M\text{-}WC}$ raktų. K_{DSRC} raktai ir atitinkami versijos numeriai, susiję su šakniniais raktais ir jų sutapimo galiojimo laikotarpiais.*

1.3.4. Priklausančios šalys

Šalys, remdamosi ERCA viešojo rakto sertifikavimo paslauga, visų pirma yra nacionalinės valdžios institucijos, kurioms pavesta įgyvendinti taisykles ir reikalavimus dėl vairavimo trukmės ir poilsio laikotarpių, kurios naudojasi ERCA sertifikatais MSCA sertifikatų autentiškumui patvirtinti. Tada MSCA sertifikatai naudojami patvirtinti įrangos sertifikatų autentiškumą, kurie savo ruožtu naudojami patvirtinant duomenų, gautų iš transporto priemonių blokų ir vairuotojo kortelių, autentiškumą.

1.3.5. Kitos priklausančios šalys yra vairuotojai, įmonės ir seminarai. Atsakomybė

MSA atsako už:
a) LT-CIA paskyrimą;
b) LT-MSCA paskyrimą;
c) LT-CP paskyrimą.
MSA yra atsakinga už tinkamą Politikos įgyvendinimą. MSA užtikrina, kad kortelės sertifikatai būtų generuojami pagal Reglamento (ES) Nr. 165/2014 ir Politikos reikalavimus, o sertifikatuose yra visa reikalinga informacija.
LT-CIA atsako už:
a) kortelės turėtojo tapatybės patikrinimą;
b) kortelių išdavimą asmenims, asmenų registravimą ir paraiškų dėl kortelių išdavimo registravimą;
c) kortelės būsenos priežiūrą.
LT-MSCA atsako už:
a) valstybių narių raktų poros generavimą;
b) valstybių narių raktų poros valdymą;
c) kortelių sertifikatų kūrimą ir registravimą;
d) išduotų sertifikatų registravimą.
LT-MSCA yra atsakinga už šioje Politikoje numatytų procedūrų laikymąsi, net jei LT-MSCA funkcijas atlieka subrangovai / paslaugų agentūros. LT-MSCA yra atsakinga už tai, kad bet kuris subrangovas / paslaugų agentūra atliktų visas funkcijas, atitinkančias sertifikavimo proceso Politikos reikalavimus ir veiklos nuostatus (PS).
LT-CP yra atsakingas už:
a) tachografo kortelių personalizavimą pagal LT-CIA prašymą;
b) asmeninių kortelių perdavimą LT-CIA.
Vartotojai bus atsakingi už:
a) laiku pateiktą kortelės paraišką LT-CIA, kur kortelė pirmą kartą išduodama, atnaujinama ar išduodama prarastai ar pavogtai kortelei pakeisti, pateiktos informacijos teisingumą;
b) tinkamą kortelės naudojimą ir PIN kodo konfidencialumą;
c) laiku informavimą LT-CIA, kad kortelė buvo prarasta, pavogta, yra blogai veikianti arba gali būti pažeista.

1.3.6. Įsipareigojimai

MSA įsipareigojimai:
a) įgyvendina Politikoje nustatytus reikalavimus;
b) skiria LT-CIA, LT-MSCA ir LT-CP;
c) organizuoja paskirtos LT-MSCA ir LT-CP, įskaitant pasirinktus subrangovus / paslaugų agentūras, auditą;
d) tvirtina LT-MSCA, LT-CP, LT-CIA veiklos nuostatus (PS);
e) informuoja LT-CIA, LT-MSCA ir LT-CP apie Politiką;
f) rengia šią Politiką ir pateikia ją patvirtinti ERCA.
CIA įsipareigojimai:
a) laikosi Politikos nustatytų reikalavimų;
b) LT-CIA tvirtina veiklos nuostatus (PS), kuriuose pateikiama nuoroda į šią Politiką;
c) tvarko kortelių turėtojų asmens duomenis (gauna paraiškas, patikrina pateiktus duomenis, patikrina pareiškėjo tapatybę);
d) perduoda personalizavimui reikalingus duomenis į LT-CP;
e) užtikrina, kad teiktų teisingą ir atitinkamą naudotojo, pateikusio paraišką kortelei, informaciją, kurią perduoda LT-MSCA ir LT-CP;
f) išduoda personalizuotas korteles;

g) perduoda PIN kodą dirbtuvės kortelių turėtojams;
h) tvarko baltuosius ir juoduosius kortelių sąrašus;
i) informuoja vartotojus apie kortelių išdavimo taisykles ir procedūras.

MSCA įsipareigojimai:
a) laikosi Politikos nustatytų reikalavimų;
b) rengia sertifikavimo veiklos nuostatus (PS), kuriame pateikiama nuoroda į šią Politiką;
c) turi pakankamus organizacinius ir finansinius išteklius, kad jie galėtų veikti pagal šioje Politikoje nustatytus reikalavimus, visų pirma prisiimti atsakomybės nuostolių riziką;
d) generuoja ir registruoja valstybių narių raktus;
e) generuoja ir registruoja kortelių sertifikatus;
f) registruoja Europos raktus ir sertifikatus;
g) dalyvauja pateikiant valstybių narių raktus ERCA sertifikuoti.

CP įsipareigojimai:
a) laikytis šios Politikos nustatytų reikalavimų;
b) pasitvirtinti veiklos nuostatus (PS), kuriame yra nuoroda į šią Politiką;
c) personalizuoti korteles, spausdinti jų turėtojų asmens duomenis ir į jas įrašyti kortelių turėtojų, valstybių narių ir Europos raktų bei sertifikatų duomenis;
d) perduoti asmenines korteles ir dirbtuvės kortelių PIN į LT-CIA;
e) turėti pakankamus organizacinius ir finansinius išteklius, kad galėtų veikti pagal šioje Politikoje nustatytus reikalavimus, visų pirma prisiimti riziką dėl atsakomybės už nuostolius;
f) informuoti LT-CIA apie kiekvieno kortelės personalizavimo ir perdavimo į LT-CIA būseną;
g) būti atsakinga už šioje Politikoje numatytų procedūrų laikymąsi, net jei dalį LT-CP funkcijų vykdo subrangovai / paslaugų agentūros;
h) būti atsakinga už asmens duomenų konfidencialumą, kol kortelė išsiunčiama į LT-CIA.

Subrangovų / paslaugų agentūrų įsipareigojimai:
Subrangovai / paslaugų agentūros (jei yra) turi įsipareigojimus MSA pagal sutartinius santykius, nustatančius jų įsipareigojimus. Nepaisant to, kad tokios sutartys buvo sudarytos, MSA yra visiškai atsakinga už bet kurios paslaugos, kuri yra reglamentuojama šioje Politikoje, vykdymą.

Kortelių turėtojų įsipareigojimai:
a) teikti tikslią ir išsamią informaciją LT-CIA pagal Politikos reikalavimus;
b) užtikrinti, kad raktai ir sertifikatai būtų naudojami tik skaitmeninėje tachografo sistemoje;
c) užtikrinti, kad kortelės būtų naudojamos tik skaitmeninėje tachografo sistemoje;
d) užtikrinti, kad būtų tinkamai pasirūpinta, kad būtų išvengta neteisėto kortelių ir įrangos privataus rakto naudojimo;
e) naudoti tik savo korteles (Reglamento (ES) Nr. 165/2014 27 straipsnio 2 dalis);
f) turėti tik vieną galiojančią vairuotojo kortelę (Reglamento (ES) Nr. 165/2014 27 straipsnio 2 dalis);
g) tik labai ypatingomis ir tinkamai pagrįstomis aplinkybėmis turėti tiek dirbtuvės kortelę, tiek įmonės kortelę; dirbtuvės ir vairuotojo korteles; keletą dirbtuvės kortelių;
h) nenaudoti sugedusios ar baigusios galioti kortelės (Reglamento (ES) Nr. 165/2014 27 straipsnio 2 dalis);
i) nedelsiant pranešti LT-CIA apie bet kurį iš šių įvykių:
- kortelės arba įrangos privatus raktas buvo pamestas, pavogtas, netinkamas arba gali būti pažeistas (Reglamento (ES) Nr. 165/2014 29 straipsnio 4 dalis);
- dėl sugedusio PIN kodo prarasta galimybė eksploatuoti dirbtuvės kortelę;
- sertifikato turinys yra netikslus.

1.4. Raktų ir sertifikatų naudojimas

Šiame skyriuje pateikiamos nuostatos, susijusios su administravimu.

ERCA šakniniai sertifikatai ir ERCA nuorodų sertifikatai naudojami ERCA išduodamų MSCA sertifikatų tikrinimui.
ERCA sertifikatai bus didžiausias PKI patikimumo taškas, ir jie bus įdėti į VU, korteles ir EGF, kaip nurodyta Įgyvendinimo reglamento (ES) 2016/799 1C priedo 11 priedėlyje. LT-MSA ir PKI dalyviai pripažįsta ERCA viešojo rakto sertifikatus, jei juos skelbia ERCA pagal ERCA politikos reikalavimus.
Valstybių narių raktai ir perkėlimo raktai yra generuojami sertifikuotoje HSM sistemoje ir saugomi fiziškai saugomoje aplinkoje, kurioje yra 24/7 saugumo kontrolė, elektroninės spynos ir vaizdo kontrolė.
Įrangos raktai yra simetriniai raktai, sukurti gaminant įrangą, kuri yra LT-MSCA sertifikuota šioms skaitmeninio tachografo sistemos dalims:
- raktai, skirti apsaugoti ryšį tarp VU ir judesio jutiklio;
- raktai, skirti apsaugoti ryšį per DSRC sąsają tarp VU ir nuotolinio ankstyvo aptikimo ryšio skaitytuvo.

ERCA savo ERCA privačius raktus naudoja tik ERCA šakniniams, su ERCA siejamiems ir MSCA sertifikatams pasirašyti, kaip numatyta Įgyvendinimo reglamento (ES) 2016/799 1C priedo 11 priedėlyje.
LT-MSCA savo valstybės narės privačius raktus naudoja tik:
- įrangos sertifikatams pasirašyti pagal Įgyvendinimo reglamento (ES) 2016/799 IC priedo 11 priedėlį;
- sertifikato pasirašymo užklausoms pasirašyti.

LT-MSCA tachografo kortelės sertifikatai, aprašyti Politikoje, niekada nėra atšaukiami ar sustabdomi.
LT-MSCA sertifikatai naudojami patikrinti LT-MSCA išduotus kortelių sertifikatus.
Card_MA sertifikatai naudojami abipusiam autentifikavimui ir sesijos raktų atitikčiai tarp Kortelės ir VU.
„Card_Sign“ sertifikatai naudojami siekiant patikrinti iš kortelės atsiųstų duomenų autentiškumą ir vientisumą.
Privatus „Card_Sign“ raktas gali būti naudojamas tik duomenims, atsisiunčiamiems iš kortelės, pasirašyti.
$K_{M\text{-}WC}$ ir atitinkamas versijos numeris pateikiami komponentų personalizuotojams, kad juos būtų galima įrengti dirbtuvės kortelėse.
K_{DSRC} ir atitinkamas versijos numeris naudojamas kontrolės ir dirbtuvės kortelėse gauti VU specifinius DSRC raktus, kurie reikalingi VU DSRC ryšiui atšifruoti ir autentiškumui bei vientisumui nustatyti.
ERCA nenaudoja simetrinių pagrindinių raktų jokiam tikslui, išskyrus platinimą MSCA.
LT-MSCA ir LT-CP nenaudoja išmaniųjų tachografų sertifikatų ir raktų, kuriais grindžiama ši Politika, bet kokiems tikslams, išskyrus pirmiau aprašytus.
LT-MSCA perduoda simetrinius pagrindinius raktus, raktus, gautus iš šių pagrindinių raktų, arba duomenis, šifruotus šiais pagrindiniais raktais, LT-CP saugiu tinklu vieninteliu tikslu, kuriam skirti raktai ir duomenys, kaip nurodyta Įgyvendinimo reglamento (ES) 2016/799 1C priedo 11 priedėlyje.

Pastaba. Kadangi Lietuvoje nėra jokių susijusių įrenginių, VU, judesio jutiklių ir EGF Išmaniųjų tachografų, sertifikatų pristatymo funkcionalumas neįgyvendintas (žr. 1.3.1.3 skirsnį). Judesio jutiklio gamintojas ir transporto priemonės įrenginio gamintojas savo pagrindinį prašymą pateikia atsakingam MSCA. LT-CP užtikrina prieinamumą $K_{M\text{-}WC}$ ir K_{DSRC} raktams, kurie bus naudojami valdymo kortelėse ir dirbtuvėse.

1.5. Sertifikavimo administravimas

1.5.1. ERCA

Europos Komisijos tarnyba, atsakinga už sertifikavimo politikos įgyvendinimą Europos lygmeniu ir pagrindinių sertifikavimo bei pagrindinių platinimo paslaugų teikimą valstybėms narėms, vadinama Europos šaknine sertifikavimo institucija (ERCA).
ERCA kontaktinis adresas yra:
Head of the Cyber and Digital Citizens' Security Unit E3
Directorate E - Space, Security and Migration
Joint Research Centre (TP 361)
European Commission
Via Enrico Fermi, 2749
I-21027 Ispra (VA)

1.5.2. MSA

Valstybės narės atsakingoji institucija (MSA) yra atsakinga už šios Politikos įgyvendinimą.
MSA yra:

Lietuvos transporto saugos administracija
Švitrigailos g. 42
LT-02309 Vilnius
Lietuvos Respublika

Toliau šiame dokumente Lietuvos transporto saugos administracija vadinama LTSA.
Kortelių išdavimo centrui (CIA) pavestas funkcijas atlieka LTSA.

1.5.3. LT-MSCA ir LT-CP

Valstybės narės personalizavimo centro (CP) funkcijas atlieka:
Thales DIS Finland Oy
Myllynkivenkuja 4, 01620 Vantaa
Finland (Suomija)

Valstybės narės sertifikavimo centro (MSCA) funkcijas atlieka:
CertSing S.A.
Oltenitei Avenue Nr. 107 A, Building C1, ground floor, CP 041303, Sector 4, Bucharest, Romania (Rumunija)
Buveinės adresas:
29A Tudor Vladimirescu Blvd., 2nd floor, District 5, Bucharest, Romania (Rumunija)
El. paštas: *cards.helpdesk@certsign.ro*

LT-MSCA arba LT-CP negali funkcijų perduoti subrangovams / paslaugų agentūroms.

1.6. Santrumpos ir sąvokos

Šiame dokumente vartojamos šios santrumpos ir sąvokos:

CA / PA	Sertifikavimo centro / personalizavimo administratorius.
CHR	Sertifikato turėtojo žyma.
CIA	Institucija, atsakinga už kortelių išdavimą bei duomenų apie išduotas korteles, jų būseną, turėtojus ir kitų su kortelių išdavimu susijusių duomenų tvarkymą.

LT-CIA	Lietuvos institucija, atsakinga už kortelių išdavimą bei duomenų apie išduotas korteles, jų būseną, turėtojus ir kitų su kortelių išdavimu susijusių duomenų tvarkymą.
CP	Juridinis asmuo, atsakingas už kortelės personalizavimą, t. y. viešų ir privačių kortelių raktų generavimą, kortelės turėtojo identifikavimą ir kitų reikalingų duomenų spausdinimą kortelėje, pateikiant šiuos duomenis.
LT-CP	Juridinis asmuo, atsakingas už kortelės personalizavimą Lietuvoje, t. y. viešų ir privačių kortelių raktų generavimą, kortelės turėtojo identifikavimą ir kitų reikalingų duomenų spausdinimą kortelėje, pateikiant šiuos duomenis.
ERCA	Europos Komisijos paskirta institucija, atsakinga už tachografų sistemoje naudojamų Europos elektroninių raktų generavimą, valstybių narių raktų sertifikavimą ir sertifikatų platinimą.
EQT	Skaitmeninio tachografo įranga (kortelės, VU ir judesio jutikliai).
EQT.C	Įrangos sertifikatas.
EQT.PK	Įrangos viešasis raktas.
EQT.SK	Įrangos privatusis raktas.
EUR.PK	Europos viešasis raktas.
EUR.SK	Europos privatusis raktas.
ISSP	Informacinės sistemos saugumo įgaliotinis.
ITSEC	Informacinių technologijų saugumo vertinimo kriterijai.
Km	Pagrindinis Europos raktas (TDES).
Km_{VU}	Transporto priemonės bloke įdiegtas TDES raktas.
Km_{WC}	Dirbtuvės kortelėse įdiegtas TDES raktas.
MS.C	Valstybės narės sertifikatas.
MS.PK	Valstybės narės viešasis raktas.
MS.SK	Valstybės narės privatusis raktas.
MSA	Institucija, atsakinga už tachografų sistemos sukūrimą, funkcionavimą bei funkcionavimo būklės stebėjimą.
LT-MSCA	Lietuvos sertifikavimo institucija
N_s	Išplėstinis judesio jutiklio serijinis numeris.
PIN	Dirbtuvės kortelės autentiškumo nustatymo kodas.
RSA	Rivest'o, Shamir'o ir Adelmann'o asimetrinio kodavimo algoritmas.
SA	Informacinės sistemos administratorius.
TDES	Trigubas DES (angl. *Triple DES*). 3 kartus ilgesnis raktas, t. y. 3 paprasti DES raktai, kuriais nuosekliai šifruojami / dešifruojami duomenys.
VU	Transporto priemonės blokas
Auditas	Veiklos patikrinimas siekiant nustatyti, ar veikla atitinka Politikoje ir veiklos nuostatų keliamus reikalavimus.
Juodasis sąrašas	Pripažintų negaliojančiomis (pamestų, pavogtų, neveikiančių, anuliuotų) ar laikinai negaliojančiomis (suspenduotų) išduotų kortelių, kortelių sertifikatų sąrašas.
Šifravimas	Duomenų (teksto) vertimo į šifruotą (koduotą) formą procesas. Šifruotas tekstas nėra suprantamas.
Konfidenciali informacija	Viešai neskelbtina informacija, kurios neteisėtas atskleidimas gali pakenkti išmaniųjų tachografų sistemos veiklai.
Kortelė	Išmanioji kortelė, turinti mikroprocesorių ir skirta nustatyti kortelės turėtojo tapatybę (arba tapatybės grupę) bei saugoti joje tam tikrus

	duomenis, kuriuos registruoja skaitmeninis tachografas. Kortelė gali būti vairuotojo, kontrolės, dirbtuvės ir įmonės.
Kortelės personalizavimas	Išmanioji kortelė, turinti mikroprocesorių ir skirta naudoti skaitmeniniame tachografe. Skaitmeninio tachografo kortelė leidžia nustatyti kortelės turėtoją (arba tapatybės grupę); duomenis galima perrašyti ir saugoti tachografo kortelėje.
Sertifikatas	Skaitmeninis sertifikatas, kuriuo yra perduodama informacija apie subjektą (pvz., pavadinimas, galiojimo data, viešasis raktas ir elektroninis CA parašas, pagal kurį galima patikrinti sertifikato autentiškumą).
ERCA viešasis raktas	Raktas, naudojamas valstybės narės sertifikatams tikrinti. ERCA privatusis raktas čia nenaudojamas, nes jis visada lieka ERCA.
Skaitmeninis tachografas	Visa įranga, skirta įrengti transporto priemonėse automatiškai arba pusiau automatiškai rodyti, registruoti ir laikyti išsamią informaciją apie šių transporto priemonių judėjimą ir tam tikrus jų vairuotojų darbo ir poilsio laikotarpius.
Raktas	Kintamasis, kuriam yra priskiriama tam tikru algoritmu sugeneruota simbolių eilutė arba simbolių blokas. Raktu galima užšifruoti pranešimą arba šifruotą pranešimą dešifruoti. Rakto ilgis yra šifravimo saugumo kriterijus.
Valstybės narės raktai	Valstybės narės parašo (angl. *signing*) raktai taip pat gali būti vadinami valstybės narės pagrindiniais raktais.
Judesio jutiklio raktai	Simetriniai raktai, įrašomi į dirbtuvės kortelę, VU ir judesio jutiklį abipusiam atpažinimui. MSCA gauna judesio jutiklio raktus iš ERCA, saugo juos ir platina gamintojams.
Privatusis raktas	Pranešimų šifravimo / dešifravimo raktas, kuris yra žinomas tik vienai ar visoms bendraujančioms pusėms. Viešojo rakto infrastruktūros atveju privatusis raktas yra naudojamas kartu su viešuoju raktu.
Viešasis raktas	Raktas, kuris yra viešai platinamas ir naudojamas pranešimams ar elektroniniam parašui dešifruoti. Viešasis raktas kartu su privačiuoju raktu sudaro asimetrinio šifravimo mechanizmą.
Perdavimo raktai	RSA raktų poros, naudojamos saugiam judesio jutiklio raktų perdavimui tarp ERCA ir MSCA.
Susijusios šalys	Juridiniai arba fiziniai asmenys, kurie naudoja sertifikatus ir / arba išmaniųjų tachografų sistemos informaciją apie sertifikatų būseną.
Vizualus personalizavimas	Informacijos spausdinimas ant kortelės.
Baltasis sąrašas	Galiojančių išduotų kortelių, kortelių sertifikatų sąrašas.
Dirbtuvė	Dirbtuvė arba įmonė, gaminanti ar montuojanti tachografus arba gaminanti transporto priemones, kuri yra patvirtinta Lietuvos Respublikoje nustatyta tvarka. Tokioje įmonėje dirbantiems mechanikams gali būti išduodamos dirbtuvės kortelės.

2. Paskelbimas ir saugojimas

2.1. Saugykla

MSCA yra atsakinga už išduotų sertifikatų talpinimą ir saugojimą saugykloje. Prieiga prie saugyklos nėra vieša.

2.2. Sertifikavimo informacijos skelbimas

Ši Politika yra viešai paskelbta internete adresu:
https://www.ltsa.lrv.lt/.

Klausimai, susiję su šia Politika, siunčiami šiuo adresu:
Lietuvos transporto saugos administracija
Švitrigailos g. 42
LT-02309 Vilnius
Lietuvos Respublika

Sertifikavimo veiklos nuostatai nėra skelbiami viešai, tačiau pateikus prašymą su jais gali susipažinti susijusios šalys.

2.3. Atnaujinimų skelbimas

Informacija apie pasikeitimus, susijusius su šia Politika, ir jos skelbimas atliekamas, kaip numatyta Politikos 9.12 skyriuje.

2.4. Prieiga prie saugyklos

Visa saugykloje skelbiama informacija turi būti skirta tik skaityti.
Prieigai prie saugyklos naudojamas saugus interneto ryšio kanalas.
Prieiga prie saugyklos turėtų būti suteikta bent LT-MSA ir LT-CP.

3. Atpažinimas ir autorizacija

Šiame skyriuje aprašoma, kaip atpažinimo ir autorizacijos procedūra turi būti atliekama pradinio ir pakartotinio rakto užklausų ir simetrinių raktų paskirstymo užklausų atveju.

3.1. Pavadinimai

3.1.1. Pavadinimų tipai

3.1.1.1. Sertifikato objektas ir jį išdavęs subjektas

Sertifikavimo institucijos nuoroda ir Sertifikato turėtojo nuoroda identifikuoja sertifikatą išdavusį subjektą ir sertifikato turinį. Jie turi būti suformuoti taip, kaip aprašyta Įgyvendinimo reglamento (ES) 2016/799 1C priede.

3.1.1.2. Raktų platinimo prašymai ir raktų platinimo žinutės

Sertifikavimo institucijos nuoroda ir Sertifikato turėtojo nuoroda identifikuoja sertifikatą išdavusį subjektą ir sertifikato turinį. Jie turi būti suformuoti taip, kaip aprašyta Įgyvendinimo reglamento (ES) 2016/799 1C priedo 11 priedėlyje, CSM_136/CSM_141 ir Įgyvendinimo reglamento (ES) 2016/799 1 priedėlyje.

3.2. Pirminis tapatybės patvirtinimas

3.2.1. Privačiojo rakto turėjimo įrodymo metodas

Kai LT-LMSCA pateikia ERCA sertifikato pasirašymo prašymus (CSR), būtina pateikti atitinkamo privačiojo rakto turėjimą per vidinį parašą, kaip nurodyta ERCA politikos 4.1.1 skirsnyje. Sertifikato pasirašymo prašymas taip pat gali turėti išorinį parašą, patvirtinantį pranešimo autentiškumą. Išorinį parašą parengia jau patvirtintas privatusis raktas, nurodytas sertifikato pasirašymo prašyme.
LT-CIA pateiktuose kortelės personalizavimo prašymuose nėra privačiųjų raktų, tačiau autentiškumas turi būti užtikrintas naudojant apsaugotą tinklą.

LT-CP, pateikiantis Kortelių sertifikatų pasirašymo prašymus (Card-CSRs), turi įrodyti atitinkamo privačiojo rakto turėjimą su LT-CP parašu ir įrodyti vientisumą bei prašyti autentifikavimo su pasirašymo prašymu.

3.2.2. Organizacijos tapatybės nustatymas

Organizacijos tapatybės nustatymo procedūros nurodomos LT-MSCA veiklos nuostatuose (PS).

3.2.3. Individualios tapatybės patvirtinimas

Individualios tapatybės nustatymo procedūros nurodomos LT-MSCA veiklos nuostatuose (PS).
LT-CIA tikrina fizinių asmenų tapatybę kortelių paraiškų vertinimo ir patvirtinimo proceso metu pagal jau patvirtintus nacionalinio vairuotojų registro įrašus ir fizinių asmenų registrą.

3.2.4. Institucijos patvirtinimas

Institucijos patvirtinamos procedūros nurodomos LT-MSCA veiklos nuostatuose (PS).
Pradinis leidimas veikti organizacijos vardu nėra kortelės paraiškų vertinimo ir patvirtinimo proceso dalis. Kortelės paraiška organizacijoms remiasi jau nustatytais įgaliotų asmenų registro įrašais.

3.2.5. Sąveikos kriterijai

LT-MSCA sertifikatui pasirašyti ir pagrindinėms platinimo paslaugoms, teikiamoms tachografų sistemai, nesinaudoja jokios išorinės sertifikavimo institucijos paslaugomis, išskyrus ERCA.
Jei LT-MSCA turi naudotis išorinės PKI paslaugomis bet kokiai kitai paslaugai ar funkcijai atlikti, būtina, kad prieš naudojimąsi paslaugomis MSA peržiūrėtų ir patvirtintų išorės PKI veiklos nuostatus.

3.3. Pakartotinio rakto užklausų atpažinimas ir autorizacija

3.3.1. Įprastas pakartotinio rakto užklausos atpažinimas ir autorizacija

Atpažinimo ir autorizacijos procedūros, taikomos pakartotiniams rakto prašymams dėl ERCA, yra apibrėžtos ERCA politikos 3.3 skyriuje.
Atpažinimo ir autorizacijos procedūros, taikomos LT-CP taikomiems pakartotiniams rakto prašymams LT-MSCA, turi būti tokios pačios, kaip aprašyta Politikos 3.2 skyriuje. Tachografo kortelių raktų generavimą atlieka LT-CP, todėl tachografo kortelių raktams netaikomi raktų prašymai.

3.4. Atšaukimo užklausų atpažinimas ir autorizacija

LT-MSCA sertifikato atšaukimo prašymų patvirtinimas aprašytas ERCA politikos 3.4 skyriuje.
Kortelės sertifikatų atšaukimas neleidžiamas. Kortelės atšaukimas tvarkomas tachografo kortelių nacionaliniame registre naudojant kortelės būseną.

4. Sertifikatų, simetrinių raktų ir šifravimo paslaugų galiojimo ciklo reikalavimai

4.1. MSCA paraiška viešojo rakto sertifikatui ir jo išdavimas

Paraiškos pasirašyti sertifikatus, jų nagrinėjimas, tikrinimas, sertifikato generavimas, platinimas ir administravimas atliekamas ERCA politikoje nustatyta tvarka.
LT-MSCA viešojo rakto sertifikatų formatas aprašytas ERCA politikos 7.1 skyriuje.
Apsikeitimas užklausomis ir atsakymai į jas atliekami ERCA politikoje nustatyta tvarka.
Sertifikatų modifikavimas draudžiamas. Sertifikatai gali būti atšaukiami ERCA politikoje numatytais atvejais.

4.1.1. Sertifikato pasirašymo prašymai

Sertifikato pasirašymo prašymą (CSR) gali pateikti tik LT-MSCA, pripažinta LT-MSA.
Europos institucija yra atsakinga už MSA pripažinimą.

Tachografo kortelių pagrindinius raktus LT-MSCA perduoda LT-CP naudodama nustatytus ir suderintus failo formatus ir pagrindinio rakto mainų parašo taisykles.
Kortelės personalizavimo prašymų duomenys siunčiami į LT-CP per apsaugotą tinklą.
Kortelių sertifikatų pasirašymo prašymuose pateikiami nepažeisti ir pasirašyti asmeninių užklausų duomenys ir juose turi būti nurodomi konkretūs raktai, pasirašyti LT-CP. LT-CP pasirašo bendrą užklausą ir išsiunčia ją LT-MSCA.
LT-MSCA atsakymas į LT-CP kortelės sertifikato pasirašymo prašymą apima prašomus sertifikatus kaip bendro pasirašyto pranešimo failo dalį.
Kortelės personalizavimo prašymą gali pateikti tik LT-CIA. Kortelių sertifikatų pasirašymo prašymus (Card-CSRs) gali pateikti tik LT-CP.
CSR formatas turi atitikti ERCA politikos 4.1.1 skyriaus reikalavimus.

4.1.2. Sertifikato paraiškos nagrinėjimas

4.1.2.1. CSR turinio tikrinimas

Pareiškėjo tapatybės nustatymo ir autentiškumo patvirtinimo tikslais LT-MSCA tikrina kiekviename gaunamame Kortelės sertifikato pasirašymo prašyme:
- LT-CIA užklausos duomenų parašo teisingumą ir galiojimą;
- LT-CP parašo sertifikato pasirašymo duomenų teisingumą ir galiojimą;
- rakto duomenų, atitinkančių prašyme nurodytą kortelės tipą, išsamumą;
- teisingus galiojančius duomenis, atitinkančius prašyme nurodytą kortelės tipą;
- klaidų pranešimų nebuvimą.

Pareiškėjo tapatybės nustatymo ir autentiškumo patvirtinimo tikslais LT-CP nagrinėja kiekvieną gaunamą Kortelės CSR atsakymą dėl:
- prašymo rezultatų (sertifikatų) teisingumo ir pagrįstumo;
- klaidų pranešimų nebuvimo.

4.1.2.2. Sertifikatų generavimas, platinimas ir administravimas

Jei visi patikrinimai yra sėkmingi, ERCA pasirašo sertifikatą, kaip aprašyta ERCA politikos 4.1.3 skyriuje.

4.1.3. Sertifikatai

LT-MSCA viešojo rakto sertifikatų formatą galima rasti ERCA politikos 7.1 skyriuje.
LT-MSCA patvirtina tik vieną kartą ir apskritai visoms užklausoms dėl valstybės narės sertifikato galiojimo.
LT-MSCA dėl kiekvieno gaunamo Kortelės sertifikato pasirašymo prašymo patvirtina, kad:
- prašomi kortelės tipai galioja;
- galiojimo pradžia (BOV) ir galiojimo pabaiga (EOV) atitinka ES reikalavimus dėl kortelės tipo galiojimo laikotarpio;
- LT-CIA parašas yra galiojantis, ir todėl personalizuotų duomenų autorizacija yra patvirtinta;
- LT-CP parašas yra galiojantis, todėl siunčiamų raktų autorizacija yra patvirtinta;
- Prašymo parašas yra galiojantis, ir todėl įrodomas prašymo vientisumas;
- raktai, kuriuos reikia pasirašyti, yra kriptografiškai tinkami ir, svarbiausia, nepažeisti ar sugadinti.

4.1.4. Keitimasis prašymais ir atsakymais

Sertifikato pasirašymo prašymams ir sertifikatams transportuoti reikia naudoti CD-R laikmenas. Vieno seanso režimu CD-R turi būti 12 cm laikmena (suformatuotas ISO 9660: 1988).
Kiti transportavimo būdai gali būti naudojami po išankstinio ERCA sutikimo. Bandymų tikslais ERCA priima ir siunčia CSR ir sertifikatus kaip el. pašto priedus.

LT-MSCA įrašo vieną ar tris kiekvieno sertifikato pasirašymo prašymo kopijas į transportavimo laikmeną, gabenamą į ERCA. Kopijos turi būti pateikiamos šešioliktainės skaičiavimo sistemos ASCII (.text faile), Base64 (.pem faile) arba dvejetainės skaičiavimo sistemos (.bin failo) formatu.
ERCA įrašo tris kiekvieno sertifikato kopijas į transportavimo laikmenas, grąžinamas LT-MSCA. Kopijos turi būti pateikiamos šešioliktainės skaičiavimo sistemos ASCII (.text faile), Base64 (.pem faile) arba dvejetainės skaičiavimo sistemos (.bin failo) formatu.
Prie kiekvieno sertifikato pasirašymo prašymo ir sertifikato turi būti pridėta popierinė kopija, suformatuota pagal šabloną, apibrėžtą ERCA politikoje. Kita popierinė duomenų kopija yra saugoma atitinkamai ERCA arba LT-MSCA.
Dėl abiejų, tiek CSR ir tiek sertifikatų, transportavimo laikmenos ir popierinės kopijos perduodamos tarp ERCA darbuotojo ir kurjerio ERCA kontroliuojamoje zonoje.

4.1.5. Sertifikato priėmimas

Kurjeris pasirašo už LT-MSCA sertifikato gavimą ERCA patalpose. LT-MSCA, gavusi sertifikatą savo patalpose, patikrina, ar:

- transportavimo laikmena yra skaitoma kompiuteriu, t. y. nėra pažeista ar sugadinta;
- sertifikato formatas atitinka ERCA politikos 7.1 skirsnio 5 lentelę;
- visos sertifikato lauko reikšmės atitinka CSR reikalaujamas vertes;
- sertifikato parašas gali būti patikrintas naudojant ERCA viešąjį pagrindinį raktą, nurodytą lauke „CAR“.

Jei kuris nors iš šių patikrinimų nepavyksta, LT-MSCA nutraukia procesą ir kreipiasi į ERCA. Sertifikato atmetimas tvarkomas pagal sertifikato atšaukimo procedūrą (Politikos 4.1.10 skyrius).
Kortelių raktų sertifikavimas yra automatiškai apdoroto atsakymo į kortelės sertifikato pasirašymo užklausą dalis. LT-CP naudoja kortelės informacijos modulyje pateiktą atsakymą, kad užbaigtų kortelės kūrimo procesą.

4.1.6. Raktų poros ir sertifikato naudojimas

Kortelių sertifikatai, kaip kortelės raktų sertifikavimo atsakymo dalis, siunčiami į LT-CP ir naudojami kortelei personalizuoti, yra išskirtinai naudojami tik kortelėse. Kortelių sertifikatai nepublikuojami.
LT-MSCA naudoja bet kurią raktų porą ir atitinkamą sertifikatą pagal šios Politikos 6.2 skyrių.
LT-MSCA užtikrina, kad LT-MSCA privatieji pasirašymo raktai būtų naudojami tik nacionalinėms kortelėms. Sertifikato pasirašymo prašymai naudojami skaitmeninėje tachografo sistemoje. LT-MSCA užtikrina, kad po nacionalinio lygmens raktų sertifikavimo LT-MSCA privatieji pasirašymo raktai naudojami tik viešųjų raktų sertifikatų, naudojamų skaitmeninio tachografo sistemoje, gamybai.
LT-CP užtikrina, kad pagrindiniai raktai, tachografo kortelių raktai ir tachografo kortelių sertifikatai būtų naudojami tik tachografo kortelių gamybai, kaip aprašyta šiame dokumente.
Kortelės naudotojas užtikrina tinkamą raktų ir sertifikatų taikymą užtikrindamas teisingą tachografo kortelių naudojimą.
Kortelės naudotojas turi užtikrinti, kad tachografo kortelės būtų naudojamos tik taip, kaip numatyta.
Visų pirma kortelės vartotojas pripažįsta, kad tachografo kortelės nėra perleidžiamos ir bet koks kitas naudojimas, išskyrus tachografų sistemas, yra draudžiamas.

4.1.7. Sertifikato pratęsimas

Sertifikato pratęsimas, t. y. galiojančio sertifikato galiojimo laikotarpio pratęsimas, yra neleidžiamas.
Kortelės raktų sertifikato pratęsimas yra neleidžiamas.

4.1.8. Pakartotinis sertifikato raktas

Pakartotinis rakto sertifikatas reiškia naujo LT-MSCA sertifikato pasirašymą, pakeičiant esamą sertifikatą. Pakartotinis rakto sertifikatas išduodamas:

- kai LT-MSCA artėja prie jo vieno (-ų) privačiojo rakto (-ų) naudojimo laikotarpio pabaigos. Tokiu atveju vėl reikia iš naujo nustatyti, kad LT-MSCA galėtų tęsti veiklą po šio laikotarpio pabaigos;
- po sertifikato atšaukimo.

Sertifikato paraiška, apdorojimas, išdavimas, priėmimas ir paskelbimas yra toks pat kaip ir pradinio rakto poroje.
LT-MSCA raktų poros gali būti reguliariai keičiamos.
LT-MSCA pakartotinio rakto sertifikato išdavimas aprašytas ERCA politikos 4.1.8 skyriuje.
Kortelių raktų sertifikavimui nėra pakartotinio rakto sertifikato išdavimo proceso. Kiekvienas kortelės sertifikato pasirašymo prašymas yra laikomas nauja paraiška.

4.1.9. Sertifikato modifikacija

Sertifikato modifikacija yra neleidžiama.

4.1.10. Sertifikato atšaukimas ir sustabdymas

Sertifikatai ir raktai, kuriems turi būti pateikti prašymai išduoti sertifikatą į ERCA, atšaukiami remiantis aprašytu ERCA politikos 4.1.10 skyriuje procesu.
Sertifikatai ir raktai, kuriems taikomas Kortelių sertifikato pasirašymo prašymas, negali būti atšaukti.
Sertifikatai ir raktai, kurie yra pažeisti ar įtariamas jų pažeidimas, kortelės sertifikato pasirašymo prašymai neturi būti naudojami kortelėms kurti ir kortelei personalizuoti.
Nuostatos, susijusios su rakto pažeidimu arba įtariamu rakto pažeidimu pagal nacionalinę pažeidimo procedūrą, kaip aprašyta šios Politikos 5.7 skirsnyje, ir gali sukelti bent vieną iš šių atidėjimų veiksmų:

- keičiamosios kortelės, kurioje yra nepažeistų raktų, išdavimas;
- pagrindinio rakto keitimas po ERCA atnaujinimo proceso;
- LT-MSCA sertifikato pakeitimas po ERCA sertifikavimo atšaukimo proceso.

Sertifikato galiojimo sustabdymas neleidžiamas.

4.1.10.1. Sertifikato atšaukimo aplinkybės

Šiuo metu Lietuvoje nenaudojama.

4.1.10.2. Kas gali teikti prašymą atšaukti

Šiuo metu Lietuvoje nenaudojama.

4.1.10.3. Atšaukimo prašymo procedūra

Šiuo metu Lietuvoje nenaudojama.

4.1.10.4. Atšaukimo prašymo atidėjimo laikotarpis

Netaikoma.

4.1.10.5. Terminas, per kurį ERCA išnagrinėja atšaukimo prašymą

Netaikoma.

4.1.10.6. Atšaukimo tikrinimo reikalavimai, taikomi suinteresuotoms šalims

Šiuo metu Lietuvoje nenaudojama.

4.1.10.7. Sertifikato būsenos išdavimo dažnumas

Šiuo metu Lietuvoje nenaudojama.

4.1.10.8. CRL didžiausias vėlavimo terminas

Šiuo metu Lietuvoje nenaudojama.

4.1.10.9. Internetinio atšaukimo / būsenos tikrinimo galimybė

Šiuo metu Lietuvoje nenaudojama.

4.1.10.10. Internetinio atšaukimo / būsenos tikrinimo reikalavimai

Šiuo metu Lietuvoje nenaudojama.

4.1.10.11. Galimos ir kitos atšaukimo skelbimo formos

Šiuo metu Lietuvoje nenaudojama.

4.1.10.12. Specialieji reikalavimai, susiję su rakto pažeidimu

Šiuo metu Lietuvoje nenaudojama.

4.1.10.13. Sertifikato galiojimo sustabdymas

Šiuo metu Lietuvoje nenaudojama.

4.1.11. Sertifikato būsenos paslauga

Sertifikato būsenos informaciją apie visus išduotus sertifikatus tvarko LT-MSCA. Ši informacija neskelbiama, bet paprašius ji bus prieinama šalims, turinčioms teisėtų interesų.

4.1.12. Prenumeratos pabaiga

ERCA sertifikato pasirašymo paslaugų taisyklių prenumeratos pabaiga yra aprašyta ERCA politikos 4.1.12 skyriuje.
Prenumeratos pabaiga LT-MSCA lygiu nėra numatyta.

4.1.13. Raktų saugojimas ir atkūrimas

Raktų saugojimas yra draudžiamas bet kuriam dalyviui. Tai taikoma LT-MSCA ir LT-CP. Tačiau raktai yra saugomi ne mažiau kaip dviejose šifruotose atsarginėse laikmenose, saugomose atskirose, saugiose vietose. Norėdami atkurti atsargines žymas, reikalingi bent du įgalioti LT-MSCA arba atitinkamai LT-CP darbuotojai.

4.2. Paraiška pagrindiniams raktams ir jų išdavimas

Paraiškos išduoti raktus, jų nagrinėjimas, tikrinimas, raktų generavimas, platinimas ir administravimas atliekami ERCA politikoje nustatyta tvarka.
Apsikeitimas užklausomis ir atsakymai į jas atliekami ERCA politikoje nustatyta tvarka.

4.2.1. Raktų platinimo prašymai

Pagrindinius platinimo prašymus (KDR) gali pateikti tik LT-MSCA arba LT-CP, kuri yra pripažintas LT-MSA. Europos institucija yra atsakinga už MSA pripažinimą.
KDR formatas turi atitikti reikalavimus, nustatytus ERCA politikos 4.2.1. skyriuje.

4.2.2. Pagrindinio rakto paraiškos nagrinėjimas

ERCA atžvilgiu raktų platinimo prašymai (KDR) atitinka tas pačias prielaidas, kurios yra nustatytos CSR, todėl KDR gali pateikti tik LT-MSCA arba LT-CP.

4.2.2.1. KDR turinio tikrinimas

Pareiškėjo tapatybės nustatymo ir autentiškumo patvirtinimo tikslais LT-MSCA arba LT-CP tikrina kiekviename gautame rakto platinimo pranešime:

- profilio, autorizacijos ir rakto identifikatorių teisingumą;
- MAC teisingumą ir galiojimą;
- ar yra klaidų pranešimuose.

4.2.2.2. KDM generavimas, platinimas ir administravimas

Jei visi patikrinimai bus sėkmingi, ERCA parengs raktų paskirstymo pranešimą (KDM), nustatydamas simetrinį raktą, kurio prašo LT-MSCA arba LT-CP, ir vykdys ERCA politikos 4.2.3 skyriuje aprašytus veiksmus.

4.2.3. Simetrinių raktų konfidencialumo ir autentiškumo apsauga

Simetrinių raktų konfidencialumo ir autentiškumo apsauga užtikrinama, kaip aprašyta ERCA politikos 4.2.3. skyriuje.

4.2.4. Rakto platinimo pranešimai

Rakto platinimo pranešimų formatas turi atitikti reikalavimus, nustatytus ERCA politikos 4.2.4. skyriuje.

4.2.5. Keitimasis užklausomis ir atsakymais

Pagrindinių platinimo užklausų ir pagrindinių paskirstymo pranešimų transportavimui reikia naudoti CD-R laikmenas. Vieno seanso režimu CD-R turi būti 12 cm laikmena (suformatuota ISO 9660: 1988).
Kiti transportavimo būdai gali būti naudojami po išankstinio ERCA sutikimo. Bandymų tikslais ERCA priima ir siunčia CSR ir sertifikatus kaip el. pašto priedus.
LT-MSCA ir / arba LT-CP įrašo vieną ar tris kiekvieno sertifikato pasirašymo prašymo kopijas į transportavimo laikmenas, gabenamas į ERCA. Kopijos turi būti pateikiamos šešioliktainės skaičiavimo sistemos ASCII (.text faile), Base64 (.pem faile) arba dvejetainės skaičiavimo sistemos (.bin failo) formatu.
ERCA įrašo tris kiekvieno sertifikato kopijas į transportavimo laikmenas, grąžinamas LT-MSCA ir / arba LT-CP. Kopijos turi būti pateikiamos šešioliktainės skaičiavimo sistemos ASCII (.text faile), Base64 (.pem faile) arba dvejetainės skaičiavimo sistemos (.bin failo) formatu.
Prie kiekvieno KDR ir KDM turi būti pridėta popierinė duomenų kopija, suformatuota pagal šabloną, apibrėžtą ERCA politikoje. Kita popierinė duomenų kopija yra saugoma atitinkamai ERCA arba LT-MSCA ir / arba LT-CP.
Dėl abiejų, tiek KDR ir tiek KDM, transportavimo laikmenos ir popierinės kopijos perduodamos tarp ERCA darbuotojo ir kurjerio ERCA kontroliuojamoje zonoje.

4.2.6. Pagrindinio rakto priėmimas

Kurjeris pasirašo už rakto platinimo pranešimo gavimą ERCA patalpose. LT-MSCA ir / arba LT-CP, gavusi rakto platinimo pranešimą savo patalpose, patikrina, ar:

- transportavimo laikmena yra skaitoma kompiuterio, t. y. nėra pažeista ar sugadinta;
- pranešimo formatas atitinka ERCA politikos 4.2.4 skirsnio 4 lentelę;
- pranešimas yra autentiškas;
- pagrindinio rakto tipas ir pranešimo versija atitinka prašomą tipą ir versiją;
- pranešime nurodytas viešas taškas yra kreivėje, kurią nurodo pagrindinio platinimo prašymas, kurį LT-MSCA ir / arba LT-CP išsiuntė ERCA.

Jei kuris nors iš šių patikrinimų nepavyksta, LT-MSCA ir / arba LT-CP nutraukia procesą ir kreipiasi į ERCA.
Jei visi šie patikrinimai bus sėkmingi, LT-MSCA ir / arba LT-CP laikysis ERCA politikos procedūrų.

4.2.7. Pagrindinio rakto naudojimas

LT-MSCA ir / arba LT-CP naudojasi bet kuriuo gautu pagrindiniu raktu vadovaudamasi ERCA politikos 6.2 skyriumi.

4.2.8. KDM atnaujinimas

„DM atnaujinimas yra esamos KDM kopijos išdavimas LT-MSCA ir / arba LT-CP, nekeičiant efemerinio viešojo rakto ar jokios kitos KDM informacijos.
KDM atnaujinimas gali vykti tik tuo atveju, jei LT-MSCA ir / arba LT-CP gautos originalios transportavimo laikmenos priemonės yra sugadintos ar sugedusios. Sugadintos ar sugedusios transportavimo laikmenos yra saugumo incidentas, apie kurį pranešama LT-MSA ir ERCA.
Po tokio pranešimo LT-MSCA ir / arba LT-CP gali išsiųsti KDM atnaujinimo užklausą į ERCA, remdamasi pradiniu raktų paskirstymo prašymu.
Pastaba. Jei LT-MSCA ir / arba LT-CP turi išsiųsti prašymą iš naujo išplatinti pagrindinį raktą, kuris jau buvo sėkmingai išplatintas LT-MSCA ir / arba LT-CP, jis generuoja naują raktų paskirstymo užklausą, naudodamas naujai sukurtą efemerinę raktų porą. Toks prašymas gali paskatinti ERCA inicijuoti rakto pažeidimo galimybę.

4.2.9. Pakartotinis pagrindinis raktas

Norėdama gauti naują versiją, LT-MSCA ir / arba LT-CP pateikia naują KDR. Naujo pagrindinio rakto prašymas turi būti pateikiamas prieš protingą laiko tarpą, kad raktus (arba išvestinius raktus ar šifruotus duomenų judesio jutiklius) būtų galima laiku įdėti į naujai išleistus komponentus.
Rakto paraiška, nagrinėjimas, platinimas ir pripažinimas yra toks pat kaip ir pradiniam raktui.

4.2.10. Simetrinio rakto pažeidimo pranešimas

Jei LT-MSCA ir / arba LT-CP nustato ar jai yra pranešta apie simetrinio rakto pažeidimą arba įtariamą rakto pažeidimą, LT-MSCA ir / arba LT-CP apie tai praneša ERCA ir LT-MSA be nereikalingo delsimo ir bent per 8 valandas nuo pažeidimo nustatymo. LT-MSCA ir / arba LT-CP savo pranešime nurodo aplinkybes, kuriomis įvyko pažeidimas. Bet koks tolesnis tyrimas ir galimi LT-MSA ir (arba) LT-MSCA ir / arba LT-CP veiksmai atliekami, kaip nurodyta šioje Politikoje. Apie LT-MSA tyrimo rezultatus pranešama ERCA.

4.2.11. Pagrindinio rakto būsenos paslauga

LT-MSCA ir / arba LT-CP neteikia jokios rakto būsenos paslaugos.
Būsena gali būti nustatyta tiesiogiai iš rakto galiojimo datos.

4.2.12. Prenumeratos pabaiga

ERCA sertifikato pasirašymo paslaugų taisyklių prenumeratos pabaiga yra aprašyta ERCA politikos 4.1.12 skyriuje.
Prenumeratos pabaiga LT-MSCA ir / arba LT-CP lygiu nėra numatyta.
ERCA pagrindinių platinimo paslaugų prenumerata baigiasi, kai LT-MSA nusprendžia nutraukti MSA. Apie tokį pakeitimą LTCA MSA praneša ERCA kaip Politikos pakeitimą.
Prenumeratos galiojimo pabaigoje LT-MSCA ir / arba LT-CP saugiai sunaikina visus jos turimus simetrinius pagrindinius raktus.

4.2.13. Raktų saugojimas ir atkūrimas

Raktų deponavimas yra aiškiai uždraustas, o tai reiškia, kad simetriniai pagrindiniai raktai negali būti eksportuojami į bet kurią sistemą, išskyrus ERCA ir LT-MSCA ir / arba LT-CP sistemas.

4.3. Valstybės narės raktų generavimas

Valstybės narės raktų poros generavimas atliekamas HSM.
Naudojama įranga ir tenkinami reikalavimai turi būti aprašyti LT-MSCA veiklos nuostatuose (PS).
Generuojant LT-MSCA raktų porą turi dalyvauti trys fiziniai asmenys. Mažiausiai vienas iš jų turi būti CAA / PA (sertifikavimo centro / personalizavimo administratorius).

Raktams generuoti turi būti naudojamas RSA algoritmas, kurio rakto ilgiai turi atitikti Įgyvendinimo reglamente (ES) 2016/799 ir Įgyvendinimo reglamento (ES) 2016/799 1C priede (1024 bitai RSA) nustatytus reikalavimus.
Raktų generavimo įrenginys turi funkcionuoti savarankiškai, be kitų įrenginių pagalbos.
Raktų generavimą turi vykdyti įgalioti asmenys fiziškai saugioje aplinkoje, taikydami ne mažesnę kaip dvigubą kontrolę, t. y. pasitelkiant technines priemones reikalaujama, kad dalyvautų bent du įgalioti asmenys, kurių vienas būtų LT-MSCA, o kitas – LT-MSA darbuotojas.
LT-MSCA turi turėti daugiau nei vieną sertifikuotų valstybės narės raktų porą, nes ERCA negali greitai pakeisti valstybių narių sertifikatų.

4.4. Valstybės narės privačiojo rakto atsarginės kopijos

Valstybės narės privačiojo rakto kopija gali būti daroma esant dvigubai kontrolei siekiant prireikus atkurti raktą. Atsarginės kopijos darymo procedūros turi būti aprašytos LT-MSCA veiklos nuostatuose (PS).

4.5. Valstybės narės raktų paviešinimas

LT-MSCA veiklos nuostatuose (PS) turi būti įtrauktos rašytinės instrukcijos, kuriose nurodomi už saugumą atsakingų LT-MSCA darbuotojų atliekami veiksmai valstybės narės privačiojo rakto paviešinimo atveju arba esant įtarimų apie rakto paviešinimą.
Tokiu atveju LT-MSCA turi bent jau:
- informuoti MSA, ERCA ir kitas LT-MSCA;
- imtis būtiniausių atkuriamųjų veiksmų, net jei vėluojama gauti ERCA atsakymą.

4.6. Valstybės narės raktų galiojimo ciklo pabaiga

LT-MSCA užtikrina, kad visada turi galiojančią, sertifikuotą valstybės narės raktų porą.
Pasibaigus valstybės narės raktų poros galiojimui, viešasis raktas turi būti archyvuojamas, o privatusis raktas turi būti sunaikintas be galimybės atkurti.
LT-MSCA veiklos nuostatuose (PS) turi būti aprašytos viešojo rakto kopijos sukūrimo ir privačiojo rakto sunaikinimo procedūros.

4.7. Judesio jutiklio raktai

LT-MSCA ir / arba LT-CP prireikus prašo ERCA išduoti judesio jutiklių pagrindinį raktą $K_{M\text{-}WC}$ ir K_{DSRC} (Įgyvendinimo reglamento (ES) 2016/799 1C priedo 11 priedėlio 3.1.3 punktas).
Jei rakto prašė LT-MSCA, ji dirbtuvės kortelės raktą $K_{M\text{-}WC}$ perduoda LT-CP, kad LT-CP galėtų raktą įrašyti į dirbtuvės kortelę.
LT-MSCA ir / arba LT-CP užtikrina, kad raktai nebus naudojami jokiais kitais tikslais ir niekada nebus paimti iš saugios LT-MSCA aplinkos. LT-CP užtikrina, kad MSCA ir / arba LT-CP saugiai įdiegia dirbtuvės raktą $K_{M\text{-}WC}$ į visas išduotas dirbtuvės korteles (Įgyvendinimo reglamento (ES) 2016/799 1C priedo 11 priedėlio 3.1.3 punktas).
LT-MSCA ir / arba LT-CP saugojimo, naudojimo ir platinimo metu apsaugo judesio jutiklių raktus, naudodami griežtos fizinio ir loginio saugumo kontrolės priemones. Raktai saugomi ir naudojami specialiame klastojimui atspariame įrenginyje, kuris atitinka reikalavimus, nustatytus ERCA politikos 6.2 skyriuje.

4.8. Kortelių sertifikatai

4.8.1. Vairuotojo kortelių sertifikatai

Vairuotojo kortelių sertifikatai išduodami tik tais atvejais, kai išduodama vairuotojo kortelė.

4.8.2. Dirbtuvės kortelių sertifikatai

Dirbtuvės kortelių sertifikatai išduodami tik tais atvejais, kai išduodama dirbtuvės kortelė.

4.8.3. Kontrolės kortelių sertifikatai

Kontrolės kortelių sertifikatai išduodami tik tais atvejais, kai išduodama kontrolės kortelė.

4.8.4. Įmonių kortelių sertifikatai

Įmonių kortelių sertifikatai išduodami tik tais atvejais, kai išduodama įmonės kortelė.

4.8.5. VU sertifikatai

Šiuo metu Lietuvoje nenaudojami.

4.8.6. EGF sertifikatai

Šiuo metu Lietuvoje nenaudojami.

4.9. Įrangos sertifikatų išdavimas

LT-MSCA užtikrina, kad išsaugomas išduodamų sertifikatų autentiškumas ir integralumas. Sertifikatų turinys nustatytas Įgyvendinimo reglamento (ES) 2016/799 1C priedo 11 priedėlyje. LT-MSCA veiklos nuostatuose (PS) turi būti aprašytas sertifikatų tvarkymas ir saugojimas.

4.10. Sertifikatų atšaukimas

LT-MSA gali prašyti atšaukti sertifikatus, išduotus LT-MSCA.

4.11. Užklausos ir platinimas

4.11.1. Duomenų įvedimas

4.11.1.1. Tachografo kortelės

Kortelių turėtojai neteikia prašymų išduoti sertifikatus. Sertifikatai jiems išduodami remiantis informacija, pateikta prašyme išduoti kortelę ir saugoma LT-CIA registre. Viešasis raktas, kuris turi būti sertifikuotas, gaunamas raktų generavimo proceso metu.
LT-CP užtikrina, kad įvedamuose duomenyse pateikiama informacija, dėl kurios sertifikato turėtojo žyma (CHR) yra unikali. LT-MSCA turi patikrinti CHR unikalumą.
Jei LT-MSCA negeneruoja įrangos raktų poros, sertifikato prašymo pateikimo metu turi būti užtikrinta, kad LT-MSCA gali patikrinti privačiojo rakto ryšį su sertifikuoti pateiktu viešuoju raktu.
Skaitmeninis parašas kortelės viešojo rakto sertifikato prašyme, padarytas atitinkamu privačiuoju raktu, suteiktų galimybę LT-MSCA įrodyti:

- rakto sertifikavimo prašymo integralumą ir kilmę neatskleidžiant privačiojo rakto;
- institucijos, kuri pateikė prašymą, nuosavybę į privatųjį raktą.

Šiuo metu Lietuvoje nenaudojami.

4.11.1.2. VU ir EGF

Šiuo metu Lietuvoje nenaudojami.

4.11.2. Įrangos sertifikatų ir informacijos platinimas

LT-CP turi perduoti visus duomenis apie į korteles įrašytus sertifikatus į LT-CIA duomenų bazę. Tokiu būdu sertifikatai, įranga ir vartotojai yra susiję tarpusavyje.
LT-CIA užtikrina, kad esant būtinybei sertifikatai būtų prieinami visoms suinteresuotoms šalims.

5. Patalpos, valdymas ir veiklos kontrolė

LT-CIA, LT-MSCA ir LT-CP privalo parengti savo veiklos nuostatus (PS), kurie taikomi įgyvendinant visus reikalavimus, nustatytus šioje Politikoje, ir kuriuos tvirtina MSA, ypač:

a) Veiklos nuostatuose (PS) nurodomos visų išorinių organizacijų, padedančių LT-CIA, LT-MSCA ir LT-CP teikti paslaugas, prievolės, įskaitant taikomą Politiką ir veiklos praktiką;

b) Veiklos nuostatai (PS) turi būti prieinami MSA. LT-CIA, LT-MSCA ir LT CP nėra įpareigoti vartotojams viešinti visų veiklos praktikos detalių ir leisti jiems jomis naudotis;

c) LT-CIA, LT-MSCA ir LT-CP vadovybė yra atsakinga už tinkamą veiklos nuostatų (PS) įgyvendinimą;

d) LT-CIA, LT-MSCA ir LT-CP nustato veiklos nuostatų (PS) peržiūrėjimo tvarką.

LT-CIA, LT-MSCA ir LT-CP nustatyta tvarka informuoja MSA apie veiklos nuostatų (PS) pakeitimus ir papildymus, kuriuos ketina priimti, ir gavę patvirtinimą nedelsdami suteikia galimybę naudotis peržiūrėtais veiklos nuostatais (PS). Smulkūs pakeitimai gali būti padaryti be MSA patvirtinimo.

5.1. Fizinės saugos priemonės

Siekiant kontroliuoti prieinamumą prie LT-MSCA arba LT-CP techninės ir programinės įrangos, įgyvendinamos fizinės saugumo priemonės. Jos apima darbo stotis bei kitą sertifikavimo ir personalizavimo techninę įrangą ir bet kurios išorinės kriptografinės techninės įrangos modulį arba kortelę. Visi fiziniai veiksmai registruojami įrašų žurnale.

LT-MSCA privalo nurodyti veiklos nuostatų (PS) tvarką, kaip bus fiziškai ir logiškai saugomi valstybės narės raktai sertifikatams pasirašyti. LT-MSCA ir LT-CP taip pat turi patalpą, kurioje saugomos LT-MSCA ir LT-CP sistemų atsarginės kopijos taip, kad jos būtų pakankamai apsaugotos nuo praradimo, suklastojimo arba neteisėto saugomos informacijos panaudojimo. Šios atsarginės kopijos saugomos ir tam, kad duomenis būtų galima atkurti, ir tam, kad svarbią informaciją būtų galima saugoti archyve. LT-MSCA ir LT-CP sistemų atsarginių kopijų kūrimo priemonės taip pat saugomos kitoje nei LT-MSCA ir LT-CP sistemos laikymo vietoje tam, kad stichinės nelaimės atveju pagrindinėje įrangoje duomenis būtų galima atkurti.

Patalpų, kuriose yra laikoma LT-MSCA ir LT-CP centrinė įranga, saugumo patikrinimas atliekamas ne rečiau kaip kas 24 valandas. Jeigu tai yra nuolat lankoma patalpa, kartą per pamainą gali būti atliekamas vizualus patikrinimas, siekiant patikrinti, ar saugiai laikomos sistemos ir visi susiję kriptografiniai įrenginiai / kortelės, jeigu jie nėra naudojami, ar tinkamai veikia fizinio saugumo sistemos (pvz., durų užraktai ir signalizacija) bei ar nebuvo bandymų įeiti jėga.

Prieigai prie fizinės vietos, kur yra laikomi valstybės narės raktai ir jų naudojimo priemonės, reikia, kad tuo pat metu dalyvautų ne mažiau kaip du asmenys, kuriems asmeniškai buvo suteikta teisė įeiti į tą zoną. Prieiga prie kitų LT-MSCA ir LT-CP patalpų suteikiama tik tam personalui, kuris vykdo Politikos 5.2.2.1 skyriuje nurodytas funkcijas. Prieiga gali būti kontroliuojama naudojant patalpų, kuriose yra sistemos, prieigos kontrolės sąrašą. Visus asmenis, kurie nėra įtraukti į prieigos kontrolės sąrašą, lydi į tą sąrašą įtrauktas asmuo. Jeigu tam tikroje vietoje prieigos kontrolės sąrašo naudoti neįmanoma, gali pakakti patikrinti, ar su sertifikavimu ir personalizavimu susijusi medžiaga, kai ji nėra naudojama, yra užrakinta saugioje patalpoje arba saugykloje.

Privatusis raktas saugomas ir naudojamas tam skirtame klastojimui atspariame (HSM) įrenginyje.

Norint pasinaudoti LT-MSCA privačiuoju raktu, būtina dviguba kontrolė. Tai reiškia, kad vienas asmuo negali turėti priemonių pasiekti aplinką, kurioje saugomas privatusis raktas. Tai nereiškia, kad įrangos sertifikatai turi būti pasirašomi esant dvigubai kontrolei. Valstybės narės privatusis raktas negali būti viešinamas.

Valstybės narės privačiojo rakto saugojimas turi būti aprašytas LT-MSCA veiklos nuostatuose (PS). Saugojimo laikmenos, naudojamos saugoti konfidencialią informaciją, pvz., standieji diskai, lustinės kortelės, HSM įrenginiai turi būti apsaugoti nuo neteisėto ar nenumatyto naudojimo, prieigos, atskleidimo ar žalos dėl žmonių veiklos ar atsitiktinių grėsmių (pvz., gaisro, vandens patekimo). Saugojimo vietoje turi būti įrengti vandens detektoriai, prijungti prie pastato apsaugos stebėjimo centro. Saugojimo vietoje turi būti įrengti dūmų ir šilumos detektoriai, prijungti prie pastato apsaugos stebėjimo centro.

Darbuotojai turi naudoti tinkamą techniką, atsižvelgdami į turimų duomenų klasifikaciją, apdirbdami naudojamas medžiagas (pvz., magnetinius ir mechaninius smulkintuvus).
Siekiant išvengti neleistino konfidencialių duomenų naudojimo, prieigos ar atskleidimo, turi būti nustatomos atitinkamos atliekų šalinimo procedūros.

5.2. Kontrolės priemonių procedūros

Siekiant užtikrinti saugias operacijas, įgyvendinamos procedūrinės kontrolės priemonės. Visų pirma pareigų atskyrimas vykdomas įgyvendinant daugiašalę svarbių užduočių kontrolę.
Galimybė naudotis LT-MSCA sistemomis suteikiama tik tiems asmenims, kurie yra tinkamai įgalioti ir kuriems reikia vykdyti užduotis. LT-MSCA įgyvendina ERCA politikos 5.2 skyriuje nurodytas prieigos kontrolės priemones.
Kiekvienas iš toliau aprašytų patikėtų vaidmenų yra priskiriamas vienam asmeniui ir privaloma turėti bent vieną jį pavaduojantį asmenį. Visos sistemos naudotojo teisės yra ribojamos pagal jų vaidmenį. Vaidmenų aprašymas ir jų koncepcija yra viešai nepublikuojamų dokumentų dalis.

5.2.1. Patikėti vaidmenys

LT-MSCA ir LT-CP, remdamiesi ERCA politika, turėtų paskirti bent tris vaidmenis. Vaidmenims suteikiami skirtingi įgaliojimai.
Norint užtikrinti, kad asmuo negalėtų daryti įtakos sistemos saugumui, kiekvienam asmeniui turi būti priskirti vaidmenys ir atsakomybė. Kiekviena vartotojo paskyra turi turėti ribotas teises, atitinkančias vartotojo vaidmenį.
Gali būti tokie vaidmenys:

a) sertifikavimo centro / personalizavimo administratorius (CA/PA);
b) informacinės sistemos administratorius (SA);
c) informacinės sistemos saugumo pareigūnas (ISSO).

Sertifikavimo / personalizavimo administratoriaus pareigos:

a) raktų generavimas;
b) sertifikatų generavimas;
c) personalizavimas ir saugus įrangos platinimas;
d) administravimo funkcijos, susijusios su LT-MSCA ir LT-CP duomenų bazių palaikymu.

Sistemos administratoriaus pareigos:

a) pradinis sistemos konfigūravimo organizavimas, įskaitant saugų sistemos įjungimą ir išjungimą;
b) pradinis naujų vartotojų paskyrų sukūrimas;
c) pradinis tinklo konfigūravimo organizavimas;
d) sistemos pakrovimo disko, reikalingo esant sistemos gedimui ir duomenų apsaugojimui nuo praradimo, sukūrimas;
e) sistemos atsarginių kopijų kūrimas, programinės įrangos atnaujinimas.

Atsarginės kopijos turi būti daromos ne rečiau kaip vieną kartą per savaitę. Padarius atsarginę kopiją, sistema turi būti perkraunama tam, kad būtų patikrintas techninės įrangos integralumas, IP adreso ir / arba vardo keitimai.
Informacinės sistemos saugumo pareigūno pareigos:

a) teisių sertifikavimo / personalizavimo administratoriams suteikimas;
b) slaptažodžių suteikimas visoms naujoms paskyroms;
c) visų būtinų sistemos įrašų archyvavimas;
d) audito žurnalo tikrinimas, ieškant sertifikavimo / personalizavimo administratoriaus darbo nusižengimų saugumo politikai. Audito žurnalo tikrinimas turi būti atliekamas ne rečiau kaip vieną kartą per savaitę;
e) asmeninis vadovavimas atliekant metinį LT-MSCA ir LT-CP įrašų auditą; dalyvavimas valstybės narės raktų generavimo procese.

5.2.2. Vaidmenų atskyrimas

Kiekvienam vaidmeniui vykdyti turi būti pasirinktas mažiausiai vienas asmuo. Visi vaidmenys turi būti atskirti.

5.2.3. Kiekvieno vaidmens identifikavimas ir autentifikavimas

Sertifikavimo / personalizavimo administratoriaus, sistemos administratoriaus ir informacinės sistemos saugumo pareigūno identifikavimas ir autentifikavimas turi atitikti veiklos nuostatus (PS) ir Politikos nuostatas.
LT-MSCA ir LT-CP vykdo griežtą prieigos teisių valdymą ir kontrolę identifikuodami ir autentifikuodami darbuotojus, atliekančius sertifikavimo procesus. Atliekant prieigos kontrolę naudojami saugumo mechanizmai, galintys atskirti patikimus vaidmenis, aprašytus šios Politikos 5.2.1 skyriuje, ir nustatyti konkrečias vaidmens funkcijas, kurias turi vykdyti vaidmeniui paskirtas asmuo.

5.2.4. MSCA ir CP informacijos saugumo valdymas

LT-MSCA ir LT-CP užtikrina, kad būtų taikomos administracinės ir valdymo procedūros, kurios būtų adekvačios ir atitiktų pripažintus standartus.
LT-MSCA ir LT-CP išlieka atsakingi už visus sertifikavimo paslaugų teikimo aspektus, net ir perdavus kai kurias funkcijas vykdyti subrangovams. LT-MSCA ir LT-CP aiškiai apibrėžia trečiųjų šalių atsakomybę ir sudaro reikalingus susitarimus, siekdami užtikrinti, kad trečiosios šalys įsipareigotų įgyvendinti visas LT-MSCA ir LT-CP reikalaujamas kontrolės priemones.
Visą laiką palaikoma informacijos saugumo infrastruktūra, kuri yra nurodyta LT-MSCA ir LT-CP veiklos nuostatuose (PS) ir yra reikalinga saugumui LT-MSCA ir LT-CP valdyti.
LT-MSCA ir LT-CP sukuria informacijos saugumo valdymo sistemą (ISMS), pagrįstą visų susijusių operacijų rizikos įvertinimu. LT-MSCA ir LT-CP užtikrina, kad ISMS politika būtų taikoma personalo mokymui, leidimams ir vaidmenims. LT-MSCA ir LT-CP ne vėliau kaip po vienerių metų nuo veiklos pradžios turi būti akredituota pagal LST EN ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai.“ standarto reikalavimus šios Politikos taikymo srityje.

5.2.5. MSCA ir CP personalo saugumas

LT-MSCA ir LT-CP savo darbuotojams paskiria patikėtus vaidmenis, užtikrindami, kad nekiltų konfliktų dėl pareigų atskyrimo. LT-MSCA atveju, pvz., ekspertų grupės narys negali būti viešojo rakto infrastruktūros saugumo pareigūnas ir atvirkščiai.
Išskyrus standartines užduotis, kurias atlieka ekspertų grupė, kritiniai saugumo veiksmai reikalauja, kad bent du asmenys, turintys skirtingus patikėtus vaidmenis (žr. Politikos 5.2.1 skyrių), bendrai vykdytų veiksmus.
Toliau pateiktiems procesams reikalingi du asmenys, turintys skirtingus patikėtus vaidmenis:

- LT-MSCA raktų generavimas – papildomai dalyvaujant LT-MSA kontaktiniam asmeniui;
- LT-MSCA raktų diegimas, aktyvinimas ir atsarginių kopijų paruošimas – papildomai dalyvaujant LT-MSA kontaktiniam asmeniui;
- LT-MSCA raktų atkūrimas;
- LT-MSCA rakto eksportavimas ir importavimas naudojant atsarginį raktą;
- apsikeitimas HSM įrenginiais, kuriuose yra laikomi LT-MSCA raktai;
- generuojant LT-CP viešąjį raktą (Card_MA/Card_Sign), naudojamą Card-CSR perduodant jį LT-MSCA.

5.2.6. Saugumo valdymo kontrolės priemonės

Sistemos funkcijos įgyvendinamos ir kontroliuojamos pagal Politikos 5.2.1 skyrių.

5.3. Personalo kontrolė

Sertifikavimo / personalizavimo administratorius turi būti nepriekaištingos reputacijos, atsakyti už savo veiksmus, susijusius su sertifikavimu / personalizavimu.
LT-MSCA ir LT-CP personalas, einantis atsakingas pareigas, įskaitant sertifikavimo / personalizavimo administratorių ir informacinės sistemos saugumo pareigūną, turi:

a) vykdyti tik tas užduotis, kurios netrukdo jo, kaip administratoriaus / pareigūno, tiesioginiam darbui;

b) nebūti atleistas iš ankstesnių pareigų už nerūpestingumą ar aplaidumą;

c) turėti jo atliekamoms užduotims reikalingą kvalifikaciją ir žinias;

d) būti patikrintas policijos ar atitinkamos organizacijos dėl patikimumo ir tenkinti nustatytus reikalavimus:

- nustatytus Vyriausybės patikimumo patikrinimo schemose;
- dėl įrašų apie kriminalinę praeitį nebuvimo;
- patenkinamo kredito patikrinimo.

Visi su LT-MSCA veikla susiję darbuotojai turi būti tinkamai apmokyti ir įgiję ekspertinių žinių, patirties ir kvalifikacijos, reikalingos siūlomoms paslaugoms ir darbo funkcijoms.
Personalo mokymas ir paskyrimas į pareigas turi būti aprašytas veiklos nuostatuose (PS) ir atliekamas pagal ERCA politikoje nustatytus reikalavimus.
LT-MSCA ir LT-CP valdo tik kvalifikuoti ir patyrę specialistai. Kiekvienas darbuotojas turi išeiti išsamius patikimumo patikrinimus.
Patikėti vaidmenys, aprašyti Politikos 5.2.1 skyriuje, įprastai paskiriami tik asmenims:

- kurie nekelia abejonių dėl saugumo svarbos suvokimo, patikimumo, skaidrumo ir lojalumo;
- kurių kitose pareigose atliekamos pareigos ir užduotys nesukelia interesų konflikto;
- kurie neveikė neatsargiai ar aplaidžiai ankstesniuose darbo santykiuose ar darbo pozicijose.

Norint gauti paskirtą LT-MSCA arba LT-CP patikimą vaidmenį, darbuotojams atliekamas saugumo patikrinimas pagal nustatytą saugumo patikrinimo tvarką.
Kiekvienas darbuotojas yra asmeniškai informuotas apie jo pareigų atsakomybės mastą ir ribas. Kiekvieno darbuotojo sutartyje yra numatomos specialios konfidencialumo sąlygos.
LT-MSCA darbuotojams, kurie naudojasi viešojo rakto infrastruktūra, būtina autentifikavimo procedūra su lustine kortele ir jai priskirtu asmeniniu PIN kodu. Prieiga prie „CA Conosle“ programos reikalauja papildomo slaptažodžio.
LT-CP darbuotojams, kurie naudojasi viešojo rakto infrastruktūra, būtina autentifikavimo procedūra su vartotojo ID ir slaptažodžiu.
Prieš pradedant eiti pareigas, darbuotojas apmokomas pagal priskirtą patikėtą vaidmenį. LT-MSCA ir LT-CP darbuotojai privalo būti susipažinę su sertifikavimo infrastruktūros programine ir techninę įranga, pagrindinėmis procedūromis bei komponentais, su kuriais jie dirba. Darbuotojai turi gerai suprasti savo darbo procesus ir jų poveikį.
Kiekvienas LT-MSCA ir LT-CP darbuotojas turi išeiti mokymus, kurie apima viešojo rakto infrastruktūros sistemą, jos organizavimą, saugumo politiką, avarinius planus, naudojamą programinę įrangą ir procedūras, už kurias darbuotojas bus atsakingas.
Kiekvienas LT-MSCA ir LT-CP darbuotojas turi išeiti reikiamus mokymus po svarbesnių sistemos, organizacijos, naudojamų priemonių ar metodų pakitimų.
LT-CP personalo neteisėti veiksmai yra sankcionuojami pagal LT-CP darbo reglamentą.

5.4. Audito žurnalų procedūra

Visi reikšmingi LT-MSCA programinės įrangos saugumo įvykiai automatiškai fiksuojami ir registruojami sistemos įvykių žurnale. Įvykiai, aprašyti ERCA politikoje, registruojami į sistemos įvykių žurnalą. LT-MSCA gali išplėsti registruojamų įvykių sąrašą, kuris aprašomas LT-MSCA veiklos nuostatuose (PS).

Jei įmanoma, sistemos žurnale pateikiama informacija, leidžianti identifikuoti asmenį ar paskyrą, kuri atliko sistemos užduotis.
Sistemos įvykių žurnalų vientisumas turi būti išlaikomas ir saugomas nuo neleistino tikrinimo, keitimo, ištrynimo ar sunaikinimo. Sistemos įvykių žurnalai turi būti saugomi laikantis procedūrų, aprašytų veiklos nuostatuose (PS).
Audito žurnalai tikrinami ir apibendrinami ne rečiau kaip kartą per mėnesį. Vykdant patikrinimą ir apibendrinimą dalyvauja ne mažiau kaip du asmenys, vykdantys SA arba ISSO funkcijas (žr. Politikos 5.2.2.1 skyrių).

5.4.1. Sistemos įvykių žurnalo atsarginių kopijų kūrimo procedūros

Sukuriamos dvi sistemos įvykių žurnalo kopijos, kurios laikomos atskirose fiziškai saugomose vietose.
Sistemos įvykių žurnalas saugomas taip, kad jį būtų galima bet kuriuo metu per jo saugojimo laikotarpį patikrinti.
Sistemos įvykių žurnalai apsaugomi nuo pašalinių asmenų.

5.5. Įrašų archyvas

Sistemos įvykių žurnalai reguliariai (bent vieną kartą per metus) analizuojami, tiriant, ar nebuvo piktybinių veiksmų. Registravimo procedūros aprašomos LT-MSCA veiklos nuostatuose (PS).
Visi įrašai saugomi neterminuotai.
Turi būti nustatytos procedūros, užtikrinančios įrašų vientisumą, autentiškumą ir konfidencialumą.

5.5.1. CIA registruojamų įvykių tipai

Informacinės sistemos įrašuose pateikiami svarbūs LT-CIA turimi duomenys:
a) asmenų prašymai išduoti korteles, tarp jų – asmens, atsakingo už prašymo priėmimą, tapatybė;
b) pasirašyti kortelių pristatymo priėmimo dokumentai;
c) dokumentai dėl sertifikatų ir susijusių kortelių;
d) prašymai atnaujinti korteles ir visi pranešimai, kuriais keičiamasi su vartotoju;
e) kortelių pakeitimo prašymai ir visi registruoti pranešimai, kuriais keičiamasi su prašymą pateikusiu asmeniu ir / arba vartotoju;
šiuo metu ir anksčiau įgyvendinti Politikos dokumentai.

5.5.2. LT-MSCA ir LT-CP registruojamų įvykių tipai

Įrašuose pateikiami visi aktualūs LT-MSCA ir LT-CP turimi duomenys, taip pat:
a) išduotų sertifikatų turinys;
b) audito žurnalai, kuriuose saugomi LT-MSCA ir LT-CP metinio audito duomenys pagal veiklos nuostatus (PS);
c) šiuo metu ir anksčiau įgyvendinti sertifikatų politikos dokumentai.
Į duomenis apie visus skaitmeniniu būdu pasirašytus elektroninius prašymus, kuriuos pateikė LT-MSCA ir LT-CP arba paslaugų agentūrų personalas (CA / PA), įtraukiami už kiekvieną prašymą atsakingo administratoriaus tapatybės duomenys ir visa informacija, kuri yra reikalinga patikrinti, ar prašymas nėra atmestinas, ir saugomi tiek laiko, kol saugomi duomenys.

5.5.3. Archyvo saugojimo laikotarpis

Archyvai laikomi ir apsaugomi nuo modifikavimo arba sunaikinimo neterminuotai.

5.5.4. Informacijos iš archyvo gavimo ir patikrinimo procedūros

LT-MSCA ir LT-CP laikosi konfidencialumo reikalavimų, kaip nurodyta Politikos 9.3 ir 9.4 skyriuose.
Atskirų transakcijų duomenys gali būti atskleisti, gavus bet kurio dalyvio, dalyvavusio transakcijoje, arba jo pripažinto atstovo prašymą.

LT-MSCA ir LT-CP, gavę prašymą, išduoda dokumentus, liudijančius, kad LT-MSCA ir LT-CP laikosi taikomų veiklos nuostatų (PS).
Siekiant padengti duomenų teikimo išlaidas, gali būti nustatytas pagrįstas administracinis mokestis.
LT-MSCA ir LT-CP užtikrina archyvo prieinamumą ir tai, kad archyve laikoma informacija per jos saugojimo laikotarpį būtų saugoma perskaitomu formatu net ir tuo atveju, jeigu LT-MSCA ir LT-CP veikla yra pertraukiama, sustabdoma arba nutraukiama.
Jeigu LT-MSCA ir LT-CP paslaugos pertraukiamos, sustabdomos arba nutraukiamos, LT-MSCA ir LT-CP siunčia pranešimą LT-CIA, siekdami užtikrinti nuolatinį archyvo prieinamumą. Visi prašymai dėl prieinamumo prie archyvo informacijos siunčiami LT-MSCA ir LT-CP arba institucijai, kurią nurodo LT-MSCA ir LT-CP, prieš nutraukiant jos veiklą.

5.6. Raktų keitimas

LT-MSCA užtikrina, kad keičiami raktai būtų generuojami kontroliuojamomis aplinkybėmis ir laikantis ERCA politikoje nustatytų procedūrų.

5.7. Atkūrimas

MSCA, CP ir subrangovai nustato standartines procedūras, skirtas apsisaugoti nuo sistemos gedimų poveikio ir juos minimizuoti. Šios standartinės procedūros apima bent saugų ir nuotolinį atsarginių duomenų kopijų saugojimą, veikiančias duomenų atkūrimo procedūras ir t. t., kurios detalizuojamos Saugumo incidentų tvarkymo procedūrų vadove. Saugumo incidentų tvarkymo procedūrų vadovas pateikiamas administratoriams ir auditoriams. Procedūrų vadovas nėra viešai prieinamas.
Visų susijusių duomenų atsarginės kopijos ir atkūrimo procedūros aprašomos atsarginių kopijų ir atkūrimo plane.
Šie įvykiai laikomi nelaimėmis:

a) privataus rakto ir (arba) pagrindinio rakto pažeidimas arba vagystė;
b) privataus rakto ir (arba) pagrindinio rakto praradimas;
c) IT įrangos gedimas.

MSCA privačių ir (arba) pagrindinių raktų pažeidimo ar vagystės atveju MSCA nedelsdama praneša apie tai MSA ir ERCA. MSA nedelsdama imasi tinkamų priemonių.
Jei MSCA privatusis raktas yra pažeistas arba įtariama, kad jis yra pažeistas, MSCA praneša apie incidentą ERCA ir MSA be reikalo nedelsdama ir bent per 8 valandas nuo aptikimo. Pranešime MSCA nurodo aplinkybes, kuriomis įvyko pažeidimas. MSA atlieka tyrimą ir apie tyrimo rezultatus pranešama ERCA.
Raktų praradimo atveju nėra efektyvaus būdo juos atkurti, todėl tam turi būti užkirstas kelias naudojant kelias atsargines šakninių raktų ir pagrindinių raktų kopijas, periodiškai jas kontroliuojant. Apsaugoti nuo IT įrangos gedimų naudojamos atsarginės kopijos. IT įrangos gedimo atveju veikimas atkuriamas ne vėliau kaip per 24 val.
LT-MSCA ir LT-CP personalizuotojai turi parengtą veiklos tęstinumo planą, kuriame išsamiai aprašoma, kaip bus tęsiama veikla įvykus įvykiui, kuris paveikia įprastas veiklos procedūras. Nustačius tokį incidentą, veiklos procedūros sustabdomos, kol bus pasiektas kompromisas, kaip tęsti procedūras. LT-MSCA ir LT-CP turi numatyti, jog dėl technologinės pažangos dabartinės IT sistemos per atitinkamą laiką gali pasenti. Veiklos tęstinumo plane turi būti apibrėžtos priemonės, skirtos suvaldyti technologijų senėjimą.

5.8. LT-MSCA ir LT-CP veiklos nutraukimas

Galutiniu LT-MSCA arba LT-CP veiklos nutraukimu yra laikomi atvejai, kai visos paslaugos, susijusios su loginiu asmeniu, yra visam laikui nutraukiamos. Juo nelaikomas atvejis, kai viena organizacija paslaugą perduoda kitai arba kai LT-MSCA paslauga iš senos valstybės narės raktų poros yra perkeliama į naują valstybės narės raktų porą arba ERCA raktą.
LT-MSA užtikrina, kad būtų vykdomos toliau išvardytos funkcijos.
Prieš nutraukdami savo veiklą, LT-MSCA ir LT-CP atlieka bent jau šias procedūras:

a) informuoja visus vartotojus ir šalis, su kuriomis LT-MSCA ir LT-CP yra pasirašę sutartis arba užmezgę kitokius ryšius;

b) viešai paskelbia turimą informaciją apie savo veiklos nutraukimą ne vėliau kaip prieš 3 mėnesius iki nutraukimo;

c) LT-MSCA ir LT-CP nutraukia visus subrangovų įgaliojimus veikti LT-MSCA ir LT-CP vardu išduodant sertifikatus.

Nutraukus LT-MSCA veiklą, LT-MSA apie tai praneša atsakingai Europos institucijai ir ERCA ir esant galimybei informuoja Europos instituciją ir ERCA apie naujai paskirtą LT-MSCA.

LT-MSA užtikrina, kad bent viena LT-MSCA nuolatos veikia jos jurisdikcijoje.

5.8.1. LT-MSCA ir LT-CP atsakomybės perleidimas

MSCA arba CP atsakomybė yra perleidžiama, kai MSA nusprendžia paskirti naują MSCA arba CP vietoj ankstesnės institucijos.

MSA užtikrina, kad būtų tinkamai perleista atsakomybė ir turtas.

Senoji MSCA perleidžia visus pagrindinius raktus naujajai MSCA MSA nustatytu būdu.

Senoji MSCA sunaikina visas raktų kopijas, kurios nebuvo perleistos.

5.8.2. LT-MSCA ir LT-CP veiklos tęstinumo planavimas

LT-MSCA ir LT-CP turi veiklos tęstinumo planą. Jame aptariami tokie atvejai:

a) rakto saugumo pažeidimas;

b) duomenų praradimas dėl, pvz., vagystės, gaisro, techninės įrangos arba programinės įrangos gedimo;

c) kitokio pobūdžio sistemos sutrikimas.

6. Techninės saugumo priemonės

6.1. Raktų poros ir simetrinio rakto generavimas ir diegimas

Kriptografinis raktų paketo generavimas gali būti atliekamas prieš pateikiant prašymą sertifikuoti raktus arba tuo pat metu, kai gaunamas prašymas sertifikuoti.

Raktų paketo generavimas turi būti atliekamas savarankiškai funkcionuojančiu įrenginiu, atitinkančiu aukščiau minėtus reikalavimus. Raktų integralumas apsaugomas iki tol, kol išduodamas sertifikatas.

6.1.1. Raktų poros generavimas

6.1.1.1. Valstybės narės raktų generavimas

LT-MSCA generuoja valstybės narės raktą pagal Įgyvendinimo reglamento (ES) 2016/799 1C priedo 11 priedėlį.

Valstybės narės raktai generuojami pagal iš anksto numatytą tvarką dalyvaujant bent dviem darbuotojams su priskirtais patikėtais vaidmenimis taip užtikrinant dvigubą kontrolę (t. y. kad dalyvautų bent du įgalioti asmenys).

Raktų generavimas atliekamas naudojant įrangos apsaugos modulį (HSM), kuriame vėliau saugomi sugeneruoti raktai.

6.1.1.2. Raktų generavimas kortelių personalizavimui

Kortelių personalizavimui skirti raktai yra generuojami išskirtinai LT-CP. LT-CP generuoja kortelių personalizavimo raktą pagal Įgyvendinimo reglamento (ES) 2016/799 1C priedo 11 priedėlį.

Vadovaujantis ERCA politikos 1.5.3 straipsniu, LT-MSA reikalauja LT-CP naudoti pagal bendruosius kriterijus sertifikuotas tachografo korteles. LT-MSA reikalauja:

- iš LT-CP, kad būtų laikomasi visų tachografo kortelės saugumo sertifikatuose nurodytų nurodymų per visą kortelių gaminimo ir galiojimo laikotarpį;

- kad privataus rakto generavimas vyktų pasinaudojant specialiuoju įrangos apsaugos moduliu (HSM), jei privataus rakto generavimo nėra galimybės atlikti su savarankiškai funkcionuojančiu įrenginiu.
- kad esant galimybei generuojant privačius ar simetrinius raktus su savarankiškai funkcionuojančiu įrenginiu raktų generavimui būtų taikomas įrangos saugumo sertifikavimas, užtikrinant, kad būtų naudojami viešai nustatyti ir tinkami kriptografinių raktų generavimo algoritmai.

Už kortelių personalizavimo raktų generavimą atsako LT-CP. Rakto generavimo dokumentacijos procedūros perduodamos LT-MSA.

6.1.1.3. Raktų generavimas perdavimui

Visi raktai perduodami LT-MSCA ir / arba LT-CP ir ERCA naudojant ERCA politikoje nustatytas priemones, laikmenas ir protokolus. Jei raktų perdavimui naudojamos fizinės laikmenos, LT-MSA paskiria įgaliotą asmenį laikmenai pernešti.
Raktų perdavimas LT-MSCA, LT-CIA ir LT-CP įgyvendinamas paskirto įgalioto asmens. Raktų perdavimas turi atitikti numatytas vidines LT-MSA saugumo procedūras.
LT-MSCA raktų sertifikavimo prašyme naudojamas ERCA politikos 4.2 skyriuje nustatytas KCR protokolas.
LT-MSCA priima ERCA viešąjį raktą ERCA politikos 4.2 skyriuje nustatytu platinimo formatu.
LT-MSCA užtikrina, kad KID ir raktų moduliai, pateikti ERCA sertifikuot ir judesio jutiklio raktui platinti, yra unikalūs LT-MSCA domene.
LT-MSCA užtikrina, kad privatieji raktai lieka HSM ir nebus perkelti vykdant rakto sertifikavimo operacijas.
LT-MSCA ir / arba LT-CP prašo ERCA judesio jutiklio rakto naudodamasis ERCA politikos 4.2 skyriuje nustatytu KDR protokolu.

6.1.2. Privačiojo rakto pristatymas naudotojui

Nėra numatytos privataus rakto pristatymo naudotojui procedūros. LT-CP generuoja raktą, perkelia jį į atitinkamą tachografo kortelę ir atsiunčia ją paštu LT-CIA.

6.1.3. Privačiojo rakto pristatymas pažymėjimus išduodančiai institucijai

Prieš vairuotojų, įmonių, dirbtuvės ir kontrolės kortelių sertifikavimą LT-CP išsiunčia sertifikato pasirašymo prašymus LT-MSCA. Prašymai turi būti pasirašyti failai. LT-MSCA turi patvirtinti parašo tinkamumą prieš sertifikavimo procedūrą. Prašymo formatas yra nustatomas LT-CP ir LT-MSCA susitarimu. Failų perdavimas turi būti paremtas nustatytu protokolu šifruotiems duomenims.

6.1.4. CA viešųjų raktų pristatymas susijusioms šalims

Valstybės viešasis raktas yra atsakymas į kiekvieną patvirtintą kortelės sertifikato pasirašymo prašymą. Atsakymai turi būti pasirašyti failai. LT-CP turi patvirtinti parašą prieš naudojant raktą kortelei personalizuoti. Atsakymo formatas yra nustatomas LT-MSCA ir LT-CP susitarimu. Failų perdavimas turi būti paremtas nustatytu protokolu šifruotiems duomenims.

6.1.5. Raktų dydžiai

Raktų dydžiai yra nustatomi pagal Įgyvendinimo reglamento (ES) 2016/799 1C priedo 11 priedėlį.
ERCA nustatė minimalų rakto ilgį CSM_50 priklausomai nuo Europos šakninio sertifikato ilgio.
LT-MSCA ir LT-CP generuoja raktus remdamiesi iš anksto nustatytu rakto ilgiu.
Pagal specifinį susitarimą ruošiamiems raktams reikia vadovautis „Išmaniųjų tachografų šifravimo raktų ir skaitmeninių sertifikatų ruošinių“ leidiniu, nurodančiu pradinį raktų ilgį (standarto įsigaliojimo data 2017 m. sausio 1 d., 00:00) 256 bitų šakniniam sertifikatui. Remiantis tokia specifikacija, pradinis valstybės narės raktų dydis (LT-MSCA_Card.PK / LT-MSCA_Card.SK) ir

tachografo rakto dydis (Card_MA / Card_Sign) taip pat turi būti 256 bitai. Nustatytas K_M, $K_{M\text{-}WC}$ and K_{DSRC} rakto dydis yra 128 bitai.
ERCA nusprendė padidinti Europos šakninio sertifikavimo raktų dydį su kiekvienu nauju galiojimo laikotarpiu. Nuo 2034 metų Europos šakninio sertifikavimo rakto dydis bus 384 bitai, o pradedant nuo 2051 metų Europos šakninio sertifikavimo rakto dydis 512 bitų.
LT-MSCA ir LT-CP raktų dydžiai turėtų atitinkamai augti.

6.1.6. Viešųjų raktų parametrų generavimas ir kokybės patikrinimas

Visi LT-MSCA ir LT-CP raktai yra generuojami naudojant HSM.

6.1.7. Raktų naudojimo tikslai

Valstybės narės raktų poros naudojamos tik tachografo kortelių sertifikatams pasirašyti.
Tachografo kortelių privatūs raktai yra naudojami tik tachografo kortelei personalizuoti.
Tachografo kortelės Card_MA turi būti naudojamos išskirtinai tais atvejais, kai reikia atlikti abipusį autentiškumo patvirtinimą ir sesijos raktų susitarimą dėl transporto priemonių blokų. Vairuotojų ir dirbtuvės kortelės turi naudoti privatų Card_Sign.SK raktą išskirtinai tais atvejais, kai reikia pasirašyti parsisiųstus duomenų failus. Vairuotojo ir dirbtuvės kortelės turi naudoti atitinkamą viešąjį raktą Card_Sign.PK išskirtinai tais atvejais, kai reikia patvirtinti kortelės sukurtą parašą.
Dirbtuvės kortelės judesio jutiklio raktai turi būti naudojami tik dirbtuvės kortelėms.
DSRC kortelės pagrindinis raktas yra naudojamas tik kontrolės ir dirbtuvės kortelėms.

6.2. Privačiojo rakto ir simetrinio rakto apsaugos ir kriptografinių modulių inžinerinės kontrolės priemonės

Privatieji raktai ir pagrindiniai raktai generuojami ir naudojami patikimame specialiajame įrenginyje, kuris:

- yra patvirtintas pagal 4 arba aukštesnį patikimo funkcionavimo garantijų įvertinimo lygį (EAL 4) laikantis ISO/IEC 15408-1:2009, Informacinės technologijos – Apsaugos metodai – IT apsaugos vertinimo kriterijai, 1, 2, 3 dalys, trečiasis leidimas 2008–2014 m. naudojant tinkamą apsaugos profilį; arba
- atitinka reikalavimus, nurodytus ISO/IEC 19790:2012, Informacinės Technologijos – Apsaugos metodai – Saugumo reikalavimai kriptografiniams modeliams, 3 lygis; arba;
- atitinka Nacionalinio standartų ir technologijų instituto (NSTI) reikalavimus, FIPS PUB 140-2, Saugumo reikalavimai kriptografiniams modeliams, 2001, 3 lygis.

Visose procedūrose su HSM įrenginiais turi dalyvauti bent du autentifikuoti darbuotojai iš LT-MSCA arba atitinkamai LT-CP, ypač generuojant, atkuriant, aktyvuojant, išjungiant raktus arba apsikeičiant HSM įrenginiais.
Visi privatūs ir pagrindiniai raktai turi būti išjungiami (nebegali būti panaudojami), jei kyla abejonių dėl saugumo užtikrinimo. LT-MSCA turi patikrinti galimus įtarimus dėl pažeidimų. Jei kylančios abejonės ir įtarimai pasitvirtina arba negali būti atmesti, raktai ir jų kopijos turi būti sunaikinami. Jei abejonės ir įtarimai nepasitvirtina ir yra atmesti, raktai aktyvuojami iš naujo.
Privačiųjų ir pagrindinių raktų sunaikinimas atliekamas naudojant HSM įrenginio funkciją raktų naikinimui.

6.2.1. Raktai kortelėse

Remiantis šia Politika įrangos privačiojo rakto galiojimo laikas negali būti ilgesnis nei sertifikato galiojimo laikas.
MSCA_Card sertifikato galiojimo laikotarpis – 7 metai ir 1 mėnuo.

6.2.2. Transporto priemonių blokų (VU) raktai

Šiuo metu Lietuvoje nenaudojami.

6.2.3. Įrangos privačiųjų raktų apsauga ir saugojimas. Kortelės

LT-CP užtikrina, kad:

a) kortelės privatusis raktas, kuris yra generuojamas saugiu kriptografiniu įrenginiu, būtų išimamas iš šio įrenginio tik tam, kad būtų įterptas į kortelę;

b) kad kortelės privatusis raktas, generuojamas saugiu kriptografiniu įrenginiu, būtų pašalintas iš tokio įrenginio iškart po jo išėmimo iš įrenginio ir įterpimo į kortelę;

c) jų pasirinkta įranga užtikrina, kad privačiuosius raktus įterpus į kortelę jų nebebūtų galima iš kortelės išimti.

6.2.4. Įrangos privačiųjų raktų apsauga ir saugojimas. Transporto priemonių blokai (VU)

Šiuo metu Lietuvoje nenaudojami.

6.2.5. Laikinas įrangos privatusis raktas ir archyvavimas

Laikini įrangos privatieji raktai negali būti nei kuriami, nei archyvuojami.

6.2.6. Įrangos viešųjų raktų archyvavimas

Visus sertifikuotus viešuosius raktus turi archyvuoti LT-MSCA.
Šiuo metu nėra archyvuotų privačiųjų raktų.

6.2.7. Raktų ir simetrinių raktų perdavimas į kriptografinį modulį arba iš jo

Privatūs valstybių narių raktai nėra persiunčiami iš kriptografinio modulio, nebent tais atvejais, kai sukuriama apsaugota atkuriama kopija specialiojoje kompiuterinėje laikmenoje.
Pagrindinio rakto importavimas ir eksportavimas yra leidžiamas tik atsarginei kopijai sukurti arba jai atkurti. K_{DSRC} ir $K_{M\text{-}WC}$ eksportavimas leidžiamas tik užšifruota forma ir tik kaip atsakas į patvirtiną užklausą iš LT-CP, kurią pateikė darbuotojas su patikėtu vaidmeniu užtikrinus dvigubą kontrolę.
Raktų perdavimo iš HSM aspektai nėra taikomi privačioms Card_MA ir Card-Sign raktų poroms. Šie raktai yra išskirtinai laikomi susijusiose tachografo kortelėse.

6.2.8. Privačiojo rakto laikymas kriptografiniame modulyje

Privatieji valstybių narių raktai, pagrindiniai raktai yra saugomi užšifruoti HSM įrenginiuose ir yra iššifruojami tik juos aktyvuojant.
Raktų saugojimo kriptografiniame modulyje aspektai nėra taikomi privačioms Card_MA ir Card_Sign raktų poroms. Šie raktai yra išskirtinai laikomi susijusiose tachografo kortelėse.

6.2.9. Privačiojo rakto aktyvavimo metodai

Privatusis valstybės narės raktas yra aktyvuojamas atsakingo LT-MSCA darbuotojo. LT-MSCA darbuotojas, atsakingas už rakto aktyvavimą, turi identifikuoti save su tinkama ID kortele. Prisijungimas prie „CA Konsolės“ reikalauja papildomo slaptažodžio apsaugos. Privačiojo rakto aktyvavimas yra ribojamas ERCA sertifikuoto valstybės narės viešojo rakto.
LT-MSA, LT-MSCA ir LT-MSCA PKI atsakingas asmuo turi dalyvauti rakto aktyvavimo procedūroje (Politikos 5.2 skyrius). Prisijungimui prie CA konsolės PKI grupės vykdytojai turi identifikuoti save su specialiai tam skirta lustine kortele ir slaptažodžiu.
Privatus valstybės narės raktas yra aktyvuojamas naudoti dvejų metų laikotarpiui, kaip tai apibrėžia ERCA. Raktas negali būti naudojamas pasibaigus jo galiojimui.
Privačiojo rakto aktyvavimo aspektai nėra taikomi privatiems Card_MA ir Card_Sign porų raktams. Atitinkamas viešasis raktas neturi galiojimo pabaigos.

6.2.10. Privačiojo rakto išjungimo metodai

Aktyvavus naują valstybės narės raktą, išjungiamas ankstesnis privatusis raktas. „CA konsolė“ palaiko tik vieno valstybės narės privačiojo rakto naudojimą vienu metu. LT-MSCA šiais atvejais nebeturi priėjimo prie išjungtų raktų.

Reikalaujamos rolės privačiųjų raktų aktyvavimui aprašomos šios Politikos 6.2.9 skyriuje.

6.2.11. Privačiojo rakto sunaikinimo metodai

Kai privatūs valstybių narių raktai išjungiami, jie turi būti sunaikinami HSM įrenginyje. Tokia pat tvarka, pasibaigus naudojimo ciklui, pagrindiniai simetriniai raktai taip pat yra sunaikinami.
Privačiųjų raktų sunaikinimas reiškia, kad visos raktų kopijos ir informacija, naudojama raktams atkurti ar regeneruoti, turi būti ištrintos iš visų saugojimo vietų.

6.3. Kitos raktų poros valdymo nuostatos

Įrangos privačiojo rakto galiojimo laikas turi atitikti Įgyvendinimo reglamento (ES) 2016/799 1C priedo 11 priedėlio reikalavimus.
Pasibaigus kortelės galiojimui, viešasis raktas turi būti archyvuojamas, o privatusis raktas turi būti sunaikintas be galimybės atkurti arba apsaugotas nuo galimybės jį vėl panaudoti.

6.3.1. Viešojo rakto archyvavimas

LT-MSCA viešojo rakto sertifikatas, kaip ir viešieji raktai, turi būti archyvuojami neribotam laikotarpiui.

6.3.2. Sertifikato ir raktų poros naudojimo laikotarpiai

Visų ERCA šakninių sertifikatų, su ERCA susietų sertifikatų ir LT-MSCA sertifikatų galiojimo laikotarpis turi atitikti Įgyvendinimo reglamento (ES) 2016/799 1C priedo 11 priedėlio reikalavimus.
Galiojimo ir naudojimo laikotarpiai nurodyti žemiau:
LT-MSCA_Card (privatusis raktas) – 2 metai;
LT-MSCA_Card (sertifikatas) – 7 metai + 1 mėnuo;
Card_MA (sertifikatas) – vairuotojo kortelė – 5 metai;
Card_MA (sertifikatas) – įmonės kortelė – 5 metai;
Card_MA (sertifikatas) – kontrolės kortelė – 2 metai;
Card_MA (sertifikatas) – dirbtuvės kortelė – 1 metai;
Card_Sign (sertifikatas) – vairuotojo kortelė – 5 metai + 1 mėnuo;
Card_Sign (sertifikatas) – dirbtuvės kortelė – 1 metai + 1 mėnuo;
$K_{M\text{-}WC}$ – 17 metų (galiojimas prasideda metai prieš EUR šakninio rakto poros galiojimo pradžią);
K_{DSRC} – 17 years (galiojimas prasideda metai prieš EUR šakninio rakto poros galiojimo pradžią).
Privatieji raktai negali būti naudojami pasibaigus privačiojo rakto naudojimo laikotarpiui.
Sertifikato įsigaliojimo data nurodo sertifikato galiojimo pradžios datą ir laiką. Tai turi būti data, kada LT-MSCA išdavė sertifikatą.
Atitinkamos vairuotojo kortelės ar dirbtuvės kortelės Card_MA ir Card_Sign sertifikatai turi turėti tą pačią sertifikato galiojimo datą.
Card_MA.SK ir Card_Sign.SK naudojimo laikas turi būti toks pat kaip atitinkamo sertifikato galiojimo laikas.

6.4. Aktyvinimo duomenys

6.4.1. Aktyvinimo duomenų generavimas ir instaliavimas

Aktyvuojant programinę įrangą, kurioje yra valdomi LT-MSCA privatieji sertifikavimo raktai, reikalingas ne mažiau kaip dviejų operatorių, kurių autentiškumą nustato sistema, bendradarbiavimas.
CA ir personalizavimo sistemų saugumo lygis neprivalo būti formaliai nustatomas, jeigu sistemos atitinka šiame skyriuje nustatytus reikalavimus.

6.4.2. Aktyvavimo duomenų apsauga

LT-MSCA ir LT-CP PKI vykdytojo patikėto vaidmens savininkas, turintis vienos ar kelių HSM įrenginio duomenų aktyvavimo dalis, visą laiką saugo šiuos duomenis uždarus, išskyrus atvejus, kai reikia aktyvuoti ar išjungti HSM įrenginį.

6.4.3. Kiti aktyvavimo duomenų aspektai

Asmenys, kontroliuojantys LT-CP raktus, turi save autentifikuoti HSM įrenginyje. Autentifikavimas turi būti atliekamas pasitelkiant tinkamas priemones (pvz., keturių akių principas).

6.5. Kompiuterių saugumo reikalavimai

LT-MSCA ir LT-CP užtikrina, kad informacinė sistema veiktų saugiai ir korektiškai, esant minimaliai gedimų rizikai. Ypač:

a) sistemos ir informacijos integralumas būtų apsaugotas nuo virusų, savavališkos ir nesankcionuotos programinės įrangos;

b) žala saugumui būtų minimizuota atliekant reguliarius sistemos patikrinimus.

LT-MSCA ir LT-CP sistema turi turėti pakankamai priemonių, kad galėtų atskirti Politikoje aprašytus vaidmenis.

Saugumo valdymo priemonės turi apimti galimybę sekti visus individualius veiksmus, galinčius turėti įtakos LT-MSCA sertifikatų išdavimui.

Informacines technologijas naudojančiuose kompiuteriuose turi būti įdiegtos saugumo priemonės.

Visi Politikoje aptariami saugumo reikalavimai taikomi ir galimiems subrangovams, kurie vykdytų LT-MSCA ir LT-CP funkcijas.

Techninės kompiuterių saugos priemonės turi būti aprašytos LT-MSCA ir LT-CP veiklos nuostatuose (PS).

6.6. Nuolatinio tikrinimo stebėsenos kontrolė

LT-MSCA ir LT-CP naudoja patikimas sistemas ir produktus, kurie yra apsaugoti nuo modifikavimo. Kiekviename bet kurio sistemos plėtojimo projekto rengimo ir reikalavimų nustatymo etape LT-MSCA ir LT-CP atlieka saugumo reikalavimų analizę arba tokia analizė atliekama LT-MSCA ir LT-CP vardu, siekiant užtikrinti, kad informacines technologijas naudojančiose sistemose būtų integruotos saugumo priemonės.

Sukuriamos visų operacinės programinės įrangos versijų, modifikacijų ir avarinių programinės įrangos pataisymų pakeitimų kontrolės procedūros. Pakeitimų valdymo procedūros turi būti dokumentuojamos ir naudojamos bet kokiems operacinei programinei įrangai skirtiems išleidimams, modifikacijoms ir (avarinių) programinės įrangos taisymams.

6.7. Tinklo saugos kontrolės priemonės

Siekiant apsaugoti LT-MSCA ir LT-CP vidinio kompiuterinio tinklo domenus nuo išorinio kompiuterinio tinklo domenų, prieinamų trečiosioms šalims, diegiamos kontrolės priemonės (ugniasienės).

Svarbūs duomenys turi būti apsaugomi, jeigu jais keičiamasi kompiuteriniais tinklais, kurie nėra saugūs.

6.8. Laiko žyma

Laiko žyma turi būti naudojama kiekvienam registruotam įvykiui sistemos įvykių žurnale. LT-MSCA veiklos nuostatuose (PS) turi būti apibrėžta, kaip laikas sinchronizuojamas ir patvirtinamas.

7. Sertifikato, CRL ir OCSP struktūra

Skaitmeninių tachografų sertifikatai naudojami tik tachografų sistemos viduje.

7.1. Sertifikato struktūra

Visi sertifikatai turi atitikti Įgyvendinimo reglamento (ES) 2016/799 1C priedo 11 priedėlyje ir 1 priedėlyje nurodytą struktūrą.

7.2. Atšauktų sertifikatų sąrašas (CRL)

LT-MSCA tachografo kortelių sertifikatai, aprašyti dokumente, niekada nepanaikinami ar nesustabdomi. Remiantis tuo, CRL nebus saugoma ir skelbiama. ERCA informacijai išduotų sertifikatų statusas gali būti peržiūrėtas internetinėje svetainėje https://dtc.jrc.ec.europa.eu/.

7.3. Interaktyvusis sertifikatų tikrinimo protokolas (OCSP)

OCSP nenaudojamas.

8. Atitikties auditas ir kiti vertinimai

LT-MSA yra atsakinga už tai, kad būtų atliktas LT-MSCA ir LT-CP auditas. LT-MSA oficialiai tvirtina audito rezultatus. LT-MSA praneša audito rezultatus ir pateikia audito ataskaitą anglų kalba ERCA.

8.1. Vertinimo dažnumas ir aplinkybės

Pirmasis MSCA ir CP, veikiančių pagal Politiką, bei jų sertifikavimo ir personalizavimo procesų auditas atliekamas per 12 mėnesių nuo veiklos pradžios. MSA, iš anksto pateikusi pranešimą, turi teisę atlikti neplanuotą auditą.
Prieš pradedant vykdyti veiklą, kuriai taikoma ši sertifikavimo politika, LT-MSA atlieka išankstinį įvertinimą, kuris parodytų, kad organizacija gali veikti pagal sertifikavimo politikos keliamus reikalavimus.

8.2. Vertintojo tapatybė / kvalifikacija

MSA atlieka auditą pati arba auditui atlikti samdo kitą instituciją / įmonę. MSA pripažįsta kompetentingos institucijos atliktą auditą.
Paskirtas vertintojas turi būti nepriklausoma įmonė, atliekanti auditus vadovaudamasi įstatymų ir teisės aktų nuostatomis.
Kad galėtų atlikti konkrečius auditus, vertintojas turi būti akredituotas atsakingos akreditacijos įstaigos. Svarbu tai, kad vertintojas turi turėti pakankamas žinias ir pageidautina, kad turėtų akreditaciją:

- atlikti informacinių sistemų saugumo auditus
- vertinti PKI ir kriptografines technologijas
- vertinti PKI programinės įrangos veikimą;
- įgyvendinti Europos Komisijos politiką ir reglamentus.

Bet kuris asmuo, pasirinktas ar siūlomas atlikti atitikties auditą, turi būti patvirtintas LT-MSA.

8.3. Vertintojo ryšys su įvertintu subjektu

Vertintojas turi būti nešališkas ir susietas bet kokiais ryšiais su vertinamuoju objektu.
Vertintojas negali būti vertinančios įmonės dalyvis ir / arba valdymo organų narys;
Vertintojas negali būti susijęs šeimos, artimos giminystės arba svainystės ryšiais su vertinamuoju.
Be anksčiau aprašytų draudimų dėl interesų konflikto, vertintojas turi sutartinius santykius su LT-MSA ir LT-MSCA dėl audito atlikimo, tačiau kitais būdais vertintojas turi būti nepriklausomas.
Vertintojas turi išlaikyti aukštus etikos standartus, kuriais užtikrina nešališkus ir nepriklausomus profesinius sprendimus, kuriems licenciją išdavusi institucija gali taikyti drausmines priemones.

8.4. Audito objektai

Auditas turi apimti atitiktį vykdomajai Politikai ir susijusias procedūras bei metodus, kuriuos dokumentavo audituojama organizacija. Atitikties audito apimtis yra šiuose dokumentuose aprašytų techninių, procedūrinių ir personalo priemonių įgyvendinimas. Keletas audito sričių:

- Identifikavimo ir autentifikavimo procedūros
- Veiklos funkcijos / paslaugos
- Organizavimas ir valdymas
- Personalo parengimas
- Fizinės, procedūrinės ir personalo apsaugos kontrolė
- Techninės apsaugos kontrolė

Įvertinus audito įrašus, turi būti nustatyta, ar yra galimi audituojamos organizacijos sistemų saugumo trūkumai. Nustatomi (galimi) trūkumai turi būti išspręsti. Audito įvertinimas ir rasti galimi trūkumai yra registruojami.
Audito metu parengiama audito ataskaita, kurioje apibrėžiami veiksmai su įgyvendinimo tvarkaraščiu, reikalingi užtikrinti šios Politikos reikalavimų vykdymą.
Audito metu taip pat atsižvelgiama į kitų paslaugas teikiančių agentūrų veiklą.

8.5. Veiksmai, kurių imamasi pažeidimų atvejais

Jeigu audito metu aptinkama trūkumų ir neatitikimų, MSA imasi atitinkamų priemonių priklausomai nuo jų rimtumo.
Audito metu nenustačius akivaizdžių neatitikimų, kitas auditas gali būti atliekamas per 24 mėnesius. LT-MSA ir LT-MSCA susitaria su vertintoju dėl būtinų veiksmų ir laikotarpio, per kurį turi būti pataisyti ar pašalinti esami neatitikimai. Abi pusės kartu prižiūri, kad būtų sėkmingai pradėti ir užbaigti reikalingi veiksmai.
Atlikus būtinus veiksmus, kitas auditas turėtų būti atliktas per 12 mėnesių laikotarpį.

8.6. Vertinimo rezultatų skelbimas

Audito rezultatai, laikantis saugumo statuso lygio, prieinami pateikus prašymą LT-MSA. Faktinės audito ataskaitos neteikiamos kitiems juridiniams asmenims, jeigu jų poreikis nėra pagrįstas.
LT-MSA išsiunčia visas auditų ataskaitas su aktualiais audito rezultatais ERCA. Šiose ataskaitose įtraukiamas rastų neatitikimų skaičius bei neatitikimų pobūdis. ERCA paprašius, LT-MSA išsiunčia visus atitikties audito rezultatus ERCA.

9. Kitos nuostatos

Šios Politikos nuostatos aiškinamos pagal Europos Sąjungos ir Lietuvos Respublikos teisės aktus.
Informacijos konfidencialumo klausimus reglamentuoja:

a) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).

b) Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

c) Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymas;

d) Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo patvirtinimo“;

e) Lietuvos standartas LST ISO/IEC 27001:2013. Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai (tapatus ISO/IEC 27001:2013), 2013 m. gruodžio 2 d.;

9.1. Mokesčiai

9.2. Finansinė atsakomybė

Finansiniai įsipareigojimai nustatyti šalių sutartyse.

9.2.1. MSCA ir CP turto valdymas

LT-MSCA ir LT-CP užtikrina, kad fizinis priėjimas prie patikimų sistemų ir itin svarbių paslaugų būtų kontroliuojamas ir būtų minimizuota jos turto fizinė rizika, ypač jei:

a) fizinis priėjimas prie įrangos, susijusios su raktų, sertifikatų generavimu ir galiojimo panaikinimo valdymu, suteikiamas tik tinkamai identifikuotiems ir įgaliotiems asmenims;

b) įgyvendinamos kontrolės priemonės, siekiant išvengti:

- turto praradimo, sugadinimo arba pažeidimo ir verslo trukdžių,
- informacijos ir informacijos apdorojimo įrangos pažeidimo ar vagystės;

c) įranga, susijusi su raktų, sertifikatų generavimu, galiojimo sustabdymo ir panaikinimo valdymu, naudojama saugioje aplinkoje, kuri fiziškai apsaugo sistemas ir paslaugas nuo saugumo pažeidimo dėl neteisėto priėjimo prie sistemų ar duomenų;

d) fizinė apsauga įvedama, sukuriant aiškiai identifikuotus raktų generavimo, sertifikatų generavimo ir galiojimo panaikinimo valdymo saugumo parametrus.

Įgyvendinamos fizinio ir aplinkos saugumo kontrolės priemonės, siekiant apsaugoti įrangos saugojimo vietos sistemos išteklius, pačios sistemos išteklius ir įrangą, kuri yra naudojama jų darbui palaikyti. LT-MSCA veiklos nuostatuose (PS) nustatoma fizinė priėjimo kontrolė, apsauga nuo stichinių nelaimių, priešgaisrinės apsaugos veiksniai, palaikančių priemonių gedimai, apsauga nuo vagystės, įsilaužimo ir įėjimo, duomenų atkūrimas nelaimių atvejais ir pan.

9.3. Juridinių asmenų informacijos privatumas

Visi privatieji raktai, kuriuos naudoja ir tvarko LT-MSCA ir LT-CP, atlikdami savo funkcijas pagal Politiką yra konfidencialūs.

Audito žurnalo įrašai ir duomenys negali būti platinami, išskyrus teisės aktų nustatytus atvejus, kai to pareikalauja kompetentingos institucijos.

Bet kuri informacija, susijusi su juridiniu asmeniu, kurią turi LT-CIA, LT-MSCA, LT-CP arba subrangovai / paslaugų agentūros ir kuri nėra pateikiama ant išduotų kortelių ar sertifikatuose, yra laikoma konfidencialia ir negali būti atskleista be išankstinio kortelės naudotojo sutikimo arba (kai taikoma) be išankstinio kortelės naudotojo darbdavio arba atstovo sutikimo, išskyrus teisės aktų nustatytus atvejus, kai to pareikalauja kompetentingos teisėsaugos institucijos.

Konfidencialia informacija taip pat laikomi:

- asmens duomenys (pvz., darbuotojų, komponentų gamintojų arba ERCA atstovų);
- privatieji raktai;
- simetriniai pagrindiniai raktai;
- įmonės ar gamybos duomenys;
- audito žurnalai (nebent prieiga reikalinga pagal įstatymus, reglamentus ar CP ar CPS nuostatas);
- išsami PKI valdymo dokumentacija;
- vidaus ar išorės auditorių audito ataskaitos.

9.4. Asmenų informacijos privatumas

Sertifikatai nėra laikomi konfidencialiais.

Asmens identifikavimo informacija arba kita informacija, susijusi su fiziniu ar juridiniu asmeniu, pateikta ant kortelių, nėra konfidenciali, išskyrus teisės aktų nustatytus atvejus.

Bet kuri informacija, susijusi su fiziniu asmeniu, kurią turi LT-CIA, LT-MSCA, LT-CP arba subrangovai / paslaugų agentūros ir kuri nėra pateikiama ant išduotų kortelių ar sertifikatuose, yra laikoma konfidencialia ir negali būti atskleista be išankstinio kortelės naudotojo sutikimo arba (kai

taikoma) be išankstinio kortelės naudotojo darbdavio arba atstovo sutikimo, išskyrus teisės aktų nustatytus atvejus, kai to pareikalauja kompetentingos teisėsaugos institucijos.

9.5. Intelektinės nuosavybės apsauga

Teisės į visus intelektinės nuosavybės objektus, kaip į Politikos vykdymo procese sukurtus rezultatus, jeigu tokie būtų sukurti, priklauso MSA maksimalia apimtimi, leidžiama teisės normų ir vadovaujantis Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymu.

9.6. Pareigos

LT-MSCA ir LT-CP įsipareigoja laikytis ERCA politikos nuostatų, taip pat šios Politikos taisyklių bei nuostatų.
Kortelės turėtojas įsipareigoja laikytis Lietuvos Respublikos teisės nuostatų, ypač tų, kurios nurodo tachografo kortelių naudojimo tvarką.
Bet kuris paslaugų teikėjas, paskirtas LT-MSA, LT-MSCA ar LT-CP, įsipareigoja laikytis ERCA politikos bei šios Politikos nuostatų.

9.7. Atsakomybės ir garantijų apribojimai

LT-MSA atsisako bet kokio pobūdžio įsipareigojimų ir garantijų, įskaitant bet kokias prekinio tinkamumo garantijas, bet kokią tinkamumo tam tikram tikslui garantiją bei bet kokią pateiktos informacijos tikslumo garantiją (išskyrus tai, jog informacija iš autentifikuoto šaltinio) ir atsisako bet kokios atsakomybės už neatsargumą ir tinkamos priežiūros trūkumą iš vartotojo ir susijusių šalių. LT-MSCA ir LT-CP įsipareigojimai ir garantijų užtikrinimas LT-MSA nustatomi pagal kontrakto ir sutarčių sąlygas. Visos kitos šių šalių garantijos yra neįtrauktos.

9.8. Atsakomybės apribojimai

LT-MSA, LT-MSCA, LT-CIA ir LT-CP atsakomybė yra ribojama tiek, kiek tai numato įstatymas.
Visų pirma LT-MSA, LT-MSCA, LT-CIA ir LT-CP nėra atsakingos už:
- nuostolius, patirtus naudojant sertifikatus ar raktų poras, pasireiškiančius dėl bet kokių kitų priežasčių, nei nurodyta šiame dokumente, PKI instrukcijoje ar pačiame sertifikate;
- nuostolius dėl *force majeure* aplinkybių.

LT-MSA, LT-MSCA, LT-CIA ir LT-CP bei jų darbuotojai atsako už nuostolius, padarytus pažeidus deramo patikrinimo reikalavimus (pvz., perduodant asmeninę informaciją ar PIN kodą kitiems asmenims).

9.9. Draudimai

Draudimų nėra.

9.10. Terminai ir nutraukimas

Politika įsigalioja kitą dieną nuo jos suderinimo su ES institucija ir patvirtinimo.

9.11. Individualūs pranešimai ir ryšiai su dalyviais

Bet kokia informacija, prašymai paaiškinti nuostatas, skundai, pranešimai ar kiti šalių susirašinėjimai vykdomi raštu, pasirašyti kvalifikuotu elektroniniu parašu. Dokumentai, adresuoti LTSA ir pasirašyti elektroniniu parašu, siunčiami el. paštu – ltsa@ltsa.lt.

9.12. Sertifikavimo politikos pakeitimų procedūros

9.12.1. Pakeitimai, atliekami apie tai neinformuojant

Vieninteliai pakeitimai, kurie gali būti padaryti Politikoje, apie tai neinformuojant, yra:
a) redakciniai pataisymai;
b) kontaktinių duomenų pakeitimai.

9.12.2. Pakeitimai, apie kuriuos informuojama

9.12.2.1. Pranešimas

Bet kuris Politikos punktas gali būti pakeistas, pranešus apie pakeitimus ERCA prieš 90 dienų. Punktų, kurie MSA sprendimu neturės reikšmingos įtakos didžiajai daugumai vartotojų arba susijusių šalių, besivadovaujančių Politika, pakeitimai gali būti atliekami, apie juos pranešus prieš 30 dienų.

9.12.2.2. Pastabų laikotarpis

Suinteresuoti vartotojai gali pateikti pastabas MSA per 15 dienų nuo pirminio pranešimo dienos.

9.12.2.3. Ką informuoti:

Informacija apie Politikos pakeitimus turi būti siunčiama:
a) LT-ERCA;
b) LT-MSCA ir LT-CP, taip pat paslaugų agentūroms.

9.12.2.4. Galutinio pranešimo apie pakeitimus laikotarpis

Jeigu, atsižvelgiant į pastabas, pasiūlytas pakeitimas yra modifikuojamas, pranešimas apie tokį pakeitimą pateikiamas ne vėliau kaip prieš 30 dienų iki pakeitimo įsigaliojimo.

9.12.3. Pakeitimai, dėl kurių reikia patvirtinti naują sertifikavimo politiką

Jeigu MSA nustato, kad Politikos pakeitimas turi reikšmingos įtakos dideliam Politikos vartotojų skaičiui, MSA pateikia pakoreguotą nacionalinę sertifikavimo politiką patvirtinti ERCA.

9.13. Ginčų nagrinėjimo tvarka

Politika vykdoma ir šalių ginčai, kilę dėl jos vykdymo, sprendžiami šalių susitarimu. Neišsprendus ginčų tarpusavio susitarimu, ginčai perduodami nagrinėti ir sprendimą priimti Europos institucijoms.

9.14. Reglamentuojantys teisės aktai

Politikos vykdymą, kūrimą, aiškinimą ir galiojimą reglamentuoja ES teisės aktai ir ERCA politika.

9.15. Atitiktis teisės aktams

Politika atitinka Reglamentą (ES) Nr. 165/2014 ir Įgyvendinimo reglamentą (ES) 2016/799. Jei Politika prieštarauja ES teisės aktams, taikomos ES teisės aktų nuostatos.

9.16. Papildomos sąlygos

9.16.1. Įrangos valdymas

Skaitmeninių tachografų sistemos įrangą sudaro:
a) kortelės;
b) transporto priemonės blokai (VU);
c) judesio jutikliai.

Skaitmeninių tachografų sistemos įrangą tvarko ir valdo šie subjektai:
a) LT-CIA (kortelių registravimas, atnaujinimas ir pan.);
b) LT-MSCA (sertifikatų, raktų generavimas);
c) LT-CP (vizualus ir elektroninis kortelių personalizavimas, platinimas, sunaikinimas);

MSA:
a) kontroliuoja skaitmeninių tachografų sistemos valdyme dalyvaujančių subjektų atliekamų funkcijų kokybę;
b) tvirtina LT-MSCA, LT-CP ir LT-CIA veiklos nuostatus (PS).

LT-CIA:
a) priima prašymus išduoti korteles;

b) tvarko kortelių turėtojų tapatybės duomenis (priima prašymus, patikrina pateiktus duomenis, įsitikina pareiškėjo tapatybe);
c) perduoda kortelių turėtojų tapatybės nustatymo duomenis LT-CP;
d) išduoda personalizuotas korteles;
e) perduoda PIN kodus dirbtuvės kortelių turėtojams;
f) tvarko baltąjį ir juodąjį kortelių sąrašus;
g) registruoja korteles ir saugo su kortelių išdavimu susijusius duomenis.

LT-CP:
a) įrašo kortelių turėtojų tapatybės nustatymo duomenis, kitus reikiamus duomenis į korteles;
b) įrašo raktus ir sertifikatus į korteles;
c) spausdina reikiamus duomenis ant kortelės;
d) perduoda personalizuotas korteles ir dirbtuvės kortelių PIN kodus LT-CIA.

LT-MSCA:
a) generuoja ir registruoja valstybės narės raktus;
b) generuoja ir registruoja kortelių sertifikatus;
c) registruoja Europos raktus ir sertifikatus;
d) pateikia valstybės narės raktus ERCA sertifikuoti;
e) perduoda kortelių sertifikatus LT-CP.

9.16.2. Kortelės

9.16.3. Kokybės kontrolė

LT-MSCA ir LT-CP funkcijos – užtikrinti, kad tik patvirtinto tipo kortelės bus personalizuojamos skaitmeninių tachografų sistemoje (Politikos 9.16.9 skyrius).

9.16.4. Prašymų išduoti korteles priėmimas

LT-CIA atlieka kortelių išdavimo funkciją. LT-CIA informuoja naudotojus apie kortelės naudojimo sąlygas. Ši informacija turi būti pateikiama lietuvių ir anglų kalbomis.
Pareiškėjas, kreipdamasis su prašymu išduoti kortelę ir atsiimdamas kortelę, sutinka su kortelės naudojimo sąlygomis.
Detaliau aprašyta LT-CIA veiklos nuostatuose (PS).

9.16.4.1. Asmens prašymas išduoti kortelę

Prašymo išduoti kortelę formą nustato MSA. Prašyme išduoti kortelę turi būti nurodyti tokie duomenys, kurie užtikrintų teisingą asmens identifikavimą.

9.16.4.2. Duomenys, apibūdinantys vairuotojo kortelę

Vairuotojo kortelę apibūdina šie duomenys:
a) asmens duomenys (vardas, pavardė, gimimo data);
b) asmens nuotrauka ir parašas;
c) vairuotojo pažymėjimo numeris.

9.16.4.3. Duomenys, apibūdinantys dirbtuvės kortelę

Dirbtuvės kortelę apibūdina šie duomenys:
a) dirbtuvės duomenys (dirbtuvės pavadinimas, adresas);
b) asmens nuotrauka ir parašas;
c) kortelės turėtojo duomenys (asmens vardas, pavardė).

9.16.4.4. Duomenys, apibūdinantys kontrolės kortelę

Kontrolės kortelę apibūdina kontrolės institucijos duomenys (kontrolės institucijos pavadinimas, adresas).

9.16.4.5. Duomenys, apibūdinantys įmonės kortelę

Įmonės kortelę apibūdina įmonės duomenys (įmonės pavadinimas, adresas, kodas).

9.16.4.6. Įsipareigojimas

Asmuo, pateikdamas LT-CIA prašymą išduoti kortelę, įsipareigoja, kad:

a) sutinka su kortelės naudojimo sąlygomis;

b) per visą kortelės galiojimo laikotarpį nuo kortelės išdavimo (kol pats kortelės turėtojas nepraneša LT-CIA):

- kortele negalėjo pasinaudoti joks pašalinis asmuo;
- visa informacija, tiesiogiai susijusi su kortele, kurią asmuo pateikė LT-CIA, yra teisinga;
- kortelė sąžiningai naudojama laikantis naudojimosi kortele apribojimų.

9.16.4.7. CIA patvirtinimo sąlygos, taikomos vairuotojo kortelei

Vairuotojo kortelė išduodama tik fiziniams asmenims, turintiems nuolatinę gyvenamąją vietą prašymo išduoti vairuotojo kortelę pateikimo valstybėje.
LT-CIA turi įsitikinti, kad asmuo, besikreipiantis su prašymu išduoti vairuotojo kortelę, neturi galiojančios vairuotojo kortelės, išduotos kitoje valstybėje narėje, ir turi galiojantį atitinkamos kategorijos vairuotojo pažymėjimą.

9.16.5. Kortelių atnaujinimas dėl besibaigiančios galiojimo datos

Dirbtuvės kortelė išduodama tik patvirtintų dirbtuvių darbuotojams.
Įmonės kortelė išduodama tik įmonei, vykdančiai vežimo veiklą.
Kontrolės kortelė išduodama tik kompetentingų kontrolės institucijų pareigūnams.
LT-CIA nustato tvarką, kuri kortelės turėtojui primintų apie artėjančią kortelės galiojimo termino pabaigą. Prašymas atnaujinti kortelę pateikiamas ta pačia tvarka kaip ir prašymas išduoti naują kortelę. (Politikos 9.16.4 skyrius).
LT-CIA išduoda naują kortelę per 15 (penkiolika) darbo dienų nuo prašymo atnaujinti vairuotojo, įmonės ar kontrolės kortelę pateikimo dienos ir per 5 (penkias) darbo dienas nuo prašymo atnaujinti dirbtuvės kortelę pateikimo dienos.

9.16.5.1. Vairuotojo kortelės

Vairuotojas pateikia prašymą atnaujinti kortelę ne vėliau kaip likus 15 (penkiolikai) dienų iki kortelės galiojimo termino pabaigos (Reglamento (ES) Nr. 165/2014 28 straipsnio 1 dalis).
LT-CIA privalo išduoti naują kortelę iki to laiko, kol pasibaigs senosios kortelės galiojimo terminas, jeigu prašymas atnaujinti kortelę buvo pateiktas laiku (Reglamento (ES) Nr. 165/2014 28 straipsnio 3 dalis).

9.16.5.2. Dirbtuvės kortelės

Pareiškėjas pateikia prašymą atnaujinti kortelę ne vėliau kaip likus 15 (penkiolikai) dienų iki kortelės galiojimo termino pabaigos.
LT-CIA privalo išduoti naują kortelę per 5 (penkias) darbo dienas nuo prašymo atnaujinti kortelę pateikimo dienos (Reglamento (ES) Nr. 165/2014 25 straipsnio 2 dalis).

9.16.5.3. Įmonės kortelės

Pareiškėjas pateikia prašymą atnaujinti kortelę ne vėliau kaip likus 15 (penkiolikai) dienų iki kortelės galiojimo termino pabaigos.
LT-CIA privalo išduoti naują kortelę iki to laiko, kol pasibaigs senosios kortelės galiojimo terminas, jeigu prašymas atnaujinti kortelę buvo pateiktas laiku.

9.16.5.4. Kontrolės kortelės

Pareiškėjas pateikia prašymą atnaujinti kortelę ne vėliau kaip likus 15 (penkiolikai) dienų iki kortelės galiojimo termino pabaigos.
LT-CIA privalo išduoti naują kortelę iki to laiko, kol pasibaigs senosios kortelės galiojimo terminas, jeigu prašymas atnaujinti kortelę buvo pateiktas laiku.

9.16.6. Kortelių atnaujinimas dėl duomenų pasikeitimo

Pasikeitus vairuotojo duomenims (vardui, pavardei, asmens kodui, gimimo datai) ar įmonės registracijos duomenims (įmonės pavadinimui, kodui, adresui), pateikiamas prašymas atnaujinti kortelę. Išdavusi naują kortelę LT-CIA paima ankstesnę kortelę ir siunčia ją išdavusios valstybės LT-CIA. (Įgyvendinimo reglamento (ES) 2016/799 30 straipsnio 3 dalis).
Vairuotojui persikėlus gyventi į kitą valstybę narę ir pasikeitus jo duomenims (vardui, pavardei, asmens kodui, gimimo datai) prašymas pateikiamas vadovaujantis naujos kortelės išdavimo taisyklėmis.
LT-CIA išduoda naują kortelę per 15 (penkiolika) darbo dienų nuo prašymo atnaujinti vairuotojo, įmonės ar kontrolės kortelę pateikimo dienos ir per 5 (penkias) darbo dienas nuo prašymo atnaujinti dirbtuvės kortelę pateikimo dienos.

9.16.7. Pamestų, pavogtų ir blogai veikiančių kortelių pakeitimas

Pamestos ir pavogtos kortelės įtraukiamos į juodąjį kortelių sąrašą, su kuriuo gali susipažinti visų valstybių narių kompetentingos institucijos.
Blogai veikiančios kortelės grąžinamos CIA. Kortelės pripažįstamos negaliojančiomis ir įtraukiamos į juodąjį kortelių sąrašą. Kortelės tiek fiziškai, tiek elektroniniu būdu sunaikinamos.
Jeigu kortelė yra pamesta, pavogta arba blogai veikianti, kortelės turėtojas turi kreiptis į CIA su prašymu pakeisti kortelę per 7 (septynias) dienas nuo pametimo dienos (Reglamento (ES) Nr. 165/2014 29 straipsnio 4 dalis).
Jeigu kortelės turėtojas laikosi šių reikalavimų, CIA išduoda pakeistą kortelę, turinčią naujus raktus ir sertifikatą per 5 (penkias) darbo dienas nuo prašymo pakeisti kortelę gavimo dienos (Reglamento (ES) Nr. 165/2014 29 straipsnio 4 dalis).
Pakeista kortelė galioja tiek pat kiek ir senoji kortelė. Jeigu keičiamos kortelės galiojimo terminas yra trumpesnis kaip šeši mėnesiai, CIA vietoj pakeistos kortelės išduoda atnaujinto laikotarpio kortelę (Įgyvendinimo reglamento (ES) 2016/799 1C priedo 7 skyrius).

9.16.8. Prašymų registravimas

Registruoti prašymus duomenų bazėje yra LT-CIA funkcija.

9.16.9. Kortelių personalizavimas

Kortelės personalizuojamos ir vizualiu, ir elektroniniu būdu. Jei šias paslaugas atlieka subrangovai / paslaugų agentūros, tai nepanaikina LT-MSCA ir LT-CP atsakomybės.

9.16.9.1. Vizualus kortelių personalizavimas

Kortelės vizualiu būdu personalizuojamos laikantis Įgyvendinimo reglamento (ES) 2016/799 1C priedo 4 skyriaus nuostatų.

9.16.9.2. Asmens duomenų įrašymas

Asmens duomenys įrašomi į kortelę pagal Įgyvendinimo reglamento (ES) 2016/799 1C priedo 2 priedėlio 4 skyriaus taisykles, atsižvelgiant į kortelės tipą.

9.16.9.3. Rakto įrašymas

Privatusis raktas įrašomas į kortelę fiziškai saugioje aplinkoje. Šis procesas turi būti kontroliuojamas. Aplinka, kurioje generuojami raktai, turi būti saugi, kad joks pašalinis asmuo negalėtų valdyti generuoto privačiojo rakto.

9.16.9.4. Sertifikato įrašymas

Sertifikatas įrašomas į kortelę prieš ją išduodant asmeniui.

9.16.9.5. Kokybės kontrolė

Siekiant užtikrinti, kad vizuali informacija ant kortelių ir elektroninė informacija, įrašyta išduotuose sertifikatuose ir kortelėse, atitiktų viena kitą ir kortelės savininko tapatybės duomenis, sukuriamos specialios dokumentuose aprašytos procedūros.
Procedūros aprašomos LT-CP veiklos nuostatuose (PS).

9.16.9.6. Neišduotų kortelių pripažinimas negaliojančiomis (sunaikinimas)

Visos personalizavimo metu pažeistos, sugadintos arba dėl kitų priežasčių neparuoštos ir neišplatintos kortelės fiziškai ir elektroniniu būdu sunaikinamos (pripažįstamos negaliojančiomis).
Visos sunaikintos (pripažintos negaliojančiomis) kortelės registruojamos sunaikintų kortelių sąraše.

9.16.10. Kortelių registravimas ir duomenų saugojimas

CP atsakinga už duomenų, kuri kortelė ir kortelės numeris yra suteiktas kuriam asmeniui, sąryšingumą. CP perduoda šiuos duomenis į CIA kortelių duomenų bazę.

9.16.11. Kortelių išdavimas asmenims

CIA atsako už kortelių išdavimą asmenims.
Personalizavimas turi būti atliekamas taip, kad personalizuotą kortelę kaip galima trumpiau reikėtų saugiai laikyti iki jos išdavimo asmeniui. Kortelės turi būti saugomos specialiame seife.
Personalizuotos ir nepersonalizuotos kortelės turi būti laikomos atskirai. Personalizuotos kortelės nedelsiant išplatinamos asmenims, kad būtų sumažinta jų praradimo rizika.
Kortelės išdavimo metu asmuo privalo pateikti asmens tapatybę patvirtinančius dokumentus.
Asmuo savo parašu patvirtina kortelės gavimą.

9.16.12. Autentiškumo nustatymo kodų (PIN) generavimas

Šio skyriaus nuostatos taikomos tik dirbtuvės kortelėms.
Dirbtuvės kortelės turi PIN kodą, kuris skirtas nustatyti kortelės autentiškumą (Įgyvendinimo reglamento (ES) 2016/799 1C priedo 11 priedėlis).
PIN kodą sudaro ne mažiau kaip 4 (keturi) skaitmenys (Įgyvendinimo reglamento (ES) 2016/799 1C priedo 13 priedėlis).

9.16.12.1. PIN kodų generavimas

PIN kodai generuojami saugioje aplinkoje, saugiai perkeliami į dirbtuvės kortelę ir tiesiogiai atspausdinami į PIN kodų vokus. PIN kodai negali būti saugomi kompiuterinėje sistemoje taip, kad galima būtų susieti PIN kodą su konkrečiu asmeniu. PIN kodų generavimo sistema turi atitikti ITSEC E3, CC EAL4 arba analogiškus saugumo reikalavimus.

9.16.12.2. PIN kodų platinimas

PIN kodai įteikiami asmeniškai.
PIN kodai ir dirbtuvės kortelės negali būti įteikiami konkrečiam asmeniui tame pačiame voke. Šie saugumo reikalavimai reikalingi tam, kad PIN kodas ir dirbtuvės kortelė nebūtų susieti tarpusavyje iki to laiko, kol jie bus išduoti konkrečiam asmeniui.

9.16.13. Kortelių sunaikinimas

Kortelė ir joje įrašyti raktai sunaikinami visam laikui. Sprendimą sunaikinti priima LT-MSA arba LT-CIA, o pačią sunaikinimo operaciją atlieka LT-CIA arba jos pasirinkti subrangovai / paslaugų agentūros.
Kortelių sunaikinimas atliekamas šiam procesui pritaikyta įranga. Sunaikinimo procese turi būti patvirtinta, kad kortelės funkcijos ir raktai yra sunaikinti. Kortelė sunaikinama ir fiziškai.
Kortelių sunaikinimas registruojamas kortelių duomenų bazėje. Sunaikintos kortelės duomenys įtraukiami į sunaikintų kortelių sąrašą.

9.17. Kitos sąlygos

9.17.1. Bendri CP / MSCA, subrangovų ir paslaugų teikėjų aspektai

Įrangos (kortelių) inicializavimas ir personalizavimas turi būti vykdomi fiziškai saugioje ir kontroliuojamoje aplinkoje. Patekimas į šią aplinką turi būti griežtai reguliuojamas, individualiai kontroliuojamas. Personalizavimo sistemą gali valdyti ne mažiau kaip du asmenys. Patekimas į aplinką ir sistemoje atlikti veiksmai turi būti registruojami žurnale.
Rakto negalima paimti iš saugios sistemos.
Jokios svarbios informacijos, susijusios su kortelių personalizavimu, negalima paimti iš saugios aplinkos.
Organizacijos (subrangovai / paslaugų teikėjai), atliekančios raktų generavimą ir kortelių personalizavimą daugiau nei vienos valstybės narės vardu, turi griežtai atskirti procesus, vykdomus kiekvienai iš jų. Kiekvienos valstybės narės atlikti veiksmai turi būti registruojami žurnale, kurį atitinkama MSA turi turėti galimybę peržiūrėti.
LT-MSCA, LT-CP, paslaugų teikėjai: atliktų veiksmų žurnale turi būti pateiktos nuorodos į atitinkamos įrangos numerius ir sertifikatus. Atitinkama MSA turi turėti galimybę peržiūrėti veiksmų žurnalą.
LT-MSCA, LT-CP, subrangovai, paslaugų teikėjai: atliktų veiksmų žurnale turi būti pateiktos nuorodos į atitinkamos įrangos numerius ir sertifikatus.