PATVIRTINTA
Valstybės įmonės Registrų centro
generalinio direktoriaus
2020 m. balandžio … d. įsakymu
Nr.

REGISTRŲ CENTRO SERTIFIKAVIMO VEIKLOS NUOSTATAI

Unikalus objekto ID (OID):	**1.3.6.1.4.1.30903.1.2.6**
Versija:	6.2
Galioja nuo:	2020-04-...

2020-04-...

TURINYS

RCSC sertifikavimo veiklos nuostatų keitimų istorija:

Versija	Data	Aprašas
0.1	2008-05-19	Nuostatų projektas
1.0	2008-06-09	Pirma versija
1.1	2009-03-05	Atliktos neesminės korekcijos ir pašalinti netikslumai sertifikatų profilių aprašuose.
2.0	2009-03-05	CPS papildyti reikalavimais naujiems RCSC sudaromiems ir tvarkomiems sertifikatams.
2.1	2010-11-24	Papildytas sertifikatų naudotojų sąrašas ir papildyti sertifikatų profiliai
2.2.	2013-05-15	Atliktos neesminės korekcijos
3.0	2017-01-09	CPS papildytas SIM įrašymo procedūros aprašu, papildyti CPS atitikimo CA veiklai tikrinimo atvejai bei patikslinti veiksmai veiklos nutraukimo atveju.
4.0	2017-04-28	Atnaujinta pagrindinė dalis CPS nuostatų vadovaujantis Europos parlamento ir tarybos reglamente Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB įtvirtintais naujais teisiniais bei techniniais reikalavimais.

5.0	2017-07-11	Atnaujinta dalis CPS nuostatų vadovaujantis Europos parlamento ir tarybos reglamente Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB įtvirtintais naujais teisiniais bei techniniais reikalavimais. Patikslintos CA bei RA funkcijos, detalizuota incidentų registravimo bei pranešimo apie juos tvarka, numatyti RA veiklos bei prisiimtų įsipareigojimų tikrinimo aspektai.
5.1	2017-10-17	Pakeitimai.
5.2	2019-05-23	Pakeitimai.
6.0	2019-05-31	Pakeitimai po Lietuvos Respublikos ryšių reguliavimo tarnybos pastabų.
6.1	2019-12-16	Pakeitimai po Lietuvos Respublikos ryšių reguliavimo tarnybos pastabų.
6.2	2020-04-...	Pakeitimai po Lietuvos Respublikos ryšių reguliavimo tarnybos pastabų.

Dokumento tvirtinimas:

Dokumento rengimas	**Pavardė**	**Data**	**Parašas**
Dokumentą tvirtino	Generalinis direktorius Saulius Urbanavičius	2020-04-...	

1. ĮVADAS

Valstybės įmonė Registrų centras (toliau – Registrų centras) yra įsteigta 1997 m. Įmonės steigėjas – Lietuvos Respublikos Vyriausybė. Įmonės savininko teises ir pareigas įgyvendinanti institucija yra Lietuvos Respublikos ekonomikos ir inovacijų ministerija. Įmonė tvarko Nekilnojamojo turto kadastrą ir registrą, Adresų registrą, Juridinių asmenų registrą, Gyventojų registrą, Hipotekos registrą, Turto arešto aktų registrą, Testamentų registrą, Vedybų sutarčių registrą, Įgaliojimų registrą, Neveiksnių ir ribotai veiksnių asmenų registrą, Sutarčių registrą, kuria, įgyvendina, plėtoja ir tvarko su šiais bei kitais registrais susijusias informacines sistemas, tvarko registrų archyvus.

Registrų centras paskirtų funkcijų efektyviam vykdymui naudoja modernias informacines technologijas. Registrų centras yra įkūręs Registrų centro Sertifikatų centrą (toliau – RCSC) – kvalifikuotų patikimumo užtikrinimo paslaugų, t. y. **kvalifikuotų elektroninių parašų ir kvalifikuotų elektroninių spaudų sertifikatų (toliau – sertifikatai)** sudarymo, tvarkymo bei kvalifikuotų elektroninių laiko žymų paslaugų teikimo padalinį.

Šie RCSC sertifikavimo veiklos nuostatai (toliau – CPS) apibrėžia sertifikavimo tarnybos, t. y. RCSC (toliau – CA) veiklos taisykles techniniu, procedūriniu ir personalo politikos klausimais.

1.1. Apžvalga

CPS detaliai apibrėžia CA veiklą sudarant bei tvarkant:

1. kvalifikuotus elektroninio parašo sertifikatus, skirtus elektroniniams parašams tvirtinti;

2. autentifikavimo sertifikatus, skirtus asmens atpažinimui elektroninėje erdvėje;

3. kvalifikuotus elektroninio spaudo sertifikatus, patvirtinančius, kad elektroninį dokumentą išdavė juridinis asmuo, užtikrinant dokumento kilmę ir vientisumą.

CA teikiamos patikimumo užtikrinimo paslaugos bei jas sudarančios dalys (pavyzdžiui: SIM, lustinės kortelės ir kt.) dėl savo prigimties bei pobūdžio negali būti specialiai pritaikytos negalią turintiems žmonėms, tačiau Registrų centro filialai yra įsteigti visoje Lietuvoje, patalpos pritaikytos priimti bei aptarnauti negalią turinčius žmones.

Sertifikatai sudaromi tik asmenims, naudojantiems CA teikiamą saugų arba kvalifikuotą elektroninio parašo kūrimo įtaisą (toliau – SSCD/QSCD).

CPS parengti remiantis šiais dokumentais, kurių RCSC laikosi teikdami paslaugas:

a) 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB (toliau – eIDAS) naujausia redakcija;

b) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/6/EB (toliau – Bendrasis asmens duomenų apsaugos reglamentas) naujausia redakcija;

c) Lietuvos Respublikos teisės aktai reglamentuojantys patikimumo užtikrinimo paslaugas, tiek kiek neprieštarauja a) punkte nurodytam teisės aktui;

d) 2016 m. balandžio 25 d. Komisijos įgyvendinimo sprendimas (ES) 2016/650, kuriuo pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje 30 straipsnio 3 dalį ir 39 straipsnio 2 dalį nustatomi kvalifikuotų parašo ir spaudo kūrimo įtaisų saugumo vertinimo standartai;

e) 2015 m. gegužės 22 d. Komisijos įgyvendinimo reglamentas (ES) 2015/806, kuriuo nustatomos kvalifikuotų patikimumo užtikrinimo paslaugų ES pasitikėjimo ženklo formos specifikacijos;

f) Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymo naujausia redakcija;

g) Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo naujausia redakcija;

h) Lietuvos Respublikos 2016 m. vasario 18 d. nutarimas Nr. 144 „Dėl patikimumo užtikrinimo paslaugų priežiūros įstaigos ir įstaigos, atsakingos už nacionalinio patikimo sąrašo sudarymą, tvarkymą ir skelbimą, paskyrimo";

i) Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2018 m. birželio 21 d. įsakymas Nr.1V-588 „Dėl kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų ir kvalifikuotų patikimumo užtikrinimo paslaugų statuso suteikimo ir jų įrašymo į nacionalinį patikimą sąrašą bei kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų veiklos ataskaitų teikimo tvarkos aprašo patvirtinimo";

j) Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2018 m. spalio 26 d. įsakymas Nr. 1V-1055 „Dėl asmens tapatybės ir papildomų specifinių požymių tikrinimo išduodant kvalifikuotus elektroninio parašo, elektroninio spaudo, interneto svetainės tapatumo nustatymo sertifikatus tvarkos aprašo patvirtinimo";

k) Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2019 m. birželio 4 d. įsakymas Nr.1V-594 „Dėl Pranešimų apie patikimumo užtikrinimo paslaugų saugumo ir (ar) vientisumo pažeidimus teikimo tvarkos aprašo patvirtinimo";

l) ETSI EN 319 403 v2.2.2: Requirements for conformity assessment bodies assessing Trust Service Providers;

m) ETSI EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers;

n) ETSI EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates;

o) ETSI EN 319 412 Certificate Profiles;

p) ETSI EN 319 421 v1.1.1: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;

q) ETSI EN 319 422 v1.1.1 Time-stamping protocol and electronic time-stamp profiles;

r) ETSI TR 119 100 v1.1.1 on Guidance on the use of standards for signatures creation and validation;

s) ETSI TS 119 101 v1.1.1 on Policy and security requirements for applications for signature creation and signature validation;

t) ETSI TR 119 300 v1.2.1 Business guidance on cryptographic suites;

u) ETSI TS 119 312 v1.3.1 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites;

v) ETSI TR 119 600 v1.2.1 Business guidance for trust service status lists providers;

w) ETSI TS 119 612 v2.1.1 Trusted Lists;

x) ETSI EN 319 422 v1.1.1 Time-stamping protocol and electronic time-stamp profiles.

CPS įgyvendina kvalifikuotų sertifikatų (elektroninių parašų ir elektroninių spaudų) taisykles (toliau – CP), kurių OID yra 1.3.6.1.4.1.30903.1.1.6.

1.2. Identifikavimas

CPS skelbiami saugykloje (*repository*) internete.

Unikalus CPS identifikatorius (OID): **1.3.6.1.4.1.30903.1.2.6**

Šiame identifikatoriuje taškais atskirti skaičiai reiškia:

Pavadinimas	Reikšmė
ISO	1
ISO pripažinta organizacija	3
JAV Gynybos departamentas	6

Internetas	1
Privati įmonė	4
IANA registruota privati įmonė	1
Valstybės įmonė Registrų centras	30903
Padalinys (Registrų centro Sertifikatų centras - RCSC)	1
Dokumento tipas (sertifikavimo veiklos nuostatai)	2
Dokumento versija	6

1.3. Sertifikatų naudotojai ir taikymo sritys

1.3.1 Sertifikatų naudotojai

Sertifikatų naudotojus sudaro patikimumo užtikrinimo paslaugų gavėjai (toliau – abonentai), kvalifikuotų elektroninių parašų bei kvalifikuotų elektroninių spaudų sertifikatų savininkai ir sertifikatais pasitikinčios šalys.

Abonentai – tai fiziniai ir juridiniai asmenys, sudarantys patikimumo užtikrinimo paslaugų sutartį su RCSC jų arba jiems atstovaujančių asmenų sertifikatams sudaryti.

Kvalifikuoto elektroninio parašo sertifikato savininkai – tai fiziniai asmenys, kurie savo elektroninius parašus tvirtina CA sudarytais kvalifikuotais sertifikatais arba sertifikatus naudoja asmens autentifikacijai elektroninėje erdvėje.

Kvalifikuoto elektroninio spaudo sertifikatų savininkai/ kūrėjai – tai juridiniai asmenys, kurie kvalifikuoto elektroninio spaudo sertifikatus naudoja kaip įrodymą, kad elektroninį dokumentą išdavė juridinis asmuo, užtikrinant dokumento kilmę bei vientisumą.

Pasitikinčios šalys – visi fiziniai ir juridiniai asmenys, kurie pasikliauja elektronine atpažintimi ar patikimumo užtikrinimo paslauga.

1.3.2 Sertifikatų naudojimo sritys

Pagal šiuos CPS sudaromi ir tvarkomi:

a) kvalifikuoti elektroninio parašo sertifikatai, skirti kvalifikuotiems elektroniniams parašams tvirtinti;

b) autentifikavimo sertifikatai, skirti asmens tapatybei elektroninėje erdvėje nustatyti;

c) kvalifikuoti elektroninio spaudo sertifikatai, užtikrinantys elektroninės formos duomenų kilmę bei vientisumą.

Sertifikatų naudojimo paskirtis nurodyta sertifikatų laukuose „key usage" ir „enhanced key usage". Sertifikatai negali būti naudojami jokiems kitiems tikslams.

CA teikia 2 (dviejų) rūšių SSCD/QSCD:

a) SSCD/QSCD (flash atmintinė, lustinės kortelė ar kita), kuri naudojama prijungiant prie darbo vietos kompiuterio;

b) SIM SSCD/QSCD kuri naudojama kartu su mobiliuoju telefonu.

Kvalifikuoti el. spaudo sertifikatai gali būti išduodami ir į nekvalifikuotus įtaisus (išduoti kartu su nekvalifikuotais spaudo kūrimo įtaisais), tokiu atveju sertifikatas sudaromas pagal 7.5.3 skyriuje nurodytą Kvalifikuoto elektroninio spaudo nekvalifikuotame įtaise profilį.

CA išduoda tik SSCD/QSCD, atitinkančius eIDAS reglamento reikalavimus (kvalifikuoto elektroninio parašo sertifikatams – eIDAS 29 str. ir 30 str., kvalifikuoto elektroninio spaudo sertifikatams – eIDAS 39 str. 1 d. ir 39 str. 2 d.).

Pagal šiuos CPS sudaromi elektroninio parašo sertifikatai juridiniams asmenims nėra išduodami, t. y. el. parašo sertifikato savininkas gali būti tik fizinis asmuo. Kvalifikuoto elektroninio spaudo sertifikato savininkas gali būti tik juridinis asmuo.

CA išduodami kvalifikuoti bei autentifikavimo el. parašo sertifikatai yra susiję su fiziniu, kvalifikuoti el. spaudo sertifikatai – su juridiniu asmeniu. CA neišduoda sertifikatų susietų su asmens užimamomis pareigomis.

1.3.3 Kvalifikuotų elektroninių parašų ir spaudų teisinė galia

a) Elektroninių parašų teisinė galia. Negalima atsisakyti pripažinti elektroninio parašo teisinės galios ir jo tinkamumo naudoti kaip įrodymą teismo procese tik dėl to, kad parašas yra elektroninis arba kad jis neatitinka kvalifikuotų elektroninių parašų reikalavimų. Kvalifikuoto elektroninio parašo teisinė galia yra lygiavertė rašytiniam parašui. Kvalifikuotas elektroninis parašas, patvirtintas vienoje valstybėje narėje išduotu kvalifikuotu sertifikatu, visose kitose valstybėse narėse pripažįstamas kaip kvalifikuotas elektroninis parašas;

b) Elektroninių spaudų teisinė galia. Negalima atsisakyti pripažinti elektroninio spaudo teisinės galios ir jo tinkamumo naudoti kaip įrodymą teismo procese tik dėl to, kad

spaudas yra elektroninis arba kad jis neatitinka kvalifikuotam elektroniniam spaudui keliamų reikalavimų. Kvalifikuotam elektroniniam spaudui taikoma prezumpcija dėl duomenų, su kuriais susietas kvalifikuotas elektroninis spaudas, vientisumo ir tų duomenų kilmės tinkamumo. Kvalifikuotas elektroninis spaudas, patvirtintas vienoje valstybėje narėje išduotu kvalifikuotu sertifikatu, visose kitose valstybėse narėse pripažįstamas kvalifikuotu elektroniniu spaudu.

1.4. RCSC organizacinė struktūra

Patikimumo užtikrinimo paslaugų teikėjo (toliau – CSP) funkcijas atlieka Registrų centras. CSP teikia kvalifikuotų elektroninio parašo ir elektroninio spaudo sertifikatų (toliau – sertifikatai) sudarymo ir tvarkymo, kvalifikuotos elektroninės laiko žymos ir kitas patikimumo užtikrinimo paslaugas. Sertifikatų sudarymo ir tvarkymo paslaugas teikia CA.

CA dalį sertifikatų sudarymo ir tvarkymo funkcijų pagal šiuos CPS deleguoja patikimumo užtikrinimo paslaugų veiklos palaikymo (toliau – Palaikymo tarnyba) ir registravimo tarnyboms (toliau – RA). Palaikymo tarnybos funkcijas atlieka Registrų centro Aptarnavimo departamento Monitoringo skyrius. RA funkcijas atlieka Registrų centro filialai ar kitos trečios šalys, su kuriomis sudarytos RA paslaugų teikimo sutartys.

CA, vadovaujantis eIDAS, išlieka atsakinga už visas teikiamas patikimumo užtikrinimo paslaugas ir vykdomą patikimumo užtikrinimo paslaugų teikimo veiklą, tačiau trečiųjų šalių teisės, pareigos bei atsakomybė visais atvejais detalizuojama sudaromose sutartyse bei CPS, CP.

CA funkcijos apima:

a) RA pateiktų prašymų sudaryti sertifikatus, nutraukti ar sustabdyti sertifikatų galiojimą, atšaukti sertifikatų galiojimo sustabdymą, autentiškumo ir teisėtumo tikrinimą;

b) Sertifikatų sudarymą;

c) SSCD parengimą ir teikimą;

d) Sertifikatų galiojimo sustabdymą, nutraukimą ir sustabdymo atšaukimą;

e) informacijos apie sertifikatų statusą teikimą.

RA funkcijos apima:

a) prašymų išduoti sertifikatus, sustabdyti ar nutraukti sertifikatų galiojimą, atšaukti sertifikatų galiojimo stabdymą priėmimą;

b) sertifikatų, išduotų RA, galiojimo sustabdymą, nutraukimą ir sustabdymo atšaukimą;

c) sutarčių sudarymą;

d) asmenų tapatybės tikrinimą;

e) SSCD parengimą pagal numatytus reikalavimus ir jų įteikimą galutiniam sertifikatų savininkui;

f) informacijos teikimą.

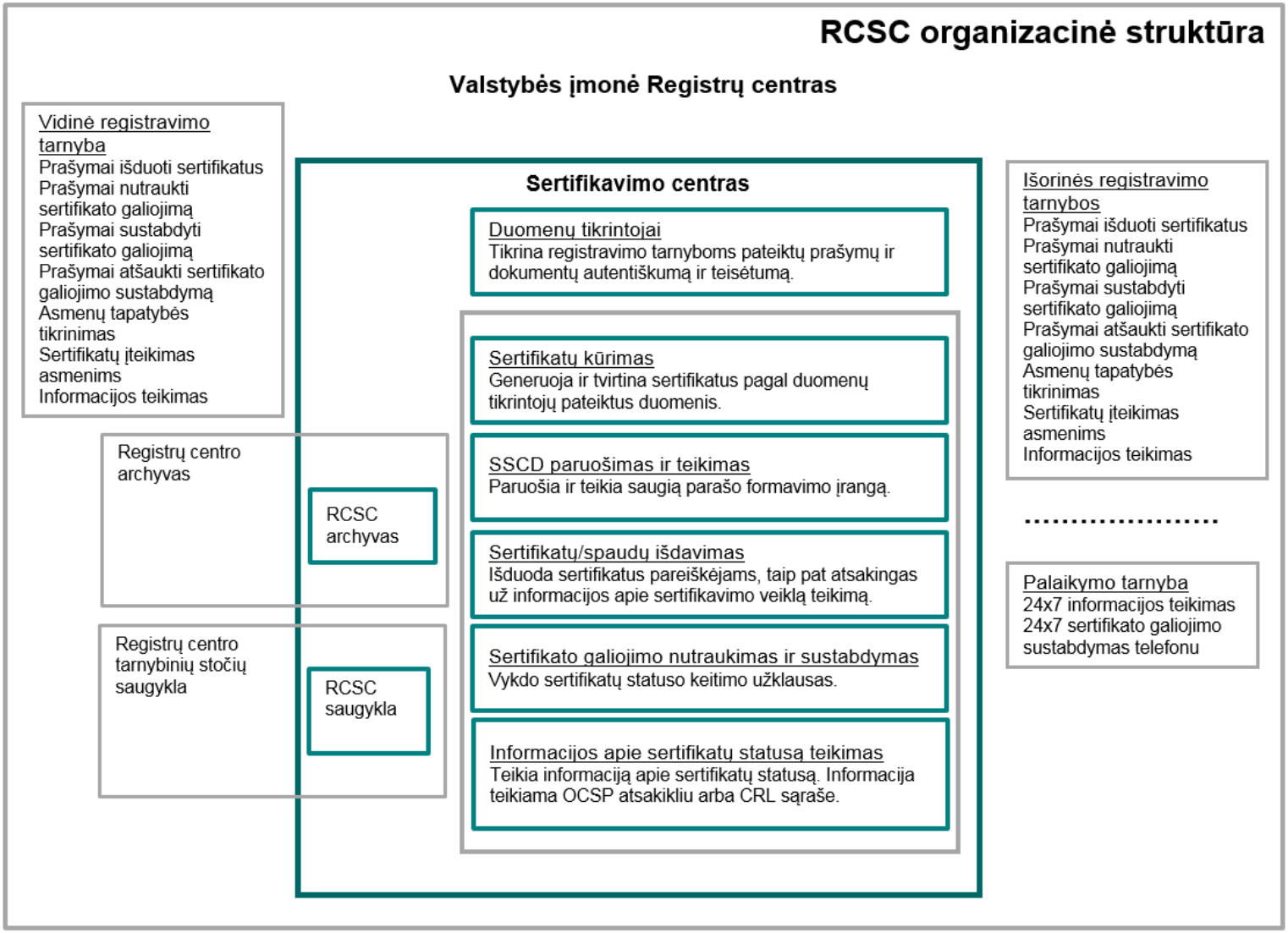
Palaikymo tarnyba veikia 7 (septynias) dienas per savaitę, 24 (dvidešimt keturias) val. per parą. Jos funkcijos apima:

a) prašymų sustabdyti sertifikatus priėmimą;

b) sertifikatų sustabdymą;

c) informacijos teikimą.

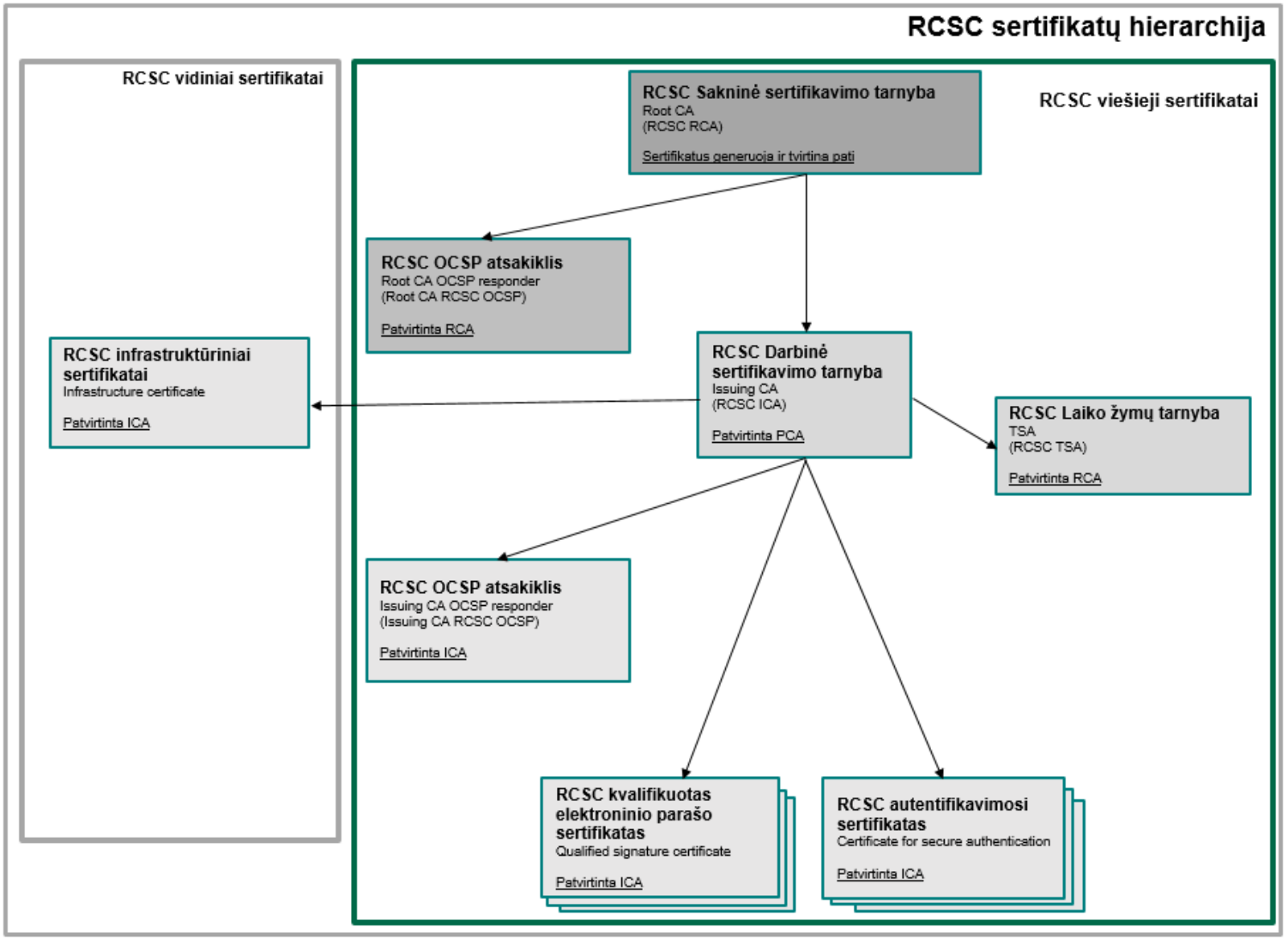
Žemiau pateikiama RCSC organizacinės struktūros schema (*Pav. 1*).



Pav. 1. RCSC organizacinė struktūra

1.5. CA sertifikatų seka

CA sertifikatų seka paremta 2 lygių CA hierarchija. Pirmojo lygio šakninė CA naudoja save pasirašantį sertifikatą (*self-signed certificate*), išduoda darbines CA ir šakninės CA OCSP atsakiklio sertifikatus, pasirašo šakninės CA CRL bei yra atjungta nuo tinklo (*off-line*) ir saugoma izoliuotoje aplinkoje. Darbinė CA išduoda laiko žymų tarnybos (toliau – TSA), asmenų, darbinės CA OCSP atsakiklio ir infrastruktūros sertifikatus ir pasirašo darbinės CA CRL.



Pav. 2. RCSC sertifikatų hierarchija

1.6. Kontaktinė informacija

1.6.1 Nuostatus išleidusi ir tvarkanti organizacija

Organizacija	Valstybės įmonė Registrų centras
Adresas	Lvovo g. 25-101, 09320 Vilnius, Lietuva
Telefonas	+370 5 268 8202
URL:	www.registrucentras.lt
El.paštas:	info@registrucentras.lt

1.6.2 Kontaktinis asmuo

Už CPS atitikimą CP ir CPS administravimą atsakingas asmuo:

Valstybės įmonės Registrų centro El. parašo sertifikatų skyriaus vadovas

Lvovo g. 25-101, 09320 Vilnius, Lietuva,

Tel.: (8 5) 2688 388

E-paštas: *info@elektroninis.lt*

Dėl saugumo bei vientisumo pažeidimų prašome susisiekti tel. 85 2688 388 arba el. paštu info@elektroninis.lt

1.6.3 Informacija apie CA teikimas paslaugas

CA tinklalapyje www.elektroninis.lt pateikiama informacija apie sertifikatų užsakymą, užsakymo būklę, CRL aktualų sąrašą, dokumentus, kuriuos būtina turėti norint įsigyti CA teikiamas paslaugas. Taip pat pateikiamos aktualios CP, CPS, TSP bei TSPS versijos.
Tinklalapyje http://info.registrucentras.lt/faq/Elektroninis.lt skelbiami dažniausiai vartotojų pateikiami klausimai bei atsakymai į juos.

2. BENDROSIOS NUOSTATOS

2.1. Įsipareigojimai

Įsipareigojimai skirstomi į dvi grupes:

a) CA įsipareigojimus, atskirai išskiriant RA ir Palaikymo tarnybos įsipareigojimus;

b) sertifikatų naudotojų įsipareigojimai, atskirai išskiriant abonentų, sertifikatų savininkų ir pasitikinčių šalių įsipareigojimus.

2.1.1 CA įsipareigojimai

CA įsipareigoja laikytis CPS 3-8 skyriuje išdėstytų reikalavimų.

CA įsipareigoja:

a) užtikrinti CA privačiųjų kriptografinių raktų (toliau - raktų) saugumą;

b) užtikrinti tinkamą fizinio/ juridinio asmens, kuriam išduodami sertifikatai identifikavimą;

c) užtikrinti prašymų išduoti sertifikatus priėmimą ir vykdymą:

- užtikrinti asmenų prašymų išduoti kvalifikuotus sertifikatus priėmimą ir vykdymą kaip tai numatyta CP ir CPS;

d) užtikrinti saugų SSCD/QSCD parengimą ir įteikimą asmenims;

e) sertifikatų naudotojams teikti tikslią ir teisingą informaciją, įgalinančią:

- patikrinti sertifikatų galiojimą;
- atkreipti dėmesį į sertifikatų naudojimo tvarką ir apribojimus;

f) priimti prašymus nutraukti ar sustabdyti sertifikatų galiojimą:

- priimti ir vykdyti prašymus nutraukti ar sustabdyti sertifikatų galiojimą kaip tai numatyta CP ir CPS;
- nutraukti sertifikatų galiojimą pasibaigus sertifikatų galiojimo sustabdymo laikotarpiui;

g) priimti prašymus atšaukti sertifikatų galiojimo sustabdymą:

- priimti ir vykdyti prašymus atšaukti sertifikatų galiojimo sustabdymą kaip tai numato CP ir CPS;

- iš atšauktų sertifikatų sąrašo (toliau – CRL) pašalinti sertifikatus, kurių galiojimo sustabdymas buvo atšauktas.

h) užtikrinti asmens duomenų apsaugą, reglamentuojamą Bendrojo asmens duomenų apsaugos reglamento bei kitų Lietuvos Respublikos teisės aktų, kiek jie neprieštarauja Bendrąjam asmens duomenų apsaugos reglamentui;

i) viešai skelbti saugykloje (repository) bet kuriuo paros metu:

- CP, CPS;

- CRL.

2.1.2 RA įsipareigojimai

RA, veikdama pagal šiuos CPS, įsipareigoja:

a) priimti asmenų prašymus sertifikatams sudaryti, patikrinti asmens tapatybę ir kitus pateiktus sertifikatams sudaryti būtinus duomenis;

b) priimti prašymus dėl sertifikatų galiojimo sustabdymo, nutraukimo ar sustabdymo atšaukimo, bei patikrinti asmens tapatybę ir jų įgaliojimus teikti tokius prašymus;

c) sustabdyti, atšaukti sertifikatų galiojimą ar atšaukti sustabdymą;

d) patikrintus ir visus reikalavimus atitinkančių prašymų duomenis perduoti CA;

e) laikantis visų CP ir CPS apibrėžtų saugumo reikalavimų, įrašyti bei perduoti sertifikatus ir SSCD/QSCD juos užsakiusiems asmenims;

f) teikti informaciją asmenims sertifikatų sudarymo ir tvarkymo klausimais;

g) jei RA funkcijas atlieka trečia šalis, ji įsipareigoja laikytis su CA pasirašytos sutarties.

2.1.3 RA veiklos vertinimas

CA periodiškai kas 1 (vienerius) metus arba po svarbių CP bei CPS pakeitimų atlieka RA prisiimtų įsipareigojimų bei funkcijų patikrą. Vertinimo metu tikrinamos šios RA atliekamos funkcijos bei prisiimti įsipareigojimai:

a) viešai RA skelbiama informacija apie sertifikatų sudarymo sąlygas;

b) asmens, norinčio įsigyti sertifikatus identifikavimo procedūra;

c) RA personalo saugumas;

d) RA išduotų sertifikatų nutraukimo ar sustabdymo procedūra;

e) dokumentacijos, gaunamos teikiant sertifikatų išdavimo paslaugą, archyvavimo procedūra, saugojimas;

f) fizinis ir procedūrinis RA naudojamų patalpų bei technikos saugumas.

2.1.4 Palaikymo tarnyba įsipareigoja

7 (septynias) dienas per savaitę 24 (dvidešimt keturias) val. per parą telefonu priimti prašymus sustabdyti sertifikato galiojimą bei techniškai sustabdyti sertifikato galiojimą ir teikti informaciją sertifikatų sudarymo ir tvarkymo klausimais.

2.1.5 Abonentų ir sertifikatų savininkų įsipareigojimai

Siekiant gauti ir naudoti sertifikatus, asmenys turi susipažinti su CP, CPS ir priimti šiuos įsipareigojimus:

a) pateikti tikslią ir visą informaciją RA, kaip to reikalauja CPS;

   - naudoti viešojo ir privačiojo raktų porą tik CP ir CPS nurodytiems tikslams laikantis sertifikate nurodytų apribojimų;

b) sertifikatų savininkų įsipareigojimai:

   - tinkamai pasirūpinti, kad jo privačiuoju raktu nepasinaudotų kiti asmenys;
   - nedelsiant, bet ne vėliau kaip per 12 (dvylika) val. informuoti CA, kai sertifikato galiojimo laikotarpiu atsitinka bent vienas iš šių įvykių:
     - pametamas, pavagiamas ar kitaip sukompromituojamas privatusis raktas;
     - atskleidžiami privačiojo rakto panaudojimą įgalinantys aktyvavimo duomenys (PIN kodas, kt.);
     - pastebimi netikslumai sertifikate arba jame prireikia daryti pakeitimus.

c) privačiojo rakto kompromitacijos atveju nedelsiant nutraukti jo naudojimą.

2.1.6 Pasitikinčių šalių įsipareigojimai

CA sudarytais sertifikatais pasitikinčios šalys turi susipažinti su CP ir CPS.

Pasitikinčios šalys privalo įsitikinti, kad sertifikatais buvo galiojantis parašo sudarymo metu. Sertifikato statusas tikrinamas naudojant OCSP protokolą arba saugykloje (*repository*) esantį CRL. Jei sertifikatai yra negaliojantys, tai parašas/ spaudas yra arba negaliojantis, arba apie parašo galiojimą sprendžiama pagal parašo laiko žymą, jei tokia yra.

Jei sertifikatai yra galiojantis, toliau parašas/ spaudas tikrinamas vadovaujantis sertifikatuose esančia informacija. Parašo tikrintojai turi atkreipti dėmesį į tai, ar nepažeisti sertifikatų naudojimo apribojimai.

2.2. Atsakomybė

Kvalifikuotus sertifikatus sudarančių patikimumo užtikrinimo paslaugų teikėjų atsakomybė nustatyta eIDAS naujausioje redakcijoje, Lietuvos Respublikos teisės aktuose, reglamentuojančiuose patikimumo užtikrinimo paslaugas, tiek, kiek neprieštarauja eIDAS, bei sudaromose sutartyse.

2.2.1 CA atsakomybė

CA atsako už:

a) sudarytų sertifikatų, juose esančių duomenų tikslumą;

b) tai, kad sudarytuose sertifikatuose nurodytas fizinis/ juridinis asmuo yra parašo formavimo duomenų, atitinkančių sertifikatuose nurodytus parašo tikrinimo duomenis, turėtojas;

c) parašo formavimo duomenų ir parašo tikrinimo duomenų atitikimą, kai jis asmens prašymu sukuria šiuos abu duomenis;

d) sertifikatų galiojimo sustabdymą ar nutraukimą laiku;

e) tinkamą informacijos apie išduotų kvalifikuotų elektroninio parašo sertifikatų galiojimo, atšaukimo skelbimą.

CA prisiima atsakomybę už naudotojų patirtus nuostolius eIDAS 13 str. ir Lietuvos Respublikos elektroninės atpažinties ir patikimumo užtikrinimo paslaugų įstatyme nustatyta tvarka.

CA prisiima atsakomybę, už sertifikatų naudotojų patirtus nuostolius, kuriuos sukėlė trečiosios šalys (RA), kurioms CA delegavo dalį savo funkcijų. CA taip pat atsako už teikiamų paslaugų kokybę bei prieinamumą, tačiau tik savo veikimo ribose, kurios apima:

a) kvalifikuotų sertifikatų kūrimo bei tvarkymo infrastruktūrą, kuri baigiasi ties Registrų centro ugniasiene, besiribojančia su viešuoju internetu;

b) kvalifikuotų elektroninių laiko žymų teikimo paslaugoje – TSA teikimui reikalingą infrastruktūrą, kuri baigiasi ties TSA infrastruktūros išorine tinklo sąsaja.

CA neatsako už trečiųjų šalių sisteminius gedimus, trikdžius (fiksuotus ne CA veikimo ribose) dėl kurių galimai sutriko teikiamų paslaugų teikimas, kokybė bei prieinamumas.

Visos sertifikatų naudojimo sąlygos, apribojimai bei taisyklės nurodytos sudaromoje sutartyje bei viešai skelbiamuose CPS bei CP. Atsižvelgiant į tai, CA neatsako už neteisėtus sertifikatų naudotojų ir kitų su CA nesusijusių šalių veiksmus bei už sertifikatų naudotojų patirtus nuostolius kai jie iš anksto tinkamai buvo informuoti apie naudojimosi sąlygas, apribojimus ir nuostoliai atsirado dėl aukščiau minėtų sąlygų, taisyklių nepaisymo. CA taip pat neprisiima atsakomybės, jei nuostoliai buvo patirti dėl:

a) gamtos jėgų, pvz., gaisro, potvynio, audros, arba kitokių aplinkybių, kaip karas, teroristinis išpuolis, epidemija ar nenugalimos jėgos (*force majeure*), kurios kontroliuoti, numatyti ar užkirsti jai kelią iš anksto buvo neįmanoma;

b) neleistino sertifikatų naudojimo (pvz., kai jis yra negaliojantis arba kai pažeidžiami sertifikato naudojimo apribojimai, taisyklės numatytos CPS, CP bei pasirašytose sutartyse).

2.3. Finansinė atsakomybė

Finansinės atsakomybės įsipareigojimams užtikrinti CA savo veiklą draudžia ne mažesne kaip Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymo 10 str. nustatyta suma.

2.3.1 Sertifikatų naudotojų kompensacijos

Sertifikatų naudotojai, dėl kurių veiksmų CA patyrė nuostolių, privalo kompensuoti nuostolius tais atvejais, kai:

a) prašantysis sudaryti sertifikatus pateikė klaidingus duomenis;

b) sertifikatų savininkas neapsaugojo savo privačiojo rakto nuo kompromitacijos;

c) pasirašantysis asmuo pažeidė su CA pasirašyto susitarimo dėl sertifikato naudojimo sąlygas.

2.4. Teisinės nuostatos ir interpretavimas

2.4.1 Pagrindiniai teisės aktai

Patikimumo užtikrinimo paslaugas, įskaitant kvalifikuotų elektroninių sertifikatų (elektroninių parašų bei elektroninių spaudų) sudarymo paslaugas (kūrimą, tikrinimą, galiojimą), sertifikatų naudotojų teises ir atsakomybę, reikalavimus patikimumo užtikrinimo paslaugų teikėjams bei jų atsakomybę nustato CPS 1.1 p. nurodyti teisės aktai.

2.4.2 Ginčų sprendimo tvarka

Bet kokie ginčai tarp CA ir sertifikatų naudotojų sprendžiami derybų keliu. Neišsprendus ginčo, jis sprendžiamas teismo tvarka, vadovaujantis galiojančiais Lietuvos Respublikos teisės aktais.

2.5. Mokesčiai

Sertifikatų sudarymo ir tvarkymo paslaugų įkainiai skelbiami saugykloje (*repository*).

CRL teikimas nėra apmokestinamas.

CA, gavusi sertifikatų savininko prašymą, sertifikato galiojimą nutraukia ir stabdo nemokamai.

CP ir CPS teikiami nemokamai saugykloje (*repository*).

2.6. Informacijos teikimas ir saugyklos

2.6.1 CA teikiama informacija

CA viešai teikiamą informaciją sudaro:

a) CP, CPS;

b) informacija apie sertifikatų statusą;

c) įvairi organizacinės paskirties ar patikimą veiklą įrodanti informacija (pvz. prašymo sudaryti sertifikatus forma, sutartis sertifikatams sudaryti, nepriklausomo CA veiklos audito išvados, skelbimai, kt.).

2.6.2 Teikiamos informacijos atnaujinimo dažnumas

CA teikiama informacija atnaujinama tokiu laiku ar dažnumu:

a) CPS pakeitimai daromi, tvirtinami ir skelbiami kaip numatyta šių CPS 8 skyriuje;

b) pačiai CA priklausančių sertifikatų duomenys, atlikus pakeitimus juose, skelbiami viešai nedelsiant;

c) CRL atnaujinamas tokiu dažnumu, kaip nurodyta 4.1.4 skyriuje;

d) kita skelbtina ir atnaujinta informacija (pvz., prašymų šablonai, CA veiklos tikrinimo išvados, kt.) skelbiama ją gavus ar parengus per protingą terminą.

2.7. Atitikties tikrinimas

a) CA veiklos atitiktis CP ir CPS tikrinama CA nustatyta vidaus tvarka;

b) Vadovaujantis eIDAS 20 str. 1 d. atitikties vertinimo įstaiga kas 24 (dvidešimt keturis) mėnesius atlieka CA auditą;

c) Vadovaujantis eIDAS 20 str. 2 d., priežiūros įstaiga bet kuriuo metu gali atlikti CA auditą arba reikalauti, kad atitikties įstaiga atliktų CA vertinimą (CA lėšomis), siekiant patvirtinti, kad teikiamos paslaugos atitinka eIDAS nustatytus reikalavimus;

d) Vadovaujantis eIDAS 20 str. 3 d., kai priežiūros įstaiga reikalauja, kad CA ištaisytų bet kuriuos eIDAS reikalavimų pažeidimus ir CA to nepadaro per priežiūros įstaigos nustatytą laikotarpį, priežiūros įstaiga, atsižvelgdama visų pirma į tokių pažeidimų mastą, trukmę ir pasekmes, gali panaikinti CA arba pažeidimo paveiktų CA teikiamų paslaugų kvalifikacijos statusą ir pranešti apie tai eIDAS 20 str. 3 d. nurodytai įstaigai, kad būtų galima atnaujinti patikimus sąrašus;

e) Patikimumo užtikrinimo paslaugų teikimo priežiūrą vykdo Vyriausybės įgaliota priežiūros įstaiga.

2.7.1 CA veiklos tikrinimo dažnumas

CA veiklos atitiktis CP ir CPS turi būti tikrinama po svarbių veiklos pakeitimų bei atnaujinimų.

2.7.2 Tikrintojai ir jų kvalifikacija

Vidinį tikrinimą atlieka Registrų centro informacinių technologijų saugumo ir tvarkymo struktūros, bei audito ypatingo pasitikėjimo pareigas einantis asmuo.

2.7.3 Veiksmai pastebėjus trūkumus

Tikrinimo protokolai įteikiami CA saugumo pareigūnui. Per 30 (trisdešimt) kalendorinių dienų saugumo pareigūnas turi raštu parengti savo nuomonę dėl protokole išdėstytų trūkumų, numatyti veiksmus ir terminus trūkumams pašalinti. Informacija apie trūkumų pašalinimą pateikiama tikrinusiai organizacijai.

Jei pastebėti trūkumai kelia pavojų patikimumo užtikrinimo paslaugų procedūrų saugumui, saugumo pareigūnas gali priimti sprendimą laikinai sustabdyti paslaugų teikimą. Tokiu atveju visi asmenys, kuriems CA yra sudaręs sertifikatus, informuojami apie tai ir jiems pranešama apie numatomą patikimumo užtikrinimo paslaugų veiklos atnaujinimo laiką.

2.7.4 Tikrinimo rezultatų skelbimas

CA veiklos nepriklausomo tikrinimo išvados dedamos į saugyklą (*repository*) ir skelbiamos viešai.

2.8. Konfidencialumo nuostatos

a) CA privalo saugoti asmenų, prašančių sudaryti sertifikatus, duomenis laikydamasis Bendrojo asmens duomenų apsaugos reglamento bei Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo, kuris įgyvendina 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvą 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kiek jis neprieštarauja Bendrąjam asmens duomenų apsaugos reglamentui. Asmens duomenys saugomi tinkamą, reikiamą laikotarpį (CPS 4.3.2 str.) (įskaitant CA nutraukus veiklą), bet ne ilgiau nei to reikia duomenų tvarkymo tikslais, apie kurį asmuo, prašantis sudaryti sertifikatą yra informuojamas, kad duomenis būtų galima panaudoti teismo procese bei taip būtų užtikrinamas veiklos tęstinumas;

b) Kai asmens duomenys nebereikalingi jų tvarkymo tikslams, jie turi būti sunaikinti, išskyrus tuos, kurie įstatymų nustatytais atvejais turi būti perduodami valstybės archyvams;

c) Siekiant apsaugoti minėtus duomenis nuo vagystės ar klastojimo, CA imasi prevencinių priemonių, susijusių su tinkama bei efektyvia fizinio, techninio, procedūrinio saugumo bei personalo patikimumo kontrole;

d) Duomenų įrašai saugomi patikimose sistemose taip, kad būtų galima patikrinti jų tikrumą, o įrašus bei pakeitimus galėtų daryti tik CA įgalioti asmenys.

2.8.1 Slaptoji informacija

Slaptoji informacija, kuri saugoma ir tvarkoma laikantis RCSC vidaus taisyklių, yra:

a) prašančiųjų sudaryti sertifikatus pateikti duomenys, išskyrus tuos, kurie atskleistini teikiant patikimumo užtikrinimo paslaugas. Visi šie duomenys gali būti atskleisti tik turint jos savininko raštišką sutikimą arba teismo sprendimą;

b) asmenų pateikta informacija (pvz., prašymai sustabdyti arba nutraukti sertifikato galiojimą). Šios informacijos dalis gali būti atskleista tik gavus informaciją pateikusio asmens sutikimą;

c) CA atliktų operacijų įrašai (log file);

d) įrašai apie patikimumo užtikrinimo paslaugų teikimo sutrikimus;

e) įrašai apie vidinius ir išorinius CA veiklos patikrinimus, jei jų paskelbimas gali sukelti pavojų CA saugumui;

f) veiksmų avariniais atvejais planai;

g) informacija apie aparatinės ir programinės įrangos apsaugojimo būdus ir patikimumo užtikrinimo paslaugų operacijų atlikimą.

2.8.2 Neslapta informacija

Į CA sudaromus sertifikatus įrašoma informacija nėra slapta. Laikoma, kad prašantieji sudaryti sertifikatus yra susipažinę su sertifikate nurodoma informacija ir yra davę sutikimą skelbti ją.

Dalis prašančiųjų sudaryti sertifikatus pateiktos ir CA teikiamos informacijos gali būti perduodama kitiems asmenims tik turint raštišką prašytojų leidimą.

Saugykloje (*repository*) laikoma ir viešai platinama informacija:

a) CP, CPS ir sertifikatų sudarymo ir tvarkymo sąlygos;

b) kainoraščiai;

c) instrukcijos vartotojams;

d) CA priklausantys sertifikatai;

e) CRL;

f) įgaliotų institucijų parengtos CA veiklos tikrinimo ataskaitų santraukos.

CA veiklos tikrinimo ataskaitų santraukose nurodoma:

a) tikrinimo apimtis;

b) tikrinusios institucijos bendrasis įvertinimas;

c) rekomendacijos CA veiklai gerinti.

2.8.3 Informacijos teikimas teisėsaugai

Slaptoji CA informacija gali būti teikiama teisėsaugos institucijų pareigūnams tik laikantis Lietuvos Respublikos teisės aktų reikalavimų.

2.9. Intelektinės nuosavybės teisės

CP ir CPS yra laisvai prieinami sertifikatų naudotojams. Naudojant CP ir CPS būtina pateikti nuorodą į šaltinį.

CA netaiko nuosavybės teisių sudarytiems sertifikatams.

3. IDENTIFIKAVIMAS IR AUTENTIFIKAVIMAS

Šiame skyriuje aprašomos asmenų, teikiančių prašymus sudaryti kvalifikuotus elektroninius sertifikatus (el. parašo, el. spaudo), sustabdyti ar nutraukti šių sertifikatų galiojimą ir atšaukti jų galiojimo sustabdymą, identifikavimo ir autentifikavimo taisyklės ir procedūros.

3.1. Sutarties sudarymas

RA privalo:

a) prieš sudarant patikimumo užtikrinimo paslaugų teikimo sutartį, informuoti sertifikatus sudaryti prašantįjį asmenį apie sertifikatų sudarymo ir tvarkymo sąlygas, apribojimus, CA, abonento ir sertifikatų savininko pareigas ir atsakomybę;

b) suteikti šią informaciją tvaria, nekintančia laike forma;

c) reikalauti, kad prašantieji sudaryti sertifikatus **fiziniai** asmenys, jų tapatybei įrodyti asmeniškai pateiktų:

- pasą arba
- asmens tapatybės kortelę;
- Lietuvos Respublikos migracijos departamento išduodamą leidimą gyventi Lietuvoje (tik Lietuvos Respublikos pilietybės neturintiems asmenims).

reikalauti, kad prašančiųjų sudaryti elektroninių spaudų sertifikatus **juridinių** asmenų atstovai asmeniškai pateiktų:

- juridinio asmens vadovas – asmens tapatybės dokumentą;
- kitas juridinio asmens atstovas – asmens tapatybės dokumentą bei įgaliojimo atstovauti juridinį asmenį originalą.

d) Kvalifikuotas teikėjas ar įgaliotoji trečioji šalis, juridinio asmens, kuriam išduodamas kvalifikuotas sertifikatas, tapatybę, kai ji nustatoma juridinio asmens įgaliotam atstovui fiziškai dalyvaujant, turi nustatyti ir pagal šiuos juridinio asmens įgalioto atstovo pateiktus dokumentus:

- registro, kuriame kaupiami ir saugomi duomenys apie juridinį asmenį, išrašą ar kitą dokumentą, jeigu pagal užsienio valstybės teisės aktus toks išrašas neišduodamas, patvirtinantį, kad juridinis asmuo įregistruotas, kuriame yra šie duomenys:
  - juridinio asmens pavadinimas;

- juridinio asmens teisinė forma;
- juridinio asmens buveinė (adresas);
- juridinio asmens kodas (jeigu pagal valstybės, kurioje juridinis asmuo yra įregistruotas, teisės aktus toks kodas yra suteikiamas);

e) pagal nacionalinės teisės aktus įsitikinti prašančiųjų sudaryti sertifikatus asmenų tapatybe ir, jei taikytina, patikrinti specifinius požymius;

f) įvertinti, ar pateiktas galiojantis asmens tapatybės dokumentas;

g) nustatyti, ar pateiktame asmens tapatybės dokumente yra būtent to asmens nuotrauka;

h) įvertinti pateikto asmens tapatybės dokumento būklę (ypač didelį dėmesį atkreipti į tai, ar nuotrauka, puslapiai ar įrašai nebuvo keičiami, taisomi ir panašiai);

i) reikalauti, kad prašantieji sudaryti sertifikatus asmenys pateiktų kontaktinius duomenis, kuriais būtų galima patikimai susisiekti su jais;

j) dokumentuoti ir išsaugoti (darant kopijas arba skaitmenines kopijas) visą informaciją, naudojamą asmens tapatybei nustatyti, įskaitant dokumento tipą, numerį bei dokumentų galiojimo apribojimus, bei specifinius požymius įrodančius dokumentus;

k) dokumentuoti ir išsaugoti sudarytą sutartį, apimančią:

- sertifikatų savininkų įsipareigojimus;
- asmens duomenų, sertifikatų ir atskirų sertifikatų duomenų skelbimo sąlygas;
- sutikimą saugoti sertifikatų savininko registracijos, SSCD/QSCD išdavimo ir kitą informaciją bei sutikimą šią informaciją pagal CP ir CPS numatytas procedūras perduoti trečiosioms šalims CA veiklos nutraukimo atveju;
- patvirtinimą, kad sertifikatų savininko suteikta informacija yra teisinga;

l) surinktus duomenis, nurodytus punktuose c)-g), saugoti sutartyje nurodytą laikotarpį, apie kurį sertifikato savininkas yra informuojamas iki sutarties pasirašymo ir kuris yra reikalingas patikimumo užtikrinimo paslaugų teikimo įrodymams teisminiuose procesuose;

m) įsipareigoti saugoti asmens duomenis, vadovaujantis Bendruoju asmens duomenų apsaugos reglamentu.

Detali asmenų tapatybės ir papildomų specifinių požymių tikrinimo išduodant kvalifikuotus sertifikatus tvarka aprašyta RCSC Asmenų registravimo ir konsultavimo taisyklėse, kurios parengtos vadovaujantis Asmens tapatybės ir papildomų specifinių požymių tikrinimo išduodant kvalifikuotus elektroninio parašo, elektroninio spaudo, interneto svetainės tapatumo nustatymo sertifikatus tvarkos aprašu, patvirtintu Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2018 m. spalio 26 d. įsakymu Nr. 1V-1055.

3.1.1 Asmenų vardų tipai (formos)

CA sudaromi sertifikatai atitinka X509 v3 standarto reikalavimus, o juose nurodomi asmenų identifikaciniai vardai (toliau tekste – DN vardai; *Distinguished Names*) sudaromi laikantis X500 standarto rekomendacijų. Sertifikate asmens DN vardo laukai, kurie užpildomi asmens prašyme sudaryti sertifikatą pateiktais duomenimis, išvardinti lentelėje toliau (*Lentelė Nr. 1*).

Lentelė Nr. 1

DN vardo lauko žymėjimas ir jo paskirtis	Nurodoma reikšmė
CA sudarytojo DN	
C (*Country* – šalis)	LT
O (Organizacija)	VI Registru Centras - I.k. 124110246
OU (*Organization Unit* – organizacijos padalinys)	Registru Centro Sertifikatų Centras
CN (*Common Name*)	VI Registru Centras RCSC (IssuingCA)
Sertifikato savininko DN	
CN (*Common Name* – asmens vardas)	Asmens vardas, pavardė / Juridinio asmens vardas
G (*Given Name* - vardas)	Asmens vardas / Juridinio asmens atstovo vardas
SN (*Surname* – pavardė)	Asmens pavardė / Juridinio asmens atstovo pavardė
Serijinis numeris	Asmens kodas / Juridinio asmens kodas
C (*Country* – šalis)	Šalis (ISO 3166 code)

CA turi reikalauti, kad sudaromuose sertifikatuose būtų nurodyti asmens vardas ir pavardė bei asmens kodas, spaudo sertifikato atveju – juridinio asmens pavadinimas, juridinio asmens atstovo vardas, pavardė bei juridinio asmens kodas.

3.1.2 Slapyvardžių naudojimas

Nedarant poveikio slapyvardžiams suteiktai teisinei galiai pagal nacionalinę teisę, vykdant elektronines operacijas nedraudžiama naudoti slapyvardžių.

CA vadovaujantis eIDAS 26 str. a) punktu, įpareigojančiu pažangųjį elektroninį parašą vienareikšmiškai susieti su pasirašančiu asmeniu, garantuoja asmenų identifikatoriaus unikalumą sudarytuose sertifikatuose. Asmens unikalus identifikatorius pagal galiojančius Lietuvos Respublikos teisės aktus yra asmens kodas. Ant CA išduodamų laikmenų fiziškai nėra rašomi jokie asmens duomenys.

3.2. Tapatybės tikrinimas prašymo išduoti sertifikatą atveju

Asmens tapatybės tikrinimo tikslai yra du: patikrinti, ar prašyme sudaryti sertifikatus nurodytas asmuo iš tikro egzistuoja ir ar prašytojas iš tikro yra tas asmuo, kuriuo prisistato.

Pirminė tapatybės tikrinimo procedūra atliekama RA (3.1 skyriaus c) ir d) punktai). Vėliau visi registracijos metu surinkti duomenys siunčiami duomenų tikrintojams.

Duomenys gaunami iš RA į CA perduodami SSL kanalu. TSP gali būti pasiektas tik iš autentifikuotų darbo vietų (tai kontroliuojama naudojant ugniasienę) ir tik autentifikuotų asmenų (atsižvelgiama į turimus sertifikatus). Visi įrašai, tiek sėkmingi, tiek klaidingi yra įrašomi logų duomenų bazėje.

Jei CA pasiekia klaidingi, netikslūs ar nepilni duomenys, sertifikatai nėra išduodami.

Sertifikatai tik juos išdavus, CDB įgauna būseną "HOLD", šiuo metu kreipiantis į OCSP yra atsakoma, kad sertifikatų statusas yra "REVOKED". Nurodoma priežastis - "CertificateHold". Sertifikatų statusą į „GOOD" pakeičia operatoriaus, kai įrenginys su įrašytais sertifikatais yra perduodamas vartotojui.

Fizinio asmens tapatybės tikrinimo procedūra apima:

a) asmens pateiktų dokumentų tikrumo ir galiojimo tikrinimą;

b) prašyme pateiktos informacijos palyginimą su kituose šaltiniuose (Gyventojų registre) esančia informacija, kad būtų įsitikinta prašyme nurodyto asmens egzistavimu ir tapatybės tikrumu.

Juridinio asmens tapatybės tikrinimo procedūra apima:

a) asmens pateiktų dokumentų tikrumo ir galiojimo tikrinimą;

b) prašyme pateiktos informacijos palyginimą su kituose šaltiniuose (Juridinių asmenų registre, Įgaliojimų registre) esančia informacija, kad būtų įsitikinta prašyme nurodyto juridinio asmens bei jo atstovo egzistavimu ir tapatybės tikrumu.

Dokumentuojama ir archyve išsaugoma visa RA pateikta ir tapatybės tikrinimui naudota informacija.

3.3. Asmens tapatybės tikrinimas sertifikatų atnaujinimo atvejais

Sertifikatų atnaujinimas CA veikloje netaikomas. Pasikeitus asmens duomenims ar kitais atvejais išduodamas naujas sertifikatas.

3.4. Sertifikato galiojimą nutraukti prašančio asmens tapatybės tikrinimas

Prašymą nutraukti sertifikatų galiojimą teikia abonentas arba sertifikato savininkas.

Tapatybės tikrinimo procedūra apima:

a) prašymą teikiant abonentui tikrinamas prašymo tikrumas ir įgaliojimai prašymui teikti;

b) prašymą teikiant sertifikatų savininkui tapatybės tikrinimo procedūra yra tokia pati kaip prašymo išduoti sertifikatą atveju (3.2. skyrius).

3.5. Sertifikato galiojimą sustabdyti prašančio asmens tapatybės tikrinimas

Prašymai sustabdyti sertifikatų galiojimą sertifikatų savininko teikiami 2 (dviem) būdais:

a) telefonu Palaikymo tarnybai. Tapatybei nustatyti, sertifikatų galiojimą sustabdyti prašantis asmuo turi pateikti šiuos duomenis:

- vardą, pavardę, gimimo datą, asmens kodą;
- atsakyti į kontrolinį klausimą;

Sertifikatų savininkui teisingai atsakius į klausimą, sertifikatas sustabdomas, o apie sertifikatų statuso pasikeitimą asmuo informuojamas iš karto.

b) atvykti į RA ir pateikti prašymą, bei asmens tapatybę leidžiantį nustatyti dokumentą. Šiuo atveju atliekamas tik pirminis tapatybės tikrinimas RA (3.1 skyriaus c) ir d) punktai).

Sertifikatų galiojimas gali būti sustabdomas įgaliotos institucijos prašymu. Tokiu atveju turi būti pateiktas popierinis arba elektroninis pasirašytas prašymas, kuriame nurodyti sertifikatų, kurių galiojimas sustabdomas, duomenys ir galiojimo sustabdymo priežastis. Sustabdžius sertifikatus įgaliotos institucijos prašymu, sertifikatų savininkas apie sertifikatų būsenos pasikeitimą informuojamas turimais kontaktiniais duomenimis.

3.6. Sertifikatų galiojimo sustabdymą atšaukiančio asmens tapatybės tikrinimas

Prašymus atšaukti sertifikatų galiojimo sustabdymą asmenys gali pateikti tik asmeniškai RA. Vienu prašymu gali būti prašoma atšaukti kelių sertifikatų galiojimo sustabdymą.

Atšaukti sertifikatų galiojimo sustabdymą prašančio asmens tapatybė tikrinama analogiškai, prašymo sustabdyti sertifikatų galiojimą atveju (žiūr. 3.5 skyrių).

4. REIKALAVIMAI VEIKLAI

Šiame skyriuje apibrėžiami reikalavimai CA veiklai viso sertifikatų gyvavimo ciklo metu.

4.1. Reikalavimai sertifikato gyvavimo ciklui

4.1.1 Sertifikato sudarymas

CA užtikrina sertifikatų sudarymo ir tvarkymo saugumą. Garantuojama, kad:

a) sertifikatai atitinka eIDAS reikalavimus kvalifikuotiems sertifikatams;

b) sertifikatų sudarymo procedūra saugiai susieta su kitomis sertifikatų gyvavimo ciklo procedūromis;

c) raktų poros generavimo procedūra yra:

- saugiai susieta su sertifikatų sudarymo procedūra;
- privatusis raktas generuojamas naudojant SSCD/QSCD atitinkančias eIDAS 29 str. ir 30 str. reikalavimus;
- parengta saugi parašo formavimo įranga saugiai perduodama sertifikatus sudaryti prašantiems asmenims.

d) sudarytame sertifikate nurodyti asmens identifikaciniai duomenys yra unikalūs ir nepriskiriami kitam asmeniui;

e) užtikrinamas sertifikatams sudaryti panaudotų duomenų konfidencialumas ir integralumas viso sertifikatų gyvavimo ciklo metu;

f) CA užtikrina RA, kurios yra išorinės CA atžvilgiu, autentiškumą, apsikeičiant sertifikatų sudarymo duomenimis;

Sertifikatai sudaromi per 7 (septynias) darbo dienas nuo prašymo gavimo.

4.1.1.1 Sertifikato duomenys

CA užtikrina, jog sudaromuose sertifikatuose bus šie duomenys:

a) nuoroda, kad sertifikatai išduoti kaip kvalifikuoti elektroninio parašo/ spaudo sertifikatai;

b) duomenų rinkinys, kuriuo vienareikšmiškai nurodomas kvalifikuotus sertifikatus išduodantis kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, nurodant bent valstybę narę, kurioje jis yra įsisteigęs:

- juridinio asmens atveju: pavadinimas ir juridinio asmens kodas;

c) pasirašančio asmens vardas, pavardė, asmens kodas, o išduodant spaudo sertifikatą – spaudo savininko pavadinimas, registracijos kodas;

d) elektroninio sertifikato patvirtinimo duomenys, atitinkantys elektroninio sertifikato kūrimo duomenis;

e) duomenys apie sertifikatų galiojimo laikotarpio pradžią ir pabaigą;

f) sertifikatų identifikacinis kodas, kuris yra unikalus CA atžvilgiu;

g) sertifikatus išduodančio CA elektroninis parašas ar spaudas;

h) vieta, kurioje galima nemokamai gauti sertifikatus, patvirtinančius g) punkte nurodytus elektroninius parašus ar spaudus;

i) paslaugų teikimo vieta, kurioje galima pasiteirauti dėl kvalifikuotų sertifikatų galiojimo;

j) jeigu elektroninio parašo kūrimo duomenys, susiję su elektroninio parašo patvirtinimo duomenimis, yra kvalifikuotame elektroninio parašo kūrimo įtaise, atitinkama tai nurodanti informacija pateikiama bent tokia forma, kad ją būtų galima tvarkyti automatizuotomis priemonėmis.

4.1.2 Sertifikato galiojimo atšaukimas

CA užtikrina sertifikatų galiojimo atšaukimą. Gautas prašymas visais atvejais užregistruojamas sertifikatų duomenų bazėje. Sertifikatai nutraukiami ir informacija apie sertifikatų galiojimo atšaukimo statusą paskelbiama ne vėliau kaip per 24 (dvidešimt keturias) valandas po prašymo gavimo dienos (CPS 4.1.4 str.). Sertifikatai netenka galios nuo jo nutraukimo momento, o nutraukimas įsigalioja nedelsiant po jo paskelbimo. Nutrauktų sertifikatų neatšaukiamumas yra realizuotas CA naudojamoje programinėje įrangoje: atšaukus sertifikatus ir jiems priskyrus būseną "revoked", ši būsena negali būti pakeista jokia kita.

4.1.2.1 Sertifikato galiojimo atšaukimo atvejai

Sertifikatų galiojimas atšaukimas tokias atvejais:

a) abonento ar sertifikatų savininko prašymu;

b) paaiškėjus, kad sertifikatų duomenys daugiau nėra teisingi;

c) paaiškėjus, kad sertifikatai buvo sudarytas remiantis neteisingais duomenimis;

d) sertifikatus išduodavęs CA nutraukia savo veiklą ir joks kitas patikimumo užtikrinimo paslaugų teikėjas neperima patikimumo užtikrinimo paslaugų teikimo veiklos;

e) CA sprendimu, paaiškėjus, kad sertifikatų savininkas nesilaiko sertifikato naudojimosi sąlygų;

f) sertifikatų savininkui praradus sertifikatus atitinkančių parašo formavimo duomenų kontrolę;

g) remdamasis sertifikatų galiojimo apribojimais, nurodytais sertifikate jį sudarant;

h) kai abonentas ar sertifikato savininkas nusprendžia nutraukti susitarimą su sertifikatus jam sudariusiu CA;

i) kai pažeidžiamas CA privačiojo rakto ir naudojamos sertifikatų tvarkymo sistemos saugumas, keliantis pavojų sudarytų sertifikatų patikimumui;

j) gavus pranešimą, kad sertifikatų savininkas tapo neveiksnus arba spaudo sertifikatų savininkas likviduojamas, išregistruojamas;

k) gavus pranešimą, kad sertifikatų savininkas mirė.

4.1.2.2 Asmenys turintys teisę kreiptis dėl sertifikato galiojimo atšaukimo

a) sertifikatų savininkas;

b) abonentas;

c) CA įgaliotasis asmuo (pvz. saugumo administratorius);

d) teisėsaugos institucijos.

4.1.3 Sertifikato galiojimo sustabdymas

Sertifikatų galiojimas, vadovaujantis nacionaliniais teisės aktais, sustabdomas per 4 (keturias) darbo valandas po prašymo gavimo. Sertifikatų sustabdymas visais atvejais nurodomas sertifikatų duomenų bazėje (CPS 4.1.4 str.), o tai, kad sertifikatai sustabdyti, matoma teikiant informaciją apie jų statusą. Sustabdyti sertifikatai netenka galios jų sustabdymo laikotarpiu.

4.1.3.1 Sertifikato galiojimo sustabdymo atvejai

Sertifikatų galiojimas sustabdomas šiais atvejais:

a) sertifikatų savininko prašymu;

b) teisėsaugos institucijų reikalavimu, siekiant užkirsti kelią nusikaltimams ;

c) gavus informacijos ar kilus įtarimui, kad sertifikatų duomenys yra neteisingi arba sertifikatų savininkas prarado sertifikatą atitinkančių parašo formavimo duomenų kontrolę.

4.1.3.2 Asmenys turintys teisę kreiptis dėl sertifikato galiojimo sustabdymo

Prašymus sustabdyti sertifikatų galiojimą gali teikti:

a) Sertifikatų savininkas;

b) CA įgaliotasis asmuo (pvz., saugumo administratorius);

c) teisėsaugos institucijos.

4.1.3.3 Sertifikato galiojimo sustabdymo atšaukimas

Sertifikatų galiojimo sustabdymas atšaukiamas gavus sertifikatų savininko arba Teisėsaugos institucijos, kurios prašymu sertifikatų galiojimas buvo sustabdytas, prašymą arba kai pasibaigia numatytas sustabdymo laikotarpis. Jei sertifikatų galiojimas buvo sustabdytas dėl šio CPS 4.1.3.2 dalies c) punkte nurodytos priežasties, sertifikatų galiojimo sustabdymas atšaukiamas gavus sertifikatų savininko prašymą ir paaiškinimą, paneigiantį CA gautą informaciją.

Kiti sertifikatų laikino sustabdymo aspektai reglamentuoti LR elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymo 12 ir 13 straipsniuose..

4.1.4 CRL atnaujinimo dažnumas

CRL atnaujinamas periodiškai netgi jei nenutraukiamas ar nesustabdomas nei vieno sertifikato galiojimas. Skelbiant eilinę CRL versiją visada nurodomas, kitos versijos skelbimo laikas. Ši informacija yra bet kuriuo metu prieinama tiek el. parašo, tiek el. spaudo sertifikatų savininkams, tiek visoms pasikliaunančioms šalims.

Informacija apie sertifikatų galiojimą, sustabdymą, atšaukimą asmeniui pateikiama jam kreipiantis su prašymu į CA. Informacija pateikiama saugiai, nemokamai bei veiksmingai.

Asmenims išduotų sertifikatų CRL ir Darbinės CA CRL atnaujinamas ne rečiau kaip kas 24 (dvidešimt keturias) val. Šakninės CA, kadangi ši tarnyba laikoma neprijungta prie tinklo, CRL atnaujinami ne rečiau kaip kas 6 (šešis) mėn.

Naujo CRL publikavimas nuo sugeneravimo iki paskelbimo užtrunka ne daugiau nei 60 (šešiasdešimt) min.

4.1.5 Sertifikatų galiojimo tikrinimo reikalavimai

Sertifikatų statusas tikrinamas naudojant OCSP atsakiklį arba remiantis CRL sąrašu. .

Parašo tikrintojai iš CA saugyklos (*repository*) turi parsisiųsti einamąją CRL versiją. Sertifikatų statuso tikrinimas, remiantis CRL, yra priimtinas, jei CRL atnaujinimo dažnumas parašo tikrintojui yra priimtinas.

4.1.5.1 Sertifikato galiojimo tikrinimas naudojantis OCSP atsakikliu

CA teikia galimybę sertifikatų būklę tikrinti naudojant OCSP atsakiklį, teikiantį informaciją apie sertifikato statusą realiu laiku. Paslauga teikiama 24 (dvidešimt keturias) val. per dieną, 7 (septynias) dienas per savaitę.

4.2. Įrašų apie CA operacijas kaupimas

4.2.1 Registruojamieji įvykiai

Svarbiausios sistemos operacijos fiksuojamos saugiame operacijų žurnale. Fiksuojamos operacijos apima:

a) užklausas sertifikatams gauti;

b) sertifikatų generavimo faktus;

c) sertifikatų statuso keitimo operacijas;

d) sertifikatų statuso tikrinimo užklausas ir atsakymus;

e) sertifikatų tarnybos sustabdymą ir paleidimą;

f) CRL generavimo ir publikavimo įrašus.

Kiekviename įraše turi būti ši informacija:

a) įvykio tipas;

b) įvykio identifikatorius;

c) įvykio data ir laikas;

d) identifikatorius arba kiti duomenys, įgalinantys nustatyti atsakingąjį už įvykį asmenį.

Informacinių sistemų, jų naudotojų ir administratorių veiksmų analizei atlikti yra sukurtas informacinių sistemų komponentų įvykių žurnalas. Fiksuojami duomenys apima:

a) informaciją apie informacinių sistemų tarnybinių stočių, taikomosios programinės įrangos ir kitų informacinių sistemų komponentų įjungimą, išjungimą ar perkrovimą. Taip pat sėkmingus/ nesėkmingus bandymus registruotis informacinių sistemų tarnybinėse stotyse, taikomojoje programinėje įrangoje, kituose informacinių sistemų komponentuose;

b) sistemų naudotojų atliekami elektroninės informacijos tvarkymo veiksmai;

c) sistemų administratorių atliekami veiksmai.

Operacijų žurnalas apsaugomas prieigos valdymo sistema ir pasirašomas infrastruktūriniu CA elektroniniu parašu.

Be operacijų žurnalo, vedami ir CA sistemų veiklos registravimo žurnalai, kurių pagalba galima stebėti sistemų darbą, gauti informaciją apie sistemų veiklos sutrikimus ir klaidas.

Diagnostikos žurnale fiksuojami detalūs sistemų veiksmai, kurie naudojami sistemų veikimo analizei, diagnostikai ir sutrikimų šalinimui. Pagrindiniai diagnostikos žurnalo naudotojai – sistemų kūrėjai ir administratoriai.

Klaidų žurnale (*Error Log*) fiksuojama informacija apie sistemų sutrikimus ir klaidas, nurodant sutrikimo laiką, šaltinį, aprašymą ir detalią informaciją.

Sistemų stebėsena gali būti atliekama ir standartinėmis programinėmis priemonėmis.

Į diagnostikos ir klaidų žurnalus įtraukiama ši informacija:

a) sistemų ugniasienių ir apsaugos nuo įsilaužimų sistemos (IDS) perspėjimai;

b) kiekvieno aparatinės ir programinės įrangos keitimo duomenys;

c) kompiuterių tinklo ir jo ryšių keitimo duomenys;

d) darbuotojų fizinio patekimo į saugias zonas ir pažeidimų duomenys;

e) slaptažodžių, PIN kodų ir darbuotojų pareigų keitimo duomenys;

f) sėkmingi ir nesėkmingi kreipiniai į CA duomenų bazes ir serverių taikomąsias programas;

g) CA raktų generavimo duomenys;

h) atsarginių kopijų, archyvinių įrašų, duomenų bazių kūrimo istorija.

4.2.2 Įrašų apie įvykius peržiūros dažnumas

CA sistemos operacijų ir veiklos registravimo žurnalai peržiūrimi ne rečiau kaip 1 (viena) kartą per mėnesį. Kiekvienas didesnės svarbos įvykis ar įvykis, atsitikęs dėl netinkamo sistemų funkcionavimo, turi būti aprašytas. Informacinių sistemų komponentų įvykių žurnalų elektroninės informacijos, susijusios su informacinių sistemų naudotojų ir informacinių sistemų administratorių atliekamais veiksmais, žurnalai peržiūrimi Registrų centro Saugos informacijos ir įvykių valdymo tvarkos apraše detalizuotais terminais bei tvarka.

4.2.3 Įrašų saugojimo periodas

CA sistemos operacijų ir veiklos registravimo žurnalai CA saugomi 10 (dešimt) metų, tolesnį saugojimą reglamentuoja Lietuvos Respublikos dokumentų ir archyvų įstatymo naujausia redakcija. Informacinių sistemų komponentų įvykių žurnalų saugojimo terminai bei tvarka detalizuoti Registrų centro Saugos informacijos ir įvykių valdymo tvarkos apraše.

4.2.4 Įrašų apsauga

CA sistemų operacijų ir veiklos registravimo žurnalų atsarginės kopijos daromos kiekvieną savaitę. Viršijus konkrečiam žurnalui numatytą įrašų kiekį, žurnalo turinys perkeliamas į archyvą. Į archyvą rašomi duomenys pasirašomi infrastruktūriniu CA elektroniniu parašu. Šifravimo raktą tvarko CA saugumo administratorius.

CA sistemos operacijų ir veiklos registravimo žurnalus peržiūrėti gali tik CA saugumo pareigūnas, CA administratorius ir auditorius. Kreipinio į žurnalą parametrai yra tokie, kad:

a) tik saugumo pareigūnas galėtų rašyti į archyvą arba ištrinti žurnalo failus;

b) būtų galimybė nustatyti bet kokį duomenų iškraipymo pažeidimą;

c) niekas neturėtų teisės pakeisti žurnalo turinio.

4.3. Duomenų archyvavimas

4.3.1 Į archyvą atiduodami duomenys

Į archyvą atiduodama:

a) CA sistemos operacijų ir veiklos registravimo žurnalai;

b) asmenų, kuriems buvo sudaryti sertifikatai, duomenų bazė;

c) sertifikatų duomenų bazė;

d) CRL sąrašai;

e) CA priklausančių raktų istorija nuo jų sugeneravimo iki sunaikinimo;

f) CA ir įgaliotų tarnybų tarpusavio susirašinėjimo ir susirašinėjimo su sertifikatų naudotojais, kuriems buvo teikiamos paslaugos, informacija.

4.3.2 Duomenų saugojimo archyve periodas

Duomenys archyve saugomi 10 (dešimt) metų, tolesnį saugojimą reglamentuoja Lietuvos Respublikos dokumentų ir archyvų įstatymas.

4.3.3 Archyvo apsauga

Archyvas saugomas laikantis Registrų centro numatytos vidinės tvarkos ir Lietuvos Respublikos dokumentų ir archyvų įstatymo.

4.3.4 Atsarginių kopijų darymas

Atsarginės kopijos įgalina atstatyti sistemos darbą po sutrikimų. Tuo tikslu daromos šios programinės įrangos ir duomenų failų kopijos:

a) instaliacinio disko su sistemos programine įranga;

b) instaliacinio disko su CA ir RA taikomosiomis programomis;

c) WWW serverio ir saugyklos instaliaciniai diskai;

d) CA sudarytų sertifikatų ir CRL istorijos kopijos;

e) saugyklos (repository) duomenų kopija;

f) asmenų, kuriems yra sudaryti sertifikatai, duomenų;

g) CA sistemų operacijų ir veiklos registravimo žurnalų.

Duomenų bazių atsarginės kopijos daromos kiekvieną dieną, o kitos informacijos – kartą per savaitę. RCSC sistemų darbas po sutrikimų atstatomas ne vėliau kaip per 48 (keturiasdešimt aštuonias) valandas.

4.4. Saugumo incidentai ir jų valdymas

CA vadovaujasi Registrų centro saugos informacijos ir įvykių valdymo tvarka. Įvykių valdymo procesu siekiama:

a) suteikti priemones išankstiniam informacinių technologijų incidentų, elektroninės informacijos saugos (kibernetinių) incidentų aptikimui ir tyrimui;

b) įvykių valdymu suteikti priemones automatiniam duomenų surinkimui, koreliavimui, informacijos pateikimui;

c) naudojantis Įvykių valdymo proceso įgyvendinimui skirtomis priemonėmis surinkti ir išsaugoti duomenis apie Registrų centro informacinių technologijų infrastruktūros veiklą. Sudaryti sąlygas sėkmingiau tirti pastebėtus informacinių technologijų, elektroninės informacijos saugos incidentus ir, esant pokyčiams Registrų centrui keliamiems reikalavimams, juos greičiau įgyvendinti.

Įvykių valdymo procesas CA atžvilgiu apima įvykius, kurie yra generuojami informacinių sistemų komponentų ir įvykių žurnalų pavidalu perduodami saugoti į techninę ar programinę įrangą, pritaikytą duomenims saugoti, ir analizuojami specializuotomis įvykių žurnalų analizės priemonėmis. Įvykių valdymo procesas apima šių įvykių tipus:

a) įvykiai, kurie pažymi normalią informacinių sistemų komponentų veiklą;

b) įvykiai, kurie pažymi neįprastą informacinių sistemų komponentų veiklą;

c) įvykiai, kurie pažymi neatitiktis informacinių sistemų komponentų veikloje.

Saugos informacijos ir įvykių valdymo tvarkos aprašas detalizuoja:

a) CA įvykių valdymo procesų efektyvumo kriterijus;

b) CA darbuotojams priskirtus vaidmenis bei jų atsakomybę;

c) CA įvykių valdymo procedūra;

d) CA pokyčių operacinę procedūrą.

4.4.1 Incidentų registravimo, identifikavimo bei analizės procedūra

CA vadovaujasi tokia tvarka:

a) fiksavus informacinių sistemos veiklos sutrikimus/ incidentus, kurie pažymi neįprastą ar neatitinkančią informacinių sistemų komponentų veiklą, tokie sutrikimai/ incidentai visais atvejais yra registruojami įvykių žurnale, kuris turi būti archyvuojamas ir apsaugotas nuo pažeidimo, praradimo, nesankcionuoto ar netyčinio pakeitimo, ar sunaikinimo siekiant užtikrinti, kad elektroninės informacijos saugos (kibernetinių) incidentų metu įvykdytų nusikalstamų veikų įrodymai būtų tinkami ir pakankami teisėsaugos institucijoms nustatyti nusikalstamų veikų faktą, o nusikalstamas veikas įvykdę asmenys negalėtų jo paneigti;
b) registravus sutrikimą/ incidentą jie vadovaujantis Saugos informacijos ir įvykių valdymo tvarkos aprašu yra prioritizuojami bei identifikuojami. Identifikavimo metu įvykio įrašas

yra atpažįstamas ir jam, priklausomai nuo specializuotų įvykių žurnalų analizės priemonių nustatymų, priskiriama kategorija ir prioritetas;

c) analizės metu yra įvertinama, ar įvykis arba įvykių visuma duotuoju laiko momentu atitinka tam tikras specializuotų įvykių žurnalų analizės priemonių nustatytas įspėjimo generavimo taisykles. Jei analizės metu specializuotos įvykių žurnalų analizės priemonės nustato, kad tam tikras įvykis arba įvykių visuma duotuoju laiko momentu atitinka tam tikras nustatytas įspėjimo generavimo taisykles, tuomet specializuotos įvykių žurnalų analizės priemonės automatiškai sugeneruoja įspėjimą;

d) informacinių sistemų komponentų administratoriai turi peržiūrėti sugeneruotą įspėjimą ir, esant reikalui, apie įspėjimą, jo turinį ir aplinkybes informuoti atsakingus asmenis;

e) paskirtasis saugumo pareigūnas turi peržiūrėti sugeneruotą įspėjimą ir įvertinti ar jis gali būti susijęs su saugumo ir vientisumo pažeidimais numatytais eIDAS 19 str. 2 d. Nustačius, jog incidentas gali būti susijęs su eIDAS 19 str. 2 d. numatytais saugumo bei vientisumo pažeidimais, saugumo pareigūnas nedelsiant, bet ne vėliau kaip per 4 (keturias) val. privalo sušaukti darbo grupę. Apie minėtus incidentus priežiūros įstaiga ir fiziniai ar juridiniai asmenys informuojami CPS 4.4.2 . 2 d. e) punkte nustatyta tvarka ne vėliau kaip per 24 (dvidešimt keturias) val.

f) Registrų centro direktoriaus įsakymu nustatyta informacinių technologijų incidentų ir elektroninės informacijos saugos (kibernetinių) incidentų valdymo tvarka turi užregistruoti atitinkamą incidentą su žyma, jog jis yra susijęs su eIDAS 19 str. 2 d. numatytu saugumo bei vientisumo pažeidimu;

g) siekiant užtikrinti atitiktį teisiniams reikalavimams ir turėti sukauptus duomenis galimiems elektroninės informacijos saugos (kibernetinių) incidentų tyrimams ateityje, visi įvykiai turi būti išsaugomi.

4.4.2 Aparatūros ir programinės įrangos gedimai

1. CA atsižvelgia į šias patikimumo užtikrinimo paslaugų patikimumui ir stabilumui turinčias grėsmes:

a) fizinis CA kompiuterinės sistemos, įskaitant kompiuterių tinklą, pažeidžiamumas. Ši grėsmė apima ir pažeidimus avarijų atvejais;

b) programinės įrangos veikimo sutrikimai, pažeidžiantys prieigą prie duomenų. Šios grėsmės siejamos su operacine sistema, vartotojų taikomosiomis programomis ir kenkėjiškomis programomis, pvz.: virusais, „Trojos arkliais“, kt.;

c) išorinio kompiuterių tinklo funkcionavimo, turinčio įtaką CA interesams, sutrikimai. Tai siejama su elektros energijos tiekimo sutrikimais ir ryšio linijų nutraukimais;

d) vidinio tinklo ar jo dalies sutrikimai.

2. Aukščiau minėtoms grėsmėms išvengti arba jų įtakai sumažinti, CA laikosi šių procedūrų:

a) **gedimų šalinimas**. Visi sertifikatų naudotojai kaip įmanoma greičiau ir konkrečios situacijos atveju geriausiai tinkančiomis priemonėmis yra informuojami apie kiekvieną rimtesnį CA sistemos ar kompiuterių tinklo sutrikimą. Yra numatytos procedūros, kurios vykdomos atsitikus kompromitaciniam įvykiui (gedimui, informacijos atskleidimui, kt.). CA įgyvendinamos prevencinės priemonės:

- daromos kiekvieno serverio ir darbo stoties diskų kopijos (*images*) ir dedamos į archyvą;
- kiekvieną dieną, laikantis 4.3.4 skyriuje aprašytų procedūrų, daromos duomenų bazių atsarginės kopijos;
- kartą per savaitę, laikantis 4.3.4 skyriuje aprašytų procedūrų, daromos kiekvieno serverio kietojo disko informacijos atsarginės kopijos;
- kompiuterių keitimas atliekamas taip, kad kietųjų diskų turiniai būtų atstatyti iš vėliausiai padarytų jų kopijų;
- po gedimo atstatytoje sistemoje testuojamas kiekvienas jos komponentas.

b) **sistemos pakeitimų darymo priežiūra**. Naudojamos sistemos programinė įranga gali būti atnaujinama tik kruopščiai ištestavus keičiamų komponentų naująsias versijas. Kiekvieną sistemoje padarytą pakeitimą turi patvirtinti CA saugumo pareigūnas. Jeigu pagal nustatytas procedūras įdiegti nauji komponentai tampa sistemos veiklos sutrikimų priežastimi, skubiai atstatoma buvusios sudėties sistema;

c) **papildomos priemonės**. Sistemai apsaugoti nuo elektros energijos tiekimo pertrūkių ir užtikrinti nepertraukiamą paslaugų teikimą naudojami atsarginiai energijos šaltiniai (UPS – *Uninterrupted Power Supply, dyzeliniai elektros generatoriai*). Jie gali teikti elektros energiją sistemai ne trumpiau kaip 96 (devyniasdešimt šešias) val.

d) **rizikos vertinimas.** Be aukščiau minėtų procedūrų, kurių yra laikomasi siekiant išvengti grėsmių ar maksimaliai sumažinti jų atsiradimo riziką, reguliariai yra rengiamas CA vertybių ir rizikos veiksnių vertinimas, kuriame atsižvelgiant į teisės aktus, organizacijos tikslus, strategiją bei politiką, veiklos procesus, informacijos apsaugos politiką, informaciją, kaip turtą, socialinę aplinką, suinteresuotų šalių lūkesčius, informacijos mainus su aplinka, yra nustatomos saugumo rizikos ribos bei pagrindinės vertybės.

e) **informavimas apie incidentus.** CA nedelsiant, tačiau bet kuriuo atveju ne vėliau kaip per 24 (dvidešimt keturias) val. nuo to momento kai sužinojo, užpildydama incidentų notifikavimo formą praneša priežiūros įstaigai ir prireikus kitoms atitinkamoms institucijoms, kaip informacijos saugumo klausimais kompetentingai nacionalinei įstaigai arba duomenų apsaugos institucijai, apie visus saugumo arba vientisumo pažeidimus, turėjusius didelį poveikį teikiamoms paslaugoms arba jas teikiant naudojamiems asmens duomenims. Priežiūros įstaigai teikiama incidentų notifikavimo forma pildoma vadovaujantis Pranešimų apie patikimumo užtikrinimo paslaugų saugumo ir (ar)

vientisumo pažeidimus teikimo tvarkos aprašu[1]. Kai saugumo ir vientisumo pažeidimas turėjo neigiamo poveikio fiziniam/ juridiniam asmeniui, CA nedelsiant praneša apie saugumo ir vientisumo pažeidimą tam fiziniam/ juridiniam asmeniui. Jei priežiūros įstaiga nustato, kad saugumo ir vientisumo pažeidimas yra svarbus visuomenei ji ją informuoja, arba nurodo CA tai padaryti. Esant tokiam priežiūros įstaigos prašymui, CA nedelsiant turimomis priemonėmis informuoja visuomenę.

4.4.3 Privačiojo rakto kompromitacija

Kai sukompromituojamas CA priklausantis privatusis raktas, kuris naudojamas sudarytiems sertifikatams ir CRL pasirašyti, arba įtariama jo kompromitacija, CA imasi tokių veiksmų:

a) sertifikatų naudotojai, nedelsiant ir bet kuriuo atveju ne vėliau kaip per 24 (dvidešimt keturias) val. nuo to momento kai CA apie tai sužinojo, informuojami apie CA privačiojo rakto kompromitaciją masinėmis informacijos platinimo ir kitomis priemonėmis;

b) sukompromituotą privatųjį raktą atitinkantis CA sertifikatas dedamas į CRL, nurodant galiojimo nutraukimo priežastį;

c) nutraukiamas visų CA asmenims sudarytų sertifikatų galiojimas, nurodant galiojimo nutraukimo priežastį.

4.4.4 Saugumo priemonės pašalinus gedimų priežastis

Atstačius sistemą po gedimo, CA saugumo pareigūnas privalo:

a) pakeisti visus prieš tai naudotus slaptažodžius;

b) atšaukti ir iš naujo suteikti prieigos prie sistemos resursų teises;

c) pakeisti visus kodus (PIN ir kt.), susijusius su fiziniu patekimu į CA patalpas ir prieiga prie sistemos komponentų;

d) peržiūrėti CA tinklo saugumo, fizinio patekimo į patalpas ir prieigos prie sistemos komponentų taisykles;

e) informuoti kiekvieną sistemos naudotoją apie sistemos atstatymą.

[1] Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2019 m. birželio 4 d. įsakymas Nr. 1V-594 „Dėl Pranešimų apie patikimumo užtikrinimo paslaugų saugumo ir (ar) vientisumo pažeidimus teikimo tvarkos aprašo patvirtinimo".

4.5. Patikimumo užtikrinimo paslaugų teikimo nutraukimas

RCSC prieš nutraukdamas patikimumo užtikrinimo paslaugų teikimo veiklą įsipareigoja veikti pagal su priežiūros įstaiga suderintą veiklos nutraukimo planą (toliau – suderintas planas), įskaitant šiuos veiksmus (kiek jie neprieštarauja suderintam planui):

a) apie tai informuoti visus asmenis, kurių sertifikatus jis sudarė ir kurių sertifikatai yra galiojantys, bei kitus patikimumo užtikrinimo paslaugų teikėjus, su kuriais yra pasirašytos laidavimo sutartys, partnerius, kuriems sutarčių pagrindu yra perduotos CSP, kaip patikimumo užtikrinimo paslaugų teikėjo funkcijos, trečiąsias šalis, kurioms sutarčių pagrindu teikiamos patikimumo užtikrinimo paslaugos, taip pat priežiūros įstaigą ne vėliau kaip prieš 9 (devynis) mėnesius;

b) atsižvelgiant į numatytą paslaugų nutraukimo datą, tačiau ne vėliau kaip prieš 6 (šešis) mėnesius priežiūros įstaigai pateikia: 1) informaciją apie veiklos perėmėją; 2) veiklos perėmimo sutartį; 3) Detalųjį kvalifikuotų patikimumo užtikrinimo paslaugų teikimo veiklos nutraukimo planą.

c) jei nusprendus nutraukti kvalifikuotų patikimumo užtikrinimo paslaugų teikimą, veikla nėra perduodama trečiajai šaliai, CSP turi užtikrinti asmenims išduotų sertifikatų gyvavimą jų galiojimo laikotarpiu bei visos surinktos (teikiant patikimumo užtikrinimo paslaugas) informacijos saugojimą, kad ją būtų galima panaudoti teismo procese kaip įrodymą. Siekiant įgyvendinti šį įsipareigojimą, CSP užtikrins OCSP ir CRL generavimo funkcijas iki visų išduotų kvalifikuotų sertifikatų galiojimo pabaigos, t. y. tiek savalaikės, tiek po atšaukimo bei prašymų sustabdyti/ atšaukti sertifikatus priėmimą ir įvykdymą.

d) Neturint galimybės užtikrinti asmenims išduotų sudarytų sertifikatų gyvavimo jų galiojimo laikotarpiu šių sertifikatų galiojimas yra nutraukiamas, o asmenims sudaromiems sertifikatams sudaryti naudojamų patikimumo užtikrinimo paslaugų teikėjų privatūs kriptografiniai raktai, taip pat atsakymams į OCSP užklausas pasirašyti skirti privatūs kriptografiniai raktai sunaikinami nedelsiant po asmenims sudarytų sertifikatų galiojimo nutraukimo. Detalios naikinimo procedūros nustatomos Detaliajame kvalifikuotų patikimumo užtikrinimo paslaugų teikimo veiklos nutraukimo plane.

e) nutraukti visų trečiųjų šalių įgaliojimus veikti CA vardu, teikiant patikimumo užtikrinimo paslaugas.

4.6. Patikimumo užtikrinimo paslaugų teikimo tęstinumo planas

CA, atsižvelgdama į grėsmes patikimumo užtikrinimo paslaugų patikimumui ir stabilumui, laikosi veiklos tęstinumo plane aprašytų taisyklių ir procedūrų, kurios yra būtinos siekiant atkurti veiklą įvykus elektroninės informacijos saugos incidentui. Elektroninės informacijos saugos incidentas, šiuo atveju suprantamas kaip įvykis ar veiksmas, kuris gali sudaryti

neleistino prisijungimo prie sertifikatų valdymo informacinės sistemos galimybę, sutrikdyti ar pakeisti jos veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti (pvz., duomenų neatitikimas ar pažeidimas, atsiradę konkretūs nesklandumai, ekrano pranešimai, neįprastas funkcionavimas, paslaugų, įrangos ar priemonių netektis, sistemos sutrikimai ar persikrovimai, žmogiškosios klaidos, fizinio saugumo pažeidimas, nesankcionuoti sistemos pakeitimai, nesankcionuota prieiga, saugos politikos neatitikimas ir kt.).

5. FIZINIO, PROCEDŪRINIO IR PERSONALO SAUGUMO KONTROLĖ

5.1. Fizinio saugumo kontrolė

CA kompiuterių sistema, operatorių darbo vietos, informacijos resursai yra įrengti ir laikomi tam tikslui skirtoje vietoje, kuri yra fiziškai apsaugota nuo neleistino patekimo į ją, įrangos sunaikinimo ar išnešimo.

Siekiant užtikrinti sertifikatų statuso, tikrinamo naudojant OCSP protokolą, paslaugos veikimo patikimumą, paslauga teikiama lygiagrečiai per dvi nepriklausomas atšakas, kurios patalpintos dvejose nutolusiose serverinėse ir veikia *Active-Active* režimu.

Prieiga prie kertinių sistemos elementų yra stebima. Kiekvienas asmenų patekimas į ją yra registruojamas, stebimas elektros energijos tiekimo stabilumas, temperatūra ir drėgmė.

Įrengiama papildoma „karšta" telefono linija, skirta automatiškai priimti ir išsaugoti asmenų balso pranešimus, kuriais prašoma stabdyti sertifikatų galiojimą, sutrikus Palaikymo tarnybos veiklai. Atstačius Palaikymo tarnybos veiklą, visi pranešimai yra apdorojami laikantis šiuose Sertifikavimo veiklos nuostatuose nustatytų reikalavimų.

5.1.1 Buveinės vieta

RCSC buveinės adresas yra:

Vinco Kudirkos g. 18-3, LT-03105 Vilnius, Lietuva.

RCSC techninės įrangos talpinimo adresai yra:

Vinco Kudirkos g. 18-3, LT-03105 Vilnius, Lietuva

Tilto g. 17, LT-01101 Vilnius, Lietuva

5.1.2 Fizinė prieiga

Bendri vidaus tvarkos reikalavimai dėl patekimo į Registrų centro patalpas detalizuoti Valstybės įmonės Registrų centro darbo tvarkos taisyklių, II skyriuje.

Fiziniam patekimui į CA patalpas bei darbuotojų veiklai patalpų viduje kontroliuoti yra įrengta vaizdo stebėjimo bei garso signalizacijos sistema, veikianti ištisą parą.

CA lankytojai priimami darbo dienomis Registrų centro direktoriaus įsakymu patvirtintomis darbo valandomis. Likusiu laiku (įskaitant nedarbo dienas) CA buveinėje gali lankytis tik RCSC vadovybės įgaliojimus turintys asmenys, kurių vardai ir pavardės yra žinomi apsaugos tarnybai.

Lankytojai patekti į RCSC patalpas gali tik lydimi RCSC įgaliotų asmenų.

Yra skiriamos 3 (trys) RSCS patalpų saugumo zonos:

a) kompiuterinės sistemos zoną;

b) operatorių ir administratorių zoną;

c) projektuotojų ir programuotojų zoną.

Kompiuterinės sistemos zona yra įrengta bendrose Registrų Centro tarnybinių stočių saugyklose. Su patikimumo užtikrinimo paslaugomis susijusi įranga yra saugoma atskiroje tarnybinių stočių spintose. Patekimą į tarnybinių stočių saugyklas reguliuoja identifikacinių kortelių sistema.

Patekimą į operatorių ir administratorių zoną reguliuoja identifikacinių kortelių sistema. Įslaptintai informacijai saugoti naudojami seifai. Prieš naudojimąsi operatoriaus ir administratoriaus terminalais patikrinami darbuotojo įgaliojimai.

Projektuotojų ir programuotojų zona yra saugoma taip pat kaip ir operatorių bei administratorių zona. Projektuotojai ir programuotojai neturi prieigos prie jautrios (įslaptintos) informacijos.

5.1.3 Elektros energijos tiekimas ir oro kondicionavimas

Registrų centro tarnybinių stočių saugyklose yra įrengtos modernios oro kondicionavimo sistemos. Nutrūkus elektros energijos tiekimui iš tinklo, atsarginiai energijos šaltiniai (4 UPS ir 3 dyzeliniai elektros energijos generatoriai) užtikrina normalų sistemos darbą 96 (devyniasdešimt šešias) valandas.

5.1.4 Apsauga nuo užpylimo vandeniu

Kompiuterinės sistemos zonoje yra įdiegti drėgmės ir vandens jutikliai. Jie yra įjungti į visų Registrų centro patalpų apsaugos sistemą. Pirminiai bei pasekmių likvidavimo veiksmai, atsakingi vykdytojai užpylimo atveju, detalizuoti sertifikatų valdymo informacinės sistemos veiklos tęstinumo detaliajame plane.

5.1.5 Priešgaisrinė apsauga

RCSC patalpose yra įdiegta priešgaisrinės apsaugos sistema, atitinkanti priešgaisrinės apsaugos tarnybos nustatytus reikalavimus. Tarnybinių stočių saugyklose įdiegtos automatinės gesinimo inertinėmis dujomis sistemos. Pirminiai bei pasekmių likvidavimo veiksmai, atsakingi vykdytojai gaisro atveju, detalizuoti sertifikatų valdymo informacinės sistemos veiklos tęstinumo detaliajame plane.

5.1.6 Informacijos laikmenų saugojimas

Priklausomai nuo informacijos svarbos, laikmenos su archyvų duomenimis ir atsarginėmis duomenų kopijomis yra saugomos ugniai atspariuose seifuose, kurie stovi operatorių ir administratorių zonose.

5.1.7 Atliekų tvarkymas

Popierius ir elektroninės laikmenos, kuriose yra RCSC veiklos saugumui įtakos turinti informacija, pasibaigus tos informacijos saugojimo terminui sunaikinamos specialiais plėšymo įrenginiais. Šifravimo raktų ir PIN kodų laikmenos yra naikinamos DIN3 klasės įrenginiais (taip naikinamos tik laikmenos, kuriose neįmanoma visiškai sunaikinti saugomos informacijos, pvz., kriptografinės kortelės).

5.2. Procedūrinio saugumo kontrolė

5.2.1 Darbuotojų pareigos

Aukštos atsakomybės pareigos, nuo kurių priklauso CA veikla yra šios:

a) **saugumo pareigūnas**. Bendra atsakomybė už saugumo politikos vykdymą. Inicijuoja ir stabdo CA paslaugas, vadovauja raktų ir kitų slaptųjų duomenų generavimui, skiria CA darbuotojams teises saugumo požiūriu ir prieigos prie sistemos teises, teikia pradinius slaptažodžius vartotojams, prižiūri tikrinimo procedūras, priima patikrinimų protokolus ir rengia atsakymus į juos, prižiūri tikrinimo metu pastebėtų trūkumų šalinimą;

b) **CA administratorius**. Atsakingas už CA sistemų administravimą. Instaliuoja ir konfigūruoja naudojamą įrangą; nustato sistemos ir tinklo parametrus.

c) **CA operatorius**. Atsakingas už kasdienes sertifikatų sudarymo ir tvarkymo procedūras, rengia duomenų atsargines kopijas;

d) **CA auditorius.** Atsakingas už registracijos žurnalų tvarkymą ir peržiūrą bei už vidinių patikrinimų atlikimą.

Šių pareigų paskirstymas užkerta kelią CA sistemos naudojimo piktnaudžiavimams. Kiekvienam sistemos naudotojui yra leistini tik jo pareigose numatyti veiksmai (3 pav.).

	Saugumo pareigūnas	CA administratorius	CA operatorius	CA auditorius
Saugumo pareigūnas		X	X	X

CA administratorius	X		X	X
CA operatorius	X	X		X
CA auditorius	X	X	X	

3 pav. Aukštos atsakomybės pareigybių matrica (X – pareigybė negalima).

5.2.2 Reikalingas darbuotojų kiekis užduočiai atlikti

Raktų, kuriuos CA naudoja sudarytiems sertifikatams arba CRL pasirašyti, generavimas ir atstatymas reikalauja ypatingo dėmesio. Generuojant ar atstatant raktus turi dalyvauti mažiausiai 4 (keturi) asmenys: 2 (du) asmenys vykdantys procedūras ir 2 (du) stebėtojai.

5.2.3 Pareigų identifikacija ir autentiškumo tikrinimas

CA darbuotojų pareigų identifikacija ir autentiškumo tikrinimas atliekami tokiais atvejais:

a) sudarant asmenų sąrašą, kuriems leidžiama patekti į CA patalpas;

b) sudarant asmenų sąrašą, kuriems leidžiama fizinė prieiga prie CA sistemos ir tinklo resursų;

c) skiriant vartotojų darbo laukus (accounts) ir slaptažodžius CA informacinėje sistemoje.

Kiekvienas patvirtinimas ar paskyrimas:

a) yra unikalus ir betarpiškai susietas su konkrečiu asmeniu;

b) jais negali būti dalinamasi su bet kuriais kitais asmenims;

c) numato ribotas funkcijas (kylančias iš konkretaus asmens pareigų).

CA operacijos, kurioms atlikti reikia paskirstytųjų (*shared*) tinklo resursų, apsaugomos griežtomis autentiškumo patvirtinimo ir siunčiamos informacijos šifravimo priemonėmis.

5.3. Personalo patikimumo kontrolė

Asmenys į darbą priimami vadovaujantis Lietuvos Respublikos darbo kodekso reikalavimais. Priėmimas į darbą įforminamas darbo sutartimi. Darbo tvarkos taisyklėse (III skyrius, 26 p.) yra nurodyti bendri darbuotojams keliami kvalifikacijos reikalavimai:

a) mokėti lietuvių kalbą;

b) turėti reikalingą išsilavinimą arba kvalifikaciją;

c) mokėti dirbti kompiuteriu ir kita organizacine technika;

d) mokėti užsienio kalbą (jeigu reikalinga).

Be minėtų bendrų reikalavimų garantuojama, kad CA pavestas pareigas atliekantys asmenys:

a) sudarantys ir tvarkantys sertifikatus turi aukštąjį išsilavinimą;

b) yra pasirašę susitarimą dėl pareigų vykdymo ir atsakomybės;

c) yra išklausę vidinius mokymus, susijusius su jiems pavestų pareigų vykdymu;

d) yra išklausę mokymus, susijusius su asmens duomenų ir konfidencialios informacijos apsauga, susipažinę su saugos dokumentais bei yra pasirašę pasižadėjimą dėl konfidencialios informacijos saugojimo jog yra susipažinę su saugos dokumentais.

e) neturi neišnykusio ar nepanaikinto teistumo už tyčinių nusikaltimų padarymą.

5.3.1 Biografijos tikrinimo procedūra

Priimamiems darbuotojams, vadovaujantis darbo tvarkos taisyklių III skyriuje, 30 p. nustatyta bendra tvarka privaloma pateikti:

a) asmens tapatybę patvirtinantį dokumentą;

b) valstybinio socialinio draudimo pažymėjimą;

c) teistumo (neteistumo) pažymą[2];

d) išsilavinimą, profesinį parengimą patvirtinančius dokumentus;

e) gyvenimo aprašymą;

f) privalomojo sveikatos patikrinimo medicininę pažymą;

g) neįgalaus asmens pažymėjimą, jei turi;

h) vaiko (-ų) gimimo liudijimą (-us);

[2] Pagal Valstybės įmonės Registrų centro generalinio direktoriaus 2019 m. rugpjūčio 30 d. įsakymą Nr. VE-421 (1.3 E) „Dėl Korupcijos prevencijos priemonių įgyvendinimo tvarkos aprašo ir Pareigybių, tikrinamų valstybės įmonėje Registrų centre pagal Lietuvos Respublikos korupcijos prevencijos įstatymo 9 straipsnį, sąrašo patvirtinimo" ir Lietuvos Respublikos korupcijos prevencijos įstatymą

i) santuokos ar ištuokos liudijimą.

Be aukščiau minėtų bendrų dokumentų, pagal kuriuos yra užvedama bei saugoma darbuotojo asmens byla, darbuotojas privalo patvirtinti, jog nėra teistas. Šis dokumentas taip pat saugomas darbuotojo asmens byloje.

5.3.2 Mokymo reikalavimai

CA darbuotojai turi būti išklausę mokymus ir susipažinę su:

a) CP ir CPS;

b) RA taisyklėmis;

c) CA ir RA saugumo reikalavimais ir jų laikymosi tikrinimo procedūromis;

d) CA ir RA sistemų programine įranga;

e) atsakomybe už sistemos atliekamų veiksmų sutrikimus;

f) galimais sistemos veikimo sutrikimais.

5.3.3 Mokymų dažnumas ir reikalavimai jiems

5.3.2 skyriuje aprašyti mokymai kartojami arba vedami papildomi mokymai, kai tik padaromi žymesni CA ar RA veiklos pakeitimai.

5.3.4 Reikalavimai samdomiems asmenims

Samdomi asmenys, atliekantys užduotis pagal sutartis (išorinių paslaugų tiekėjai, programinės įrangos kūrėjai, kt.), tikrinami laikantis tokių pačių procedūrų, kurios taikomos CA darbuotojams. Be to, samdomus asmenis, atliekančius užduotis CA patalpose, turi lydėti CA darbuotojas.

5.3.5 Darbuotojams teikiami dokumentai

CA užtikrina savo darbuotojams prieigą prie šių dokumentų:

a) CP ir CPS;

b) reikiamų valstybės registrų;

c) CA sistemos naudotojų teisių ir pareigų aprašų.

6. TECHNINIO SAUGUMO KONTROLĖ

6.1. Kriptografinių raktų poros generavimas ir instaliavimas

6.1.1 Raktų porų generavimas

CA raktų poros generuojamos specialiai tam skirtu darbo vietos kompiuteriu (*workstation*), sujungtu su aparatiniu saugumo moduliu (kriptografiniu moduliu). Aparatinis saugumo modulis atitinka FIPS PUB 140-2 standarto trečiojo saugumo lygio (*Level3*) reikalavimus. Raktų porų generavimo veiksmai yra registruojami, nurodoma jų atlikimo data ir pasirašomi visų generavimo procese dalyvavusių asmenų. Padaryti įrašai yra saugomi, nes jų vėliau gali prireikti atliekant tikrinimus.

Visi asmenims sudaromų sertifikatų privatieji raktai yra generuojami aparatinėmis priemonėmis, todėl raktai yra apsaugoti nuo kopijavimo ar kitokio neteisėto panaudojimo. Sertifikatai sudaromi tik asmenims naudojantiems CA teikiamą SSCD/QSCD, atitinkančius eIDAS 29 str. ir 30 str. reikalavimus.

6.1.2 Viešojo rakto perdavimas sertifikato sudarytojui

CA sudaro sertifikatus asmenims, kurių raktai generuojami CA parengtoje SSCD/QSCD. Sugeneruotas viešasis raktas saugiomis priemonėmis perduodamas CA.

6.1.2.1 SSCD/QSCD parengimas ir perdavimas naudotojui

CA SSCD/QSCD parengimo ir perdavimo naudotojui procesuose taikomos saugumo užtikrinimo priemonės:

a) išduodama tik SSCD/QSCD: kvalifikuoto elektroninio parašo sertifikatams – atitinkanti eIDAS 29 str. ir 30 str., o kvalifikuoto elektroninio spaudo sertifikatams atitinkanti eIDAS 39 str. 1 d. ir 39 str. ir 2 d. nustatytus reikalavimus.

b) iki SSCD/QSCD priskyrimo asmeniui ir sertifikato generavimo inicijavimo, SSCD/QSCD yra saugiai sandėliuojama, laikantis visų SSCD/QSCD gamintojo instrukcijų;

c) priskyrus SSCD/QSCD asmeniui arba sugeneravus SSCD/QSCD viešojo rakto sertifikatą, privataus rakto aktyvavimo duomenys (PIN) yra apsaugoti (apsauginiame voke arba po apsauginiu dažų sluoksniu) taip užtikrinama, kad aktyvavimo duomenų nesankcionuotos peržiūros atvejai būti aptinkami iki SSCD/QSCD perdavimo asmeniui arba SSCD/QSCD perdavimo asmeniui metu;

d) išduodant SSCD/QSCD yra atliekama asmens identifikavimo procedūra, fiksuojama tiksli SSCD/QSCD perdavimo data ir laikas minučių tikslumu;

e) SSCD/QSCD išduodami tik asmeniui atvykus į RA, SSCD/QSCD nėra siunčiamas ar perduodamas naudotojui kitais kanalais.

6.1.4 CA viešojo rakto perdavimas vartotojams

CA savo viešąjį raktą, kuris atitinka sudarytiems asmenų sertifikatams ir CRL pasirašyti naudojamą privatųjį raktą, platina vartotojams tokiais būdais:

a) sertifikatas yra padėtas viešai prieinamoje saugykloje (*repository*);

b) sertifikatas platinamas drauge su programine įranga, įgalinančia naudotis CA paslaugomis.

6.1.5 Raktų dydžiai

CA generuoja tokio dydžio raktus:

Šakninės sertifikavimo tarnybos raktai RSA 4096 bitų ilgio;

Darbinės sertifikavimo tarnybos raktai RSA 2048 bitų ilgio;

Asmenims generuojami raktai RSA 2048, bitų ilgio arba ECC 256.

6.1.6 Aparatinis/programinis raktų generavimas

CA raktai generuojami aparatiniais saugumo moduliais (kriptografiniais moduliais) atitinkančiais CP reikalavimus.

Asmenims raktai generuojami tik aparatiniu būdu.

6.2. Privačiojo rakto apsauga

CA ir prašantieji sudaryti sertifikatus asmenys privačiajam raktui generuoti ir saugoti naudoja patikimas sistemas, apsaugančias privatųjį raktą nuo pametimo, atskleidimo, pakeitimo ar nesankcionuoto panaudojimo. CA, generuojantis raktus ir rengiantis SSCD/QSCD, asmenų prašymu, privalo saugiai perduoti ją užsakiusiems asmenims ir įpareigoti juos saugoti savo privačiuosius raktus.

CA sertifikato teikimo funkciją atlieka įrenginys TSP – ncipher netHSM 2000, Thales nShield Connect HSM 1500+, ncipher nShield F3 500 PCI, nchiper nShield F3 2000 PCI, atitinkantis FIPS 140-2 Level 3 Certified reikalavimus. Sertifikato Nr.: 2148, 1195, 1708, 1198, 1741.HSM naudojami pagal gamintojo numatytus reikalavimus, t. y. kodavimo algoritmus, raktų ilgius ir kt. Raktų generavimo procedūros atliekamos pagal gamintojo pateiktus reikalavimus.

6.2.1 Kriptografinių modulių standartai

CA naudojami aparatiniai saugumo moduliai (kriptografiniai moduliai) gavo ne žemesnį EAL 4 ar aukštesnio lygio standartą pagal ISO/IEC 15408 ar lygiaverčius nacionaliniu arba tarptautiniu mastu pripažintus IT saugumo vertinimo kriterijus; arba ISO/IEC 19790 ar FIPS PUB 140-2 3 lygio reikalavimus.
Asmenims rengiama SSCD/QSCD, kuri atitinka kvalifikuotam elektroninio parašo kūrimo įtaisui keliamus reikalavimus (eIDAS 29 str. ir 30 str.) ir kvalifikuotam elektroninio spaudo kūrimo įtaisui keliamus reikalavimus (eIDAS 39 str. 1 d. ir 39 str. 2 d.).

6.2.2 Privačiųjų raktų saugojimo reikalavimai

CA privatieji raktai gali būti atstatomi ir jų kopijos saugomos tik naudojantis su kriptografine techninę įranga susietomis sisteminėmis kortelėmis, kurių kiekvienoje saugomas fragmentas šifravimo rakto, kuriuo užšifruota CA privačiojo rakto kopija, duomenų.

CA nedaro asmenims sugeneruotų privačiųjų raktų kopijų.

6.2.3 CA privačiųjų raktų atstatymas

CA privatieji raktai atstatomi naudojant su kriptografine įranga susietomis sisteminėmis kortelėmis, kurių kiekvienoje saugoma dalis kriptografinio rakto, kuriuo užšifruota CA privataus rakto kopija. CA privačiųjų raktų atstatymo procedūra analogiška CA raktų generavimo procedūrai.

6.2.4 Privačiojo rakto įvedimas į kriptografinį modulį

Kadangi kiekvieno hierarchinio lygmens CA turi atskirą kriptografinį modulį, raktų įvedimo ir išvedimo procedūros taikomos tik privačiojo rakto atstatymo ir atsarginės kopijos darymo atvejais.

6.2.5 Privačiojo rakto aktyvavimas

Privačiojo rakto aktyvacija (prieigos prie rakto atvėrimas) atliekama kiekvieną kartą, kai tik to prireikia. Aktyvuotą raktą galima naudoti tol, kol jis nebus deaktyvuotas.

Aktyvacijos ir deaktyvacijos procedūrų atlikimas priklauso nuo rakto saugotojo, nuo raktu apsaugomų duomenų svarbos ir nuo to, ar rakto aktyvacija išlieka vienai operacijai, sesijai ar neribotą laiką.

Sudarytiems sertifikatams ir CRL pasirašyti skirtas CA privatusis raktas sugeneruotas kriptografiniame modulyje išlieka, tol, kol fiziškai jis nesunaikinamas ar neištrinamas.

Privačiojo rakto aktyvacija visada prasideda saugumo pareigūno autentiškumo patvirtinimu. Tam naudojama elektroninė identifikacinė kortelė, kurią turi tik saugumo administratorius. Įkišus kortelę į kriptografinį modulį ir įvedus PIN kodą, privatusis raktas bus aktyvus tol, kol kortelė nebus ištraukta. Kiekvienas CA privačiojo rakto aktyvavimas fiksuojamas įrašu saugiame operacijų žurnale.

Sertifikatų savininko privatusis raktas, kuris laikomas CA jam parengtoje SSCD/QSCD, aktyvuojamas įvedus PIN kodą.

6.2.6 Privačiojo rakto deaktyvavimas

CA privačiojo rakto deaktyvacija atliekama pasibaigus kiekvienai rakto naudojimo sesijai. Tam iš aparatinio kriptografinio modulio ištraukiama saugumo administratoriaus identifikacinė kortelė. Kiekvienas privačiojo rakto deaktyvavimas yra fiksuojamas saugiame operacijų žurnale.

Sertifikatų savininko privatusis raktas deaktyvuojamas pabaigus dokumentų pasirašymo elektroniniais parašais arba autentifikavimosi sesiją arba atjungus SSCD/QSCD.

6.2.7 Privačiojo rakto sunaikinimas

CA privačiojo rakto sunaikinimas reiškia fizinį laikmenų, kuriose saugomas raktas sunaikinimą. Kiekvienas privačiojo rakto sunaikinimas fiksuojamas įrašu saugiame operacijų žurnale.

6.2.8 Raktų naudojimo periodai

Viešojo rakto (tuo pačiu ir privačiojo rakto) galiojimo terminas nurodomas kiekviename sertifikate (žiūr. 7. skyrių).

Šakninės sertifikavimo tarnybos rakto galiojimo periodas yra 27 (dvidešimt septyni) metų.

Darbinės sertifikavimo tarnybos rakto galiojimo periodas yra 9 (devyni) metai.

Asmenims sudaromų sertifikatų (kartu ir raktų) galiojimo periodas yra nuo 2 (dvejų) iki 5 (penkerių) metų.

Sertifikatų galiojimo pradžios terminas paprastai sutampa su sertifikatų sudarymo data. Draudžiama sertifikatuose nurodyti ankstesnį arba vėlesnį sertifikatų galiojimo pradžios terminą, nei jų sudarymo data.

6.3. Kompiuterių sauga

CA ir kitų tarnybų kompiuteriai turi tokias apsaugos priemones:

a) operacinės sistemos ir taikomųjų programų lygiu numatytas privalomas registravimosi priemones;

b) savo nuožiūrai paliktas prieigos kontrolės priemones;

c) prisijungimams tikrinti reikiamų duomenų kaupimą;

d) įgalinančias atskirti pareigas, leistinas sistemoje;

e) prisijungiančių asmenų pareigų identifikavimo ir autentifikavimo priemones;

f) kriptografines informacijos apsaugos priemones, perduodant ją tinklu ir saugant duomenų bazėse;

g) archyvo apie kompiuterius ir duomenis tvarkymo istorijos fiksavimo kontrolės tikslams priemones;

h) patikimas darbuotojų ir jų pareigų kaitos fiksavimo priemones;

i) nesankcionuotos prieigos prie kompiuterinių resursų valdymo ir informavimo priemones.

6.4. Techninės kontrolės gyvavimo ciklas

Techninės kontrolės gyvavimo ciklas apima CA sistemos kūrimo ir tvarkymo saugumo kontrolę. Sistemos saugumas siejamas su kūrimo aplinka, personalu, kūrimo priemonių saugumu, konfigūracijos valdymu sistemos priežiūros metu.

6.4.1 Sistemos kūrimo kontrolė

Kiekviena taikomoji programa, prieš diegiant ją į CA kompiuterių sistemą, yra pasirašoma elektroniniu parašu. Tai įgalina kontroliuoti jų versijas ir apsisaugoti nuo neleistinų papildymų ar klastočių.

Panašaus griežtumo taisyklių laikomasi ir aparatinės įrangos atveju. Ypatingas dėmesys skiriamas:

a) aparatinės įrangos ar jos komponentų pristatymo į jos diegimo vietą maršruto įvertinimą ir sekimą (tai labai svarbu aparatinių kriptografinių modulių atveju);

b) keitimams skirta aparatinė įranga pristatoma į numatytą vietą panašiai, kaip ir originalioji įranga; keitimus atlieka patikimas ir kvalifikuotas personalas, laikantis CA nustatytų saugumo taisyklių.

6.4.2 Saugumo reikalavimų laikymosi kontrolė

Saugumo reikalavimų laikymosi kontrolės tikslas yra prižiūrėti, kad CA sistema veiktų teisingai ir būtų išlaikyta patvirtinta jos konfigūracija.

Sistemos konfigūracijos keitimai modifikuojant ar atnaujinant ją, fiksuojami ir kontroliuojami. Sistemos konfigūracijos keitimai atliekami laikantis CA nustatytų saugumo taisyklių.

CA naudojamos kontrolės priemonės įgalina nenutrūkstamai tikrinti programinės įrangos integralumą, versiją ir autentiškumą.

6.5. Tinklo sauga

CA sistemoje realizuota kelių saugos lygių architektūra. Prieiga internetu prie bet kurio sistemos segmento yra apsaugota LST ISO/IEC 15408 E4 saugumo lygio ugniasiene ir apsaugos nuo įsilaužimų sistema. Šakninė sertifikavimo tarnyba veikia *offline* režimu.

6.6. Kriptografinio modulio inžinerijos kontrolė

Kriptografinio modulio inžinerijos kontrolė apima reikalavimus, kurių turi būti laikomasi kuriant, gaminant ir transportuojant modulį į paskirties vietą.

CA turi užtikrinti, kad:

a) HSM nebuvo pažeistas iki jo pristatymo;

b) HSM būtų apsaugotas nuo pažeidimų naudojant jį patikimumo užtikrinimo paslaugų teikimo veiklai vykdyti;

c) sertifikatams, CRL sąrašams, OCSP pranešimams ir kitai svarbiai informacijai pasirašyti naudojama kriptografinė įranga veiktų tinkamai;

d) pasibaigus HSM naudojimo laikotarpiui, jame esantys raktai būtų sunaikinti.

CA naudoja kriptografinius modulius ne žemesnio nei FIPS 140-3 ir Common Criteria EAL 4+ reikalavimus.

7. SERTIFIKATO IR CRL PROFILIAI

Sudaromi sertifikatai atitinka ETSI EN 319 422 v1.1.1 Time-stamping protocol and electronic time-stamp profiles Ir **ETSI EN 319 412 Certificate Profiles** standartų reikalavimus.

7.1. Šakninės CA sertifikato profilis

X.509 V1 pagrindiniai laukai	**Kritinis**	**Atributas**	**Reikšmė**
Version			*V3*
Serial number			*Automatiškai sudaromas šakninio CA*
Signature algorithm			*sha256RSA*
Issuer			*CN = RCSC RootCA* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 27 metai*
Subject			*CN = RCSC RootCA* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Public key			*RSA (4096 Bits)*
X.509 V3 Plėtiniai			
Subject Key Identifier	Ne		*RCSC RootCA viešojo rakto 160 bitų ilgio hash reikšmė*
CA Version	Ne		*V0.0*
Key Usage	Taip		*Certificate Signing, Off-line CRL Signing, CRL Signing (06)*
Basic Constraints	Taip		*Subject Type=CA* *Path Length Constraint=None*

7.2 Šakninės CA OCSP atsakymų pasirašymo sertifikato profilis

X.509 V1 pagrindiniai laukai	**Kritinis**	**Atributas**	**Reikšmė**
Version			*V3*
Serial number			*Automatiškai sudaromas šakninio CA*
Signature algorithm			*sha256RSA*
Issuer			*CN = RCSC RootCA* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data +6 metai*
Subject			*CN = RCSC RootCA OCSP* *OU = RCSC*

			O = VI Registru centras - i.k. 124110246 *C = LT*
Public key			*RSA (2048 Bits)*
X.509 V3 Plėtiniai			
Subject Key Identifier	Ne	Key Identifier	*RCSC RootCA OCSP viešojo rakto 160 bitų ilgio hash reikšmė*
Authority Key Identifier	Ne	Key Identifier	*RCSC RootCA viešojo rakto 160 bitų ilgio hash reikšmė*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.7*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Key Usage	Ne		*Digital Signature (80)*
Enhanced Key Usage	Ne		*OCSP pasirašymas (1.3.6.1.5.5.7.3.9)*

7.3 Darbinės CA sertifikato profilis

X.509 V1 pagrindiniai laukai	**Kritinis**	**Atributas**	**Reikšmė**
Version			*V3*
Serial number			*Automatiškai sudaromas šakninio CA*
Signature algorithm			*sha256RSA*
Issuer			*CN = RCSC RootCA* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 9 metai*
Subject			*CN = RCSC IssuingCA* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Public key			*RSA (2048 Bits,)*
X.509 V3 Plėtiniai			
Subject Key Identifier	Ne	Key Identifier	*RCSC IssuingCA viešojo rakto 160 bitų ilgio hash reikšmė*
CA Version	Ne		*V0.0*
Certificate Policies	Ne	Policy Identifier	*2.5.29.32.0*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Certificate Template Name	Ne		*Sisteminis šablono identifikatorius*
Authority Key Identifier	Ne	Key Identifier	*RCSC RootCA viešojo rakto 160 bitų ilgio hash reikšmė*

CRL Distribution Points	Ne	Distribution Point Name	*http://csp2.rcsc.lt/cdp/RCSC_RootCA.crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp2.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp2.rcsc.lt/aia/RCSC_RootCA.crt*
Basic Constraints	Taip		*Subject Type=CA* *Path Length Constraint=None*
Key Usage	Taip		*Certificate Signing, Off-line CRL Signing, CRL Signing (06)*

7.4 Darbinės CA OCSP atsakymų pasirašymo sertifikato profilis

X.509 V1 pagrindiniai laukai	**Kritinis**	**Atributas**	**Reikšmė**
Version			*V3*
Serial number			*Automatiškai sudaromas šakninio CA*
Signature algorithm			*sha256RSA*
Issuer			*CN = RCSC IssingCA* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 3 metai*
Subject			*CN = RCSC IssuingCA OCSP* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Public key			*RSA (2048 Bits)*
X.509 V3 Plėtiniai			
Subject Key Identifier	Ne	Key Identifier	*RCSC IssuingCA OCSP viešojo rakto 160 bitų ilgio hash reikšmė*
Authority Key Identifier	Ne	Key Identifier	*RCSC IssuingCA viešojo rakto 160 bitų ilgio hash reikšmė*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.7*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Key Usage	Taip		*Digital Signature, Non-Repudiation (c0)*
Enhanced Key Usage	Ne		*OCSP pasirašymas (1.3.6.1.5.5.7.3.9)*

7.5 Kvalifikuotų sertifikatų skirtų elektroniniams parašams tvirtinti profiliai

7.5.1. Kvalifikuoto elektroninio parašo sertifikato su įrašytu elektroninio pašto adresu profilis

X.509 V1 pagrindiniai laukai	**Kritinis**	**Atributas**	**Reikšmė**
Version			*V3*
Serial number			*Automatiškai sudaromas, unikalus sertifikato, išduoto darbinio CA, serijinis numeris*
Signature algorithm			*sha256RSA* arba *sha256ECC*
Issuer			*CN = RCSC IssuingCA* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 2-3 metai (RSA 2048 bits)* *Išdavimo data +4-5 metai (ECC 256 bits)*
Subject			*Serial Number=Asmens kodas* *CN= vardas ir pavardė* *G = asmens vardas* *SN = asmens pavardė* *C= LT* *E=Elektroninio pašto adresas*
Public key			*RSA (2048Bits)* arba *ECC (256 Bits)*
X.509 V3 plėtiniai			
Subject alternative name	Ne		*RFC822 Name=elektroninio pašto adresas*
Subject Key Identifier	Ne	Key Identifier	*Asmens viešojo rakto 160 bitų ilgio hash reikšmė*
Authority Key Identifier	Ne	Key Identifier	*RCSC darbinio CA viešojo rakto 160 bitų ilgio hash reikšmė*
CRL Distribution Points	Ne	Distribution Point Name	*http://csp2.rcsc.lt/cdp/RCSC_IssuingCA.crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp2.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp2.rcsc.lt/aia/RCSC_IssuingCA.crt*
Certificate Template Information	Ne	Template	*Sisteminis šablono identifikatorius*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.7*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*

Application Policies	Ne	Application Certificate Policy	*Policy Identifier=Document Signing* *Policy Identifier=Secure Email*
Qualified Certificate Statement	Ne	EU Qualified Certificate statement	*Id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)*
		SSCD statement	*id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)*
Key Usage	Taip		*Digital Signature, Non-Repudiation (c0)*
Enhanced Key Usage	Ne		*Dokumentų pasirašymas (1.3.6.1.4.1.311.10.3.12)* *Saugus elektroninis paštas (1.3.6.1.5.5.7.3.4)*

7.5.2. Kvalifikuoto elektroninio spaudo sertifikato su įrašytu elektroninio pašto adresu profilis

X.509 V1 pagrindiniai laukai	**Kritinis**	**Atributas**	**Reikšmė**
Version			*V3*
Serial number			*Automatiškai sudaromas, unikalus sertifikato, išduoto darbinio CA, serijinis numeris*
Signature algorithm			*sha256RSA* arba *sha256ECC*
Issuer			*CN = RCSC IssuingCA* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 2-3 metai (RSA 2048 bits)* *Išdavimo data +4-5 metai (ECC 256 bits)*
Subject			*Serial Number= Juridinio asmens kodas* *CN= Juridinio asmens pavadinimas* *C= LT* *E= Elektroninio pašto adresas*
Public key			*RSA (2048 Bits)* arba *ECC (256 Bits)*
X.509 V3 plėtiniai			
Subject alternative name	Ne		*RFC822 Name=elektroninio pašto adresas*
Subject Key Identifier	Ne	Key Identifier	*Asmens viešojo rakto 160 bitų ilgio hash reikšmė*
Authority Key Identifier	Ne	Key Identifier	*RCSC darbinio CA viešojo rakto 160 bitų ilgio hash reikšmė*
CRL Distribution Points	Ne	Distribution Point Name	*http://csp2.rcsc.lt/cdp/RCSC_IssuingCA.crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp2.rcsc.lt/ocspresponder.rcsc*

		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp2.rcsc.lt/aia/RCSC_IssuingCA.crt*
Certificate Template Information	Ne	Template	*Sisteminis šablono identifikatorius*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.7*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Application Policies	Ne	Application Certificate Policy	*Policy Identifier=Document Signing* *Policy Identifier=Secure Email*
Qualified Certificate Statement	Ne	EU Qualified Certificate statement	*Id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)*
		SSCD statement	*id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)*
		Qualified Certificate Type	*id-etsi-qcs-QcType (0.4.0.1862.1.6)* *id-etsi-qct-eseal (0.4.0.1862.1.6.2)*
Key Usage	Taip		*Digital Signature, Non-Repudiation (c0)*
Enhanced Key Usage	Ne		*Dokumentų pasirašymas (1.3.6.1.4.1.311.10.3.12)* *Saugus elektroninis paštas (1.3.6.1.5.5.7.3.4)*

7.5.3. Kvalifikuoto elektroninio spaudo sertifikato nekvalifikuotame įtaise profilis

X.509 V1 pagrindiniai laukai	**Kritinis**	**Atributas**	**Reikšmė**
Version			*V3*
Serial number			*Automatiškai sudaromas, unikalus sertifikato, išduoto darbinio CA, serijinis numeris*
Signature algorithm			*sha256RSA* arba *sha256ECC*
Issuer			*CN = RCSC IssuingCA* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 2-3 metai (RSA 2048 bits)* *Išdavimo data +4-5 metai (ECC 256 bits)*
Subject			*Serial Number= Juridinio asmens kodas* *CN= Juridinio asmens pavadinimas* *C= LT* *E= Elektroninio pašto adresas*
Public key			*RSA (2048 Bits)* arba *ECC (256 Bits)*
X.509 V3 plėtiniai			
Subject alternative name	Ne		*RFC822 Name=elektroninio pašto adresas*

Subject Key Identifier	Ne	Key Identifier	*Asmens viešojo rakto 160 bitų ilgio hash reikšmė*
Authority Key Identifier	Ne	Key Identifier	*RCSC darbinio CA viešojo rakto 160 bitų ilgio hash reikšmė*
CRL Distribution Points	Ne	Distribution Point Name	*http://csp2.rcsc.lt/cdp/RCSC_IssuingCA.crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp2.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp2.rcsc.lt/aia/RCSC_IssuingCA.crt*
Certificate Template Information	Ne	Template	*Sisteminis šablono identifikatorius*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.7*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Application Policies	Ne	Application Certificate Policy	*Policy Identifier=Document Signing* *Policy Identifier=Secure Email*
Qualified Certificate Statement	Ne	EU Qualified Certificate statement	*Id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)*
		Qualified Certificate Type	*id-etsi-qcs-QcType (0.4.0.1862.1.6)* *id-etsi-qct-eseal (0.4.0.1862.1.6.2)*
Key Usage	Taip		*Digital Signature, Non-Repudiation (c0)*
Enhanced Key Usage	Ne		*Dokumentų pasirašymas (1.3.6.1.4.1.311.10.3.12)* *Saugus elektroninis paštas (1.3.6.1.5.5.7.3.4)*

7.5.4. Kvalifikuoto elektroninio parašo sertifikato be įrašyto elektroninio pašto adreso profilis

X.509 V1 pagrindiniai laukai	**Kritinis**	**Atributas**	**Reikšmė**
Version			*V3*
Serial number			*Automatiškai sudaromas, unikalus sertifikato, išduoto darbinio CA, serijinis numeris*
Signature algorithm			*sha256RSA* arba *sha256ECC*
Issuer			*CN = RCSC IssuingCA* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*

Valid to			*Išdavimo data + 2-3 metai (RSA 2048 bits)* *Išdavimo data +4-5 metai (ECC 256 bits)*
Subject			*Serial Number= Asmens kodas* *CN= vardas ir pavardė* *G = asmens vardas* *SN = asmens pavardė* *C= LT*
Public key			*RSA (2048 Bits)* arba *ECC (256 Bits)*
X.509 V3 plėtiniai			
Subject Key Identifier	Ne	Key Identifier	*Asmens viešojo rakto 160 bitų ilgio hash reikšmė*
Authority Key Identifier	Ne	Key Identifier	*RCSC darbinio CA viešojo rakto 160 bitų ilgio hash reikšmė*
CRL Distribution Points	Ne	Distribution Point Name	*http://csp2.rcsc.lt/cdp/RCSC_IssuingCA.crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp2.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp2.rcsc.lt/aia/RCSC_IssuingCA.crt*
Certificate Template Information	Ne	Template	*Sisteminis šablono identifikatorius*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.7*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Application Policies	Ne	Application Certificate Policy	*Policy Identifier=Document Signing* *Policy Identifier=Secure Email*
Qualified Certificate Statement	Ne	EU Qualified Certificate statement	*Id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)*
		SSCD statement	*id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)*
Key Usage	Taip		*Digital Signature, Non-Repudiation (c0)*
Enhanced Key Usage	Ne		*Dokumentų pasirašymas (1.3.6.1.4.1.311.10.3.12)* *Saugus elektroninis paštas (1.3.6.1.5.5.7.3.4)*

7.5.5. Kvalifikuoto juridinio asmens darbuotojo sertifikato profilis

X.509 V1 pagrindiniai laukai	**Kritinis**	**Atributas**	**Reikšmė**
Version			*V3*
Serial number			*Automatiškai sudaromas, unikalus sertifikato, išduoto darbinio CA, serijinis numeris*

Signature algorithm			*sha256RSA* arba *sha256ECC*
Issuer			*CN = RCSC IssuingCA* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 2-3 metai (RSA 2048 bits)* *Išdavimo data +4-5 metai (ECC 256 bits)*
Subject			*Serial Number=suteiktas unikalus identifikatorius ** *CN=vardas ir pavardė* *G = asmens vardas* *SN = asmens pavardė* *OU= padalinio pavadinimas* *O=įmonės pavadinimas* *C= LT* *E= elektroninio pašto adresas*
Public key			*RSA (2048Bits)* arba *ECC (256 Bits)*
X.509 V3 plėtiniai			
Subject alternative name	Ne		*RFC822 Name=elektroninio pašto adresas*
Subject Key Identifier	Ne	Key Identifier	*Asmens viešojo rakto 160 bitų ilgio hash reikšmė*
Authority Key Identifier	Ne	Key Identifier	*RCSC darbinio CA viešojo rakto 160 bitų ilgio hash reikšmė*
CRL Distribution Points	Ne	Distribution Point Name	*http://csp2.rcsc.lt/cdp/RCSC_IssuingCA.crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp2.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp2.rcsc.lt/aia/RCSC_IssuingCA.crt*
Certificate Template Information	Ne	Template	*Sisteminis šablono identifikatorius*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.7*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Application Policies	Ne	Application Certificate Policy	*Policy Identifier=Document Signing* *Policy Identifier=Secure Email*

Qualified Certificate Statement	Ne	EU Qualified Certificate statement	*Id-etsi-pcs-QcCompliance (0.4.0.1862.1.1)*
		SSCD statement	*id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)*
Key Usage	Taip		*Digital Signature, Non-Repudiation (c0)*
Enhanced Key Usage	Ne		*Dokumentų pasirašymas (1.3.6.1.4.1.311.10.3.12)* *Saugus elektroninis paštas (1.3.6.1.5.5.7.3.4)*

** Suteiktas unikalus identifikatorius – sudaromas iš juridinio asmens kodo ir įmonės darbuotojo tabelio numerio. Unikalus identifikatorius generuojamas – XXXXXXXXXX (kuris yra įmonės kodas Juridinių asmenų registre) / YYYY (kuris yra įmonės darbuotojo tabelio numeris).*

7.6 Sertifikatų, skirtų saugiam autentifikavimui, profiliai

7.6.1 Parašo, skirto saugiam autentifikavimui, su įrašytu elektroninio pašto adresu, sertifikato profilis

X.509 V1 pagrindiniai laukai	**Kritinis**	**Atributas**	**Reikšmė**
Version			*V3*
Serial number			*Automatiškai sudaromas, unikalus sertifikato, išduoto darbinio CA, serijinis numeris*
Signature algorithm			*sha256RSA* arba *sha256ECC*
Issuer			*CN = RCSC IssuingCA* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 2-3 metai (RSA 2048 bits)* *Išdavimo data +4-5 metai (ECC 256 bits)*
Subject			*Serial Number=Asmens kodas* *CN= vardas ir pavardė* *G = asmens vardas* *SN = asmens pavardė* *C= LT* *E=Elektroninio pašto adresas*
Public key			*RSA (2048 Bits)* arba *ECC (256 Bits)*
X.509 V3 plėtiniai			
Subject alternative name	Ne		*RFC822 Name=elektroninio pašto adresas*
Subject Key Identifier	Ne	Key Identifier	*Asmens viešojo rakto 160 bitų ilgio hash reikšmė*
Authority Key Identifier	Ne	Key Identifier	*RCSC darbinio CA viešojo rakto 160 bitų ilgio hash reikšmė*
CRL Distribution Points	Ne	Distribution Point Name	*http://csp2.rcsc.lt/cdp/RCSC_IssuingCA.crl*

Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp2.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp2.rcsc.lt/aia/RCSC_IssuingCA.crt*
Certificate Template Information	Ne	Template	*Sisteminis šablono identifikatorius*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.7*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Application Policies	Ne	Application Certificate Policy	*Policy Identifier=Client Authentication*
Key Usage	Taip		*Digital Signature (80)*
Enhanced Key Usage	Ne		*Client Authentication (1.3.6.1.5.5.7.3.2)*

7.6.2 Spaudo, skirto saugiam autentifikavimui, su įrašytu elektroninio pašto adresu, sertifikato profilis

X.509 V1 pagrindiniai laukai	**Kritinis**	**Atributas**	**Reikšmė**
Version			*V3*
Serial number			*Automatiškai sudaromas, unikalus sertifikato, išduoto darbinio CA, serijinis numeris*
Signature algorithm			*sha256RSA* arba *sha256ECC*
Issuer			*CN = RCSC IssuingCA* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 2-3 metai (RSA 2048 bits)* *Išdavimo data +4-5 metai (ECC 256 bits)*
Subject			*Serial Number= Juridinio asmens kodas* *CN= Juridinio asmens pavadinimas* *C= LT* *E=Elektroninio pašto adresas*
Public key			*RSA (2048 Bits)* arba *ECC (256 Bits)*
X.509 V3 plėtiniai			
Subject alternative name	Ne		*RFC822 Name= elektroninio pašto adresas*
Subject Key Identifier	Ne	Key Identifier	*Asmens viešojo rakto 160 bitų ilgio hash reikšmė*
Authority Key Identifier	Ne	Key Identifier	*RCSC darbinio CA viešojo rakto 160 bitų ilgio hash reikšmė*

CRL Distribution Points	Ne	Distribution Point Name	*http://csp2.rcsc.lt/cdp/RCSC_IssuingCA.crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp2.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp2.rcsc.lt/aia/RCSC_IssuingCA.crt*
Certificate Template Information	Ne	Template	*Sisteminis šablono identifikatorius*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.7*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Application Policies	Ne	Application Certificate Policy	*Policy Identifier=Client Authentication*
Key Usage	Taip		*Digital Signature (80)*
Enhanced Key Usage	Ne		*Client Authentication (1.3.6.1.5.5.7.3.2)*

7.6.3 Sertifikato, skirto saugiam autentifikavimui, be įrašyto elektroninio pašto adreso, profilis

X.509 V1 pagrindiniai laukai	**Kritinis**	**Atributas**	**Reikšmė**
Version			*V3*
Serial number			*Automatiškai sudaromas, unikalus sertifikato, išduoto darbinio CA, serijinis numeris*
Signature algorithm			*sha256RSA* arba *sha256ECC*
Issuer			*CN = RCSC IssuingCA* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 2-3 metai (RSA 2048 bits)* *Išdavimo data +4-5 metai (ECC 256 bits)*
Subject			*Serial Number=Asmens kodas* *CN= vardas ir pavardė* *G = asmens vardas* *SN = asmens pavardė* *C= LT*
Public key			*RSA (2048 Bits)* arba *ECC (256 Bits)*
X.509 V3 plėtiniai			
Subject Key Identifier	Ne	Key Identifier	*Asmens viešojo rakto 160 bitų ilgio hash reikšmė*
Authority Key Identifier	Ne	Key Identifier	*RCSC darbinio CA viešojo rakto 160 bitų ilgio hash reikšmė*

CRL Distribution Points	Ne	Distribution Point Name	*http://csp2.rcsc.lt/cdp/RCSC_IssuingCA.crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp2.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp2.rcsc.lt/aia/RCSC_IssuingCA.crt*
Certificate Template Information	Ne	Template	*Sisteminis šablono identifikatorius*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.7*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Application Policies	Ne	Application Certificate Policy	*Policy Identifier=Client Authentication*
Key Usage	Taip		*Digital Signature (80)*
Enhanced Key Usage	Ne		*Client Authentication (1.3.6.1.5.5.7.3.2)*

7.6.4 Juridinio asmens darbuotojo sertifikato, skirto saugiam autentifikavimui, profilis

X.509 V1 pagrindiniai laukai	**Kritinis**	**Atributas**	**Reikšmė**
Version			*V3*
Serial number			*Automatiškai sudaromas, unikalus sertifikato, išduoto darbinio CA, serijinis numeris*
Signature algorithm			*sha256RSA* arba *sha256ECC*
Issuer			*CN = RCSC IssuingCA* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 2-3 metai (RSA 2048 bits)* *Išdavimo data +4-5 metai (ECC 256 bits)*
Subject			*Serial Number=suteiktas unikalus identifikatorius ** *CN=vardas ir pavardė* *G = asmens vardas* *SN = asmens pavardė* *OU= padalinio pavadinimas* *O=įmonės pavadinimas* *C= LT* *E= elektroninio pašto adresas*
Public key			*RSA (2048 Bits)* arba *ECC (256 Bits)*
X.509 V3 plėtiniai			

Subject alternative name	Ne		*RFC822 Name=elektroninio pašto adresas*
Subject Key Identifier	Ne	Key Identifier	*Asmens viešojo rakto 160 bitų ilgio hash reikšmė*
Authority Key Identifier	Ne	Key Identifier	*RCSC darbinio CA viešojo rakto 160 bitų ilgio hash reikšmė*
CRL Distribution Points	Ne	Distribution Point Name	*http://csp2.rcsc.lt/cdp/RCSC_IssuingCA.crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp2.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp2.rcsc.lt/aia/RCSC_IssuingCA.crt*
Certificate Template Information	Ne	Template	*Sisteminis šablono identifikatorius*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.7*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Application Policies	Ne	Application Certificate Policy	*Policy Identifier=Client Authentication*
Key Usage	Taip		*Digital Signature (80)*
Enhanced Key Usage	Ne		*Client Authentication (1.3.6.1.5.5.7.3.2)*

** Suteiktas unikalus identifikatorius – sudaromas iš juridinio asmens kodo ir įmonės darbuotojo tabelio numerio. Unikalus identifikatorius generuojamas – XXXXXXXXXX (kuris yra įmonės kodas Juridinių asmenų registre) / YYYY (kuris yra įmonės darbuotojo tabelio numeris).*

7.7 CRL profiliai

7.7.1 Šakninės CA CRL profilis

CRL pagrindiniai laukai	**Atributas**	**Reikšmė**
Version		*V2*
Issuer		*CN = RCSC RootCA* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Effective date		*Išdavimo data ir laikas*
Next update		*Išdavimo data ir laikas + 6 mėnesiai ir 3 savaitės*
Signature algorithm		*Sha256RSA*
Sertifikatai, kurių galiojimą sustabdytas arba nutrauktas		

Serial number		*Sustabdyto arba nutraukto galiojimo sertifikato serijinis numeris*
Revocation date		*Sertifikato galiojimo sustabdymo arba nutraukimo data ir laikas*
CRL reason code		*Sertifikato galiojimo sustabdymo arba nutraukimo priežastis*
CRL Plėtiniai		
Authority Key Identifier	Key Identifier	*RCSC šakninio CA viešojo rakto 160 bitų ilgio hash reikšmė*
CA Version		*V0.0*
CRL Number		*Suteiktas automatiškai šakninio CA*
Next CRL Publish		*Išdavimo data ir laikas + 6 mėnesiai*

7.7.2 Darbinės CA CRL profilis

CRL pagrindiniai laukai	**Atributas**	**Reikšmė**
Version		*V2*
Issuer		*CN = RCSC IssuingCA* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Effective date		*Išdavimo data ir laikas*
Next update		*Išdavimo data ir laikas + 36 valandos*
Signature algorithm		*Sha256RSA*
Sertifikatai, kurių galiojimą sustabdytas arba nutrauktas		
Serial number		*Sustabdyto arba nutraukto galiojimo sertifikato serijinis numeris*
Revocation date		*Sertifikato galiojimo sustabdymo arba nutraukimo data ir laikas*
CRL reason code		*Sertifikato galiojimo sustabdymo arba nutraukimo priežastis*
CRL Plėtiniai		
Authority Key Identifier	Key Identifier	*RCSC darbinio CA viešojo rakto 160 bitų ilgio hash reikšmė*
CA Version		*V0.0*
CRL Number		*Suteiktas automatiškai darbinio CA*
Next CRL Publish		*Išdavimo data ir laikas + 24 valandos*

8. SERTIFIKAVIMO VEIKLOS NUOSTATŲ ADMINISTRAVIMAS

Šiame skyriuje pateikiami CPS administravimo reikalavimai.

Naujos versijos galiojimo pradžia nurodyta CPS dokumento viršelyje. Naujausia CPS versija publikuojama saugykloje (*repository*) internete.

8.1. CPS keitimo procedūros

CPS gali būti keičiami pastebėjus juose klaidas, iškilus reikalui atnaujinti juos arba gavus susijusių šalių pasiūlymus.

Nuostatų pakeitimai skirstomi į dvi kategorijas:

a) esminiai pakeitimai, apie kuriuos turi būti pranešama vartotojams ir keičiamas nuostatų OID;

b) neesminiai pakeitimai, apie kuriuos neprivaloma pranešti kitoms šalims, ir nuostatų OID nėra keičiamas.

Atlikus esminius pakeitimus keičiamas naujos CPS redakcijos versijos pirmas skaitmuo, bei atitinkamai OID versijos elementas (paskutinis skaitmuo). Atlikus neesminius pakeitimus keičiami naujos CPS redakcijos versijos antras ir tolimesni skaitmenys.

Neesminiai pakeitimai galimi tais atvejais, kai CPS keičiama rekomendacinio, paaiškinamojo, tikslinamojo pobūdžio informacija arba keičiasi už CPS tvarkymą atsakingų asmenų kontaktiniai duomenys.

Kitais atvejais pakeitimai yra esminiai ir po kiekvieno CPS pakeitimo keičiamas jų unikalus identifikatorius. Visais atvejais, jei pakeitimai įtakoja patikimumo užtikrinimo paslaugų saugumo lygio pasikeitimus, pakeitimai yra esminiai.

CPS prižiūrimi, keičiami ir tvirtinami laikantis tokios procedūros:

e) CA už saugumo politiką atsakingi darbuotojai kas 1 (vienerius) metus skaičiuojant nuo paskutinės CPS redakcijos peržiūri ir įsitikina CPS aktualumu. Jei peržiūros metu nustatytas poreikis keisti CPS, inicijuojamas CPS keitimas;

f) CPS pakeitimus inicijuoja CA arba sertifikatų naudotojai;

g) CA už saugumo politiką atsakingi darbuotojai rengia naują CPS redakciją;

h) visais atvejais apie naują CPS redakcija bei apie bet kokius CA teikiamų paslaugų pasikeitimus informuojama priežiūros įstaiga (1) apie bet kokius kvalifikuotų patikimumo užtikrinimo paslaugų teikimo pakeitimus – nedelsdami, bet ne vėliau kaip per 3 darbo

dienas nuo šių pakeitimų dienos; (2) apie numatomą veiklos nutraukimą – ne vėliau kaip prieš 9 mėnesius iki veiklos nutraukimo dienos.

9. SĄVOKŲ APIBRĖŽIMAI IR SANTRUMPOS

Abonentas *(subscriber)* – asmuo (fizinis/ juridinis), sudarantis sutartį su CA vieno ar daugiau asmenų, kuriems sudaromas elektroninio. parašo ar elektroninio spaudo sertifikatas (sertifikatų savininkų) vardu. Abonentas gali būti kartu ir sertifikato savininkas.

Aktyvavimo duomenys – tai duomenys (pvz. PIN kodas, slaptažodis, biometriniai duomenys ar kt.), kuriuos būtina įvesti, norint pasinaudoti kriptografiniu moduliu ir privačiuoju raktu. Aktyvavimo duomenys, kaip ir privatusis raktas, turi būti saugomi ir neatskleidžiami.

Aparatinis saugumo modulis (kriptografinis saugumo modulis*), (Hardware security module - HSM)* – aparatinė ir programinė įranga, kuri naudojama kriptografinių raktų poroms – privatiesiems ir viešiesiems raktams generuoti, saugoti ir/arba elektroniniams parašams kurti.

Atšauktų sertifikatų sąrašas *(CRL – Certificate/ Seal Revocation List)* – Sertifikatų centro periodiškai (arba neatidėliotinai) leidžiamas, jo pasirašomas sąrašas sertifikatų, kurių galiojimas nutrauktas ar sustabdytas. Tokiame sąraše paprastai nurodomas jį sudariusio Sertifikatų centro vardas, sąrašo sudarymo data, numatoma kitos sąrašo versijos išleidimo data, nebegaliojančių sertifikatų serijiniai numeriai, galiojimo nutraukimo ar sustabdymo laikas ir priežastys.

Autentifikavimas – tikrumo arba asmens tapatybės nustatymo procesas, ar iš tikro asmuo yra tas, kuo jis prisistato, ar iš tikro daiktas atitinka originalą.

Autentifikavimo sertifikatas – asmens atpažinimo elektroninėje erdvėje sertifikatas, patvirtinantis arba leidžiantis nustatyti asmens tapatybę elektroninėje erdvėje.

Autentifikuojantysis asmuo – veiksnus fizinis asmuo, kuris turi parašo formavimo įrangą ir naudojasi parašo formavimo duomenimis autentifikuodamasis elektroninėje erdvėje.

Elektroninis parašas – elektroninės formos duomenys, kurie prijungti prie kitų elektroninės formos duomenų arba logiškai susieti su jais ir kuriuos pasirašantis asmuo naudoja pasirašydamas.

Elektroninis spaudas – elektroninės formos duomenys, prijungti prie kitų elektroninės formos duomenų arba su jais logiškai susieti, kad būtų užtikrinta pastarųjų kilmė ir vientisumas.

Elektroninė atpažintis – elektroninių asmens tapatybės duomenų, kuriais nurodomas konkretus fizinis ar juridinis asmuo arba juridiniam asmeniui atstovaujantis fizinis asmuo, naudojimo procesas.

Elektroninė laiko žyma – elektroninės formos duomenys, kuriais kiti elektroninės formos duomenys susiejami su tam tikru laiku ir taip sukuriamas įrodymas, kad pastarieji egzistavo tuo metu.

Kompromitacija – privačiojo rakto pametimas, pavogimas, modifikavimas, neteisėtas panaudojimas arba kitoks saugos pažeidimas.

Kriptografinis modulis – žiūr. Aparatinis saugumo modulis.

Kvalifikuotas elektroninis parašas – pažangusis elektroninis parašas, sukurtas naudojant kvalifikuotą elektroninio parašo kūrimo įtaisą ir patvirtintas kvalifikuotu elektroninio parašo sertifikatu.

Kvalifikuotas elektroninio parašo sertifikatas – elektroninio parašo sertifikatas, kurį išduoda kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas ir kuris atitinka jam eIDAS nustatytus reikalavimus.

Kvalifikuoto elektroninio parašo sertifikato savininkai – tai fiziniai asmenys, kurie savo elektroninius parašus tvirtina CA sudarytais kvalifikuotais sertifikatais arba sertifikatus naudoja asmens autentifikacijai elektroninėje erdvėje.

Kvalifikuoto elektroninio spaudo sertifikato savininkai – tai juridiniai asmenys, kurie kvalifikuotą elektroninį spaudą naudoja kaip įrodymą, kad elektroninį dokumentą išdavė juridinis asmuo, užtikrinant dokumento kilmę bei vientisumą.

K**valifikuotas elektroninio parašo arba elektroninio spaudo kūrimo įtaisas** *(SSCD/QSCD – Qualified Signature (Seal) Creation Device)* – elektroninio parašo arba elektroninio spaudo kūrimo įtaisas (sukonfigūruota programinė arba aparatinė įranga, naudojama elektroniniam parašui arba elektroniniam spaudui kurti), atitinkantis eIDAS nustatytus reikalavimus ir įtrauktas į Europos Komisijos sąrašą.

Kvalifikuotas elektroninis spaudas – pažangusis elektroninis spaudas, sukurtas naudojant kvalifikuotą elektroninio spaudo kūrimo įtaisą ir patvirtintas kvalifikuotu elektroninio spaudo sertifikatu.

Kvalifikuotas elektroninio spaudo sertifikatas – elektroninio spaudo sertifikatas, kurį išduoda kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas ir kuris atitinka jam eIDAS nustatytus reikalavimus.

Kvalifikuotas elektroninis spaudas nekvalifikuotame įtaise – pažangusis elektroninis spaudas, sukurtas naudojant nekvalifikuotą elektroninio spaudo kūrimo įtaisą ir patvirtintas kvalifikuotu elektroninio spaudo sertifikatu.

Kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas – patikimumo užtikrinimo paslaugų teikėjas, teikiantis vieną ar daugiau kvalifikuotų patikimumo užtikrinimo paslaugų, kuriam priežiūros įstaiga yra suteikusi kvalifikacijos statusą.

Kvalifikuotų sertifikatų (elektroninių parašų ir elektroninių spaudų) taisyklės *(Qualified Certificate/ Seal Policy – CP)* – sertifikatų sudarymo ir naudojimo taisyklės, parengtos pagal eIDAS reikalavimus, nustatančios Sertifikatų centro, sertifikato savininko bei pasitikinčių šalių teises ir pareigas. Kvalifikuotų sertifikatų taisykles renkasi parašo naudotojai, tvirtina ir įgyvendina Sertifikatų centras. Kvalifikuotų sertifikatų taisyklės rengiamos parašo naudotojų grupės iniciatyva Sertifikatų centro arba pasirenkamos iš Lietuvos standarto LST ETSI TS 101 456 „Strateginiai reikalavimai, keliami kvalifikuotus sertifikatus išduodantiems sertifikavimo paslaugų teikėjams".

Laiko žymos paslaugų teikėjas *(TSA – Time-Stamping Authority)* – paslaugų teikėjas teikiantis laiko žymos formavimo paslaugas.

Naudotojai – sertifikatų savininkai ir sertifikatais pasitikinčios šalys.

Parašo naudotojai – asmenys, kurie savo veikloje naudoja elektroninį parašą arba iš kitų asmenų gauna pasirašytus duomenis.

Pasirašantis asmuo – veiksnus fizinis asmuo, kuris sukuria elektroninį parašą.

Pasitikinčios šalys *(relying parties)* – fizinis ar juridinis asmuo, kuris pasikliauja elektronine atpažintimi ar patikimumo užtikrinimo paslauga.

Privatusis raktas – unikalūs duomenys, kuriuos asmuo naudoja kurdamas elektroninį parašą (parašo formavimo duomenys).

Patikimumo užtikrinimo paslauga – elektroninė už atlygį teikiama paslauga, kuri apima: 1) elektroninių parašų, elektroninių spaudų ar elektroninių laiko žymų kūrimą, patikrinimą ir patvirtinimą; 2) interneto svetainių tapatumo nustatymo sertifikatų kūrimą, patvirtinimą ir patikrinimą; 3) elektroninių parašų, spaudų ar su tomis paslaugomis susijusių sertifikatų ilgalaikį išsaugojimą.

Patikimumo užtikrinimo paslaugų teikėjas *(CSP - Certification Service Provider, Trust service provider)* – fizinis ar juridinis asmuo, teikiantis vieną ar daugiau patikimumo užtikrinimo paslaugų.

Pažangusis elektroninis parašas – elektroninis parašas, kuris atitinka visus šiuos reikalavimus: 1) yra vienareikšmiškai susietas su pasirašančiu asmeniu; 2) leidžia identifikuoti pasirašantį asmenį; 3) yra sukurtas naudojant elektroninio parašo kūrimo duomenis, kuriuos tik pats pasirašantis asmuo gali labai patikimai naudoti;; 4) yra susietas su juo pasirašytais duomenimis taip, kad bet koks šių duomenų pakeitimas yra pastebimas.

Raktų pora – matematiškai susijusių kriptografinių raktų pora: privačiojo ir viešojo.

Registravimo tarnyba *(RA – Registration Authority)* – patikimumo užtikrinimo paslaugų teikėjo padalinys arba atskiras juridinis asmuo, sudaręs sutartį su patikimumo užtikrinimo paslaugų teikėju, priimantis ir tikrinantis asmenų prašymus sertifikatams sudaryti, nutraukti galiojimą ir atšaukti galiojimo sustabdymą.

Saugi parašo formavimo įranga *(SSCD – Secure Signature Creation Device)* – aparatinė arba programinė įranga, kurioje generuojami (ar į kurią įrašomi) ir saugomi privatusis ir viešasis raktai bei sertifikatai ir kuri naudojama el. parašams kurti ar asmens tapatybei nustatyti. Ji turi atitikti visus šiuos reikalavimus: (1) parašo formavimo duomenis, naudojamus elektroniniam parašui sukurti, praktiškai įmanoma gauti tik vienintelį kartą, ir užtikrinamas jų slaptumas; (2) parašo formavimo duomenų, naudojamų elektroniniam parašui sukurti, atkurti praktiškai neįmanoma, ir nuo elektroninio parašo klastočių apsaugo esamos technologijos; (3) parašo formavimo duomenis, naudojamus elektroniniam parašui sukurti, pasirašantis asmuo gali patikimai apsaugoti nuo kitų asmenų; (4) parašo formavimo įranga, kuriant elektroninį parašą, nekeičia pasirašomų duomenų ir netrukdo pasirašančiam asmeniui stebėti tuos duomenis prieš pasirašant.

Saugykla *(repository)* – sertifikatų ir kitos RCSC informacijos duomenų bazė, naudotojams prieinama tiesiogiai (*on-line*) bet kuriuo metu internete adresu: www.rcsc.lt/repository/.

Saugos taisyklės – aukščiausios svarbos dokumentas, apibrėžiantis Sertifikatų centro saugios veiklos taisykles.

Sertifikatas – elektroninis liudijimas, kuris susieja viešąjį raktą (parašo tikrinimo duomenis) su pasirašančiu asmeniu ir patvirtina arba leidžia nustatyti pasirašančio asmens tapatybę.

Sertifikato savininkas *(subject)* – fizinis asmuo kuriam (kurio vardu) sudaromas sertifikatas. Kvalifikuotų sertifikatų atveju sertifikato savininkas yra pasirašantis asmuo, autentifikavimo sertifikato atveju – autentifikuojantysis asmuo.

Sertifikatų seka – pasirašančio asmens parašą patvirtinančių sertifikatų rinkinys, susidedantis iš pasirašančio asmens sertifikato, pastarąjį sertifikatą sudariusio ir jį pasirašiusio paslaugų teikėjo sertifikato ir kitų (arba nė vieno) tokiu būdu susijusių paslaugų teikėjų sertifikatų, pasibaigiantis paslaugų teikėjo, kuris pats sau sudaro ir pasirašo sertifikatą, sertifikatu.

Sertifikavimo tarnyba *(CA – Certification Authority)* – patikimumo užtikrinimo paslaugų teikėjas, sudarantis ir tvarkantis asmenų sertifikatus.

Sertifikavimo veiklos nuostatai *(CPS – Certification Practice Statement)* – kvalifikuotus sertifikatus sudarančio Sertifikatų centro patvirtintos pagrindinės veiklos taisyklės.

Spaudo kūrėjas – juridinis asmuo, kuris sukuria elektroninį spaudą.

Sistema (patikima sertifikatų tvarkymo sistema) – kompiuterių aparatinė ir programinė įranga, taip pat procedūros, pakankamu lygiu apsaugotos nuo įsibrovimo ir neleistino panaudojimo, veikiančios tinkamai ir patikimai, sukomplektuotos numatytoms funkcijoms vykdyti, įgalinančios įgyvendinti nustatytas saugos taisykles.

Viešasis raktas – unikalūs duomenys, kurie naudojami elektroniniam parašui tikrinti (parašo tikrinimo duomenys).

Viešųjų raktų infrastruktūra *(PKI – Public Key Infrastructure)* – sertifikatais pagrįstos viešųjų raktų kriptografinės sistemos sandara, organizacija, metodai, tvarkos ir procedūros.

CA –	Sertifikavimo tarnyba (Certification Authority)
CDB -	Sertifikatų duomenų bazė
CP –	Kvalifikuotų sertifikatų (elektroninių parašų ir elektroninių spaudų) taisyklės (Qualified Certificate (Electronic Signature and Electronic Seal) Policy)
CPS –	Sertifikavimo veiklos nuostatai (Certification Practice Statement)
CSP –	Patikimumo užtikrinimo paslaugų teikėjas (Certification Service Provider/Trust Service Provider)
CRL –	Atšauktų sertifikatų sąrašas (Certificate Revocation List)
DN –	Asmens unikalus identifikacinis vardas (Distinguished Name)
ECC -	Elipsinės kreivės kriptografija (elliptic curve cryptography)
ETSI –	Europos telekomunikacijų standartizavimo institutas; European Telecommunication Standardisation Institute
FIPS –	Jungtinių Amerikos Valstijų informacijos apdorojimo standartai (Federal Information Processing Standards)
IDS –	Įsilaužimų atskleidimo sistema (Intrusion Detection System)
LAN –	Vietinis kompiuterių tinklas (Local Area Network)
LST –	Lietuvos standartizacijos tarnyba
OID –	Unikalus objekto identifikatorius (Object Identifier)

OCSP –	Tiesioginės prieigos protokolas informacijai apie sertifikato statusą gauti (Online Certificate Status Protocol)
QSCD –	Kvalifikuotas elektroninio parašo arba elektroninio spaudo kūrimo įtaisas
PIN –	Asmens identifikacinis skaičius (Personal Identification Number)
PKI –	Viešojo rakto infrastruktūra (Public Key Infrastructure)
RA –	Registravimo tarnyba (Registration Authority)
RCSC –	Registrų centro Sertifikatų centras
RFC –	Prašome komentarų standartizavimo tarnyba (Request For Comments)
RSA –	RSA asimetrinio šifravimo algoritmas *(Rivest-Shamir-Adelman algorithm)*
SHA-1 –	Saugus e. duomenų santraukos gavimo algoritmas 1 *(Secure Hash Algorithm 1)*
SHA-256 –	Saugus e. duomenų santraukos gavimo algoritmas 256 *(Secure Hash Algorithm 2561)*
SSCD –	Saugi parašo formavimo įranga *(Secure Signature Creation Device)*
UPS –	Atsarginis energijos šaltinis *(Uninterrupted Power Supply)*
TSP –	Laiko žymos teikimo taisyklės (*Time-Stamping Policy*)
TSPS –	Laiko žymos teikimo veiklos nuostatai (*Time-Stamping Practice Statement*)

10. ŠALTINIAI

1	ETSI EN 319 403 v2.2.2:	ETSI EN 319 403 v2.2.2: Requirements for conformity assessment bodies assessing Trust Service Providers;
2	ETSI EN 319 401 v2.1.1	ETSI EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers;
3	ETSI EN 319 411	ETSI EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates
4	ETSI EN 319 412	ETSI EN 319 412 Certificate Profiles
5	ETSI EN 319 421 v1.1.1	ETSI EN 319 421 v1.1.1: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps
6	ETSI EN 319 422 v1.1.1	ETSI EN 319 422 v1.1.1 Time-stamping protocol and electronic time-stamp profiles
7	ETSI TR 119 100 v1.1.1	ETSI TR 119 100 v1.1.1 on Guidance on the use of standards for signatures creation and validation
8	ETSI TS 119 101 v1.1.1	ETSI TS 119 101 v1.1.1 on Policy and security requirements for applications for signature creation and signature validation
9	ETSI TR 119 300 v1.2.1	ETSI TR 119 300 v1.2.1 Business guidance on cryptographic suites
10	ETSI TS 119 312 v1.3.1	ETSI TS 119 312 v1.3.1 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
11	ETSI TR 119 600 v1.2.1	ETSI TR 119 600 v1.2.1 Business guidance for trust service status lists providers
12	ETSI TS 119 612 v2.1.1	ETSI TS 119 612 v2.1.1 Trusted Lists
13	ETSI EN 319 422 v1.1.1	ETSI EN 319 422 v1.1.1 Time-stamping protocol and electronic time-stamp profiles
14	ISO/IEC 19790:2006	Information Technology – Security Techniques – Security Requirements for Cryptographic Modules.

15	FIPS PUB 140-2	Security Requirements for Cryptographic Modules. http://www.nist.gov/cmvp.
16	FIPS 112	Password Usage. http://csrs.nist.gov/fips/.
17	ITU-T	Recommendation X.509 – Information Technology – Open System Interconnection – The Directory: Authentication Framework, June 1997 (equivalent ISO/IEC9594-8).
18	VeriSign CPS -	VeriSign Certification Practice Statement. http://www.verisign.com.
19	LST ISO/IEC 15408:1999(E)	Information technology – Security techniques – Evaluation criteria for IT security.