RCSC SERTIFIKAVIMO VEIKLOS NUOSTATAI

Unikalus objekto ID (OID): **1.3.6.1.4.1.30903.1.2.3**
Versija: 2.1
Galioja nuo: 2010-11-24

2010-11-24

Turinys

1. ĮVADAS 6
1.1. APŽVALGA 6
1.2. IDENTIFIKAVIMAS 7
1.3. SERTIFIKATŲ NAUDOTOJAI IR TAIKYMO SRITYS 7
1.3.1 Sertifikatų naudotojai 7
1.3.2 Sertifikatų naudojimo sritys 8
1.4. RCSC ORGANIZACINĖ STRUKTŪRA 8
1.5. CA SERTIFIKATŲ SEKA 11
1.6. KONTAKTINĖ INFORMACIJA 13
1.6.1 Nuostatus išleidusi ir tvarkanti organizacija 13
1.6.2 Kontaktinis asmuo 13
2. BENDROSIOS NUOSTATOS 14
2.1. ĮSIPAREIGOJIMAI 14
2.1.1 CA įsipareigojimai 14
2.1.2 RA įsipareigojimai 15
2.1.3 Palaikymo tarnybos įsipareigojimai 15
2.1.4 Abonentų ir sertifikatų savininkų įsipareigojimai 16
2.1.5 Pasitikinčių šalių įsipareigojimai 16
2.2. ATSAKOMYBĖ 17
2.2.1 CA atsakomybė 17
2.3. FINANSINĖ ATSAKOMYBĖ 17
2.3.1 Sertifikatų naudotojų kompensacijos 17
2.4. TEISINĖS NUOSTATOS IR INTERPRETAVIMAS 18
2.4.1 Pagrindiniai teisės aktai 18
2.4.2 Ginčų sprendimo tvarka 18
2.5. MOKESČIAI 18
2.6. INFORMACIJOS TEIKIMAS IR SAUGYKLOS 18
2.6.1 CA teikiama informacija 18
2.6.2 Teikiamos informacijos atnaujinimo dažnumas 19
2.7. ATITIKTIES TIKRINIMAS 19
2.7.1 CA veiklos tikrinimo dažnumas 19
2.7.2 Tikrintojai ir jų kvalifikacija 19
2.7.3 Tikrinamieji dalykai 19
2.7.4 Veiksmai pastebėjus trūkumus 20
2.7.5 Tikrinimo rezultatų skelbimas 20
2.8. KONFIDENCIALUMO NUOSTATOS 20
2.8.1 Slaptoji informacija 20
2.8.2 Neslapta informacija 21
2.8.3 Informacijos teikimas teisėsaugai 22
2.9. INTELEKTINĖS NUOSAVYBĖS TEISĖS 22
3. IDENTIFIKAVIMAS IR AUTENTIFIKAVIMAS 23
3.1. PRADINĖ REGISTRACIJA 23
3.1.1 Asmenų vardų tipai (formos) 24
3.1.2 Pseudonimų naudojimas 25
3.1.3 Vardų unikalumas 25
3.2. TAPATYBĖS TIKRINIMAS PRAŠYMO IŠDUOTI SERTIFIKATĄ ATVEJU 25
3.3. ASMENS TAPATYBĖS TIKRINIMAS SERTIFIKATŲ ATNAUJINIMO ATVEJAIS 25
3.4. SERTIFIKATO GALIOJIMĄ NUTRAUKTI PRAŠANČIO ASMENS TAPATYBĖS TIKRINIMAS 25
3.5. SERTIFIKATO GALIOJIMĄ SUSTABDYTI PRAŠANČIO ASMENS TAPATYBĖS TIKRINIMAS 26
3.6. SERTIFIKATO GALIOJIMO SUSTABDYMĄ ATŠAUKIANČIO ASMENS TAPATYBĖS TIKRINIMAS 26

4. REIKALAVIMAI VEIKLAI 27
4.1. REIKALAVIMAI SERTIFIKATO GYVAVIMO CIKLUI 27
4.1.1 Sertifikato sudarymas 27
4.1.2 Sertifikato galiojimo nutraukimas 27
4.1.3 Sertifikato galiojimo sustabdymas 29
4.1.4 CRL atnaujinimo dažnumas 29
4.1.5 Sertifikatų galiojimo tikrinimo reikalavimai 30
4.2. ĮRAŠŲ APIE CA OPERACIJAS KAUPIMAS 30
4.2.1 Registruojamieji įvykiai 30
4.2.2 Įrašų apie įvykius peržiūros dažnumas 32
4.2.3 Įrašų saugojimo periodas 32
4.2.4 Įrašų apsauga 32
4.3. DUOMENŲ ARCHYVAVIMAS 32
4.3.1 Į archyvą atiduodami duomenys 32
4.3.2 Duomenų saugojimo archyve periodas 33
4.3.3 Archyvo apsauga 33
4.3.4 Atsarginių kopijų darymas 33
4.4. GEDIMŲ ŠALINIMAS IR RAKTŲ KOMPROMITACIJA 33
4.4.1 Aparatūros ir programinės įrangos gedimai 33
4.4.2 Privačiojo rakto kompromitacija 35
4.4.3 Saugumo priemonės pašalinus gedimų priežastis 35
4.5. SERTIFIKAVIMO PASLAUGŲ TEIKIMO NUTRAUKIMAS IR 35

5. FIZINIO, PROCEDŪRINIO IR PERSONALO SAUGUMO KONTROLĖ 37
5.1. FIZINIO SAUGUMO KONTROLĖ 37
5.1.1 Buveinės vieta 37
5.1.2 Fizinė prieiga 37
5.1.3 Elektros energijos tiekimas ir oro kondicionavimas 38
5.1.4 Apsauga nuo užpylimo vandeniu 38
5.1.5 Priešgaisrinė apsauga 38
5.1.6 Informacijos laikmenų saugojimas 38
5.1.7 Atliekų tvarkymas 38
5.2. PROCEDŪRINIO SAUGUMO KONTROLĖ 38
5.2.1 Darbuotojų pareigos 38
5.2.2 Reikalingas darbuotojų kiekis užduočiai atlikti 39
5.2.3 Pareigų identifikacija ir autentiškumo tikrinimas 39
5.3. PERSONALO PATIKIMUMO KONTROLĖ 40
5.3.1 Biografijos tikrinimo procedūra 40
5.3.2 Mokymo reikalavimai 40
5.3.3 Mokymų dažnumas ir reikalavimai jiems 40
5.3.4 Reikalavimai samdomiems asmenims 41
5.3.5 Darbuotojams teikiami dokumentai 41

6. TECHNINIO SAUGUMO KONTROLĖ 42
6.1. KRIPTOGRAFINIŲ RAKTŲ POROS GENERAVIMAS IR INSTALIAVIMAS 42
6.1.1 Raktų porų generavimas 42
6.1.2 Viešojo rakto perdavimas sertifikato sudarytojui 42
6.1.3 CA viešojo rakto perdavimas vartotojams 42
6.1.4 Raktų dydžiai 42
6.1.5 Aparatinis/programinis raktų generavimas 43
6.2. PRIVAČIOJO RAKTO APSAUGA 43
6.2.1 Kriptografinių modulių standartai 43
6.2.2 Privačiųjų raktų saugojimo reikalavimai 43

6.2.3 CA privačiųjų raktų atstatymas 43
6.2.4 Privačiojo rakto įvedimas į kriptografinį modulį 43
6.2.5 Privačiojo rakto aktyvavimas 44
6.2.6 Privačiojo rakto deaktyvavimas 44
6.2.7 Privačiojo rakto sunaikinimas 44
6.2.8 Raktų naudojimo periodai 44
6.3. KOMPIUTERIŲ SAUGA 45
6.4. TECHNINĖS KONTROLĖS GYVAVIMO CIKLAS 45
6.4.1 Sistemos kūrimo kontrolė 46
6.4.2 Saugumo reikalavimų laikymosi kontrolė 46
6.5. TINKLO SAUGA 46
6.6. KRIPTOGRAFINIO MODULIO INŽINERIJOS KONTROLĖ 46
7. SERTIFIKATO IR CRL PROFILIAI 48
7.1. ŠAKNINĖS CA SERTIFIKATO PROFILIS 48
7.1. ŠAKNINĖS CA OCSP ATSAKYMŲ PASIRAŠYMO SERTIFIKATO PROFILIS 48
7.2. NUOSTATŲ CA SERTIFIKATO PROFILIS 49
7.1. NUOSTATŲ CA OCSP ATSAKYMŲ PASIRAŠYMO SERTIFIKATO PROFILIS 50
7.2. DARBINĖS CA SERTIFIKATO PROFILIS 51
7.1. DARBINĖS CA OCSP ATSAKYMŲ PASIRAŠYMO SERTIFIKATO PROFILIS 52
7.2. KVALIFIKUOTŲ SERTIFIKATŲ SKIRTŲ ELEKTRONINIAMS PARAŠAMS TVIRTINTI PROFILIAI 53
7.2.1 Kvalifikuoto sertifikato su įrašytu elektroninio pašto adresu profilis 53
7.2.1 Kvalifikuoto sertifikato be įrašyto elektroninio pašto adreso profilis 54
7.2.2 Kvalifikuoto sertifikato įrašomo į SIM SSCD profilis 56
7.3. SERTIFIKATŲ SKIRTŲ SAUGIAM AUTENTIFIKAVIMUI PROFILIAI 57
7.3.1 Sertifikato, skirto saugiam autentifikavimui, su įrašytu elektroninio pašto adresu, profilis 57
7.3.1 Sertifikato, skirto saugiam autentifikavimui, be įrašyto elektroninio pašto adreso profilis 58
7.3.2 Sertifikato, skirto saugiam autentifikavimui, įrašomo į SIM SSCD profilis 59
7.4. CRL PROFILIAI 60
7.4.1 Šakninės CA CRL profilis 60
7.4.2 Nuostatų CA CRL profilis 61
7.4.3 Darbinės CA CRL profilis 61
8. SERTIFIKAVIMO VEIKLOS NUOSTATŲ ADMINISTRAVIMAS 63
8.1. CPS KEITIMO PROCEDŪROS 63
9. SĄVOKŲ APIBRĖŽIMAI IR SANTRUMPOS 64
10. ŠALTINIAI 69

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	Papidytas sertifikatų naudotojų sąrašas ir papildyti sertifikatų profiliai

Dokumento tvirtinimas:

Dokumento rengimas	Pavardė	Data	Parašas
Dokumentą tvirtino	Kęstutis Sabaliauskas	2010-11-24	

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 teisingumo ministerija. Įmonė tvarko Nekilnojamojo turto kadastrą ir registrą, Adresų registrą, Juridinių asmenų 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 įsteigęs Registrų centro sertifikavimo centrą (toliau – RCSC) – kvalifikuotų sertifikatų sudarymo ir tvarkymo paslaugų teikimo padalinį.

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

1.1. Apžvalga

CPS detaliai apibrėžia CA veiklą sudarant bei tvarkant kvalifikuotus sertifikatus, skirtus elektroniniams parašams tvirtinti ir autentifikavimo sertifikatus, skirtus asmens atpažinimui elektroninėje erdvėje.

Sertifikatai sudaromi tik asmenims naudojantiems CA teikiamą saugią elektroninio parašo formavimo įrangą (toliau – SSCD).

CPS parengti remiantis šiais dokumentais:

a) Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimu Nr. 2108 „Dėl reikalavimų kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams, reikalavimų elektroninio parašo įrangai, kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarkos ir elektroninio parašo priežiūros reglamento patvirtinimo“ (Žin., 2003, Nr. 2-47; 2010, Nr. 21-991);

b) LST ETSI TS 101 456 „Reikalavimai, keliami kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams“ standartu;

c) RFC 2527. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. March 1999. http://www.ietf.org/rfc/rfc2527.txt;

d) LST ETSI TS 101 862 V1.3.3 (2006-01) „Kvalifikuoto sertifikato profilis“ standartu;

e) RFC 3280 ”Internet X.509 Public Key Infrastructure Certificate and CRL Profile”.

CPS įgyvendina kvalifikuotų sertifikatų taisykles (toliau – CP), kurių OID yra 1.3.6.1.4.1.30903.1.1.3.

1.2. Identifikavimas

CPS skelbiami saugykloje (*repository*) internete.

Unikalus CPS identifikatorius (OID): **1.3.6.1.4.1.30903.1.2.3**

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 sertifikavimo centras - RCSC)	1
Dokumento tipas (sertifikavimo veiklos nuostatai)	2
Dokumento versija	3

1.3. Sertifikatų naudotojai ir taikymo sritys

1.3.1 Sertifikatų naudotojai

Sertifikatų naudotojus sudaro sertifikavimo paslaugų abonentai (toliau-abonentai), sertifikatų savininkai ir sertifikatu pasitikinčios šalys.

Abonentai - tai fiziniai ir juridiniai asmenys, sudarantys sertifikavimo paslaugų sutartį su RCSC jiems atstovaujančių asmenų sertifikatams sudaryti.

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

Pasitikinčios šalys – visi fiziniai ir juridiniai asmenys, kurie pasitiki CA išduotais kvalifikuotais sertifikatais patvirtintais elektroniniais parašais ir sertifikatais, kaip tapatybės įrodymais elektroninėje erdvėje.

1.3.2 Sertifikatų naudojimo sritys

Pagal šiuos CPS sudaromi ir tvarkomi:

a) kvalifikuoti sertifikatai, skirti kvalifikuotiems elektroniniams parašams tvirtinti;

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

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

CA teikia 2 rūšių SSCD:

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

b) SIM SSCD kuri naudojama kartu su mobiliuoju telefonu.

Kiekviena CA teikiama SSCD rūšis yra trečiojo SSCD tipo (*SSCD type 3*), SSCD saugumas pagal standartą ISO/IEC 15408 yra ne žemesnio kaip EAL4 įvertinimo.

Pagal šiuos CPS sudaromi sertifikatai juridiniams asmenims nėra išduodami, t.y. sertifikato savininkas gali būti tik fizinis asmuo.

1.4. RCSC organizacinė struktūra

Sertifikavimo paslaugų teikėjo (toliau – CSP) funkcijas atlieka Registrų centras. CSP teikia sertifikatų sudarymo ir tvarkymo, laiko žymos ir kitas sertifikavimo paslaugas. Sertifikatų sudarymo ir tvarkymo paslaugas teikia CA.

CA dalį sertifikatų sudarymo ir tvarkymo funkcijų pagal šiuos CPS deleguoja sertifikavimo veiklos palaikymo (toliau – Palaikymo tarnyba) ir registravimo tarnyboms (toliau – RA). RA funkcijas atlieka RC filialai ar kitos trečios šalys, su kuriomis sudarytos RA paslaugų teikimo sutartys.

CA yra išlieka atsakinga už visas teikiamas sertifikavimo paslaugas ir vykdomą sertifikavimo veiklą.

CA funkcijos apima:

c) RA pateiktų prašymų sudaryti sertifikatą, nutraukti ar sustabdyti sertifikato galiojimą, atšaukti sertifikato galiojimo sustabdymą, autentiškumo ir teisėtumo tikrinimą;

d) sertifikatų sudarymą;

e) SSCD parengimą ir teikimą;

f) sertifikatų galiojimo sustabdymą, nutraukimą ir sustabdymo atšaukimą;

g) informacijos apie sertifikatų statusą teikimą.

RA funkcijos apima:

a) prašymų išduoti sertifikatą, sustabdyti ar nutraukti sertifikato galiojimą, atšaukti sertifikato galiojimo stabdymą priėmimą ir perdavimą CA;

b) sutarčių sudarymą;

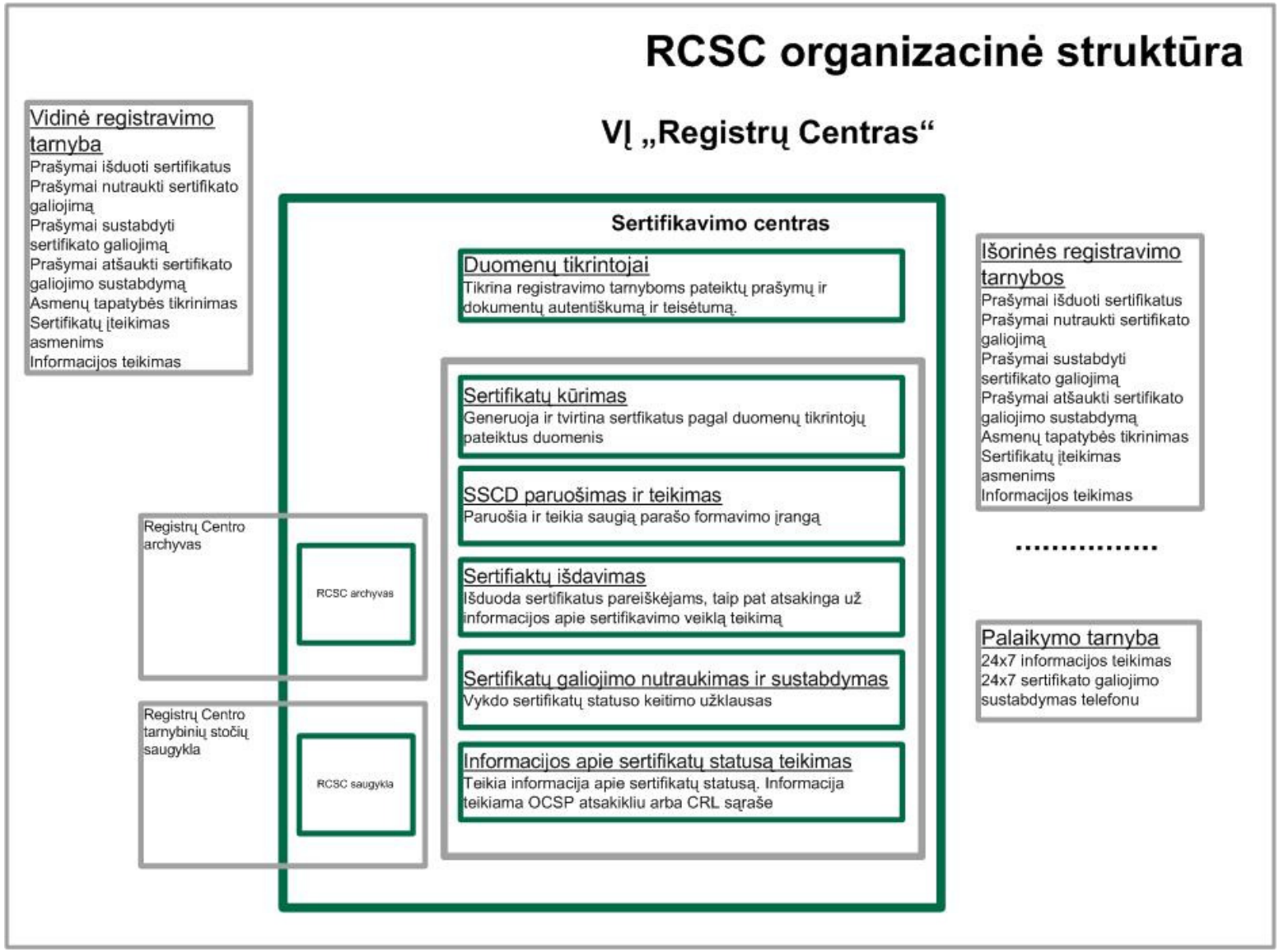
c) asmenų tapatybės tikrinimą;

d) sertifikatų ir SSCD įteikimą asmenims;

e) informacijos teikimą.

Palaikymo tarnyba veikia 7 dienas per savaitę, 24 val. per parą ir telefonu priima prašymus sustabdyti sertifikato galiojimą bei teikia informaciją.

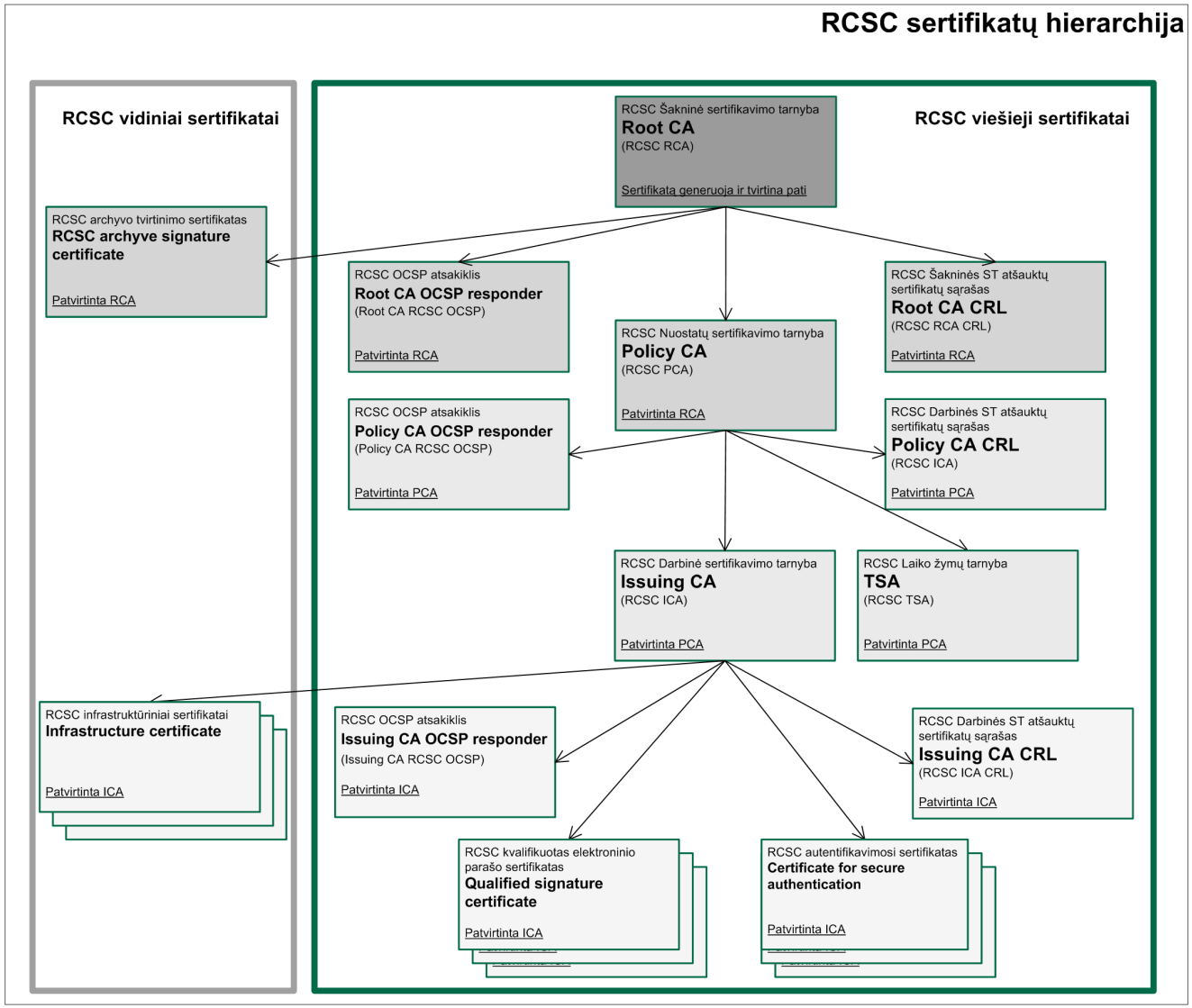
žemiau pateikiama RCSC organizacinės struktūros schema (*Pav. 1*).



Pav. 1. RCSC organizacinė struktūra

1.5. CA sertifikatų seka

CA sertifikatų seka paremta 3 lygių CA hierarchija. Pirmojo lygio šakninė CA naudoja save pasirašantį sertifikatą (*self-signed certificate*), išduoda sertifikatus nuostatų CA, šakninės CA OCSP pranešimų tvirtinimui, šakninės CA CRL tvirtinimui, archyvų tvirtinimui bei yra atjungta nuo tinklo (*off-line*) ir saugoma izoliuotoje aplinkoje. Nuostatų CA išduoda sertifikatus darbinei CA, nuostatų CA OCSP pranešimų tvirtinimui, nuostatų CA CRL tvirtinimui ir laiko žymų tarnybai (toliau – TSA). Nuostatų CA tai pat laikoma atjungta nuo tinklo ir saugoma izoliuotoje aplinkoje. Darbinė CA išduoda sertifikatus asmenims, darbinės CA OCSP pranešimų tvirtinimui, darbinės CA CRL tvirtinimui ir infrastruktūros sertifikatus



Pav. 2. RCSC sertifikatų hierarchija

1.6. Kontaktinė informacija

1.6.1 Nuostatus išleidusi ir tvarkanti organizacija

Organizacija	Valstybės įmonė Registrų centras
Adresas	V. Kudirkos g. 18, LT-03105 Vilnius, Lietuva
Telefonas	+370 5 268 8202
Faksas	+370 5 268 8311
URL:	http://www.registrucentras.lt
El.paštas:	info@registrucentras.lt

1.6.2 Kontaktinis asmuo

Už CPS atitikimą CP ir CPS administravimą atsakingas asmuo:

Saulius Kvedaravičius,

Valstybės įmonės Registrų centras Informacinių komunikacijų skyriaus vedėjas,

V. Kudirkos g. 18, LT-03105 Vilnius, Lietuva,

Tel.: +370 5 2688 268,

Faks.: +370 5 2688 311,

E-paštas: *Saulius.Kvedaravicius@registrucentras.lt*.

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 yra atsakinga už šių įsipareigojimų vykdymą ir tuo atveju, jei atskirų procedūrų vykdymas ar paslaugų teikimas yra perduotas trečiosioms šalims.

CA įsipareigoja:

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

b) užtikrinti tinkamą asmens, kuriam išduodamas sertifikatas identifikavimą;

c) užtikrinti prašymų išduoti sertifikatus priėmimą ir vykdymą:

- užtikrinti asmenų prašymų išduoti kvalifikuotus sertifikatus priėmimą ir vykdymą kaip tai numatyta CP ir CPS;
- užtikrinti saugų SSCD parengimą ir įteikimą asmenims;

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

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

e) priimti prašymus nutraukti ar sustabdyti sertifikato galiojimą:

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

f) priimti prašymus atšaukti sertifikato galiojimo sustabdymą:

- priimti ir vykdyti prašymus atšaukti sertifikato galiojimo sustabdymą kaip tai numato CP ir CPS;
- iš atšauktų sertifikatų sąrašo (toliau – CRL) pašalinti sertifikatus, kurių galiojimo sustabdymas buvo atšauktas.

g) užtikrinti asmens duomenų apsaugą, reglamentuojamą Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo (Žin., 1996, Nr. 63-1479; 2008, Nr. 22-804);

h) viešai skelbti saugykloje (*repository*) bet kuriuo paros metu:

- CP, CPS ir sertifikatų sudarymo bei tvarkymo sąlygas;
- 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) patikrintus ir visus reikalavimus atitinkančių prašymų duomenis perduoti CA;

d) laikantis visų CP ir CPS apibrėžtų saugumo reikalavimų, perduoti sertifikatus ir SSCD juos užsakiusiems asmenims;

e) teikti informaciją asmenims sertifikatų sudarymo ir tvarkymo klausimais;

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

2.1.3 Palaikymo tarnybos įsipareigojimai

Palaikymo tarnyba įsipareigoja:

a) 7 dienas per savaitę 24 val. per parą telefonu priimti prašymus sustabdyti sertifikato galiojimą ir teikti informaciją sertifikatų sudarymo ir tvarkymo klausimais;

b) įsipareigoja tvirtai laikytis su CA pasirašytos sutarties.

2.1.4 Abonentų ir sertifikatų savininkų įsipareigojimai

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

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

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

Sertifikatų savininkų įsipareigojimai:

c) tinkamai pasirūpinti, kad jo privačiuoju raktu nepasinaudotų kiti asmenys;

d) nedelsiant 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.

e) privačiojo rakto kompromitacijos atveju nedelsiant nutraukti jo naudojimą.

2.1.5 Pasitikinčių šalių įsipareigojimai

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

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

Jei sertifikatas yra galiojantis, toliau parašas tikrinamas vadovaujantis sertifikate esančia informacija. Parašo tikrintojai turi atkreipti dėmesį į tai, ar nepažeisti sertifikato naudojimo apribojimai.

2.2. Atsakomybė

Kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų atsakomybė nustatyta Lietuvos Respublikos elektroninio parašo įstatymo (Žin., 2000, Nr. 61-1827; Žin., 2002, Nr. 64-2572) trečiajame skirsnyje.

2.2.1 CA atsakomybė

CA prisiima atsakomybę už naudotojų patirtus nuostolius šiais atvejais:

a) jei CA, teikdama paslaugą, nesilaikė CP ir CPS;

b) jei CA neužtikrino savo privačiojo rakto saugumo arba teikiamų paslaugų saugumo.

CA prisiima atsakomybę, už sertifikatų naudotojų patirtus nuostolius, kuriuos sukėlė trečios šalys, kurioms CA delegavo dalį savo funkcijų.

CA neatsako sertifikatų naudotojų ir kitų su CA nesusijusių šalių veiksmus. CA neprisiima atsakomybės, jei nuostoliai buvo patirti dėl:

a) gamtos jėgų, pvz., gaisro, potvynio, audros, arba kitokių aplinkybių, kaip karas, teroristinis išpuolis, epidemija ir panašiai;

b) neleistino sertifikatų naudojimo (pvz., kai jis yra negaliojantis arba kai pažeidžiami sertifikato naudojimo apribojimai).

2.3. Finansinė atsakomybė

Finansinės atsakomybės įsipareigojimams užtikrinti CA savo veiklą draudžia 100.000 litų (šimtu tūkstančių litų) suma vienam draudiminiam įvykiui vienerių metų laikotarpiu.

2.3.1 Sertifikatų naudotojų kompensacijos

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

a) prašantysis sudaryti sertifikatą pateikė klaidingus duomenis;

b) sertifikato 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

Elektroninio parašo kūrimą, tikrinimą, galiojimą, parašo naudotojų teises ir atsakomybę, sertifikavimo paslaugas, įskaitant kvalifikuotų sertifikatų sudarymo paslaugas, reikalavimus jų teikėjams bei atsakomybę, nustato:

a) Lietuvos Respublikos elektroninio parašo įstatymas;

b) Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimas Nr. 2108 „Dėl reikalavimų kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams, reikalavimų elektroninio parašo įrangai, kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarkos ir elektroninio parašo priežiūros reglamento patvirtinimo“ (Žin., 2003, Nr. 2-47; 2010, Nr. 21-991).

2.4.2 Ginčų sprendimo tvarka

Bet kokie ginčai tarp CA ir sertifikatų naudotojų sprendžiami derybų keliu. Neišsprendus ginčo, jis sprendžiamas teismo tvarka.

2.5. Mokesčiai

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

CRL teikimas nėra apmokestinamas.

CA, gavusi sertifikato 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 ir sertifikatų sudarymo ir tvarkymo sąlygos;

b) informacija apie sertifikato statusą;

c) įvairi organizacinės paskirties ar patikimą veiklą įrodanti informacija (pvz. prašymo sudaryti sertifikatą forma, sutartis sertifikatui 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 4.1.6 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

CA veiklos atitiktis CP ir CPS tikrinama CA nustatyta vidaus tvarka. Išorinis nepriklausomas auditas nėra numatytas. Kvalifikuotų sertifikatų sudarymo paslaugų teikimo priežiūrą vykdo Informacinės visuomenės plėtros komitetas prie LR Vyriausybės.

2.7.1 CA veiklos tikrinimo dažnumas

CA veiklos atitiktis CP ir CPS turi būti tikrinama ne rečiau kaip kas vienerius metus.

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 Tikrinamieji dalykai

CA veiklai įvertinti yra tikrinama:

a) fizinis saugumas;

b) sertifikatą sudaryti prašančiųjų asmenų tapatybės tikrinimo procedūra;

c) sertifikavimo paslaugos ir jų teikimo galiniams vartotojams procedūros;

d) programinės įrangos ir sistemos prieigos kompiuterių tinklų saugumas;

e) personalo patikimumas;

f) registracijos žurnalų ir sistemos tvarkymo procedūros;

g) informacijos atsarginių kopijų darymas ir naudojimas;

h) archyvų tvarkymo procedūros;

i) įrašai apie CA struktūros keitimus;

j) įrašai apie aparatinės ir programinės įrangos tikrinimą ir priežiūrą.

2.7.4 Veiksmai pastebėjus trūkumus

Vidinio ir išorinio tikrinimo protokolai įteikiami CA saugumo pareigūnui. Per 30 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 sertifikavimo 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 sertifikavimo veiklos atnaujinimo laiką.

2.7.5 Tikrinimo rezultatų skelbimas

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

2.8. Konfidencialumo nuostatos

CA privalo saugoti asmenų, prašančių sudaryti sertifikatus, duomenis laikydamasis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo.

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 sertifikavimo paslaugas; visi šie duomenys gali būti atskleisti tik turint jos savininko raštišką sutikimą arba teismo patvirtintą orderį;

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 sertifikavimo paslaugų 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 sertifikavimo 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) informacija apie RCSC pravestus mokymus;

g) 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 sertifikatus, sustabdyti ar nutraukti sertifikatų galiojimą ir atšaukti sertifikatų galiojimo sustabdymą identifikavimo ir autentifikavimo taisyklės ir procedūros.

3.1. Pradinė registracija

Prašantysis sudaryti kvalifikuotą sertifikatą asmuo turi atvykti į RA asmeniškai.

RA privalo:

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

b) suteikti šią informaciją tvaria, nekintančia laike forma;

c) reikalauti, kad prašantieji sudaryti sertifikatus asmenys, jų tapatybei įrodyti pateiktų Lietuvos Respublikos pasą, asmens tapatybės kortelę ar leidimą gyventi;

d) įsitikinti prašančiųjų sudaryti sertifikatus asmenų tapatybe jiems fiziškai atvykus į RA, tiesiogiai patikrinant pateiktus tapatybės įrodymus, pvz. patikrinant fotonuotraukos ar biometrinių duomenų atitikimą;

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

f) dokumentuoti ir išsaugoti visą informaciją, naudojamą asmens tapatybei nustatyti, įskaitant dokumento tipą, numerį bei dokumentų galiojimo apribojimus;

g) dokumentuoti ir išsaugoti sudarytą sutartį, apimančią:

   - sertifikato savininko įsipareigojimus;
   - asmens duomenų, sertifikato ir atskirų sertifikato duomenų skelbimo sąlygas;
   - sutikimą saugoti sertifikato savininko registracijos, SSCD išdavimo ir kitą informaciją bei sutikimą šią informaciją pagal CP ir CPS numatytas procedūras perduoti trečioms šalims CA veiklos nutraukimo atveju;

- patvirtinimą, kad sertifikato savininko suteikta informacija yra teisinga;

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

i) įsipareigoti saugoti asmens duomenis vadovaujantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu.

Detali asmenų registravimo tvarka aprašyta RCSC Asmenų registravimo ir konsultavimo taisyklėse.

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 below (*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 Sertifikavimo Centras
CN (*Common Name*)	VI Registru Centras RCSC (IssuingCA)
Sertifikato savininko DN	
CN (*Common Name* – asmens vardas)	Asmens vardas, pavardė
G (*Given Name* - vardas)	Asmens vardas
SN (*Surname* – pavardė)	Asmens pavardė
Serijinis numeris	Asmens kodas
C (*Country* – šalis)	Šalis (ISO 3166 code)

CA turi reikalauti, kad sudaromame sertifikate būtų nurodyti asmens vardas ir pavardė bei asmens kodas.

3.1.2 Pseudonimų naudojimas

Pseudonimų naudojimas CA sudaromuose sertifikatuose neleidžiamas.

3.1.3 Vardų unikalumas

CA garantuoja asmenų identifikatoriaus unikalumą sudarytuose sertifikatuose. Asmens unikalus identifikatorius yra asmens kodas.

3.2. Tapatybės tikrinimas prašymo išduoti sertifikatą atveju

Asmens tapatybės tikrinimo tikslai yra du: patikrinti ar prašyme sudaryti sertifikatą 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.

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.

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 sertifikato nutraukti sertifikato galiojimą teikia abonentas arba sertifikato savininkas.

Tapatybės tikrinimo procedūra apima:

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

b) prašymą teikiant sertifikato 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 sertifikato galiojimą sertifikato savininko teikiami 2 būdais:

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

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

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).

Sertifikato galiojimas gali būti sustabdomas įgaliotos institucijos prašymu. Tokiu atveju turi būti pateiktas popierinis arba elektroninis pasirašytas prašymas, kuriame nurodyti sertifikato, kurio galiojimas sustabdomas, duomenys ir galiojimo sustabdymo priežastis.

3.6.Sertifikato galiojimo sustabdymą atšaukiančio asmens tapatybės tikrinimas

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

Atšaukti sertifikato galiojimo sustabdymą prašančio asmens tapatybė tikrinama analogiškai, prašymo sustabdyti sertifikato 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 Lietuvos Respublikos elektroninio parašo įstatymo reikalavimus kvalifikuotiems sertifikatams;

b) sertifikatai atitinka LST ETSI 101 862 „Kvalifikuotų sertifikatų sandara" standarto reikalavimus kvalifikuotų sertifikatų formatui;

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

d) raktų poros generavimo procedūra yra:

- saugiai susieta su sertifikato sudarymo procedūra;
- privatusis raktas generuojamas naudojant SSCD type 3, kurios saugumas pagal standartą ISO/IEC 15408 gavo ne žemesnį kaip EAL4 įvertinimą;
- parengta saugi parašo formavimo įranga saugiai perduodama sertifikatus sudaryti prašantiems asmenims.

e) sudarytame sertifikate nurodyti asmens identifikaciniai duomenys (DN vardas) yra unikalūs ir nepriskiriami kitam asmeniui;

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

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

h) sertifikatas sudaromas per 7 darbo dienas nuo prašymo gavimo.

4.1.2 Sertifikato galiojimo nutraukimas

CA užtikrina sertifikato galiojimo nutraukimą ne vėliau kaip per 8 darbo valandas po prašymo gavimo.

4.1.2.1 Sertifikato galiojimo nutraukimo atvejai

Sertifikato galiojimas nutraukimas tokias atvejais:

a) abonento ar sertifikato savininko prašymu;

b) paaiškėjus, kad sertifikato duomenys daugiau nėra teisingi;

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

d) sertifikatą išduodavęs CA nutraukia savo veiklą ir joks kitas sertifikavimo paslaugų teikėjas neperima sertifikavimo veiklos;

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

f) sertifikato savininkui praradus sertifikatą atitinkančių parašo formavimo duomenų kontrolę;

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

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

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

j) gavus pranešimą, kad sertifikato savininkas tapo neveiksnus;

k) gavus pranešimą, kad sertifikato savininkas mirė.

4.1.2.2 Kas turi teisę kreiptis dėl sertifikato galiojimo nutraukimo

Prašymus nutraukti sertifikato galiojimą gali teikti:

a) sertifikato savininkas;

b) abonentas;

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

d) Teisėsaugos institucijos.

4.1.3 Sertifikato galiojimo sustabdymas

Sertifikato galiojimas sustabdomas per 4 darbo valandas po prašymo gavimo.

4.1.3.1 Sertifikato galiojimo sustabdymo atvejai

Sertifikato galiojimas sustabdomas šiais atvejais:

a) sertifikato savininko prašymu;

b) Teisėsaugos institucijų reikalavimu, siekiant užkirsti kelią nusikaltimams;

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

4.1.3.2 Kas turi teisę kreiptis dėl sertifikato galiojimo sustabdymo

Prašymus sustabdyti sertifikato galiojimą gali teikti:

a) sertifikato savininkas;

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

c) Teisėsaugos institucijos.

4.1.3.3 Sertifikato galiojimo sustabdymo atšaukimas

Sertifikato galiojimo sustabdymas atšaukiamas gavus sertifikato savininko arba Teisėsaugos institucijos, kurios prašymu sertifikato galiojimas buvo sustabdytas, prašymą. Jei sertifikato galiojimas buvo sustabdytas dėl šio straipsnio 4.1.5.1 dalies c) punkte nurodytos priežasties, sertifikato galiojimo sustabdymas atšaukiamas gavus sertifikato savininko prašymą ir paaiškinimą, paneigiantį CA gautą informaciją.

4.1.3.4 Sertifikato galiojimo sustabdymo periodo ribos

Sertifikato galiojimo sustabdymo neatšaukus per 30 kalendorinių dienų, sertifikato galiojimas nutraukiamas.

4.1.4 CRL atnaujinimo dažnumas

CRL atnaujinamas periodiškai netgi jei nenutraukimas ar nesustabdomas nei vieno sertifikato galiojimas. Skelbiant eilinę CRL versiją visada nurodomas, kitos versijos skelbimo laikas.

Asmenims išduotų sertifikatų CRL ir Darbinės CA CRL atnaujinamas ne rečiau kaip kas 24 val. Šakninės ir Nuostatų CA, kadangi šios tarnybos laikomos neprijungtos prie tinklo, CRL atnaujinami ne rečiau kaip kas 3 mėn.

4.1.5 Sertifikatų galiojimo tikrinimo reikalavimai

Sertifikato statusas tikrinamas remiantis CRL sąrašu arba naudojant OCSP atsakiklį. Jei sertifikatas yra nebegaliojantis ir parašas neturi laiko žymos, parašas yra atmetamas. Esant laiko žymai, įsitikinama laiko žymės sertifikato galiojimu ir kad laiko žyma buvo išduota anksčiau nei nutrauktas pasirašiusio asmens sertifikato galiojimas.

4.1.5.1 Sertifikato galiojimo tikrinimas naudojant CRL sąrašą

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

4.1.5.2 Sertifikato galiojimo tikrinimas naudojantis OCSP atsakikliu

CA teikia galimybę sertifikato būklę tikrinti ir naudojant OCSP atsakiklį, teikiantį informaciją apie sertifikato statusą realiu laiku. Paslauga teikiama 24 val. per dieną, 7 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) sertifikato generavimo faktus;

c) sertifikato 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.

Operacijų žurnalas apsaugomas prieigos valdymo sistema ir pasirašomas infrastruktūriniu CA skaitmeniniu 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 kartą per mėnesį. Kiekvienas didesnės svarbos įvykis ar įvykis, atsitikęs dėl netinkamo sistemų funkcionavimo, turi būti aprašytas.

4.2.3 Įrašų saugojimo periodas

CA sistemos operacijų ir veiklos registravimo žurnalai CA saugomi 10 metų, tolesnį saugojimą reglamentuoja Lietuvos Respublikos dokumentų ir archyvų įstatymas (Žin., 1995, Nr. 107-2389; 2004, Nr.57-1982).

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 skaitmeniniu 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 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 valandas.

4.4. Gedimų šalinimas ir raktų kompromitacija

4.4.1 Aparatūros ir programinės įrangos gedimai

CA atsižvelgia į šias sertifikavimo paslaugų patikimumui ir stabilumui įtaką 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.

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 val.

4.4.2 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 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.

4.4.3 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.

4.5. Sertifikavimo paslaugų teikimo nutraukimas ir

RCSC prieš nutraukdamas sertifikavimo paslaugų teikimo veiklą įsipareigoja:

a) apie tai informuoti visus asmenis, kurių sertifikatus jis sudarė ir kurių sertifikatai yra galiojantys, taip pat Informacinės visuomenės plėtros komitetą prie Lietuvos Respublikos Vyriausybės ne vėliau kaip prieš vieną mėnesį;

b) jei joks kitas sertifikavimo paslaugų teikėjas neperima veiklos, nutraukti visų jo sudarytų sertifikatų galiojimą;

c) parengti susitarimą su kitu sertifikavimo paslaugų tiekėju, o tokio neradus – su Informacinės visuomenės plėtros komitetu prie Lietuvos Respublikos Vyriausybės, dėl sukauptų duomenų perėmimo, saugojimo ir teikimo pasitikinčioms šalims.

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

5.1.1 Buveinės vieta

RCSC buveinės adresas yra:

V. Kudirkos g. 18, LT-03105 Vilnius, Lietuva.

5.1.2 Fizinė prieiga

Fiziniam patekimui į CA patalpas kontroliuoti yra įrengta stebėjimo 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 RSCS patalpų saugumo zonos:

a) kompiuterinės sistemos zoną;

b) operatorių ir administratorių zoną;

c) projektuotojų ir programuotojų zoną.

Kompiuterinės sistemos zona yra įrengta bendroje Registrų Centro tarnybinių stočių saugykloje. Su sertifikavimo paslaugomis susijusi įranga yra saugoma atskiroje tarnybinių stočių spintoje. Patekimą į tarnybinių stočių saugyklą 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 saugykloje yra įrengta moderni oro kondicionavimo sistema. Nutrūkus elektros energijos tiekimui iš tinklo, atsarginiai energijos šaltiniai (2 UPS ir 2 dyzeliniai elektros energijos generatoriai) užtikrina normalų sistemos darbą 96 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.

5.1.5 Priešgaisrinė apsauga

RCSC patalpose yra įdiegta priešgaisrinės apsaugos sistema, atitinkanti priešgaisrinės apsaugos tarnybos nustatytus reikalavimus. Tarnybinių stočių saugykloje įdiegta automatinė gesinimo inertinėmis dujomis sistema.

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 vidinio ir išorinio 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.

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 asmenys: 2 asmenys vykdantys procedūras ir 2 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

Garantuojama, kad CA jiems pavestas pareigas atliekantys asmenys:

a) turi aukštąjį išsilavinimą;

b) yra pasirašę susitarimą dėl pareigų vykdymo ir atsakomybės;

c) yra išklausę tobulinimo kursus, susijusius su jiems pavestų pareigų vykdymu;

d) yra išklausę mokymus, susijusius su asmens duomenų ir konfidencialios informacijos apsauga.

5.3.1 Biografijos tikrinimo procedūra

Taikoma Registrų centro darbuotojų biografijos tikrinimo procedūra. Registrų centre negali dirbti teisti asmenys.

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 naudojantiem CA teikiamą SSCD type 3, kurios saugumas pagal standartą ISO/IEC 15408 gavo ne žemesnį kaip EAL4 įvertinimą

6.1.2 Viešojo rakto perdavimas sertifikato sudarytojui

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

6.1.3 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.

6.1.4 Raktų dydžiai

CA generuoja tokio dydžio raktus:

Šakninės sertifikavimo tarnybos raktai 4096 bitų ilgio;

Nuostatų sertifikavimo tarnybos raktai 2048 bitų ilgio;

Darbinės sertifikavimo tarnybos raktai 2048 bitų ilgio;

Asmenims generuojami raktai 2048 arba 1024 bitų ilgio.

6.1.5 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 sertifikatą 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, asmenų prašymu, privalo saugiai perduoti ją užsakiusiems asmenims ir įpareigoti juos saugoti savo privačiuosius raktus.

6.2.1 Kriptografinių modulių standartai

CA naudojami aparatiniai saugumo moduliai (kriptografiniai moduliai) ir asmenims rengiama SSCD atitinka LST CWA 14167, LST CWA 14168 (atitinkamai ir FIPS 140-2, LST ISO/IEC 15408) standartų reikalavimus.

6.2.2 Privačiųjų raktų saugojimo reikalavimai

CA privatieji raktai gali būti atstatomi ir jų kopijos saugomos tik naudojantis su kriptografine technine 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.

Sertifikato savininko privatusis raktas, kuris laikomas CA jam parengtoje SSCD, 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.

Sertifikato savininko privatusis raktas deaktyvuojamas pabaigus dokumentų pasirašymo elektroniniais parašais arba autentifikavimosi sesiją arba atjungus SSCD.

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 16 metų.

Nuostatų sertifikavimo tarnybos rakto galiojimo periodas yra 8 metai.

Darbinės sertifikavimo tarnybos rakto galiojimo periodas yra 4 metai.

Asmenims sudaromų sertifikatų (kartu ir raktų) galiojimo periodas yra 2 arba 1 metai.

Sertifikato galiojimo pradžios terminas paprastai sutampa su sertifikato sudarymo data. Draudžiama sertifikate nurodyti ankstesnį arba vėlesnį sertifikato galiojimo pradžios terminą, nei jo sudarymo data.

6.3. Kompiuterių sauga

CA ir kitų tarnybų kompiuteriai turi tokias apsaugos priemones:

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

d) savo nuožiūrai paliktas prieigos kontrolės priemones;

e) prisijungimams tikrinti reikiamų duomenų kaupimą;

f) įgalinančias atskirti pareigas, leistinas sistemoje;

g) prisijungiančių asmenų pareigų identifikavimo ir autentifikavimo priemones;

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

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

j) patikimas darbuotojų ir jų pareigų kaitos fiksavimo priemones;

k) 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 ir nuostatų sertifikavimo tarnybos 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 sertifikavimo 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 atitinkančius LST CWA 14167-2, LST CWA 14167-3, LST CWA 14168 standartų reikalavimus.

7. SERTIFIKATO IR CRL PROFILIAI

Sudaromi sertifikatai atitinka LST ETSI 101 862 „Kvalifikuotų sertifikatų sandara" standarto 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			*sha1RSA*
Issuer			*CN = VI Registru Centras RCSC (RootCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 16 metų*
Subject			*CN = VI Registru Centras RCSC (RootCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Public key			*RSA (4096 Bits)*
X.509 V3 Plėtiniai			
1.3.6.1.5.5.7.1.3	Taip		*Plėtinio OID reikšmė*
Subject Key Identifier	Ne		*Šakninio CA viešojo rakto hash reikšmė SHA1 algoritmu.*
CA Version	Ne		*V0.0*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.1*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Qualified Certificate Statement	Ne	QC statement	*Id-etsi-pcs-QcCompliance (0.4.0.1862.1.1)*
	Ne	SSCD statement	*id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)*
	Ne	Retention period	*10 metų*
Key Usage	Taip		*Certificate Signing, Off-line CRL Signing, CRL Signing (06)*
Basic Constraints	Taip		*Subject Type=CA* *Path Length Constraint=None*
Properties			
Thumbprint algorithm			*sha1*
Thumbprint			*Šakninio CA sertifikato santrauka*

7.1. 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			*sha1RSA*
Issuer			*CN = VI Registru Centras RCSC (RootCA)* *OU = Registru Centro Sertifikavimo Centras*

			O = VI Registru Centras - I.k. 124110246 *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data +3 metai*
Subject			*CN = VI Registru Centras OCSP (RootCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Public key			*RSA (4096 Bits)*
X.509 V3 Plėtiniai			
Subject Key Identifier	Ne	Key Identifier	*OCSP atsakymų pasirašymo viešojo rakto hash reikšmė SHA1 algoritmu.*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.2*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Key Usage	Ne		*Digital Signature, Non-Repudiation (c0)*
Authority Key Identifier	Ne	Key ID	*Šakninio CA viešojo rakto hash reikšmė SHA1 algoritmu.*
Properties			
Thumbprint algorithm			*sha1*
Thumbprint			*OCSP sertifikato santrauka*

7.2. Nuostatų CA sertifikato profilis

X.509 V1 pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			*V3*
Serial number			*Automatiškai sudaromas šakninio CA*
Signature algorithm			*sha1RSA*
Issuer			*CN = VI Registru Centras RCSC (RootCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 8 metai*
Subject			*CN = VI Registru Centras RCSC (PolicyCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Public key			*RSA (2048 Bits)*
X.509 V3 Plėtiniai			
Subject Key Identifier	Ne	Key Identifier	*Nuostatų CA viešojo rakto hash reikšmė SHA1 algoritmu.*
1.3.6.1.5.5.7.1.3	Taip		*Plėtinio OID reikšmė*
CA Version	Ne		*V0.0*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.1*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Qualified Certificate Statement	Ne	QC statement	*Id-etsi-pcs-QcCompliance (0.4.0.1862.1.1)*
	Ne	SSCD statement	*id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)*

	Ne	Retention period	*10 metų*
Certificate Template Name	Ne		*Sisteminis šablono identifikatorius*
Authority Key Identifier	Ne	Key Identifier	*Šakninio CA viešojo rakto hash reikšmė SHA1 algoritmu.*
CRL Distribution Points	Ne	Distribution Point Name	*URL=http://csp.rcsc.lt/CDP/VI%20Registru%20Centras%20RCSC%20(RootCA)([CRL versija]).crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp.rcsc.lt/AIA/VI%20Registru%20Centras%20RCSC%20(RootCA) ([RootCA sertifikato numeris]).crt*
Basic Constraints	Taip		*Subject Type=CA* *Path Length Constraint=None*
Key Usage	Taip		*Certificate Signing, Off-line CRL Signing, CRL Signing (06)*
Properties			
Thumbprint algorithm			*sha1*
Thumbprint			*Nuostatų CA sertifikato santrauka*

7.1. Nuostatų CA OCSP atsakymų pasirašymo sertifikato profilis

X.509 V1 pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			*V3*
Serial number			*Automatiškai sudaromas šakninio CA*
Signature algorithm			*sha1RSA*
Issuer			*CN = VI Registru Centras RCSC (RootCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 3 metai*
Subject			*CN = VI Registru Centras OCSP (PolicyCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Public key			*RSA (2048 Bits)*
X.509 V3 Plėtiniai			
Subject Key Identifier	Ne	Key Identifier	*OCSP atsakymų pasirašymo viešojo rakto hash reikšmė SHA1 algoritmu.*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.2*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Key Usage	Ne		*Digital Signature, Non-Repudiation (c0)*

Authority Key Identifier	Ne	Key ID	*Šakninio CA viešojo rakto hash reikšmė SHA1 algoritmu.*
CRL Distribution Points	Ne	Distribution Point Name	*URL=http://csp.rcsc.lt/CDP/VI%20Registru%20Centras%20RCSC%20(RootCA)([CRL versija]).crl*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp.rcsc.lt/AIA/VI%20Registru%20Centras%20RCSC%20(RootCA) ([RootCA sertifikato numeris]).crt*
Properties			
Thumbprint algorithm			*sha1*
Thumbprint			*OCSP sertifikato santrauka*

7.2. Darbinės CA sertifikato profilis

X.509 V1 pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			*V3*
Serial number			*Automatiškai sudaromas nuostatų CA*
Signature algorithm			*sha1RSA*
Issuer			*CN = VI Registru Centras RCSC (PolicyCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 4 metai*
Subject			*CN = VI Registru Centras RCSC (IssuingCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Public key			*RSA (2048 Bits)*
X.509 V3 Plėtiniai			
Subject Key Identifier	Ne	Key Identifier	*Darbinio CA viešojo rakto hash reikšmė SHA1 algoritmu.*
1.3.6.1.5.5.7.1.3	Taip		*Plėtinio OID reikšmė*
CA Version	Ne		*V0.0*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.1*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Qualified Certificate Statement	Ne	QC statement	*Id-etsi-pcs-QcCompliance (0.4.0.1862.1.1)*
	Ne	SSCD statement	*id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)*
	Ne	Retention period	*10 metų*
Certificate Template Name	Ne		*Sisteminis šablono identifikatorius*
Authority Key Identifier	Ne	Key Identifier	*Nuostatų CA viešojo rakto hash reikšmė SHA1 algoritmu.*

CRL Distribution Points	Ne	Distribution Point Name	*URL=http://csp.rcsc.lt/CDP/VI%20Registru%20Centras%20RCSC%20(PolicyCA)([CRL versija]).crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp.rcsc.lt/AIA/VI%20Registru%20Centras%20RCSC%20(PolicyCA) ([PolicyCA sertifikato numeris]).crt*
Basic Constraints	Taip		*Subject Type=CA* *Path Length Constraint=None*
Key Usage	Taip		*Certificate Signing, Off-line CRL Signing, CRL Signing (06)*
Properties			
Thumbprint algorithm			*sha1*
Thumbprint			*Darbinio CA sertifikato santrauka*

7.1. 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			*sha1RSA*
Issuer			*CN = VI Registru Centras RCSC (PolicyCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 3 metai*
Subject			*CN = VI Registru Centras OCSP (IssuingCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Public key			*RSA (2048 Bits)*
X.509 V3 Plėtiniai			
Subject Key Identifier	Ne	Key Identifier	*OCSP atsakymų pasirašymo viešojo rakto hash reikšmė SHA1 algoritmu.*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.2*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Key Usage	Ne		*Digital Signature, Non-Repudiation (c0)*
Authority Key Identifier	Ne	Key ID	*Šakninės CA viešojo rakto hash reikšmė SHA1 algoritmu.*
CRL Distribution Points	Ne	Distribution Point Name	*URL=http://csp.rcsc.lt/CDP/VI%20Registru%20Centras%20RCSC%20(PolicyCA)([CRL versija]).crl*

		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp.rcsc.lt/AIA/VI%20Registru%20Centras%20RCSC%20(PolicyCA) ([PolicyCA sertifikato numeris]).crt*
Properties			
Thumbprint algorithm			*sha1*
Thumbprint			*OCSP sertifikato santrauka*

7.2. Kvalifikuotų sertifikatų skirtų elektroniniams parašams tvirtinti profiliai

7.2.1 Kvalifikuoto 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			*sha1RSA*
Issuer			*CN = VI Registru Centras RCSC (IssuingCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 2 metai*
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)*
X.509 V3 plėtiniai			
Subject alternative name	Ne		*RFC822 Name=elektroninio pašto adresas*
Subject Key Identifier	Ne	Key Identifier	*Asmens viešojo rakto hash reikšmė SHA1 algoritmu.*
Authority Key Identifier	Ne	Key Identifier	*Darbinio CA viešojo rakto hash reikšmė SHA1 algoritmu.*
CRL Distribution Points	Ne	Distribution Point Name	*URL=http://csp.rcsc.lt/CDP/VI%20Registru%20Centras%20RCSC%20(IssuingCA)([CRL versija]).crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp.rcsc.lt/ocspresponder.rcsc*

		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp.rcsc.lt/AIA/VI%20Registru%20Centras%20RCSC%20(IssuingCA)([IssuingCA sertifikato numeris]).crt*
Certificate Template Information	Ne	Template	*Sisteminis šablono identifikatorius*
Enhanced Key Usage	Ne		*Document Signing (1.3.6.1.4.1.311.10.3.12)* *Secure Email (1.3.6.1.5.5.7.3.4)*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.2.3*
		Policy Qualifier Id=User Notice	*This statement is a statement by the issuer that this certificate is issued as a Qualified certificate according Annex I and II of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, as implemented in the law of the country specified in the issuer field of this certificate. Sis sertifikatas yra kvalifikuotas sertifikatas pagal ES direktyvos 1999/93/EC del Bendrijos elektroninio paraso pagrindu I ir II priedus ir Lietuvos elektroninio paraso istatyma.*
		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	Statement ID	*Id-etsi-pcs-QcCompliance (0.4.0.1862.1.1)*
SSCD statement	Ne	Statement ID	*id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)*
Retention Period	Ne		*10 metų*
Key Usage	Taip		*Digital Signature, Non-Repudiation (c0)*
Properties			
Thumbprint algorithm			*SHA1*
Thumbprint			*Asmens sertifikato santrauka*

7.2.1 Kvalifikuoto 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			*sha1RSA*
Issuer			*CN = VI Registru Centras RCSC (IssuingCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 2 metai*
Subject		Serial Number	*Asmens kodas*
		CN	*Bendrinis vardas: suteiktas vardas ir pavardė*
		G	*Asmens vardas*

		SN	*Asmens pavardė*
		C	*LT*
Public key			*RSA (2048 Bits)*
X.509 V3 plėtiniai			
Subject Key Identifier	Ne	Key Identifier	*Asmens viešojo rakto hash reikšmė SHA1 algoritmu.*
Authority Key Identifier	Ne	Key Identifier	*Darbinio CA viešojo rakto hash reikšmė SHA1 algoritmu.*
CRL Distribution Points	Ne	Distribution Point Name	*URL=http://csp.rcsc.lt/CDP/VI%20Registru%20Centras%20RCSC%20(IssuingCA)([CRL versija]).crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp.rcsc.lt/AIA/VI%20Registru%20Centras%20RCSC%20(IssuingCA)([IssuingCA sertifikato numeris]).crt*
Certificate Template Information	Ne	Template	*Sisteminis šablono identifikatorius*
Enhanced Key Usage	Ne		*Document Signing (1.3.6.1.4.1.311.10.3.12)* *Secure Email (1.3.6.1.5.5.7.3.4)*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.2.3*
		Policy Qualifier Id=User Notice	*This statement is a statement by the issuer that this certificate is issued as a Qualified certificate according Annex I and II of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, as implemented in the law of the country specified in the issuer field of this certificate. Sis sertifikatas yra kvalifikuotas sertifikatas pagal ES direktyvos 1999/93/EC del Bendrijos elektroninio paraso pagrindu I ir II priedus ir Lietuvos elektroninio paraso istatyma.*
		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	Statement ID	*Id-etsi-pcs-QcCompliance (0.4.0.1862.1.1)*
SSCD statement	Ne	Statement ID	*id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)*
Retention Period	Ne		*10 metų*
Key Usage	Taip		*Digital Signature, Non-Repudiation (c0)*
Properties			
Thumbprint algorithm			*SHA1*
Thumbprint			*Asmens sertifikato santrauka*

7.2.2 Kvalifikuoto sertifikato įrašomo į SIM SSCD profilis

X.509 V1 pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			*V3*
Serial number			*Automatiškai sudaromas, unikalus sertifikato, išduoto darbinio CA, serijinis numeris*
Signature algorithm			*sha1RSA*
Issuer			*CN = VI Registru Centras RCSC (IssuingCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 2 metai*
Subject		Serial Number	*Asmens kodas*
		CN	*Bendrinis vardas: suteiktas vardas ir pavardė*
		G	*Asmens vardas*
		SN	*Asmens pavardė*
		C	*LT*
Public key			*RSA (1024 Bits)*
X.509 V3 plėtiniai			
Subject Key Identifier	Ne	Key Identifier	*Asmens viešojo rakto hash reikšmė SHA1 algoritmu.*
Authority Key Identifier	Ne	Key Identifier	*Darbinio CA viešojo rakto hash reikšmė SHA1 algoritmu.*
CRL Distribution Points	Ne	Distribution Point Name	*URL=http://csp.rcsc.lt/CDP/VI%20Registru%20Centras%20RCSC%20(IssuingCA)([CRL versija]).crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp.rcsc.lt/AIA/VI%20Registru%20Centras%20RCSC%20(IssuingCA)([IssuingCA sertifikato numeris]).crt*
Certificate Template Information	Ne	Template	*Sisteminis šablono identifikatorius*
Enhanced Key Usage	Ne		*Document Signing (1.3.6.1.4.1.311.10.3.12)* *Secure Email (1.3.6.1.5.5.7.3.4)*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.2.3*

		Policy Qualifier Id=User Notice	*This statement is a statement by the issuer that this certificate is issued as a Qualified certificate according Annex I and II of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, as implemented in the law of the country specified in the issuer field of this certificate. Sis sertifikatas yra kvalifikuotas sertifikatas pagal ES direktyvos 1999/93/EC del Bendrijos elektroninio paraso pagrindu I ir II priedus ir Lietuvos elektroninio paraso istatyma.*
		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	Statement ID	*Id-etsi-pcs-QcCompliance (0.4.0.1862.1.1)*
SSCD statement	Ne	Statement ID	*id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)*
Retention Period	Ne		*10 metų*
Key Usage	Taip		*Digital Signature, Non-Repudiation (c0)*
Properties			
Thumbprint algorithm			*SHA1*
Thumbprint			*Asmens sertifikato santrauka*

7.3. Sertifikatų skirtų saugiam autentifikavimui profiliai

7.3.1 Sertifikato, skirto saugiam autentifikavimui, 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			*sha1RSA*
Issuer			*CN = VI Registru Centras RCSC (IssuingCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 2 metai*
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)*
X.509 V3 plėtiniai			
Subject alternative name	Ne		*RFC822 Name=elektroninio pašto adresas*
Subject Key Identifier	Ne	Key Identifier	*Asmens viešojo rakto hash reikšmė SHA1 algoritmu.*

Authority Key Identifier	Ne	Key Identifier	*Darbinio CA viešojo rakto hash reikšmė SHA1 algoritmu.*
CRL Distribution Points	Ne	Distribution Point Name	*URL=http://csp.rcsc.lt/CDP/VI%20Registru%20Centras%20RCSC%20(IssuingCA)([CRL versija]).crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp.rcsc.lt/AIA/VI%20Registru%20Centras%20RCSC%20(IssuingCA)([IssuingCA sertifikato numeris]).crt*
Certificate Template Information	Ne	Template	*Sisteminis šablono identifikatorius*
Enhanced Key Usage	Ne		*Client Authentication (1.3.6.1.5.5.7.3.2)*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.2.3*
		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)*
Properties			
Thumbprint algorithm			*SHA1*
Thumbprint			*Asmens sertifikato santrauka*

7.3.1 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			*sha1RSA*
Issuer			*CN = VI Registru Centras RCSC (IssuingCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 2 metai*
Subject			*Serial Number=Asmens kodas* *CN= vardas ir pavardė* *G = asmens vardas* *SN = asmens pavardė* *C= LT*
Public key			*RSA (2048 Bits)*
X.509 V3 plėtiniai			

Subject Key Identifier	Ne	Key Identifier	*Asmens viešojo rakto hash reikšmė SHA1 algoritmu.*
Authority Key Identifier	Ne	Key Identifier	*Darbinio CA viešojo rakto hash reikšmė SHA1 algoritmu.*
CRL Distribution Points	Ne	Distribution Point Name	*URL=http://csp.rcsc.lt/CDP/VI%20Registru%20Centras%20RCSC%20(IssuingCA)([CRL versija]).crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp.rcsc.lt/AIA/VI%20Registru%20Centras%20RCSC%20(IssuingCA)([IssuingCA sertifikato numeris]).crt*
Certificate Template Information	Ne	Template	*Sisteminis šablono identifikatorius*
Enhanced Key Usage	Ne		*Client Authentication (1.3.6.1.5.5.7.3.2)*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.2.3*
		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)*
Properties			
Thumbprint algorithm			*SHA1*
Thumbprint			*Asmens sertifikato santrauka*

7.3.2 Sertifikato, skirto saugiam autentifikavimui, įrašomo į SIM SSCD profilis

X.509 V1 pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			*V3*
Serial number			*Automatiškai sudaromas, unikalus sertifikato, išduoto darbinio CA, serijinis numeris*
Signature algorithm			*sha1RSA*
Issuer			*CN = VI Registru Centras RCSC (IssuingCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 2 metai*
Subject			*Serial Number=Asmens kodas* *CN= vardas ir pavardė* *G = asmens vardas* *SN = asmens pavardė* *C= LT*

Public key			*RSA (1024 Bits)*
X.509 V3 plėtiniai			
Subject Key Identifier	Ne	Key Identifier	*Asmens viešojo rakto hash reikšmė SHA1 algoritmu.*
Authority Key Identifier	Ne	Key Identifier	*Darbinio CA viešojo rakto hash reikšmė SHA1 algoritmu.*
CRL Distribution Points	Ne	Distribution Point Name	*URL=http://csp.rcsc.lt/CDP/VI%20Registru%20Centras%20RCSC%20(IssuingCA)([CRL versija]).crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp.rcsc.lt/AIA/VI%20Registru%20Centras%20RCSC%20(IssuingCA)([IssuingCA sertifikato numeris]).crt*
Certificate Template Information	Ne	Template	*Sisteminis šablono identifikatorius*
Enhanced Key Usage	Ne		*Client Authentication (1.3.6.1.5.5.7.3.2)*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.2.3*
		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)*
Properties			
Thumbprint algorithm			*SHA1*
Thumbprint			*Asmens sertifikato santrauka*

7.4. CRL profiliai

7.4.1 Šakninės CA CRL profilis

CRL pagrindiniai laukai	Atributas	Reikšmė
Version		*V2*
Issuer		*CN = VI Registru Centras RCSC (RootCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Effective date		*Išdavimo data ir laikas*
Next update		*Kito atnaujinimo data ir laikas*
Signature algorithm		*sha1RSA*
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	*Šakninio CA viešojo rakto hash reikšmė SHA1 algoritmu*
CA Version		*V0.0*
CRL Number		*Suteiktas automatiškai šakninio CA*
Next CRL Publish		*Publikavimo (išdavimo) data + 3 mėnesiai*

7.4.2 Nuostatų CA CRL profilis

CRL pagrindiniai laukai	**Atributas**	**Reikšmė**
Version		*V2*
Issuer		*CN = VI Registru Centras RCSC (PolicyCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Effective date		*Išdavimo data ir laikas*
Next update		*Kito atnaujinimo data ir laikas*
Signature algorithm		*sha1RSA*
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	*Nuostatų CA viešojo rakto hash reikšmė SHA1 algoritmu*
CA Version		*V0.0*
CRL Number		*Suteiktas automatiškai nuostatų CA*
Next CRL Publish		*Publikavimo (išdavimo) data + 3 mėnesiai*

7.4.3 Darbinės CA CRL profilis

CRL pagrindiniai laukai	**Atributas**	**Reikšmė**
Version		*V2*
Issuer		*CN = VI Registru Centras RCSC (IssuingCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Effective date		*Išdavimo data ir laikas*
Next update		*Kito atnaujinimo data ir laikas*
Signature algorithm		*sha1RSA*
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	*Darbinio CA viešojo rakto hash reikšmė SHA1 algoritmu*
CA Version		*V0.0*

CRL Number		*Suteiktas automatiškai darbinio CA*
Next CRL Publish		*Publikavimo (išdavimo) data + 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 sertifikavimo paslaugų saugumo lygio pasikeitimus, pakeitimai yra esminiai.

CPS prižiūrimi, keičiami ir tvirtinami laikantis tokios procedūros:

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

b) CPS pakeitimus inicijuoja CA arba sertifikatų naudotojai;

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

d) apie naują CPS redakcija informuojama elektroninio parašo priežiūros institucija;

9. SĄVOKŲ APIBRĖŽIMAI IR SANTRUMPOS

Abonentas *(subscriber)* – asmuo sudarantis sutartį su CA vieno ar daugiau asmenų, kuriems sudaromas 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 Revocation List)* – sertifikavimo centro periodiškai (arba neatidėliotinai) leidžiamas, jo pasirašomas sąrašas sertifikatų, kurių galiojimas nutrauktas ar sustabdytas.Tokiame sąraše paprastai nurodomas jį sudariusio sertifikavimo centro vardas, sąrašo sudarymo data, numatoma kitos sąrašo versijos išleidimo data, nebegaliojančių sertifikatų serijiniai numeriai, galiojimo nutraukimo ar sustabdymo laikai 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 (**parašas**) - duomenys, kurie įterpiami, prijungiami ar logiškai susiejami su kitais duomenimis pastarųjų autentiškumui patvirtinti ir pasirašančiam asmeniui identifikuoti.

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

Kriptografinis modulis – žiūr. Aparatinis saugumo modulis.

Kvalifikuotas elektroninis parašas - saugus elektroninis parašas, sukurtas saugia parašo formavimo įranga (SSCD) ir patvirtintas galiojančiu kvalifikuotu sertifikatu.

Kvalifikuotas sertifikatas - sertifikatas, kurį sudarė Lietuvos Respublikos Vyriausybės ar jos įgaliotos institucijos nustatytus reikalavimus atitinkantis sertifikatų centras.

Kvalifikuotų sertifikatų taisyklės *(Qualified Certificate Policy – CP)* – sertifikato taisyklės, kuriose įtraukti Europos Parlamento ir Tarybos direktyvos 1999/93/EB „Dėl Bendrijos elektroninių parašų reguliavimo sistemos" I ir II priedo reikalavimai.

Laiko žyma – tai duomenys, kurie yra logiškai susieti su kitais duomenimis ir patvirtina, kad tie kiti duomenys egzistavo iki žymoje nurodyto laiko. Elektroninio parašo laiko žyma yra įrodymas, kad parašas buvo sukurtas iki žymoje nurodyto laiko.

Laiko žymos paslaugų teikėjas *(TSA – Time-Stamping Authority)* - sertifikavimo 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 turi parašo formavimo įrangą (privatųjį raktą) ir sukuria elektroninį parašą.

Pasitikinčios šalys *(relying party)* – asmenys gaunantys sertifikatų savininkų pasirašytus duomenis ir sertifikatus bei siekiančios įsitikinti sertifikatų savininkų tapatybe bei kita sertifikatuose nurodyta informacija.

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

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

Registravimo tarnyba *(RA – Registration Authority)* – sertifikatų tarnybos padalinys arba atskiras juridinis asmuo, sudaręs sutartį su sertifikatų tarnyba, 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, vartotojams prieinama tiesiogiai (*on-line*) bet kuriuo metu internete adresu www.rcsc.lt/repository/.

Saugus elektroninis parašas - elektroninis parašas, kuris atitinka visus šiuos reikalavimus: (1) yra vienareikšmiškai susietas su pasirašančiu asmeniu; (2) leidžia identifikuoti pasirašantį asmenį; (3) yra sukurtas priemonėmis, kurias pasirašantis asmuo gali tvarkyti tik savo valia; (4) yra susijęs su pasirašytais duomenimis taip, kad bet koks šių duomenų pakeitimas yra pastebimas.

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.

Sertifikato taisyklės *(Certificate Policy)* – sertifikato sudarymo ir naudojimo taisyklės, 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".

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 paslaugų teikėjas *(CSP - Certification Service Provider)* - įmonė, neturinti juridinio asmens teisių, arba juridinis asmuo, sudarantis sertifikatus arba teikiantis kitas paslaugas, susijusias su elektroniniu parašu.

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

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

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)*

CP – Kvalifikuotų sertifikatų taisyklės *(Certificate Policy*)

CPS – Sertifikavimo veiklos nuostatai *(Certification Practice Statement)*

CSP - Sertifikavimo paslaugų teikėjas *(Certification Service Provider)*

CRL - Atšauktų sertifikatų sąrašas *(Certificate Revocation List)*

CWA - CEN darbo grupės susitarimas *(CEN Workgroup Agreement)*

DN - Asmens unikalus identifikacinis vardas *(Distinguished Name)*

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)*

IETF - Interneto inžinierinių uždavinių sprendėjai *(Internet Engineering Task Force)*

LAN – Vietinis kompiuterių tinklas *(Local Area Network)*

LST – Lietuvos standartizacijos tarnyba

OID – Unikalus objekto identifikatorius *(Object Ientifier)*

OCSP - Tiesioginės prieigos protokolas informacijai apie sertifikato statusą gauti *(Online Certificate Status Protocol)*

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)*

SSCD - Saugi parašo formavimo įranga *(Secure Signature Creation Device)*

UPS - Atsarginis energijos šaltinis *(Uninterrupted Power Supply)*

10. ŠALTINIAI

[1] ETSI TS 101 456 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates. http://portal.etsi.org/esi/el-sign.asp.

[2] ETSI TS 101 862 Qualified Certificate Profile. http://portal.etsi.org/esi/el-sign.asp.

[3] ETSI SR 002 176 Electronic Signatures and Infrastructures (ESI): Algorithms and Parameters for Secure Electronic Signatures. http://portal.etsi.org/esi/el-sign.asp.

[4] CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements. http://www.uninfo.polito.it/WS_Esign/docs.htm#published.

[5] CWA 14167-2 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP). http://www.uninfo.polito.it/WS_Esign/docs.htm#published.

[6] CWA 14167-3 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP). http://www.uninfo.polito.it/WS_Esign/docs.htm#published.

[7] CWA 14168 Secure Signature-Creation Devices, version 'EAL 4'. http://www.uninfo.polito.it/WS_Esign/docs.htm#published.

[8] CWA 14170 Security Requirements for Signature Creation Applications http://www.uninfo.polito.it/WS_Esign/docs.htm#published.

[9] CWA 14171 General Guidelines for Electronic Signature Verification. http://www.uninfo.polito.it/WS_Esign/docs.htm#publis

hed.

[10] RFC 2459 — Internet X.509 Public Key Infrastructure Certificate and CRL Profile. http://www.ietf.org/rfc/rfc2459.txt.

[11] RFC 3280 — Internet X.509 Public Key Infrastructure. Certificate and CRL Profile. http://www.ietf.org/rfc/rfc3280.txt.

[12] RFC 3647 — Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework. http://www.ietf.org/rfc/rfc3647.txt.

[13] RFC 3739 — Internet X.509 Public Key Infrastructure. Qualified Certificate Profile. http://www.ietf.org/rfc/rfc3739.txt.

[14] RFC 3125 — Electronic Signature Policies. http://www.ietf.org/rfc/rfc3125.txt.

[15] ISO/IEC 19790:2006 — Information Technology – Security Techniques – Security Requirements for Cryptographic Modules.

[16] FIPS PUB 140-2 — Security Requirements for Cryptographic Modules. http://www.nist.gov/cmvp.

[17] FIPS 112 — Password Usage. http://csrs.nist.gov/fips/.

[18] ITU-T — Recommendation X.509 – Information Technology – Open System Interconnection – The Directory: Authentication Framework, June 1997 (equivalent ISO/IEC9594-8).

[19] VeriSign CPS - — VeriSign Certification Practice Statement. http://www.verisign.com.

[20] LST ISO/IEC 15408:1999(E) — Information technology – Security techniques – Evaluation criteria for IT security.