PATVIRTINTA
Valstybės įmonės Registrų centro
generalinio direktoriaus
įsakymu Nr. VE-676

VALSTYBĖS ĮMONĖS REGISTRŲ CENTRO ELEKTRONINĖS ATPAŽINTIES, NUOTOLINIO ELEKTRONINIO PARAŠO IR ELEKTRONINIO SPAUDO SERTIFIKAVIMO VEIKLOS NUOSTATAI

Unikalus objekto ID (OID): **1.3.6.1.4.1.30903.1.6.1**

Versija: 1.2

Galioja nuo: 2024-10-25

Registrų centro elektroninės atpažinties, nuotolinio elektroninio parašo ir elektroninio spaudo sertifikavimo veiklos nuostatų keitimų istorija:

Versija	Data	Aprašas
1.0	2022-11-11	Pirma versija
1.1	2023-03-31	Atliktos korekcijos pagal Lietuvos Respublikos ryšių reguliavimo tarnybos pateiktas pastabas.
1.2	2024-09-12	Nuostatai papildyti informacija dėl kvalifikuotos elektroninės atpažinties paslaugų; pakeistas nuostatų pavadinimas; atnaujinti kontaktiniai duomenys; atnaujinti Registrų centro padalinių pavadinimai.

Turinys

1. Įvadas

Valstybės įmonė Registrų centras (toliau - Registrų centras, Įmonė) yra įsteigta 1997 m. Įmonės steigėjas – Lietuvos Respublikos Vyriausybė. Įmonės savininko teises ir pareigas įgyvendinanti institucija yra Lietuvos Respublikos ekonomikos ir inovacijų ministerija.

Registrų centras yra kvalifikuotos elektroninės atpažinties ir kvalifikuotų patikimumo užtikrinimo paslaugų teikėjas. Registrų centro sertifikavimo tarnyba (angl. certification authority) (toliau – CA, RCSC) bei Registrų centro registravimo tarnybos (angl. registration authority) (toliau RA) – Registrų centro klientų aptarnavimo centrai bei išorinės organizacijos, su kuriomis yra sudarytos atitinkamos funkcijų delegavimo sutartys, teikia kvalifikuotos elektroninės atpažinties, **kvalifikuotų elektroninių parašų ir kvalifikuotų elektroninių spaudų sertifikatų (toliau – sertifikatai)** sudarymo, tvarkymo bei kvalifikuotų elektroninių laiko žymų paslaugas. Sertifikatai sudaromi ir tvarkomi bei kvalifikuotos elektroninės laiko žymos sudaromos Lietuvos Respublikos teritorijoje. Šie Registrų centro elektroninės atpažinties, nuotolinio elektroninio parašo ir nuotolinio elektroninio spaudo sertifikavimo veiklos nuostatai (toliau – CPS (angl. Certification Practice Statement)) reglamentuoja CA ir RA veiklą sudarant ir išduodant nuotolinio elektroninio parašo, kuris naudojamas ir kaip elektroninė atpažinties priemonė, ir nuotolinio elektroninio spaudo sertifikatus.

1.1. Apžvalga

Šie CPS reglamentuoja Registrų centro veiklą sudarant ir išduodant:

a) Kvalifikuotą elektroninio parašo skaitmeninį sertifikatą – **QSignC-R-QSCD**, kuris gali būti naudojamas tik su nuotolinio kvalifikuoto elektroninio parašo kūrimo įrenginiu – R-QSCD, į kurį yra įrašytas privatus raktas, susietas su sertifikate esančiu viešu raktu. R-QSCD įrenginį valdo kvalifikuotas patikimumo užtikrinimo paslaugos teikėjas pasirašančio asmens, kuriam sertifikatas yra išduotas, vardu. Reikalavimai sertifikato sudarymui ir išdavimui nustatyti remiantis ETSI EN 119 431-1 standarto EUCSP taisyklėmis. Kvalifikuotas nuotolinio elektroninio parašo skaitmeninis sertifikatas yra naudojamas ir kaip kvalifikuotos elektroninės atpažinties priemonė.

b) Kvalifikuotą elektroninio spaudo skaitmeninį sertifikatą – **QSealC-R-QSCD**, kuris gali būti naudojami tik su nuotolinio kvalifikuoto elektroninio spaudo kūrimo įrenginiu – R-QSCD, į kurį yra įrašytas privatus raktas, susietas su sertifikate esančiu viešu raktu. R-QSCD įrenginį valdo kvalifikuotas patikimumo užtikrinimo paslaugos teikėjas pasirašančio asmens, kuriam sertifikatas yra išduotas, vardu. Reikalavimai sertifikato sudarymui ir išdavimui nustatyti remiantis ETSI EN 119 431-1 standarto EUCSP taisyklėmis.

c) Nuotolinio kvalifikuoto elektroninio parašo bei nuotolinio kvalifikuoto elektroninio spaudo kriptografinių raktų aktyvavimo transakcijų pasirašymo sertifikatą – **R-SIC,** kuris išduodamas nuotolinio kvalifikuoto elektroninio parašo bei nuotolinio kvalifikuoto elektroninio spaudo kriptografinių raktų aktyvavimo priemonei. Reikalavimai sertifikato sudarymui ir išdavimui nustatyti remiantis ETSI EN 319 411-1 standarto OVCP taisyklėmis.

Šie nuostatai yra išleidžiami lietuvių ir anglų kalbomis. Dokumento struktūra atitinka RFC 3647 standarte ,,Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework" nustatytus reikalavimus. Šie CPS įgyvendina Registrų centro Sertifikavimo veiklos taisykles (toliau – CP), kurių OID yra 1.3.6.1.4.1.30903.1.5.1 sudarant ir išduodant **QSealC-R-QSCD** bei **QSignC-R-QSCD** tipo sertifikatus.

1.2. Dokumento pavadinimas ir identifikavimas

Šių CPS unikalus identifikatorius (OID – Object identifier) yra **1.3.6.1.4.1.30903.1.6.1**.

Lentelė Nr. 1. CPS unikalaus identifikatoriaus laukų reikšmės

Reikšmė	**Kodas**
ISO – International Organization for Standardization	1
Organizacijos identifikavimo schemos, registruotos pagal ISO/IEC 6523-2 (Organization identification schemes registered according to ISO/IEC 6523-2)	3
OSI tinklas JAV Gynybos departamentui (Open System Interconnection (OSI) network for the Department of Defense (DoD))	6

Internetas	1
Privatūs projektai	4
IANA registruotos privačios įmonės	1
Valstybės įmonė Registrų centras	30903
Padalinys (RCSC)	1
Dokumento tipas – Elektroninės atpažinties, nuotolinio elektroninio parašo ir nuotolinio elektroninio spaudo sertifikavimo veiklos nuostatai	6
Dokumento versija	1

Naujausia CPS versija pateikiama RCSC saugykloje (*repository*).[1]

1.3. Viešųjų raktų infrastruktūros dalyviai

1.3.1. Sertifikavimo tarnybos

Registrų centras, kaip patikimumo užtikrinimo paslaugų teikėjas, valdo šias sertifikavimo tarnybas: Šakninę sertifikavimo tarnybą (Root CA) – RCSC RCA bei Darbinę sertifikavimo tarnybą (Issuing CA) – RCSC CA (jos abi sudaro CA, RCSC).

CA sudaro ir išduoda Šakninės sertifikavimo tarnybos, Darbinės sertifikavimo tarnybos, fizinių asmenų autentifikavimo elektroninė erdvėje, kvalifikuoto elektroninio parašo bei kvalifikuoto elektroninio spaudo sertifikatus, TSL / SSL sertifikatus, nuotolinio parašo / spaudo kriptografinių raktų aktyvavimo patvirtinimo sertifikatus, tvarko atšauktų sertifikatų sąrašą.

Sertifikatą išdavusios tarnybos pavadinimas įrašomas sertifikato lauke „Issuer".

CA funkcijų vykdymą užtikrina:

a) E. parašo skyrius, atsakingas už šių CPS parengimą ir paslaugų teikimo procedūrų nustatymą bei jų vykdymo priežiūrą, sertifikatų sudarymą, atšaukimą ir atšauktų sertifikatų sąrašo sudarymą ir skelbimą;

b) Aptarnavimo departamentas – Registrų centro struktūrinis padalinys, atsakingas už kreipinių stabdyti sertifikatų galiojimą priėmimą ir sertifikatų galiojimo stabdymą;

c) Klientų aptarnavimo ir nuotolinių kanalų aptarnavimo centrai – Registrų centro struktūrinis padalinys, atsakingas už klientų konsultavimą sertifikatų sudarymo ir tvarkymo klausimais;

d) IT infrastruktūros departamentas, atsakingas už sertifikatų sudarymo, tvarkymo, kvalifikuotų elektroninių laiko žymų techninės ir programinės įrangos veikimo priežiūrą bei administravimą.

[1] https://ltid.lt/

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

CA funkcijos apima:

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

b) sertifikatų sudarymą;

c) nuotolinio parašo / spaudo kriptografinių raktų aktyvavimo priemonės (toliau – Nuotolinio parašo / spaudo aktyvavimo priemonė) išdavimą;

d) sertifikatų galiojimo sustabdymą, nutraukimą ir sustabdymo atšaukimą;

e) informacijos apie sertifikatų statusą teikimą.

1.3.2. Registravimo tarnybos

Registravimo tarnyba (RA) vykdo sertifikatų naudotojų identifikavimą ir autentifikavimą, priima jų prašymus išduoti ir atnaujinti sertifikatus, stabdyti jų galiojimą.

Registravimo tarnybos funkcijas atlieka Registrų centro klientų aptarnavimo centrai bei išorinės organizacijos, su kuriomis yra pasirašytos atitinkamos Registravimo tarnybos funkcijų delegavimo sutartys.

RA funkcijos apima:

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

b) sertifikatų galiojimo sustabdymą, nutraukimą ir sustabdymo atšaukimą;

c) asmenų tapatybės tikrinimą bei prašymo duomenų autentiškumo patvirtinimą;

d) informacijos apie elektroninės atpažinties, nuotolinio parašo / spaudo užsakymo ir įdiegimo procesą teikimą.

1.3.3. Abonentai ir sertifikatų savininkai

Abonentas *(subscriber)* – tai fizinis ar juridinis asmuo, prašantis sudaryti elektroninio parašo ar elektroninio spaudo sertifikatą.

Sertifikato savininkas *(subject)* – fizinis ar juridinis asmuo, kuriam (kurio vardu) sudaromas autentikavimo elektroninėje erdvėje, elektroninio parašo, elektroninio spaudo skaitmeninis sertifikatas.

Kvalifikuotą nuotolinio elektroninio parašo sertifikatą, kuris gali būti naudojamas ir kaip kvalifikuota elektroninės atpažinties priemonė **QSignC-R-QSCD** gali užsakyti tik fizinis asmuo, kurio vardu yra prašoma sudaryti šį sertifikatą. **QSignC-R-QSCD** sertifikatų savininkais gali būti tik fiziniai asmenys.

Elektroninio spaudo sertifikatą **QSealC-R-QSCD** gali užsakyti tik fizinis asmuo, kuriam tokią teisę yra suteikęs juridinis asmuo, kurio vardu yra prašoma sudaryti šį sertifikatą. **QSealC-R-QSCD** sertifikatų savininkais gali būti tik juridiniai asmenys, įregistruoti ES šalies narės Juridinių asmenų registre.

R-SIC sertifikatas išduodamas nuotolinio kvalifikuoto elektroninio parašo bei nuotolinio kvalifikuoto elektroninio spaudo kriptografinių raktų aktyvavimo priemonei el. parašo ar el. spaudo sertifikatus užsakančio asmens iniciatyva.

1.3.4. Pasitikinčios šalys

Pasitikinčios šalys yra Registrų centro tvarkomos informacinės sistemos ir registrai, fiziniai ar juridiniai asmenys, naudojantys elektroninius dokumentus ar duomenis, patvirtintus šios viešųjų raktų infrastruktūros (angl. PKI) išduotais sertifikatais.

1.4. Sertifikatų naudojimas

1.4.1. Tinkamas sertifikatų naudojimas

Pagal šiuos CPS sudaromi ir tvarkomi:

a) **QSignC-R-QSCD** kvalifikuoti elektroninio parašo sertifikatai, skirti kvalifikuotiems elektroniniams parašams tvirtinti;

b) **QSealC-R-QSCD** kvalifikuoti elektroninio spaudo sertifikatai, skirti kvalifikuotiems elektroniniams spaudams tvirtinti;

c) **R-SIC** sertifikatai, skirti nuotolinio kvalifikuoto elektroninio parašo bei nuotolinio kvalifikuoto elektroninio spaudo kriptografinių raktų aktyvavimo transakcijų pasirašymui.

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

QSignC-R-QSCD, **QSealC-R-QSCD**, **R_SIC** sertifikatai sudaromi į CA valdomą nuotolinio kvalifikuoto elektroninio parašo ir spaudo kūrimo įrenginį (remote electronic signature and seal creation device).

Kvalifikuoto elektroninio parašo bei autentikavimo elektroninėje erdvėje sertifikatai juridiniams asmenims nėra išduodami, t. y. šių sertifikatų savininkas gali būti tik fizinis asmuo. Kvalifikuoto elektroninio spaudo sertifikato savininkas gali būti tik juridinis asmuo. CA neišduoda sertifikatų, susietų su asmens užimamomis pareigomis.

1.4.2. Draudžiamas sertifikatų naudojimas

Sertifikato savininkui išduodami sertifikatai negali būti naudojami:

a) bet kokiai neteisėtai veiklai (įskaitant kibernetines atakas, bandymus klastoti asmens tapatybę ir pan.);

b) išduoti (patvirtinti) kitus naujus skaitmeninius sertifikatus;

c) patvirtinti informaciją apie šio ar kitų sertifikatų galiojimą;

d) netikrų dokumentų ar informacijos (pvz., dokumentų, skirtų sistemų ar procesų testavimui) elektroninių parašų patvirtinimui.

R-SIC sertifikatai negali būti naudojami elektroninių dokumentų, duomenų ar transakcijų tvirtinimui kvalifikuotu elektroniniu parašu ar spaudu.

1.5. Nuostatų valdymas

1.5.1. Nuostatus patvirtinusi ir tvarkanti organizacija

Organizacija	Valstybės įmonė Registrų centras
Adresas	Studentų g. 39, 08106 Vilnius, Lietuva
Telefonas	+370 5 268 8262
URL:	www.registrucentras.lt
El. paštas:	info@registrucentras.lt

1.5.2. Kontaktinis asmuo

Už CPS atitikimą CP ir CPS administravimą atsakingas asmuo:

Valstybės įmonės Registrų centro E. parašo skyriaus vadovė

Studentų g. 39, 08106 Vilnius, Lietuva, tel. +3705 268 8262

El. paštas: info@ltid.lt

Dėl saugumo bei vientisumo pažeidimų prašome susisiekti tel. +370 5 2511999 arba el. paštu info@ltid.lt .

1.5.3. Informacija apie CA teikiamas paslaugas

CA tinklalapyje https://ltid.lt pateikiama informacija apie sertifikatų užsakymą, užsakymo būklę, CRL aktualų sąrašą, dokumentus, kuriuos būtina turėti norint įsigyti CA teikiamas paslaugas. Taip pat pateikiamos aktualios CP bei CPS versijos.

1.6. Apibrėžimai ir sutrumpinimai

Abonentas *(subscriber)* – asmuo (fizinis / juridinis), prašantis sudaryti elektroninio parašo ar elektroninio spaudo sertifikatus savo ar kitų asmenų vardu.

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

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

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

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

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

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

Juridinio asmens atstovas – fizinis asmuo, turintis teisę atstovauti įmonei užsakant ir išduodant elektroninio spaudo sertifikatus

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

Kriptografinis modulis – žiūrėti **Aparatinis saugumo modulis**.

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

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

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

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

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

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

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

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

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

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

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

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

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

Pažangusis elektroninis spaudas – elektroninis spaudas, kuris atitinka visus šiuos reikalavimus: 1) yra vienareikšmiškai susietas su spaudo kūrėju; 2) pagal jį galima nustatyti spaudo kūrėjo tapatybę; 3) yra sukurtas naudojant elektroninio spaudo kūrimo duomenis, kuriuos spaudo kūrėjas gali labai patikimai pats naudoti kurdamas elektroninį spaudą; 4) yra susietas su juo patvirtintais duomenimis taip, kad bet koks šių duomenų pakeitimas yra pastebimas.

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

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

Saugykla *(repository)* – sertifikatų ir kitos patikimumo užtikrinimo paslaugų teikėjo informacijos saugykla, naudotojams prieinama tiesiogiai (*on-line*) bet kuriuo metu internete adresu: www.rcsc.lt/repository/.

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 – autentifikuojantis asmuo.

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

Spaudo kūrėjas – juridinis asmuo, kuris sukuria elektroninį spaudą.

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

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

CA	Registrų centro sertifikavimo tarnyba (Certification Authority), valdanti šias sertifikavimo tarnybas: Šakninę sertifikavimo tarnybą (Root CA) – RCSC RCA bei Darbinę sertifikavimo tarnybą (Issuing CA) – RCSC ICA (jos abi vadinamos CA).
CP	Registrų centro kvalifikuotų sertifikatų (elektroninių parašų ir elektroninių spaudų) taisyklės (Qualified Certificate (Electronic Signature and Electronic Seal) Policy)
CPS	Šie Registrų centro sertifikavimo veiklos nuostatai (Certification Practice Statement)
CSP	Patikimumo užtikrinimo paslaugų teikėjas (Certification Service Provider/Trust Service Provider)
CRL	Atšauktų sertifikatų sąrašas (Certificate Revocation List)
DN	Asmens unikalus identifikacinis vardas (Distinguished Name)
ECC	Elipsinės kreivės kriptografija (elliptic curve cryptography)
eSUS	Registrų centro sertifikatų tvarkymo savitarnos sistema

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	Atvirų standartų organizacija (Internet Engineering Task Force)
LAN	Vietinis kompiuterių tinklas (Local Area Network)
LST	Lietuvos standartizacijos tarnyba
OID	Unikalus objekto identifikatorius (Object Identifier)
OCSP	Tiesioginės prieigos protokolas informacijai apie sertifikato statusą gauti (Online Certificate Status Protocol)
QSCD	Kvalifikuotas elektroninio parašo arba elektroninio spaudo kūrimo įtaisas
PKI	Viešojo rakto infrastruktūra (Public Key Infrastructure)
RA	Registrų centro registravimo tarnyba (Registration Authority) – Registrų centro klientų aptarnavimo centrai bei išorinės organizacijos, su kuriomis yra sudarytos atitinkamos funkcijų delegavimo sutartys.
RCSC	Žiūrėti **CA**
RFC	IETF organizacijos dokumentas, kuriame pateikiamos techninės ir organizacinės pastabos apie internetą. (Request For Comments)
RSA	RSA asimetrinio šifravimo algoritmas *(Rivest-Shamir-Adelman algorithm)*
R-QSCD	Kvalifikuoto elektroninio parašo ir kvalifikuoto elektroninio spaudo kūrimo įrenginys, kurį valdo kvalifikuotas patikimumo užtikrinimo paslaugos teikėjas pasirašančio asmens, kuriam sertifikatas yra išduotas, vardu ir atitinkantis eIDAS 29-30 straipsniuose ir 39 straipsnio 1-2 dalyse nustatytus reikalavimus.
SHA-1	Saugus e. duomenų santraukos gavimo algoritmas 1 *(Secure Hash Algorithm 1)*
SHA-256	Saugus e. duomenų santraukos gavimo algoritmas 256 *(Secure Hash Algorithm 2561)*
UPS	Atsarginis energijos šaltinis *(Uninterrupted Power Supply)*

2. Sertifikavimo informacijos skelbimas ir saugyklos

2.1. Saugyklos

Abonentams, sertifikatų savininkams ir pasitikinčioms šalims aktualią informaciją, susijusią su sertifikatų užsakymu išdavimu ir naudojimu, CA saugo viešai prieinamoje informacijos saugykloje (repository) (toliau – Saugykla).

CA užtikrina, kad Saugykloje skelbiama informacija bus prieinama 24 val. per parą ir 7 dienas per savaitę, užtikrinant 99% jos pasiekiamumą.

2.2. Sertifikavimo informacijos skelbimas

CA per viešai prieinamą Saugyklą adresu https://www.elektroninis.lt skelbia:

a) Šakninės sertifikavimo tarnybos (Root CA), Darbinės sertifikavimo tarnybos (Issuing CA), laiko žymų tarnybos (TSA) sertifikatus;

b) CA išduotų ir atšauktų sertifikatų duomenis;

c) Registrų centro kvalifikuotų sertifikatų (elektroninių parašų ir elektroninių spaudų) taisykles – CP (Certificate Policy), šiuos Registrų centro sertifikavimo veiklos nuostatus – CPS;

d) elektroninio spaudo sertifikatų užsakymo, išdavimo ir naudojimo sąlygas ir taisykles;

e) elektroninio parašo sertifikatų užsakymo, išdavimo ir naudojimo sąlygas ir taisykles;

f) instrukcijas naudotojams;

g) įgaliotų institucijų parengtas CA veiklos tikrinimo ataskaitų santraukas.

CP ir CPS skelbiami lietuvių ir anglų kalbomis.

2.3. Informacijos skelbimo terminai ir dažnumas

Šakninės sertifikavimo tarnybos (Root CA), Darbinės sertifikavimo tarnybos (Issuing CA), laiko žymų tarnybos (TSA) sertifikatai yra skelbiami iš karto po jų sudarymo.

Informacija CA išduotų ir atšauktų sertifikatų saugykloje atnaujinama iš karto sustabdžius ar atšaukus bet kurio CA išduoto sertifikato galiojimą.

CP, CPS, elektroninės atpažinties, elektroninio parašo sertifikatų užsakymo, išdavimo ir naudojimo sąlygos ir taisyklės bei elektroninio spaudo sertifikatų užsakymo, išdavimo ir naudojimo sąlygos ir taisyklės keičiamos pasikeitus teisinei, techninei ar organizacinei aplinkai, darančiai įtaką patikimumo užtikrinimo paslaugų teikimui, atsiradus naujoms paslaugoms ar nutraukus buvusių paslaugų teikimą. Naujos šių dokumentų versijos per 3 darbo dienas po jų patvirtinimo Registrų centro generalinio direktoriaus įsakymu pateikiamos priežiūros įstaigai ir per 5 darbo dienas po jų patvirtinimo paskelbiamos viešai.

Kita informacija skelbiama ją gavus ar parengus per protingą terminą.

Registrų centras privalo pateikti einamųjų metų elektroninės atpažinties ir patikimumo užtikrinimo veiklos ataskaitą priežiūros įstaigai ne vėliau kaip iki kitų metų vasario 1 dienos.

3. Identifikavimas ir autentikavimas

3.1. Vardai

3.1.1. Galimos vardų reikšmės

Pagal šiuos CPS CA sudaromi sertifikatai atitinka ITU-T X.509 v3 standarto reikalavimus, o juose nurodomi asmenų identifikaciniai vardai (toliau tekste – DN vardai; *Distinguished Names*) sudaromi laikantis IETF RFC 5280 ir ETSI EN 319 412 standartų rekomendacijų. Pagal šiuos CPS sudaromų sertifikatų DN lauko reikšmės pateiktos žemiau esančiose lentelėse.

QSignC-R-QSCD sertifikatams

DN vardo lauko žymėjimas ir jo paskirtis	**Nurodoma reikšmė**
CA sudarytojo DN	
C (*Country* – šalis)	LT
O (Organizacija)	VĮ Registrų centras, kodas 124110246
OU (*Organization Unit* – organizacijos padalinys)	RCSC
CN (*Common Name*)	RCSC IssuingCA-2
Sertifikato savininko DN	
CN (*Common Name* – bendrinis pavadinimas)	Asmens pavardė, vardas, fizinio asmens identifikatoriaus semantinis identifikatorius ir asmens kodas
G (*Given Name* - vardas)	Asmens vardas
SN (*Surname* – pavardė)	Asmens pavardė
SERIALNUMBER (Serijinis numeris)	Fizinio asmens identifikatoriaus semantinis identifikatorius ir asmens kodas
C (*Country* – šalis)	Šalis (ISO 3166 code)

QSealC-R-QSCD sertifikatams

DN vardo lauko žymėjimas ir jo paskirtis	**Nurodoma reikšmė**
CA sudarytojo DN	
C (*Country* – šalis)	LT
O (Organizacija)	VĮ Registrų centras, kodas 124110246
OU (*Organization Unit* – organizacijos padalinys)	RCSC
CN (*Common Name*)	RCSC IssuingCA-2

Sertifikato savininko DN	
CN (*Common Name* – bendrinis pavadinimas)	Juridinio asmens pavadinimas
O (Organizacija)	Juridinio asmens pavadinimas nacionaliniame registre
2.5.4.97 (OID)	Juridinio asmens semantikos identifikatorius ir juridinio asmens kodas
C (*Country* – šalis)	Šalis (ISO 3166 code)

R-SIC sertifikatams

DN vardo lauko žymėjimas ir jo paskirtis	**Nurodoma reikšmė**
CA sudarytojo DN	
C (*Country* – šalis)	LT
O (Organizacija)	VĮ Registrų centras, kodas 124110246
OU (*Organization Unit* – organizacijos padalinys)	RCSC
CN (*Common Name*)	RCSC IssuingCA-2
Sertifikato savininko DN	
CN (*Common Name* – bendrinis pavadinimas)	Paskyros arba vartotojo informacija
SERIALNUMBER (Serijinis numeris)	
C (*Country* – šalis)	Šalis (ISO 3166 code)
E (Email address – Elektroninio pašto adresas)	Elektroninio pašto adresas

CA sudaromuose elektroninio parašo ir autentifikavimo elektroninėje erdvėje sertifikatuose yra nurodoma asmens vardas ir pavardė bei asmens kodas, elektroninio spaudo sertifikato atveju – juridinio asmens pavadinimas bei juridinio asmens kodas.

3.1.2. Slapyvardžių naudojimas

Slapyvardžių ar pseudonimų naudojimas nėra leidžiamas.

3.2. Tapatybės patvirtinimas

3.2.1. Privataus rakto turėjimo patvirtinimas

Sertifikatų savininkų privatūs raktai yra sukuriami ir saugomi R-QSCD. Privataus rakto aktyvavimui yra naudojama sertifikatų savininkui CA išduodama ir R-QSCD registruojama Nuotolinio parašo / spaudo aktyvavimo priemonė. R-QSCD privatus raktas yra aktyvuojamas sertifikatų savininkui naudojant nuotolinio parašo / spaudo aktyvavimo priemonę, pasirašant R-QSCD pateiktą

užklausą. Užklausos pasirašymui naudojamas šios priemonės privatus raktas, apsaugotas sertifikato savininko pasirinktu autentikavimo kodu. Nuotolinio parašo / spaudo aktyvavimo priemonės raktų pora ir atitinkami autentikavimo kodai bei jai skirtas R-SIC sertifikatas yra generuojami šios įrangos registracijos R-QSCD metu.

R-QSCD yra išsaugomi ir tarpusavyje susiejami:

a) sertifikato savininko identifikaciniai duomenys;

b) sertifikato savininkui išduoti nuotolinio parašo / spaudo kriptografiniai raktai bei atitinkami skaitmeniniai sertifikatai;

c) sertifikato savininkui išduotos nuotolinio parašo / spaudo aktyvavimo priemonės viešas raktas bei CA išduotas R-SIC sertifikatas.

Nuotolinio parašo / spaudo aktyvavimo priemonė gali būti išduota ir registruota bei naudojama aktyvuoti privatų raktą mobilaus ryšio įrenginių pritaikytų neįgaliesiems pagalba.

3.2.2. Juridinio asmens tapatybės patvirtinimas

QSealC-R-QSCD kvalifikuotus elektroninio spaudo sertifikatai užsakomi abonentui pildant ir teikiant CA užsakymą. Užsakyme abonentas turi pateikti:

a) juridinio asmens pavadinimą;

b) juridinio asmens teisinės formos duomenis;

c) buveinės adresą;

d) juridinio asmens kodą Lietuvos Respublikos juridinių asmenų registre (toliau – JAR) arba kitos Europos Sąjungos (toliau – ES) šalies narės, Islandijos, Lichtenšteino ar Norvegijos verslo registre (toliau – ES šalių verslo registrai);

e) juridinio asmens vadovo ar kito fizinio asmens, turinčio teisę atstovauti šį juridinį asmenį duomenis – vardą, pavardę, asmens identifikacinį numerį, asmens tapatybės dokumento numerį, įgaliojimo duomenis (jei užsakymą teikia ne organizacijos vadovas), elektroninio pašto adresą bei mobilaus telefono numerį.

Užsakant šiuos sertifikatus yra tikrinama juridinio asmens tapatybė bei užsakyme pateikti įmonės duomenys, lyginant juos su JAR bei ES šalių verslo registruose esančia informacija. Elektroninio spaudo sertifikatą gali užsakyti tik fizinis asmuo, turintis teisę atstovauti įmonei užsakant ir išduodant elektroninio spaudo sertifikatus (toliau – Juridinio asmens atstovas). Fizinio asmens teisė atstovauti Lietuvos Respublikoje registruotam juridiniam asmeniui tikrinama JAR. Kitais atvejais asmuo turi pateikti dokumentą, įrodantį, kad tokia teisė jam suteikta.

Juridinio asmens atstovo tapatybė tikrinama ir patvirtinama vienu iš toliau šiuose CPS nurodytų būdų:

a) asmeniui fiziškai atvykus į RA padalinį;

b) nuotoliniu būdu, užsakymą išduoti sertifikatą patvirtinus galiojančiu kvalifikuotu elektroniniu parašu.

Juridinio asmens ir Įmonės atstovo tapatybės patikrinimas ir patvirtinimas vykdomas vadovaujantis šiuose CPS nustatytomis procedūromis ir asmens tapatybės ir papildomų specifinių požymių tikrinimo išduodant kvalifikuotus elektroninio parašo, elektroninio spaudo, interneto svetainės tapatumo nustatymo sertifikatus tvarka, patvirtinta Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2018 m. spalio 26 d. įsakymu Nr. 1V-1055.

R-SIC sertifikatai išduodami patvirtinus asmens tapatybę, **QSealC-R-QSCD** sertifikatų išdavimo proceso metu.

3.2.2.1. Juridinio asmens ir juridinio asmens atstovo tapatybės patvirtinamas jam atvykus į RA padalinį

Pagrindiniai Juridinio asmens ir juridinio asmens atstovo tapatybės patikrinimo ir patvirtinimo procedūros etapai:

1) juridinio asmens atstovas užpildo elektroninį arba atvykęs į RA pateikia „popierinį" prašymą išduoti elektroninį spaudo sertifikatą;

2) CA naudodamasi programinėmis priemonėmis patikrina prašyme pateiktų juridinio asmens duomenų autentiškumą, jų atitikimą JAR ar ES šalių verslo registruose esančiai informacijai;

3) CA naudodamasi programinėmis priemonėmis JAR patikrina prašyme nurodyto fizinio asmens teisę atstovauti LR įregistruotai įmonei;

4) jeigu yra užsakoma elektroninio spaudo sertifikatas įmonei, registruotai kitoje ES šalyje narėje, RA specialistas patikrina fizinio asmens pateiktų dokumentų, kuriais jam yra suteikta teisė įmonės vardu užsakyti ir gauti el. parašo sertifikatą, galiojimą ir autentiškumą;

5) RA specialistas:

a) pagal pateiktą asmens tapatybės dokumentą nustato prašymą pateikusio asmens tapatybę;

b) palygina asmens tapatybės dokumente bei dokumentuose, patvirtinančiuose fizinio asmens teisę atstovauti juridiniam asmeniui (jeigu tokie turėjo būti pateikti), esančių asmens duomenų atitikimą prašyme pateiktai informacijai.

6) Juridinio asmens ir juridinio asmens atstovo tapatybė laikoma patvirtinta, jeigu tenkinamos šios sąlygos:

a) prašyme pateikti duomenys atitinka JAR ar ES šalių verslo registruose esančią informaciją;

b) pateiktas asmens tapatybės dokumentas priklauso prašymą pateikusiam juridinio asmens atstovui ir jo asmens tapatybės duomenys visiškai atitinka prašyme esančius.

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

3.2.2.2. Juridinio asmens ir juridinio asmens atstovo tapatybės patvirtinamas nuotoliniu būdu, prašymą išduoti sertifikatą patvirtinus galiojančiu kvalifikuotu elektroniniu parašu

Šiuo būdu gali būti patvirtinta tik LR registruotų juridinių asmenų ir jų atstovų tapatybė.

Pagrindiniai Juridinio asmens ir juridinio asmens atstovo tapatybės patikrinimo ir patvirtinimo procedūros etapai:

1) juridinio asmens atstovas užpildo elektroninį prašymą išduoti el. parašą ir pasirašo kvalifikuotu elektroniniu parašu;

2) CA naudodamasi programinėmis priemonėmis tikrina:

a) prašyme pateiktų duomenų autentiškumą, jų atitikimą JAR esančiai informacijai, prašyme nurodyto fizinio asmens teisę atstovauti juridiniam asmeniui;

b) elektroninio parašo galiojimą;

c) elektroninio parašo sertifikate esančių asmens duomenų atitikimą prašyme nurodyto juridinio asmens atstovo duomenims;

d) ar asmeniui elektroninio parašo sertifikatą išdavęs patikimumo užtikrinimo paslaugų tiekėjas yra įtrauktas į Registrų centro sudarytą šių paslaugų tiekėjų, kuriais yra pasitikima, sąrašą;

3) asmens tapatybė laikoma patvirtinta, jeigu tenkinamos šios sąlygos:

a) prašyme pateikti duomenys atitinka JAR ar ES šalių verslo registruose esančią informaciją;

b) prašymas pasirašytas galiojančiu kvalifikuotu elektroniniu parašu;

c) kvalifikuoto elektroninio parašo sertifikate duomenys visiškai atitinka prašyme nurodyto juridinio asmens atstovo duomenis;

d) kvalifikuoto elektroninio parašo sertifikatas yra išduotas patikimumo užtikrinimo paslaugų teikėjo, įtraukto į Registrų centro sudarytą šių paslaugų tiekėjų, kuriais yra pasitikima, sąrašą.

Patvirtinus asmens tapatybę, CA naudodamasi programinėmis priemonėmis sugeneruoja Vienkartinį eID, kuris yra išsiunčiamas jam el. paštu ir SMS žinute.

CA archyve išsaugoma visa tapatybės tikrinimui naudota informacija.

3.2.3. Fizinio asmens tapatybės patvirtinimas

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

QSignC-R-QSCD kvalifikuoti elektroninio parašo sertifikatai užsakomi abonentui pildant ir teikiant CA prašymą. Prašyme turi būti pateikiami:

a) vardas, pavardė;

b) unikalus asmens identifikacinis numeris Lietuvos Respublikos gyventojų registre (toliau – Gyventojų registras) ar Užsieniečių registre;

c) galiojančio asmens tapatybės dokumento numeris;

d) elektroninio pašto adresas;

e) mobiliojo telefono numeris.

Išduodant šiuos sertifikatus yra tikrinama fizinio asmens, kurio vardu sudaromi sertifikatai, tapatybė bei prašyme pateikti duomenys. Fizinio asmens tapatybė patvirtinama vienu iš šių būdų:

a) asmeniui fiziškai atvykus į RA padalinį;

b) nuotoliniu būdu, prašymą išduoti sertifikatą pasirašius galiojančiu kvalifikuotu elektroniniu parašu.

Asmens duomenys tikrinami pagal Gyventojų, Užsieniečių registre esančią informaciją.

Asmenų tapatybės patikrinimas ir patvirtinimas vykdomas vadovaujantis šiuose CPS nustatytomis procedūromis ir asmens tapatybės ir papildomų specifinių požymių tikrinimo išduodant kvalifikuotus elektroninio parašo, elektroninio spaudo, interneto svetainės tapatumo nustatymo sertifikatus tvarka, patvirtinta Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2018 m. spalio 26 d. įsakymu Nr. 1V-1055 .

R-SIC sertifikatai išduodami patvirtinus asmens tapatybę **QSignC-R-QSCD** sertifikatų išdavimo proceso metu.

3.2.3.1. Fizinio asmens tapatybės patvirtinamas jam atvykus į RA padalinį

Tapatybės tikrinimo procedūra atliekama asmeniui fiziškai atvykus į RA padalinį. Fizinio asmens tapatybės tikrinimo procedūra apima:

a) asmens pateiktų asmens tapatybės dokumentų tikrumo ir galiojimo tikrinimą;

b) prašyme pateiktos informacijos palyginimą su duomenimis, pateiktais asmens tapatybės dokumente.

Asmuo, norėdamas patvirtinti savo asmens tapatybę, turi pateikti vieną iš šių dokumentų:

a) galiojantį pasą;

b) galiojančią asmens tapatybės kortelę;

c) leidimą gyventi Lietuvoje (tik Lietuvos Respublikos pilietybės neturintiems asmenims);

d) Lietuvos Respublikos migracijos departamento išduodamą teisės gyventi Lietuvoje pažymėjimą (tik Lietuvos Respublikos pilietybės neturintiems asmenims).

Tikrinant pateiktą asmens tapatybės dokumentą yra būtina:

a) įvertinti, ar pateiktas asmens tapatybės dokumentas yra galiojantis;

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

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

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

Pagrindiniai asmens tapatybės patikrinimo ir patvirtinimo procedūros etapai:

1) asmuo užpildo elektroninį arba atvykęs į RA pateikia „popierinį" prašymą išduoti el. parašo sertifikatą; RA specialistas paslaugos gavėjui patiekia ,,Elektroninio parašo sertifikatų prašymo, išdavimo ir naudojimo sąlygas ir taisykles", su kuriomis susipažinęs asmuo prašyme fiksuoja susipažinimo ir sutikimo jų laikytis datą ir laiką, jeigu nėra duomenų, kad asmuo su jomis susipažino pildydamas elektroninį prašymą;

2) CA naudodamasi programinėmis priemonėmis patikrina prašyme pateiktų duomenų autentiškumą, jų atitikimą Gyventojų, Užsieniečių registre esančiai informacijai;

3) RA specialistas:

a) pagal pateiktą asmens tapatybės dokumentą nustato prašymą pateikusio asmens tapatybę;

b) palygina asmens tapatybės dokumente esančių asmens duomenų atitikimą prašyme pateiktai informacijai;

c) CA informacinėje sistemoje patvirtina prašymą pateikusio asmens tapatumą bei atspausdina ir abonentui teikia pasirašyti prašymą;

4) asmens tapatybė laikoma patvirtinta, jeigu tenkinamos šios sąlygos:

a) prašyme pateikti duomenys atitinka Gyventojų, Užsieniečių registre esančią informaciją;

b) pateiktas asmens tapatybės dokumentas priklauso prašymą pateikusiam asmeniui ir jo asmens tapatybės duomenys visiškai atitinka prašyme esančius.

RA dokumentų archyve išsaugoma asmens pasirašytas prašymas. CA išduodamų e. parašo ir e. spaudo tvarkymo taikomųjų sistemų elektroniniuose žurnaluose registruojami ir išsaugomi visi įvykiai, susiję su prašymo ruošimu, teikimu ir priėmimu bei asmens tapatybės nustatymu ir patvirtinimu.

Neįgaliajam asmeniui pateikus motyvuotą prašymą RA, RA specialistas gali atvykti į šio asmens gyvenamą vietą ir priimti jo prašymą išduoti el. parašo sertifikatą bei patvirtinti asmens tapatybę.

3.2.3.2. Fizinio asmens tapatybės patvirtinamas nuotoliniu būdu, prašymą išduoti sertifikatą pasirašant galiojančiu kvalifikuotu elektroniniu parašu

Pagrindiniai asmens tapatybės patikrinimo ir patvirtinimo procedūros etapai:

1) asmuo susipažįsta su ,,Elektroninio parašo sertifikatų užsakymo, išdavimo ir naudojimo sąlygomis ir taisyklėmis" bei patvirtina sutikimą jų laikytis, užpildo elektroninį prašymą išduoti el. parašo sertifikatą bei pasirašo kvalifikuotu elektroniniu parašu;

2) CA naudodamasi programinėmis priemonėmis tikrina:

a) prašyme pateiktų duomenų autentiškumą, jų atitikimą Gyventojų, Užsieniečių registre esančiai informacijai;

b) elektroninio parašo galiojimą;

c) elektroninio parašo sertifikate esančių asmens duomenų atitikimą prašyme pateiktai informacijai;

d) ar asmeniui elektroninio parašo sertifikatą išdavęs patikimumo užtikrinimo paslaugų tiekėjas yra įtrauktas į Registrų centro sudarytą šių paslaugų tiekėjų, kuriais yra pasitikima, sąrašą.

3) asmens tapatybė laikoma patvirtinta, jeigu tenkinamos šios sąlygos:

a) prašyme pateikti duomenys atitinka Gyventojų, Užsieniečių registre esančią informaciją;

b) prašymas pasirašytas galiojančiu kvalifikuotu elektroniniu parašu;

c) kvalifikuoto elektroninio parašo sertifikate duomenys visiškai atitinka prašyme nurodytus duomenis;

d) kvalifikuoto elektroninio parašo sertifikatas yra išduotas patikimumo užtikrinimo paslaugų teikėjo, įtraukto į Registrų centro sudarytą šių paslaugų tiekėjų, kuriais yra pasitikima, sąrašą.

Patvirtinus asmens tapatybę, CA naudodamasi programinėmis priemonėmis sugeneruoja Vienkartinį eID, kuris, yra išsiunčiamas jam el. paštu ir SMS žinute.

Asmens prašymas, užpildytas ir pasirašytas kvalifikuotu e. parašu, išsaugomas CA elektroninių dokumentų archyve. Registrų centro išduodamų e. parašo ir e. spaudo tvarkymo taikomųjų sistemų elektroniniuose žurnaluose registruojami ir išsaugomi visi įvykiai, susiję su prašymo ruošimu, teikimu ir priėmimu bei asmens tapatybės nustatymu ir patvirtinimu.

Neįgalūs asmenys susipažinti su ,,Elektroninio parašo sertifikatų užsakymo, išdavimo ir naudojimo sąlygomis ir taisyklėmis", patvirtinti sutikimą jų laikytis, užpildyti elektroninį prašymą išduoti el. parašo sertifikatą bei patvirtinti savo asmens tapatybę gali nuotoliniu būdu tam naudodami neįgaliesiems pritaikytas kompiuterines darbo vietas ir/ar mobilaus ryšio įrenginius.

3.2.4. Netikrinami Abonento duomenys

Tikrinami visi Abonento pateikti duomenys.

3.3. Identifikavimas ir autentikavimas užsakant naują raktų porą (Re-key Requests)

Taikomi 3.2 nustatyti reikalavimai.

3.4. Identifikavimas ir autentikavimas stabdant ar atšaukiant sertifikatų galiojimą

CA užtikrina prašymų sustabdyti ar atšaukti išduotų sertifikatų galiojimą priėmimą ir vykdymą 7 dienas per savaitę, 24 val. per parą.

Sertifikatų savininkas gali pateikti prašymą laikinai sustabdyti CA išduotų sertifikatų galiojimą šiais būdais:

a) internetu, per sertifikatų tvarkymo savitarnos sistemą (toliau – eSUS): asmens tapatybė ir teisė teikti prašymą nustatoma eSUS asmens autentikavimo ir autorizacijos priemonėmis (šį būdą numatoma įgyvendinti ateityje);

b) skambinant palaikymo tarnybai telefonu +370 5 2511999: asmens tapatybė ir teisę teikti prašymą nustatoma skambinančiajam pateikus savo vardą, pavardę, gimimo datą, asmens kodą ir atsakius į kontrolinį klausimą;

c) atvykus į RA: asmens tapatybė ir teisę teikti prašymą nustatoma pagal pateiktą asmens dokumentą.

Prašymą atšaukti CA išduotų sertifikatų galiojimo sustabdymą ir nutraukti CA išduotų sertifikatų galiojimą sertifikatų savininkas gali šiais būdais:

a) internetu, per sertifikatų tvarkymo savitarnos sistemą (toliau - eSUS): asmens tapatybė ir teisė teikti prašymą nustatoma eSUS asmens autentikavimo ir autorizacijos priemonėmis (šį būdą numatoma įgyvendinti ateityje);

b) atvykus į RA: asmens tapatybė ir teisę teikti prašymą nustatoma pagal pateiktą asmens dokumentą.

Teikiant prašymą atšaukti **QSealC-R-QSCD** sertifikato galiojimo sustabdymą ar nutraukti šio sertifikato galiojimą papildomai yra tikrinama asmens teisė atstovauti juridiniam asmeniui, kuriam šis sertifikatas buvo išduotas. Asmens teisė atstovauti LR įregistruotam juridiniam asmeniui tikrinama pagal JAR esančią informaciją. Asmens teisė atstovauti kitoje ES šalyje narėje įregistruotam juridiniam asmeniui tikrinama pagal asmens pateiktą dokumentą, kuriuo patvirtinami tokie įgaliojimai.

4. Reikalavimai sertifikatų gyvavimo ciklui

4.1. Prašymų išduoti sertifikatus teikimas

Prieš pateikdamas prašymą išduoti sertifikatą abonentas turi būti informuotas apie sertifikatų sudarymo ir tvarkymo sąlygas, apribojimus, CA, abonento ir sertifikatų savininko pareigas ir

atsakomybę, renkamus asmens duomenis, asmens duomenų atskleidimą viešinant elektroniniu parašu pasirašytus dokumentus. CA turi užtikrinti, kad ši informacija būtų viešai prieinama internete lietuvių ir anglų kalbomis.

CA privalo:

1) aiškiai nurodyti, kokios CP yra taikomos;
2) informuoti apie sertifikatų naudojimo ribojimus;
3) informuoti apie sertifikatų naudotojų įsipareigojimus;
4) teikti informaciją, kaip tikrinti sertifikatų galiojimą;
5) informuoti apie CA prisiimamą atsakomybę ir jos ribojimus;
6) informuoti apie registravimo metu surinktos informacijos laikymo periodą;
7) informuoti apie laikotarpio, kurį laikomi CA veiklos duomenys, trukmę;
8) informuoti apie ginčų sprendimo procedūras;
9) teikti informaciją apie su veikla susijusius įstatymus.

Sertifikatų sudarymo ir tvarkymo sąlygos, apribojimai, CA, sertifikatų savininko pareigos ir atsakomybė abonentui yra pateikiama ,,Elektroninio spaudo sertifikatų užsakymo, išdavimo ir naudojimo bei elektroninio parašo sertifikatų užsakymo, išdavimo ir naudojimo sąlygose ir taisyklėse". Šioms taisyklėms yra suteikiamas unikalus objekto identifikatorius (OID). CA patvirtinus naujas šių taisyklių versijas joms yra suteikiamas naujas OID. Visos šių taisyklių versijos yra skelbiamos viešai internete adresu https://ltid.lt/. Kiekviena taisyklių versija yra saugoma Registrų centro dokumentų archyve ne mažiau kaip 10 metų nuo jos galiojimo pabaigos. Abonentas prieš teikdamas prašymą išduoti sertifikatą privalo susipažinti su šiomis taisyklėmis bei patvirtinti įsipareigojimą laikytis jose nustatytų paslaugų teikimo sąlygų visą CA išduotų sertifikatų galiojimo laikotarpį. Susipažinti su elektroninės atpažinties, elektroninio spaudo bei elektroninio parašo sertifikatų užsakymo, išdavimo ir naudojimo sąlygomis ir taisyklėmis bei patvirtinti įsipareigojimą jų laikytis asmuo gali:

a) elektroniniu būdu pildydamas elektroninį prašymą;

b) perskaitęs RA specialisto pateiktą aktualią taisyklių versiją ir patvirtinęs sutikimą jų laikytis, teikdamas „popierinį" prašymą.

Susipažinimo su šiomis taisyklėmis ir patvirtinimo jų laikytis duomenys (data ir laikas bei taisyklių OID) į prašymą įtraukiami automatiškai, jeigu prašymas pildomas elektroniniu būdu arba įrašomas RA specialisto, jeigu prašymas teikiamas ir paslaugos gavėjo asmens tapatybė patvirtinama jam atvykus į RA.

Prašymą išduoti sertifikatus gali pateikti ne jaunesnis kaip 18 m. amžiaus fizinis asmuo. Prašymą išduoti **QSignC-R-QSCD** sertifikatus jaunesnis kaip 18 m., bet vyresnis kaip 14 m., asmuo gali pateikti tik kartu su rašytiniu tėvų ar globėjų sutikimu.

Prašymą išduoti **QSealC-R-QSCD** tipo sertifikatus gali pateikti tik juridinio asmens atstovas.

Prašymas išduoti sertifikatus gali būti pateiktas:

a) atvykus į RA;

b) elektroniniu būdu per eSUS;

c) elektroniniu būdu per CA išduotą nuotolinio parašo / spaudo kriptografinių raktų aktyvavimo priemonę.

Prašymai išduoti **QSignC-R-QSCD**, **QSealC-R-QSCD** sertifikatus pildomi 3.2.2. ir 3.2.3 nurodyta tvarka. Elektroniniu būdu teikiant prašymą išduoti sertifikatą, turi būti patikrintas prašyme nurodyto mobilaus telefono numerio ir / ar elektroninio pašto adreso priklausymas abonentui bei jo gebėjimas valdyti šiuos įrenginius.

Prašymą išduoti **R-SIC** sertifikatą generuoja nuotolinio parašo / spaudo kriptografinių raktų aktyvavimo priemonė, abonentui pradėjus procedūrą jos registravimo CA valdomame R-QSCD įrenginyje.

4.2. Prašymų išduoti sertifikatus apdorojimas

4.2.1. Identifikavimo ir autentikavimo funkcijų vykdymas

Pildydamas prašymą abonentas pasirenka asmens tapatybės patvirtinimo būdą. Asmens tapatybės patvirtinimas atliekamas laikantis 3.2.2. ir 3.2.3 skyriuose nurodytų procedūrų.

Pasirinkus tapatybės patvirtinimą nuotoliniu būdu, prašymą išduoti sertifikatą pasirašant kvalifikuotu elektroniniu parašu, abonento identifikavimas bei tapatybės ir prašyme pateiktų duomenų autentiškumo patvirtinimas atliekamas automatiškai, CA naudodamasi programinėmis priemonėmis lygina prašymo ir kvalifikuoto el. parašo sertifikate esančius duomenis.

Pasirinkus tapatybės patvirtinimą nuotoliniu būdu, pasinaudojant tapatybės patvirtinimo paslaugų tiekėjo paslaugomis, abonento identifikavimas bei tapatybės ir prašyme pateiktų duomenų autentiškumo patvirtinimas atliekamas automatiškai, CA naudodamasi programinėmis priemonėmis lygina prašyme esančius ir tapatybės patvirtinimo paslaugų tiekėjo pasirašytus abonento asmens duomenis.

4.2.2. Prašymų išduoti sertifikatus priėmimas ir atmetimas

Pateiktas prašymas yra priimamas ir perduodamas vykdyti jeigu:

a) prašyme pateikti visi privalomi asmens, kurio vardu parašoma išduoti sertifikatą, duomenys;

b) asmuo valdo prašyme nurodytą el. pašto dėžutę bei mobilų telefoną;

c) prašymą teikiančio asmens tapatybė patvirtinta vienu iš 3.2 skyriuje nustatytų būdų.

Prašymas išduoti sertifikatą yra atmetamas jeigu:

a) prašymą išduoti QSealC-R-QSCD sertifikatus pateikė jaunesnis negu 18 m. amžiaus fizinis asmuo;

b) prašymą išduoti QSignC-R-QSCD sertifikatą pateikė jaunesnis negu 14 m. amžiaus fizinis asmuo;

c) prie prašymo išduoti QSignC-R-QSCD sertifikatą pateikto jaunesnio negu 18 m. amžiaus fizinio asmens nėra pridėtas galiojantis tėvų ar globėjų rašytinis sutikimas;

d) prašyme yra pateikti ne visi privalomi duomenys;

e) asmuo nepatvirtino susipažinimo ir sutikimo su sertifikatų užsakymo, išdavimo ir naudojimo sąlygomis, CA, abonento ir sertifikatų savininko pareigomis bei atsakomybe, renkamais asmens duomenis;

f) prašymą išduoti QSealC-R-QSCD sertifikatą teikiantis asmuo neturi galiojančių įmonės įgaliojimų jos vardu užsakyti ir gauti šiuos sertifikatus;

g) prašyme pateikti duomenys neatitinka Lietuvos Respublikos valstybės registruose esančių asmens duomenų;

h) prašyme nurodyto asmens tapatybė nėra patvirtinta vienu iš šiame CP nustatytu būdų;

i) prašyme nurodyti asmens duomenys nesutampa su asmens duomenimis, gautais asmens tapatybės patvirtinimo metu;

j) prašyme nėra duomenų (data ir laikas bei taisyklių OID) apie abonento sutikimą laikytis elektroninio spaudo ar elektroninio parašo sertifikatų užsakymo, išdavimo ir naudojimo sąlygų ir taisyklių.

Visais atvejais asmuo yra informuojamas apie jo teikto parašymo atmetimo priežastis.

4.2.3. Prašymų išduoti sertifikatus apdorojimo terminai

Sertifikatai sudaromi iš karto po abonento prašymo priėmimo ir jo tapatybės patvirtinimo.

4.3. Sertifikatų sudarymas

CA sudaryti sertifikatai išsaugomi R-QSCD įrenginyje, kurį valdo kvalifikuotos elektroninės atpažinties ir kvalifikuotų patikimumo užtikrinimo paslaugų teikėjas pasirašančio asmens, kuriam sertifikatas yra išduotas, vardu ir kuris yra susietas su asmeniui išduotomis jų aktyvavimo nuotoliniu būdu priemonėmis bei joms išduotu R-SIC sertifikatu.

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

a) sertifikatai atitinka eIDAS reikalavimus sertifikatams;

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

c) raktų poros generavimo procedūra yra:

- saugiai susieta su sertifikatų sudarymo procedūra;
- privatusis raktas generuojamas naudojant R-QSCD;

d) **QSignC-R-QSCD**, **QSealC-R-QSCD** sertifikatai R-QSCD įrenginyje yra saugiai ir vienareikšmiškai susieti su jo aktyvavimui (jo privataus rakto aktyvavimui) skirtu R-SIC sertifikatu;

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

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

CA užtikrina, jog sudaromuose sertifikatuose bus šie duomenys:

g) nuoroda, kad sertifikatai išduoti kaip kvalifikuoti elektroninio parašo arba kvalifikuoti elektroninio spaudo sertifikatai;

h) duomenų rinkinys, kuriuo vienareikšmiškai nurodomas sertifikatus išduodantis kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, nurodant bent valstybę narę, kurioje jis yra įsisteigęs; juridinio asmens atveju – pavadinimas ir juridinio asmens kodas;

i) pasirašančio asmens vardas, pavardė, asmens kodas, o išduodant kvalifikuotą elektroninio spaudo sertifikatą – spaudo savininko pavadinimas, juridinio asmens kodas;

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

k) duomenys apie sertifikatų galiojimo laikotarpio pradžią ir pabaigą;

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

m) sertifikatus išduodančio CA sertifikatas;

n) išdavusi sertifikatus šalis.

4.4. Sudarytų sertifikatų išdavimas

Naujai sudaryti **QSignC-R-QSCD** ir **QSealC-R-QSCD** sertifikatai nėra fiziškai perduodami sertifikatų savininkui, jam yra tik suteikiama prieiga prie jų CA valdomame R-QSCD įrenginyje.

4.5. Kriptografinių raktų porų ir sertifikatų naudojimas

Išreikšdamas sutikimą su sertifikatų užsakymo, išdavimo ir naudojimo sąlygomis sertifikatų savininkas įsipareigoja:

a) užsakant sertifikatus CA teikti aktualius ir teisingus duomenis, reikalingus sertifikato išdavimui;

b) pasikeitus įrašytiems į sertifikatą duomenims nedelsiant apie tai informuoti CA;

c) išduotą sertifikatą ir atitinkamas kriptografinių raktų poras naudoti pagal paskirtį ir apribojimus, apibrėžtus sertifikato naudojimo sąlygose;

d) apsaugoti CA išduotus elektroninio parašo / spaudo kūrimo įrenginius nuo trečių šalių neteisėto naudojimosi jais;

e) apsaugoti CA išduotas nuotolinio elektroninio parašo / spaudo kriptografinių raktų aktyvavimo priemones nuo trečių šalių neteisėto naudojimosi jomis;

f) neatskleisti CA išduotų kriptografinių raktų aktyvavimo kodų trečiosioms šalims;

g) nustoti naudotis išduotais sertifikatais bei raktų pora ir nedelsiant parnešti CA jeigu:

- buvo parasta CA išduoto elektroninio parašo / spaudo kūrimo įrenginio kontrolė ar trečiosioms šalims tapo žinomi kriptografinių raktų aktyvavimo kodai;
- buvo parasta CA išduotos nuotolinio elektroninio parašo / spaudo kriptografinių raktų aktyvavimo priemones kontrolė ar tračiosioms šalims tapo žinomi prieigos prie jos kodai.

4.6. Sertifikatų atnaujinimas

Yra leidžiamas tik išduotų **QSignC-R-QSCD** ir **QSealC-R-QSCD** tipo sertifikatų atnaujinimas.

Sertifikatai gali būti atnaujinami jeigu:

a) sertifikato galiojimas yra nepasibaigęs, nėra sustabdytas ar atšauktas;

b) sertifikato savininkas prašymą atnaujinti sertifikatą pasirašo kvalifikuotu elektroniniu parašu ar spaudu, patvirtintu šiuo sertifikatu;

c) sertifikato savininko asmens duomenys įrašyti į prašomą atnaujinti sertifikatą yra nepasikeitę;

d) CA nuotolinio parašo / spaudo kūrimo infrastruktūra, kurioje saugomi sertifikato savininko kriptografiniai raktai, užtikrina saugių kriptografinių algoritmų naudojimą;

e) CA Sertifikatų savininkui išduota nuotolinio parašo / spaudo kriptografinių raktų aktyvavimo priemonė yra saugi ir CA sprendimu gali būti naudojama nauju sertifikato galiojimo laikotarpiu.

4.7. Naujos raktų poros išduotam sertifikatui kūrimas (Certificate Re-key)

Procesas yra negalimas.

4.8. Išduoto sertifikato duomenų keitimas

Procesas yra negalimas.

4.9. Sertifikatų galiojimo sustabdymas ir atšaukimas

Sertifikatų sustabdymo ir atšaukimo prašymų teikimo procedūra aprašyta 3.4 skyriuje. Informacija apie sertifikato galiojimo sustabdymą ar nutraukimą pasitikinčioms šalims turi būti prieinama ne vėliau kaip per 60 min. nuo CA ar RA sprendimo sustabdyti ar nutraukti sertifikato

galiojimą priėmimo momento. Jeigu išduoto kvalifikuoto elektroninio parašo sertifikato ar kvalifikuoto elektroninio spaudo sertifikato galiojimas yra atšaukiamas, jis netenka galios nuo jo atšaukimo momento, o jo statuso jokiomis aplinkybėmis negalima atkurti.

4.9.1. Sertifikatų galiojimo sustabdymas

Sertifikatų galiojimas sustabdomas tokiais atvejais:

1) sertifikato savininko prašymu;

2) teisėsaugos institucijų motyvuotu reikalavimu, siekiant užkirsti kelią nusikalstamoms veikoms; teisėsaugos institucijų nurodytam terminui;

3) CA iniciatyva:

a) gavus informacijos, kad kvalifikuoto elektroninio parašo sertifikato ir kvalifikuoto elektroninio spaudo sertifikato duomenys gali būti neteisingi;

b) gavus informacijos, kad asmuo, kuriam išduotas kvalifikuoto elektroninio parašo sertifikatas ar kvalifikuoto elektroninio spaudo sertifikatas, gali būti praradęs šių sertifikatų kriptografinių raktų aktyvavimo priemonės kontrolę.

Sustabdžius išduotų sertifikatų galiojimą dėl šiame skyriuje įvardintų 3) a) ir 3) b) priežasčių ne vėliau kaip per 24 valandas nuo jų galiojimo sustabdymo momento CA apie tai praneša sertifikatų savininkui elektroniniu paštu arba telefonu, nurodydamas sustabdymo priežastį ir trukmę. Taip pat sertifikatų savininkas yra informuojamas apie teisę per 30 darbo dienų nuo kvalifikuoto elektroninio parašo sertifikato ir kvalifikuoto elektroninio spaudo sertifikato galiojimo sustabdymo dienos elektroniniu paštu laisva forma pateikti prašymą, paaiškinimą ir patvirtinančius įrodymus, kuriais paneigiama kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo gauta informacija, kurios pagrindu buvo sustabdytas kvalifikuoto elektroninio parašo sertifikato ir kvalifikuoto elektroninio spaudo sertifikato galiojimas.

Sertifikatų galiojimo sustabdymas atšaukiamas:

1) gavus sertifikato savininko prašymą atstatyti jo ankstesniu prašymu sustabdyto sertifikato galiojimą;

2) gavus teisėsaugos institucijos, kurios prašymu sertifikatų galiojimas buvo sustabdytas, prašymą arba kai pasibaigia numatytas sustabdymo laikotarpis;

3) gavus sertifikatų savininko prašymą ir paaiškinimą, paneigiantį CA gautą informaciją, jei sertifikatų galiojimas buvo sustabdytas dėl šio skyriaus 3) a) ir 3) b) priežasčių.

4.9.2. Sertifikatų galiojimo atšaukimas

Sertifikatų galiojimas nutraukiamas tokias atvejais:

1) sertifikato savininko prašymu;

2) CA iniciatyva:

a) paaiškėjus, kad sertifikatų duomenys nėra teisingi;

b) paaiškėjus, kad sertifikatai buvo sudaryti remiantis klaidingais duomenimis;

c) kai CA nutraukia savo veiklą ir joks kitas patikimumo užtikrinimo paslaugų teikėjas neperima patikimumo užtikrinimo paslaugų teikimo veiklos;

d) paaiškėjus, kad sertifikatų savininkas nesilaiko sertifikato naudojimosi sąlygų;

e) sertifikatų savininkui praradus sertifikatus atitinkančių parašo / spaudo formavimo duomenų kontrolę;

f) kai remiamasi sertifikatų galiojimo apribojimais, nurodytais sertifikate jį sudarant;

g) kai abonentas ar sertifikato savininkas nusprendžia nutraukti sutartį su sertifikatus jam sudariusiu CA;

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

i)gavus pranešimą, kad sertifikatų savininkas tapo neveiksnus srityje, susijusioje su sertifikatų panaudojimu;

j) gavus pranešimą, kad sertifikatų savininkas mirė, kvalifikuoto elektroninio spaudo atveju – juridinis asmuo buvo likviduotas;

k) teisės aktų nustatyta tvarka nustačius, kad sertifikatų savininkui išduoti sertifikatai ir (ar) R-QSCD nebeatitinka eIDAS reikalavimų;

3) teisėsaugos institucijų motyvuotu reikalavimu, siekiant užkirsti kelią nusikalstamoms veikoms.

Nustačius, kad paslaugos gavėjui išduoti sertifikatai nebeatitinka eIDAS reikalavimų apie būsimą sertifikatų atšaukimą sertifikatų savininkas yra informuojamas raštu elektroniniu paštu ne vėliau kaip prieš 10 darbo dienų.

Atšaukus išduotų sertifikatų galiojimą CA iniciatyva, išskyrus šio skyriaus 2) i), 2) j) ir 3) atvejus, ne vėliau kaip per 24 valandas nuo jų galiojimo atšaukimo momento CA apie tai praneša sertifikatų savininkui.

Sertifikato galiojimo statusas turi būti pakeistas ne vėliau kaip per 24 valandas nuo sertifikato savininko prašymo ar teisėsaugos institucijų reikalavimo nedelsiant sustabdyti ar nutraukti sertifikato galiojimą nuo pateikimo momento.

Data nuo kada sertifikato galiojimas turi būti nutraukiamas gali būti nustatytas:

a) sertifikato savininko, savo iniciatyva teikiančio prašymą jį nutraukti;

b) CA iniciatyva priėmus sprendimą nutraukti sertifikato galiojimą nutraukimą.

4.10. Sertifikatų galiojimo statuso patikrinimo paslaugos

CA teikia paslaugas, leidžiančias patikrinti išduotų sertifikatų galiojimo atšaukimą arba sustabdymą.

CA sudaro ir viešai internete skelbia CRL, kuris atnaujinamas ne rečiau kaip kas 24 (dvidešimt keturias) valandas. CRL yra pasirašomas CA kvalifikuotu elektroniniu parašu, kiekviename CRL yra nurodomas kito CRL išleidimo laikas. Taip pat CA teikia sertifikatų galiojimo atšaukimo arba sustabdymo patikrinimo realiame laike OCSP atsakikliu paslaugas.

Šios paslaugos yra prieinamos viešai, 24 (dvidešimt keturias) valandas per parą, 7 (septynias) dienas per savaitę.

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

CA turi užtikrinti skelbiamos informacijos apie išduotų sertifikatų galiojimo sustabdymą ar atšaukimą integralumą ir autentiškumą.

4.11. Sertifikatų naudojimo terminai

Sertifikatų savininkas nutraukia CA išduotų sertifikatų naudojimą pateikdamas prašymą atšaukti jų galiojimą. Taip sertifikatų naudojimas yra nutraukiamas, kai natūraliai pasibaigia jų galiojimo terminas ar jie yra CA atšaukiami.

4.12. Kriptografinių raktų saugojimas ir atkūrimas

CA valdomame nuotolinio kvalifikuoto elektroninio parašo ir spaudo kūrimo įrenginyje, sertifikuotame pagal eIDAS 30 str. nuostatas, saugo nuotolinio parašo ar spaudo sertifikatų savininkams išduotus privačius raktus. Visais kitais atvejais privatūs raktai CA nėra saugomi ir nėra daromos jų kopijos.

5. Įrangos, valdymo ir veiklos procesų kontrolė

5.1. Fizinės apsaugos kontrolė

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

Siekiant užtikrinti nuotolinio el. parašo bei el. spaudo paslaugų teikimą, 24 (dvidešimt keturias) valandas per parą, 7 (septynias) dienas per savaitę, R-QSCD ir kita šių paslaugų teikimui skirta IT infrastruktūra yra dubliuota ir veikia dvejose nutolusiose serverinėse *Active-Active* režimu.

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

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

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

5.1.1. Fizinė prieiga

Bendri vidaus tvarkos reikalavimai dėl patekimo į Registrų centro patalpas detalizuoti Registrų centro darbo tvarkos taisyklių VII skyriuje.

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

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

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

Yra skiriamos 3 (trys) CA patalpų saugumo zonos:

a) kompiuterinės sistemos zona;
b) operatorių ir administratorių zona;
c) projektuotojų ir programuotojų zona.

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

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

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

5.1.2. Elektros energijos tiekimas ir oro kondicionavimas

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

5.1.3. Apsauga nuo užpylimo vandeniu

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

5.1.4. Priešgaisrinė apsauga

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

5.1.5. 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.

5.1.6. Atliekų tvarkymas

Popieriniai dokumentai , kuriose yra CA veiklos saugumui įtakos turinti informacija, pasibaigus tos informacijos saugojimo terminui sunaikinami specialiais plėšymo įrenginiais, atitinkančiais ne mažesnę nei P4 saugumo klasę. Elektroninės laikmenos yra naikinamos DIN3 klasės įrenginiais (taip naikinamos tik laikmenos, kuriose neįmanoma visiškai sunaikinti saugomos informacijos, pvz., kriptografinės kortelės).

5.2. Procedūrų kontrolė

5.2.1. Darbuotojų rolės

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

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

b) **CA administratoriai** – atsakingi už CA sistemų administravimą, instaliuoja ir konfigūruoja naudojamą įrangą, nustato sistemos ir tinklo parametrus, daro sistemų ir duomenų atsargines kopijas, reikalui esant atstato sistemų veikimą;

c) **CA operatorius** – atsakingas už kasdienines sertifikatų sudarymo ir tvarkymo procedūras bei kasdieninę CA valdomų sertifikatų sudarymo ir tvarkymo bei nuotolinio parašo / spaudo sistemų veikimo priežiūrą;

d) **CA sistemų auditorius** – atsakingas už CA sistemų operacijų, įvykių ir klaidų registracijos žurnalų tvarkymą, peržiūrą bei už vidinių patikrinimų atlikimą;

e) **RA pareigūnas** – atsakingas už asmenų identifikavimą ir tapatybės patvirtinimą jiems fiziškai dalyvaujant.

5.2.2. Reikalingas darbuotojų kiekis užduočiai atlikti

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

5.2.3. Pareigų identifikacija ir autentiškumo tikrinimas

CA darbuotojų pareigų identifikacija ir autentiškumo tikrinimas atliekami tokiais atvejais:

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

b) sudarant asmenų sąrašą, kuriems leidžiama fizinė prieiga prie CA sistemų 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) juo 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.

5.2.4. Darbuotojų pareigų atskyrimas

Pareigų paskirstymas ir atskyrimas užkerta kelią CA sistemų naudojimo neteisėtiems tikslams pasiekti. Kiekvienam sistemos naudotojui yra leistini tik jo pareigose numatyti veiksmai (3 pav.).

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

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

CA turi užtikrinti patikimumo užtikrinimo paslaugų teikimo sistemos saugų ir tinkamą veikimą ir minimalią sutrikimų riziką.

CA turi užtikrinti, kad:

a) CA įrangos ir valdomos informacijos integralumas būtų apsaugotas nuo kompiuterinių virusų ir kito programinio pažeidžiamumo;

b) būtų tiksliai apibrėžtos pranešimų apie pažeidimus ir reagavimo į iškilusias grėsmes procedūros bei jos įgyvendinamos tokiu būdu, kad jų žala būtų minimizuojama;

c) CA sistemose naudojami informacijos kaupikliai ir nešėjai būtų apsaugoti nuo gedimų, vagystės, nesankcionuotos prieigos ar susidėvėjimo. Informacija būtų apsaugota atsižvelgiant į nustatytą saugumo lygį (3.4.2 skyrius);

d) būtų nustatytos procedūros visoms su sertifikatų kūrimu ir valdymu susijusioms pareigybėms;

e) būtų atliekamas nuolatinis sistemos būklės monitoringas, kad būtų galima laiku prognozuoti, kada atlikti sistemos plėtrą ar padidinti pajėgumus;

f) CA saugumo procedūros būtų atskirtos nuo kitų procedūrų. Saugumo procedūros apima: veiklos procedūrų ir atsakomybių nustatymą, saugų sistemų plėtros planavimą, apsaugą nuo žalingų programų, patalpų priežiūrą, tinklo valdymą, aktyvią audito žurnalų stebėseną, įvykių analizę, informacijos nešiklių valdymą ir apsaugą, duomenų ir programinės įrangos apsikeitimą. Šios operacijos turi būti valdomos ypatingo pasitikėjimo pareigas užimančio personalo, tačiau jas atlikti gali ir žemesnės kvalifikacijos specialistai, jei tai aprašyta saugumo politikos ar kituose dokumentuose.

5.3. Personalo kontrolė

5.3.1. Personalo patikimumo kontrolė

Asmenys į darbą priimami vadovaujantis Lietuvos Respublikos darbo kodekso reikalavimais bei Registrų centro darbo tvarkos taisyklėse (toliau – Darbo tvarkos taisyklės) nustatyta tvarka. Priėmimas į darbą įforminamas darbo sutartimi. CA pavestas pareigas atliekančių asmenų kvalifikacijai keliami šie bendri reikalavimai:

a) mokėti lietuvių kalbą;
b) turėti reikalingą išsilavinimą arba kvalifikaciją;
c) mokėti dirbti kompiuteriu ir kita organizacine technika;
d) mokėti užsienio kalbą (jeigu reikalinga).

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

a) sudarantys ir tvarkantys sertifikatus, turi aukštąjį išsilavinimą;

b) yra pasirašę susitarimą dėl pareigų vykdymo ir atsakomybės;

c) yra pasirašę pasižadėjimą saugoti Registrų centro tvarkomų asmens ir kitų duomenų paslaptį, laikytis duomenų saugos reikalavimų;

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

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

5.3.2. Darbuotojų tikrinimo procedūra

Priimami darbuotojai tikrinami vadovaujantis Darbo tvarkos taisyklių 11 punkte nustatyta bendra tvarka.

Be minėtos patikrinimo procedūros, pagal kurias yra užvedama bei saugoma darbuotojo asmens byla, darbuotojas privalo patvirtinti, jog nėra teistas, pateikdamas teistumo (neteistumo) pažymą[2]. Šis dokumentas taip pat saugomas darbuotojo asmens byloje.

5.3.3. Reikalavimai mokymams

CA darbuotojai turi būti išklausę mokymus ir susipažinę su:

a) CP ir CPS;

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

c) CA ir RA sistemų programine įranga;

d) asmens duomenų apsaugos reikalavimais;

e) atsakomybe už sistemos atliekamų veiksmų sutrikimus;

f) galimais sistemos veikimo sutrikimais.

5.3.4. Mokymų dažnumas ir reikalavimai jiems

Mokymai vykdomi kartą per metus arba gali būti vedami papildomi mokymai, kai tik padaromi žymesni CA ar RA veiklos pakeitimai. Mokymai gali būti vykdomi nuotoliniu būdu.

5.3.5. Reikalavimai tretiesiems asmenims

Tretieji asmenys, atliekantys užduotis pagal sutartis (išorinių paslaugų teikėjai, programinės įrangos kūrėjai, kt.), turi atitikti tokius pačius kvalifikacinius reikalavimus, kurie taikomi CA darbuotojams (5.3 papunktis, išskyrus a) dalį), tikrinami laikantis tokių pačių procedūrų, kurios

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

taikomos CA darbuotojams. Be to, trečiuosius asmenis, atliekančius užduotis CA patalpose, turi lydėti CA darbuotojas. CA deleguoja ir apibrėžia atitinkamus reikalavimus tretiesiems asmenims pagal užduotis numatytas sutartyje. Tretieji asmenys yra atsakingi už nustatytų reikalavimų laikymąsi.

5.4. Žurnalinių įrašų registravimas

5.4.1. Registruojamieji įvykiai

Svarbiausios operacijos fiksuojamos operacijų ir veiklos registravimo žurnaluose:

a) sertifikatų generavimo ir tvarkymo įvykiai;

b) abonentų registracijos įvykiai;

c) nuotolinio parašo / spaudo kūrimo transakcijų aptarnavimo įvykiai;

d) saugumo, sistemos veikimo sutrikimo įvykiai.

Fiksuojami sertifikatų generavimo ir tvarkymo įvykiai apima:

a) užklausas sertifikatams gauti;

b) sertifikatų generavimo faktus;

c) sertifikatų statuso keitimo operacijas;

d) sertifikatų statuso tikrinimo užklausas ir atsakymus;

e) sertifikatų tarnybos sustabdymą ir paleidimą;

f) CRL generavimo ir publikavimo įrašus.

Fiksuojami Abonentų registracijos įvykiai apima:

a) asmens tapatybę patvirtinančių duomenų surinkimą, tikrinimą ir susiejimą su abonentu;

b) abonento registraciją;

c) abonento registracijos duomenų keitimą;

d) abonentui išduotos nuotolinio parašo / spaudo kriptografinių raktų aktyvavimo priemonės registraciją.

Fiksuojami nuotolinio parašo / spaudo kūrimo transakcijų aptarnavimo įvykiai apima:

a) kreipinių sukurti el. parašą / spaudą aptarnavimą;

b) nuotolinio parašo / spaudo kriptografinių raktų aktyvavimo įvykius.

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 asmenį už įvykį.

5.4.2. Įrašų apie įvykius peržiūros dažnumas

CA sistemų operacijų ir veiklos registravimo žurnalai peržiūrimi periodiškai, siekiant nustatyti galimus sistemų veikimo sutrikimus, sistemų netinkamą funkcionavimą, išskirtų IT techninės infrastruktūros resursų išnaudojimą, sistemų saugos bei duomenų saugos įvykius ir incidentus.

5.4.3. Įrašų saugojimo periodas

CA sistemos operacijų ir veiklos registravimo žurnalai CA archyve saugomi 10 (dešimt) metų. Informacinių sistemų komponentų įvykių žurnalai turi būti centralizuotai saugomi ne trumpiau kaip 1 (vienerius) metus.

5.4.4. Įrašų apsauga

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

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

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

b) būtų galimybė nustatyti bet kokį duomenų iškraipymo pažeidimą;

c) niekas neturėtų teisės pakeisti žurnalo turinio.

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

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

b) sistemų naudotojų atliekamus elektroninės informacijos tvarkymo veiksmus;

c) sistemų administratorių atliekamus veiksmus;

d) identifikatorius arba kitus duomenis, įgalinančius nustatyti atsakingąjį asmenį už įvykį.

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

Be operacijų žurnalo vedami ir CA sistemų veiklos registravimo žurnalai, kuriuose 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. Galima valdyti diagnostikos žurnalo įrašų detalumą, gaunant labiau detalią arba mažiau detalią informaciją apie tam tikrus sistemos veiksmus.

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 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.

5.5. Žurnalinių įrašų archyvavimas

5.5.1. Į duomenų archyvą perduodami duomenys

Į duomenų archyvą perduodama:

a) CA sistemos operacijų ir veiklos registravimo žurnalai;

b) asmenų, kuriems buvo sudaryti sertifikatai, duomenys;

c) įvykių, susijusių su prašymų išduoti sertifikatus rengimu, teikimu ir priėmimu bei asmens tapatybės nustatymu ir patvirtinimu, duomenys;

a) sertifikatų duomenys;

b) CRL sąrašai;

c) CA priklausančių raktų istorija nuo jų sugeneravimo iki sunaikinimo.

5.5.2. Į dokumentų archyvą perduodami duomenys

Į archyvą perduodami:

a) prašymai išduoti, atšaukti ir sustabdyti sertifikatus;

b) asmens tapatybės dokumentų kopijos (vadovaujantis Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2018 m. spalio 26 d. įsakymo Nr. 1V-1055 „Dėl asmens tapatybės ir papildomų specifinių požymių tikrinimo išduodant kvalifikuotus elektroninio parašo, elektroninio spaudo, interneto svetainės tapatumo nustatymo sertifikatus tvarkos aprašo patvirtinimo“ 7.5 papunkčiu);

c) įgaliojimai atstovauti juridinį asmenį.

5.5.3. Duomenų ir dokumentų saugojimo archyve periodas

Duomenys ir dokumentai archyve saugomi 10 (dešimt) metų, vėliau jie naikinami.

5.5.4. Archyvo apsauga

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

5.5.5. Atsarginių kopijų darymas

Atsarginės kopijos įgalina atstatyti sistemos darbą po sutrikimų, todėl siekiant šio tikslo daromos tokios programinės įrangos ir duomenų failų kopijos:

a) CA sistemų programinės įrangos instaliacinių paketų;

b) CA sudarytų sertifikatų ir CRL istorijos;

c) saugyklos (repository) duomenų;

d) asmenų, kuriems yra sudaryti sertifikatai, duomenų;

e) CA sistemų operacijų ir veiklos registravimo žurnalų.

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

5.6. Veiklos sutrikimų ir tęstinumo valdymas

5.6.1. Incidentų ir veiklos įvykių valdymo procedūros

Informacinių technologijų incidentų ir elektroninės informacijos saugos įvykiai valdomi vadovaujantis Registrų centro saugos informacijos ir įvykių valdymo tvarka. Įvykių valdymo procesu siekiama:

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

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

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

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

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

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

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

Saugos informacijos ir įvykių valdymo tvarkos aprašas detalizuoja:

a) CA įvykių valdymo procesų efektyvumo kriterijus;

b) CA darbuotojams priskirtus vaidmenis bei jų atsakomybę;

c) CA įvykių valdymo procedūrą;

d) CA pokyčių operacinę procedūrą.

CA vadovaujasi tokia incidentų registravimo, identifikavimo bei analizės procedūra:

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

b) vadovaujantis saugos informacijos ir įvykių valdymo tvarkos aprašu registravus sutrikimą / incidentą jam teikiama pirmenybė bei jis identifikuojamas. Identifikavimo metu įvykio įrašas yra atpažįstamas ir jam, priklausomai nuo specializuotų įvykių žurnalų analizės priemonių nustatymų, priskiriama kategorija ir prioritetas;

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

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

e) paskirtasis saugumo pareigūnas turi peržiūrėti sugeneruotą įspėjimą ir įvertinti, ar jis gali būti susijęs su saugumo ir vientisumo pažeidimais, numatytais eIDAS 19 straipsnio 2 dalyje. Nustačius, jog incidentas gali būti susijęs su eIDAS 19 straipsnio 2 dalyje numatytais saugumo bei vientisumo pažeidimais, saugumo pareigūnas nedelsiant, bet ne vėliau kaip per 4 (keturias) val., privalo sušaukti darbo grupę;

f) jei paskirtasis saugumo pareigūnas nustato, kad incidentas susijęs su asmens duomenų saugumo pažeidimu, apie tai nedelsiant informuoja duomenų apsaugos pareigūną;

g) incidentas, susijęs su saugumo bei vientisumo pažeidimu, turėjusiu didelį poveikį teikiamoms elektroninės atpažinties ir patikimumo užtikrinimo paslaugoms arba jas teikiant naudojamiems asmens duomenims, vadovaujantis Registrų centro direktoriaus įsakymu patvirtintomis informacinių technologijų incidentų valdymo taisyklėmis bei kibernetinių ir elektroninės informacijos saugos incidentų valdymo tvarka, turi būti užregistruotas su žyma, jog jis yra susijęs su eIDAS 19 straipsnio 2 dalyje numatytu saugumo bei vientisumo pažeidimu;

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

CA nedelsiant, tačiau bet kuriuo atveju ne vėliau kaip per 24 (dvidešimt keturias) val. nuo to momento, kai sužinojo, užpildydama incidentų notifikavimo formą, praneša priežiūros įstaigai ir, prireikus kitoms atitinkamoms institucijoms, kaip informacijos saugumo klausimais kompetentingai nacionalinei įstaigai arba Valstybinei duomenų apsaugos inspekcijai, apie visus saugumo arba vientisumo pažeidimus, turėjusius didelį poveikį teikiamoms paslaugoms arba jas teikiant naudojamiems asmens duomenims. Priežiūros įstaigai teikiama incidentų notifikavimo forma pildoma vadovaujantis ,,Pranešimų apie patikimumo užtikrinimo paslaugų saugumo ir (ar) vientisumo pažeidimus teikimo tvarkos aprašu“[3]. Kai saugumo ir vientisumo pažeidimas turėjo neigiamo poveikio fiziniam / juridiniam asmeniui, CA nedelsiant praneša apie saugumo ir vientisumo pažeidimą tam fiziniam / juridiniam asmeniui. Jei priežiūros įstaiga nustato, kad saugumo ir vientisumo pažeidimas yra svarbus visuomenei, ji ją informuoja arba nurodo CA tai padaryti. Esant tokiam priežiūros įstaigos prašymui, CA nedelsiant turimomis priemonėmis informuoja visuomenę.

5.6.2. Aparatinės ir programinės įrangos gedimai

CA atsižvelgia į šias elektroninės atpažinties ir patikimumo užtikrinimo paslaugų patikimumui ir stabilumui turinčias grėsmes:

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

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

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

d) vidinio tinklo ar jo dalies sutrikimai.

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

Siekdama išvengti arba sumažinti aukščiau minėtų grėsmių įtaką, 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 daromos duomenų bazių atsarginės kopijos;
- kartą per savaitę daromos kiekvieno serverio kietojo disko informacijos atsarginės kopijos;
- kompiuterių keitimas atliekamas taip, kad kietųjų diskų turiniai būtų atstatyti iš vėliausiai padarytų jų kopijų;
- po gedimo atstatytoje sistemoje testuojamas kiekvienas jos komponentas;

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

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

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

5.6.3. Privataus rakto kompromitacija

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

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

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

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

5.6.4. Patikimumo užtikrinimo paslaugų teikimo tęstinumo planas

CA, atsižvelgdama į grėsmes elektroninės atpažinties ir patikimumo užtikrinimo paslaugų patikimumui ir stabilumui, laikosi veiklos tęstinumo plane aprašytų taisyklių ir procedūrų, kurios yra būtinos siekiant atkurti veiklą įvykus elektroninės informacijos saugos incidentui. Elektroninės informacijos saugos incidentas šiuo atveju suprantamas kaip įvykis ar veiksmas, kuris gali sudaryti neleistino prisijungimo prie sertifikatų valdymo informacinės sistemos galimybę, sutrikdyti ar pakeisti jos veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti (pvz., duomenų neatitikimas ar pažeidimas, atsiradę konkretūs nesklandumai, ekrano pranešimai, neįprastas funkcionavimas, paslaugų, įrangos ar priemonių netektis, sistemos sutrikimai ar persikrovimai, žmogiškosios klaidos, fizinio saugumo pažeidimas, nesankcionuoti sistemos pakeitimai, nesankcionuota prieiga, saugos politikos neatitikimas ir kt.).

5.6.5. Saugumo priemonės atstačius sistemų veikimą

Atstačius sistemą po saugumo incidento pašalinimo, 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.

CA turi užtikrinti, kad gedimų atveju, įskaitant CA privačiojo rakto, skirto sertifikatams pasirašyti, kompromitaciją, būtų imamasi visų įmanomų priemonių CA veiklai atstatyti kaip galima greičiau.

5.7. CA veiklos nutraukimas

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

a) apie tai informuoti visus asmenis, kurių sertifikatus jis sudarė ir kurių sertifikatai yra galiojantys, bei kitus patikimumo užtikrinimo paslaugų teikėjus, su kuriais yra pasirašytos laidavimo

sutartys, partnerius, kuriems sutarčių pagrindu yra perduotos CSP, kaip patikimumo užtikrinimo paslaugų teikėjo funkcijos, trečiąsias šalis, kurioms sutarčių pagrindu teikiamos patikimumo užtikrinimo paslaugos, taip pat priežiūros įstaigą ne vėliau kaip prieš 9 (devynis) mėnesius;

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

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

d) neturint galimybės užtikrinti asmenims išduotų sertifikatų gyvavimo ciklo šių sertifikatų galiojimas yra nutraukiamas, o sertifikatams sudaryti naudojami CA privatūs kriptografiniai raktai, taip pat atsakymams į OCSP užklausas pasirašyti skirti privatūs kriptografiniai raktai sunaikinami nedelsiant po asmenims sudarytų sertifikatų galiojimo nutraukimo. Detalios naikinimo procedūros nustatomos detaliajame kvalifikuotos elektroninės atpažinties ir kvalifikuotų patikimumo užtikrinimo paslaugų teikimo veiklos nutraukimo plane;

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

6. Techninės saugumo kontrolės priemonės

6.1. Raktų porų generavimas ir diegimas

6.1.1. CA kriptografinių raktų porų generavimas

CA kriptografinius raktus gali generuoti tik Registrų centro pasitikėjimą turintys asmenys, kuriems toks vaidmuo yra suteiktas. CA kriptografinių raktų, skirtų pasirašinėti išduodamus sertifikatus, generavimo procese turi dalyvauti bent du Registrų centro pasitikėjimą turintys asmenys, kuriems toks vaidmuo yra suteiktas. Sugeneravus raktų porą surašomas procedūros vykdymo protokolas, kurį pasirašo procedūroje dalyvavę asmenys.

6.1.2. Kriptografinių raktų porų generavimas CA išduodamiems sertifikatams

Patvirtinus asmens tapatybę, asmens pateikto prašymo išduoti **QSignC-R-QSCD** ar **QSealC-R-QSCD** sertifikatus duomenys yra registruojami R-QSCD. Kartu R-QSCD yra generuojamos ir

išsaugomos raktų poros bei susiejama su asmens, kurio vardu bus išduodamas sertifikatas, prašymo duomenimis. Sukūrus raktų porą R-QSCD generuoja užklausą išduoti **QSignC-R-QSCD** ar **QSealC-R-QSCD** sertifikatus.

Sudarant **QSignC-R-QSCD** ir **QSealC-R-QSCD** sertifikatus kriptografinių raktų pora yra susiejama su sertifikatų savininkui išduota jų aktyvavimo nuotoliniu būdu priemone ir jai išduotu R-SIC sertifikatu.

R-SIC sertifikatams raktų pora generuojama ir saugoma CA sertifikatų savininkui išduotoje nuotolinio parašo / spaudo kriptografinių raktų aktyvavimo priemonėje.

6.1.3. Privataus rakto perdavimas sertifikato savininkui

Su **QSignC-R-QSCD** ir **QSealC-R-QSCD** sertifikatais susieti privatūs raktai nėra perduodami sertifikatų savininkui ir yra saugomi CA valdomame R-QSCD įrenginyje.

6.1.4. Privataus rakto perdavimas sertifikatų išdavėjui

Viešas raktas CA yra perduodamas tik **R-SIC** sertifikatų užsakymo ir sudarymo proceso metu, patvirtinus asmens, kuriam yra išduodami **QSignC-R-QSCD** ir **QSealC-R-QSCD** sertifikatai, tapatybę.

6.1.5. CA viešojo rakto perdavimas pasitikinčioms šalims

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

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

b) sertifikatas ir viešas raktas pridedamas prie asmeniui sudaryto ir išduoto el. parašo ar el. spaudo sertifikato.

6.1.6. Kriptografinių raktų dydžiai

CA generuoja tokio dydžio raktus:

a) Šakninės sertifikavimo tarnybos raktai RSA 4096 bitų ilgio;

b) Darbinės sertifikavimo tarnybos raktai ne mažesni nei RSA 4096 bitų ilgio;

c) asmenims R-QSCD generuojami raktai ne mažesni nei ECC 256 bitų ilgio arba ECC 384.

Sertifikatų savininkui išduotoje nuotolinio parašo / spaudo kriptografinių raktų aktyvavimo priemonėje generuojami raktai ne mažesni nei RSA 2048 bitų ilgio.

6.1.7. Kriptografinių raktų parametrų generavimas ir kokybės tikrinimas

Vieši raktai generuojami panaudojant atsitiktinių skaičių sekos generatorių, jų kokybę užtikrina R-QSCD HSM modulis, kuris yra sertifikuotas pagal ETSI EN 419 221-5 standarto reikalavimus.

6.1.8. Raktų naudojimo paskirtis

CA nustato sertifikatų rakto naudojimą pagal siūlomą taikymo sritį. Ši informacija pateikiama X.509 v3 rakto naudojimo lauke.

6.2. Privataus rakto apsauga ir kriptografinių modulių techninė kontrolė

6.2.1. Kriptografinių modulių standartai ir kontrolė

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.

R-QSCD yra sertifikuotas paskirtos atitinkamos viešosios ar privačiosios įstaigos pagal eIDAS reglamento 30 straipsnį. R-QSCD kriptografinis modulis (CM) yra įtrauktas į parengtą kvalifikuotų elektroninio parašo / antspaudo kūrimo priemonių, kurias ES šalys naudoja kvalifikuoto elektroninio parašo / antspaudo kūrimo paslaugoms, sąrašą, kai kvalifikuoto elektroninio parašo kūrimo aplinką valdo paslaugų teikėjas pasirašiusiųjų vardu.

R-QSCD SAM (Signature Activation Module) ir CM moduliai yra sertifikuoti ne mažesniu nei EAL4 papildytu su „AVA_VAN.5" lygiu pagal bendrųjų kriterijų patikimo funkcionavimo garantijų įvertinimo lygius (angl. Common Criteria on the Evaluation Assurance Level). R-QSCD įtaisas ir jo moduliai yra apsaugoti nuo klastojimo ir neteisėtos prieigos.

6.2.2. Privačių raktų saugojimas (*key escrow*)

Sertifikatų savininkų privatūs raktai saugomi R-QSCD SAM modulyje kaip saugūs binariniai objektai.

CA neperduoda sertifikatų savininkų privačių raktų trečiosioms šalims.

6.2.3. Privačių kriptografinių raktų atsarginių kopijų darymas ir atstatymas

CA privatieji raktai gali būti atstatomi ir jų kopijos saugomos tik naudojantis su kriptografine techninė įranga susietomis sisteminėmis kortelėmis, kur kiekvienoje iš jų saugomas fragmentas šifravimo rakto, kuriuo užšifruota CA privačiojo rakto kopija, duomenų. Privačiajam raktui atstatyti

reikalingos bent 2 (dvi) iš minimaliai 4 (keturių) tokių sisteminių kortelių. Darant kopijas, saugant ir atstatant CA privatų raktą privalo dalyvauti bent 2 (du) ypatingo pasitikėjimo pareigas užimantys darbuotojai ir tai turi būti atliekama fiziškai saugioje aplinkoje.

Sertifikatų savininkų privačių raktų kopijos saugiai perduodamos ir saugomos rezerviniame R-QSCD.

R-SIC sertifikatų privatūs raktai saugomi nuotolinio parašo / spaudo kriptografinių raktų aktyvavimo priemonės kriptografinių raktų saugykloje ir negali būti daromos bet kokios jų kopijos.

6.2.4. Privačių raktų archyvavimas

Privatūs raktai negali būti archyvuojami ir pasibaigus jų naudojimo terminui turi būti patikimai sunaikinti.

6.2.5. Privataus rakto perdavimas į kriptografinį modulį arba iš jo

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

Sertifikatų savininkų privatūs raktai generuojami R-QSCD CM modulyje ir kaip saugūs binariniai objektai per vidinę R-QSCD sąsają perduodami saugoti R-QSCD SAM moduliui.

R-QSCD SAM gavus sertifikato savininko autorizuotą užklausą aktyvuoti privatų raktą, privatus raktas, kaip saugus binarinis objektas, kartu su pasirašomų duomenų santrauka perduodamas R-QSCD CM, kur yra sukuriami el. parašo / spaudo duomenys.

Domenų mainai tarp R-QSCD CM ir SAM modulių organizuojami CEN EN 419 221-5 standarte apibrėžtu protokolu.

6.2.6. Privataus rakto saugojimas kriptografijos modulyje

Sertifikatų savininkų privatūs raktai yra generuojami R-QSCD CM modulyje, o saugomi R-QSCD SAM modulyje.

6.2.7. Privataus rakto aktyvavimo metodas

Pagrindiniai sertifikato savininko privataus rakto aktyvavimo etapai:

1) R-QSCD SAM, gavęs užklausą sukurti el. parašo / spaudo duomenis, sukuria ir išsiunčia sertifikato savininko nuotolinio parašo / spaudo aktyvavimo priemonei reikalavimą patvirtinti (autorizuoti) privataus rakto aktyvavimą R-QSCD įrenginyje;

2) sertifikato savininkas įvesdamas autentikavimo kodą aktyvuoja nuotolinio parašo / spaudo aktyvavimo priemonės kriptografinių raktų saugykloje esantį privatų raktą ir pasirašo

reikalavimą patvirtinti (autorizuoti) privataus rakto aktyvavimą R-QSCD įrenginyje bei išsiunčia jį R-QSCD SAM;

3) R-QSCD SAM, gavęs sertifikato savininko patvirtintą leidimą aktyvuoti jam priklausantį privatų raktą ir patikrinęs šios autorizacijos duomenų teisingumą, užklausą sukurti el. parašo / spaudo duomenis perduoda R-QSCD CM moduliui;

4) R-QSCD CM modulis sukuria prašomo el. parašo / spaudo duomenis ir rezultatus grąžina R-QSCD SAM.

QSignC-R-QSCD sertifikatų privačių raktų aktyvavimui R-QSCD nuotolinio parašo / spaudo aktyvavimo priemonėje naudojamas autentikavimo kodas, susietas su privačiu raktu, esančiu nuotolinio parašo / spaudo aktyvavimo priemonės kriptografinėje saugykloje. Autentikavimo kodo ilgis – ne mačiau kaip 4 skaitmenys.

6.2.8. Privataus rakto deaktyvavimo metodas

R-QSCD CM įvykdžius R-QSCD SAM pateiktą el. parašo / spaudo kūrimo užklausą, R-QSCD CM modulyje sunaikinami tam naudoto privataus rakto duomenys.

Sertifikatų savininkui pasirašius R-QSCD SAM pateiktą reikalavimą patvirtinti (autorizuoti) privataus rakto aktyvavimą R-QSCD įrenginyje, pasirašymui naudotas nuotolinio parašo / spaudo aktyvavimo priemonės R-SIC sertifikato privatus raktas nėra kaip nors papildomai išsaugomas šios priemonės atmintyje ir be pakartotinio autentikavimo kodo įvedimo negali būti naudojamas kitoms R-QSCD SAM užklausoms patvirtinti.

6.2.9. Privataus rakto sunaikinimas

Atšaukus **QSignC-R-QSCD** ir **QSealC-R-QSCD** sertifikatų galiojimą R-QSCD priemonėmis yra sunaikinami su šiais sertifikatais susieti privatūs raktai.

6.3. Kiti raktų poros valdymo aspektai

6.3.1. Viešųjų raktų archyvavimas

Vieši raktai yra archyvuojami ir saugomi kartu su atitinkamais sertifikatais.

6.3.2. Sertifikatų ir juos atitinkančių raktų porų naudojimo terminai

Sertifikatų ir raktų porų naudojimo periodai:

Sertifikato pavadinimas	Raktų ilgis	Raktų ir sertifikato galiojimo laikas
Root CA	RSA4096	27 metai
Issuing CA-2	RSA4096	9 metai
QSignC-R-QSCD	ECC256	3 metai

QSealC-R-QSCD	ECC256	3 metai
R-SIC	ECC256	3 metai

6.4. Kriptografinių raktų aktyvavimo duomenys

6.4.1. Kriptografinių raktų aktyvavimo duomenų generavimas ir diegimas

QSignC-R-QSCD bei **QSealC-R-QSCD** sertifikatų privatūs raktai aktyvuojami sertifikatų savininkui nuotolinio parašo / spaudo aktyvavimo priemone pasirašant R-QSCD SAM modulio suformuotą atitinkamą reikalavimą. Šiam parašui sukurti reikalingi duomenys – raktų pora bei sertifikatas – sukuriami nuotolinio parašo / spaudo aktyvavimo priemonės įdiegimo ir registracijos R-QSCD metu, patvirtinus abonento asmens tapatybę.

Pagrindiniai proceso etapai:

1) įdiegus nuotolinio parašo / spaudo aktyvavimo priemonės programinę įrangą, šios priemonės kriptografinių raktų saugykloje sugeneruojama raktų pora. Sugeneruoti privatūs kriptografiniai raktai susiejami su abonento pasirinktu autentikavimo nuotolinio parašo / spaudo aktyvavimo priemonėje kodu;

2) nuotolinio parašo / spaudo aktyvavimo priemonė generuoja užklausą išduoti R-SIC sertifikatą ir perduoda CA nuotolinio parašo / spaudo kūrimo infrastruktūrai, kuri išduoda R-SIC sertifikatą ir registruoja jį R-QSCD.

R-SIC sertifikatams raktų pora generuojama ir saugoma CA sertifikatų savininkui išduotoje nuotolinio parašo / spaudo aktyvavimo priemonės kriptografinių raktų saugykloje.

6.4.2. Aktyvavimo duomenų apsauga

Nuotolinio parašo / spaudo aktyvavimo priemonės privatus raktas, kuriuo sertifikatų savininkas pasirašo R-QSCD SAM suformuotą reikalavimą aktyvuoti R-QSCD saugomus privačius raktus, apsaugotas autentikavimo kodais.

6.4.3. Kiti aktyvavimo duomenų aspektai

Sąsaja tarp nuotolinio parašo / spaudo aktyvavimo priemonės ir CA nuotolinio parašo / spaudo kūrimo infrastruktūros yra organizuojama šifruotais duomenų perdavimo kanalais.

CA nuotolinio parašo / spaudo kūrimo infrastruktūra užtikrina ryšį tarp nuotolinio parašo / spaudo aktyvavimo priemonės ir R-QSCD SAM modulio pagal ETSI techninės specifikacijos TS 119 432 reikalavimus, realizuojančius „Sole Control Assurance Level 2" (SCAL2).

6.5. Kompiuterių saugumo kontrolė

CA ir kitų tarnybų kompiuteriai turi tokias apsaugos priemones:

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

b) prieigos kontrolės priemones;

c) prisijungimui tikrinti reikiamų duomenų kaupimo priemones;

d) įgalinančias atskirti pareigas, leistinas sistemoje, priemones;

e) prisijungiančių asmenų pareigų identifikavimo ir autentifikavimo priemones;

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

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

h) patikimas darbuotojų ir jų pareigų kaitos fiksavimo priemones;

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

6.6. Kompiuterinių sistemų gyvavimo ciklo saugumo kontrolė

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

6.6.1. Sistemų kūrimo ir keitimo 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;

c) keitimus atlieka patikimas ir kvalifikuotas personalas, laikantis CA nustatytų saugumo taisyklių.

6.6.2. 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.

6.7. Kompiuterių tinklo saugumo kontrolė

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

7. Sertifikatų, CRL ir OCSP profiliai

7.1. Sertifikatų profiliai

7.1.1. Šakninės CA sertifikato profilis

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

7.1.2. Darbinės CA sertifikato profilis

X.509 V1 pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			*V3*
Serial number			*Automatiškai sudaromas šakninio CA*

Signature algorithm			*sha256RSA*
Issuer			*CN = RCSC RootCA* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 9 metai*
Subject			*CN = RCSC IssuingCA-2* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Public key			*RSA (4096 Bits)*
X.509 V3 plėtiniai			
Subject Key Identifier	Ne	Key Identifier	*RCSC IssuingCA viešojo rakto 160 bitų ilgio hash reikšmė*
CA Version	Ne		*V0.0*
Certificate Policies	Ne	Policy Identifier	*2.5.29.32.0*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Certificate Template Name	Ne		*Sisteminis šablono identifikatorius*
Authority Key Identifier	Ne	Key Identifier	*RCSC RootCA viešojo rakto 160 bitų ilgio hash reikšmė*
CRL Distribution Points	Ne	Distribution Point Name	*http://csp2.rcsc.lt/cdp/RCSC_RootCA.crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*http://ocsp2.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp2.rcsc.lt/aia/RCSC_RootCA.crt*
Basic Constraints	Taip		*Subject Type=CA* *Path Length Constraint=None*
Key Usage	Taip		*Certificate Signing, Off-line CRL Signing, CRL Signing (06)*

7.1.3. Šakninės CA OCSP atsakymų pasirašymo sertifikato profilis

X.509 V1 pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			*V3*
Serial number			*Automatiškai sudaromas šakninio CA*
Signature algorithm			*sha256RSA*
Issuer			*CN = RCSC RootCA*

			OU = RCSC *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data +6 metai*
Subject			*CN = RCSC RootCA OCSP* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Public key			*RSA (2048 Bits), RSA (3072 Bits), RSA (4096 Bits)*
X.509 V3 plėtiniai			
Subject Key Identifier	Ne	Key Identifier	*RCSC RootCA OCSP viešojo rakto 160 bitų ilgio hash reikšmė*
Authority Key Identifier	Ne	Key Identifier	*RCSC RootCA viešojo rakto 160 bitų ilgio hash reikšmė*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.5.1*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Key Usage	Ne		*Digital Signature (80)*
Enhanced Key Usage	Ne		*OCSP pasirašymas (1.3.6.1.5.5.7.3.9)*

7.1.4. Darbinės CA OCSP atsakymų pasirašymo sertifikato profilis

X.509 V1 pagrindiniai laukai	**Kritinis**	**Atributas**	**Reikšmė**
Version			*V3*
Serial number			*Automatiškai sudaromas šakninio CA*
Signature algorithm			*sha256RSA*
Issuer			*CN = RCSC IssingCA-2* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 3 metai*
Subject			*CN = RCSC IssuingCA-2 OCSP* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Public key			*RSA (3072 Bits), RSA (4096 Bits)*
X.509 V3 plėtiniai			
Subject Key Identifier	Ne	Key Identifier	*RCSC IssuingCA OCSP viešojo rakto 160 bitų ilgio hash reikšmė*
Authority Key Identifier	Ne	Key Identifier	*RCSC IssuingCA arba RCSC IssingCA-2 viešojo rakto 160 bitų ilgio hash reikšmė*
	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.5.1*

Certificate Policies		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Key Usage	Taip		*Digital Signature, Non-Repudiation (c0)*
Enhanced Key Usage	Ne		*OCSP pasirašymas (1.3.6.1.5.5.7.3.9)*

7.1.5. Kvalifikuotų sertifikatų, skirtų elektroniniams parašams ir spaudams tvirtinti, profiliai

7.1.5.1. Kvalifikuoto nuotolinio elektroninio parašo sertifikato profilis

X.509 V1 pagrindiniai laukai	**Kritinis**	**Atributas**	**Reikšmė**
Version			*V3*
Serial number			*Automatiškai sudaromas, unikalus sertifikato, išduoto darbinio CA, serijinis numeris*
Signature algorithm			*sha256RSA* arba *sha256ECC*
Issuer			*CN = RCSC IssingCA-2* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 2-3 metai (ECC 256 bits)* *Išdavimo data + 3-5 metai (ECC 384 bits)*
Subject			*Serial Number = PNOLT – asmens kodas* *CN = asmens pavardė, asmens vardas,* *PNOLT – asmens kodas* *G = asmens vardas* *SN = asmens pavardė* *C = LT*
Public key			*ECC (256 Bits) arba ECC (384 Bits)*
X.509 V3 plėtiniai			
Subject Key Identifier	Ne	Key Identifier	*Asmens viešojo rakto 160 bitų ilgio hash reikšmė*
Authority Key Identifier	Ne	Key Identifier	*RCSC darbinio CA viešojo rakto 160 bitų ilgio hash reikšmė*
CRL Distribution Points	Ne	Distribution Point Name	*http://csp2.rcsc.lt/cdp/RCSC_IssuingCA-2.crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp2.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp2.rcsc.lt/aia/RCSC_IssuingCA.crt*

Certificate Template Information	Ne	Template	*Sisteminis šablono identifikatorius*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.5.1*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Application Policies	Ne	Application Certificate Policy	*Policy Identifier=Document Signing* *Policy Identifier=Secure Email*
Qualified Certificate Statement	Ne	EU Qualified Certificate statement	*Id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)* *id-qcs-pkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)*
		SSCD statement	*id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)*
Key Usage	Taip		*Digital Signature, Non-Repudiation (c0)*
Enhanced Key Usage	Ne		*Dokumentų pasirašymas (1.3.6.1.4.1.311.10.3.12)* *Saugus elektroninis paštas (1.3.6.1.5.5.7.3.4)* *Asmens autentikavimas (1.3.6.1.5.5.7.3.2)*

7.1.5.2. Kvalifikuoto nuotolinio elektroninio spaudo sertifikato profilis

X.509 V1 pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			*V3*
Serial number			*Automatiškai sudaromas, unikalus sertifikato, išduoto darbinio CA, serijinis numeris*
Signature algorithm			*sha256RSA* arba *sha256ECC*
Issuer			*CN = RCSC IssuingCA-2* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 2-3 metai (ECC 256 bits)* *Išdavimo data + 3-5 metai (ECC 384 bits)*
Subject			*O = Organizacijos pavadinimas* *CN = Organizacijos pavadinimas* *SERIALNUMBER = Juridinio asmens identifikatorius (įmonės kodas)* *2.5.4.97 = NTRLT – Juridinio asmens identifikatorius (įmonės kodas)* *C = LT*
Public key			*ECC (256 Bits)* arba *ECC (384 Bits)*
X.509 V3 plėtiniai			
Subject alternative name	Ne		*RFC822 Name = elektroninio pašto adresas*

Subject Key Identifier	Ne	Key Identifier	*Asmens viešojo rakto 160 bitų ilgio hash reikšmė*
Authority Key Identifier	Ne	Key Identifier	*RCSC darbinio CA viešojo rakto 160 bitų ilgio hash reikšmė*
CRL Distribution Points	Ne	Distribution Point Name	*http://csp2.rcsc.lt/cdp/RCSC_IssuingCA-2.crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp2.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp2.rcsc.lt/aia/RCSC_IssuingCA-2.crt*
Certificate Template Information	Ne	Template	*Sisteminis šablono identifikatorius*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.5.1*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Application Policies	Ne	Application Certificate Policy	*Policy Identifier=Document Signing* *Policy Identifier=Secure Email*
Qualified Certificate Statement	Ne	EU Qualified Certificate statement	*Id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)* *id-qcs-pkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)*
		SSCD statement	*id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)*
		Qualified Certificate Type	*id-etsi-qcs-QcType (0.4.0.1862.1.6)* *id-etsi-qct-eseal (0.4.0.1862.1.6.2)*
Key Usage	Taip		*Digital Signature, Non-Repudiation (c0)*
Enhanced Key Usage	Ne		*Dokumentų pasirašymas (1.3.6.1.4.1.311.10.3.12)* *Saugus elektroninis paštas (1.3.6.1.5.5.7.3.4)*

7.1.5.3. Juridinio asmens darbuotojo kvalifikuoto nuotolinio elektroninio parašo sertifikato profilis

X.509 V1 pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			*V3*
Serial number			*Automatiškai sudaromas, unikalus sertifikato, išduoto darbinio CA, serijinis numeris*
Signature algorithm			*sha256RSA* arba *sha256ECC*
Issuer			*CN = RCSC IssuingCA-2* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*

Valid to			*Išdavimo data + 2-3 metai (ECC 256 bits)* *Išdavimo data + 3-5 metai (ECC 384 bits)*
Subject			*Serial Number = suteiktas unikalus identifikatorius** *CN = vardas ir pavardė* *G = asmens vardas* *SN = asmens pavardė* *OU = padalinio pavadinimas* *O = įmonės pavadinimas* *C = LT*
Public key			*ECC (256 Bits)* arba *ECC (384 Bits)*
X.509 V3 plėtiniai			
Subject alternative name	Ne		*RFC822 Name = elektroninio pašto adresas*
Subject Key Identifier	Ne	Key Identifier	*Asmens viešojo rakto 160 bitų ilgio hash reikšmė*
Authority Key Identifier	Ne	Key Identifier	*RCSC darbinio CA viešojo rakto 160 bitų ilgio hash reikšmė*
CRL Distribution Points	Ne	Distribution Point Name	*http://csp2.rcsc.lt/cdp/RCSC_IssuingCA-2.crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp2.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp2.rcsc.lt/aia/RCSC_IssuingCA-2.crt*
Certificate Template Information	Ne	Template	*Sisteminis šablono identifikatorius*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.5.1*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Application Policies	Ne	Application Certificate Policy	*Policy Identifier=Document Signing* *Policy Identifier=Secure Email*
Qualified Certificate Statement	Ne	EU Qualified Certificate statement	*Id-etsi-pcs-QcCompliance (0.4.0.1862.1.1)* *id-qcs-pkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)*
		SSCD statement	*id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)*
Key Usage	Taip		*Digital Signature, Non-Repudiation (c0)*
Enhanced Key Usage	Ne		*Dokumentų pasirašymas (1.3.6.1.4.1.311.10.3.12)* *Saugus elektroninis paštas (1.3.6.1.5.5.7.3.4)*

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

7.1.5.4. Nuotolinio kvalifikuoto elektroninio parašo bei nuotolinio kvalifikuoto elektroninio spaudo, skirto kriptografinių raktų aktyvavimui, sertifikato profilis

X.509 V1 pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			*V3*
Serial number			*Automatiškai sudaromas, unikalus sertifikato, išduoto darbinio CA, serijinis numeris*
Signature algorithm			*sha256RSA*
Issuer			*CN = RCSC IssuingCA-2* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 2-3 metai (ECC 256 bits)* *Išdavimo data + 3-5 metai (ECC 384 bits)*
Subject			*CN = paskyros arba vartotojo informacija* *C = LT* *E = Elektroninio pašto adresas*
Public key			*RSA (2048 Bits)* arba *ECC (256 Bits)*
X.509 V3 plėtiniai			
Subject alternative name	Ne		*RFC822 Name = elektroninio pašto adresas*
Subject Key Identifier	Ne	Key Identifier	*Viešojo rakto 160 bitų ilgio hash reikšmė*
Authority Key Identifier	Ne	Key Identifier	*RCSC darbinio CA viešojo rakto 160 bitų ilgio hash reikšmė*
CRL Distribution Points	Ne	Distribution Point Name	*http://csp2.rcsc.lt/cdp/RCSC_IssuingCA-2.crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp2.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp2.rcsc.lt/aia/RCSC_IssuingCA-2.crt*
Certificate Template Information	Ne	Template	*Sisteminis šablono identifikatorius*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.5.1*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Application Policies	Ne	Application Certificate Policy	*Policy Identifier=Client Authentication*

Key Usage	Taip		*Digital Signature (80)*
Enhanced Key Usage	Ne		*Client Authentication (1.3.6.1.5.5.7.3.2)*

7.2. CRL Profile

CA sudaro ir skelbia CRL sąrašus laikantis RFC 5280 reikalavimų.

7.2.1. Šakninės CA CRL profilis

CRL pagrindiniai laukai	Atributas	Reikšmė
Version		*V2*
Issuer		*CN = RCSC RootCA* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Effective date		*Išdavimo data ir laikas*
Next update		*Išdavimo data ir laikas + 6 mėnesiai ir 3 savaitės*
Signature algorithm		*Sha256RSA*
Sertifikatai, kurių galiojimas sustabdytas arba nutrauktas		
Serial number		*Sustabdyto arba nutraukto galiojimo sertifikato serijinis numeris*
Revocation date		*Sertifikato galiojimo sustabdymo arba nutraukimo data ir laikas*
CRL reason code		*Sertifikato galiojimo sustabdymo arba nutraukimo priežastis*
CRL plėtiniai		
Authority Key Identifier	Key Identifier	*RCSC šakninio CA viešojo rakto 160 bitų ilgio hash reikšmė*
CA Version		*V0.0*
CRL Number		*Suteiktas automatiškai šakninio CA*
Next CRL Publish		*Išdavimo data ir laikas + 6 mėnesiai*

7.2.2. Darbinės CA CRL profilis

CRL pagrindiniai laukai	Atributas	Reikšmė
Version		*V2*
Issuer		*CN = RCSC IssuingCA arba RCSC IssingCA-2* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*
Effective date		*Išdavimo data ir laikas*
Next update		*Išdavimo data ir laikas + 36 valandos*
Signature algorithm		*Sha256RSA*
Sertifikatai, kurių galiojimas		

sustabdytas arba nutrauktas		
Serial number		*Sustabdyto arba nutraukto galiojimo sertifikato serijinis numeris*
Revocation date		*Sertifikato galiojimo sustabdymo arba nutraukimo data ir laikas*
CRL reason code		*Sertifikato galiojimo sustabdymo arba nutraukimo priežastis*
CRL plėtiniai		
Authority Key Identifier	Key Identifier	*RCSC darbinio CA viešojo rakto 160 bitų ilgio hash reikšmė*
CA Version		*V0.0*
CRL Number		*Suteiktas automatiškai darbinio CA*
Next CRL Publish		*Išdavimo data ir laikas + 24 valandos*

7.3. OCSP Profile

OCSP atsakiklis veikia pagal RFC 6960 nustatytus reikalavimus

Laukas	Privalomumas	Reikšmė	Apibūdinimas
ResponseStatus	*Taip*	*0 for successful or error code*	*Užklausos rezultatas*
ResponseBytes			
ResponseType	*Taip*	*id-pkix-ocsp-basic Type of the response*	*Užklausos tipas*
BasicOCSPResponse	*Taip*		
tbsResponseData	*Taip*		
Version	*Taip*	*1*	*Version of the response format*
responderID	*Taip*	*CN = RCSC IssuingCA-2 OCSP* *OU = RCSC* *O = VI Registru centras - i.k. 124110246* *C = LT*	*Išskirtinis OCSP atsakiklio pavadinimas*
producedAt	*Taip*		*Data, kada atsakas į OCSP buvo pasirašytas*
Responses	*Taip*		
certID	*Taip*		*CertID laukus pagal RFC 6960, 4.1.1 punktas*
certStatus	*Taip*		*Sertifikato būsena:* *geras – sertifikatas išduotas ir nėra atšauktas arba sustabdytas;* *atšauktas – sertifikatas atšauktas arba sustabdytas;* *nežinoma – sertifikato išdavėjas yra neatpažintas šio OCSP atsakiklio.*
revocationTime	*Ne*		*Sertifikato atšaukimo arba galiojimo pabaigos data*

revocationReason	*Ne*		*Atšaukimo priežasties kodas pagal RFC 5280*
thisUpdate	*Taip*		*Data, kada buvo kreiptasi dėl sertifikato būsenos į duomenų bazę*
nextUpdate	*Taip*		*Laikas, kada arba iki kada bus pasiekiama informacija apie sertifikato galiojimo būseną*
Archive Cutoff	*Ne*		*CA sertifikato galiojimo pradžios data*
Nonce	*Ne*		*Reikšmė kopijuojama iš užklausos, jei ji įtraukta. Remiantis RFC 6960, 4.4.1 punktas*
Extended Revoked Definition	*Ne*	*NULL*	*Identifikatorius, kurio semantika sertifikato būsenos OCSP atsakyme atitinka išplėstinį apibrėžimą RFC 6960, 2.2 skirsnyje*
signatureAlgorithm	*Taip*	*sha256WithRSAEncryption*	*Pasirašymo algoritmas pagal RFC 5280*
signature	*Taip*		
certificate	*Taip*		*Privataus rakto, naudojamo atsakymui pasirašyti, sertifikatas*

8. Atitikties auditas bei kiti vertinimai

8.1. Atitikties vertinimo dažinis ar aplinkybės

Vadovaudamasi eIDAS 20 straipsnio 1 dalimi atitikties vertinimo įstaiga kas 24 (dvidešimt keturis) mėnesius atlieka CA teikiamų paslaugų atitikties vertinimą – auditą.

Vadovaudamasi eIDAS 20 straipsnio 2 dalimi priežiūros įstaiga bet kuriuo metu gali atlikti CA auditą arba reikalauti, kad atitikties įstaiga atliktų CA vertinimą (CA lėšomis), siekdama patvirtinti, kad teikiamos paslaugos atitinka eIDAS nustatytus reikalavimus.

8.2. Atitikties vertintojo kvalifikacija

Auditą atlieka akredituota atlikti kvalifikuotos elektroninės atpažinties ir kvalifikuotų patikimumo užtikrinimo paslaugų teikėjo ir jo teikiamų kvalifikuotų elektroninės atpažinties bei patikimumo užtikrinimo paslaugų atitikties vertinimą atitikties vertinimo įstaiga pagal Europos Parlamento ir Tarybos reglamentą EB Nr. 765/2008.

8.3. Atitikties vertintojo ryšys su vertinamuoju subjektu

Atitikties vertinimo įstaiga ir jos paskirtas auditorius turi būti visiškai nepriklausomas nuo Registrų centro ir nesusijęs su Registrų centro valdoma IT technine ir programine infrastruktūra.

8.4. Vertinamos temos

Auditas apima personalo, procesų, informacinių sistemų, IT ir ryšio techninės infrastruktūros, elektroninės atpažinties, patikimumo užtikrinimo paslaugų teikimo taisyklių ir nuostatų atitikties eIDAS bei kituose Europos Sąjungos teisės aktuose bei standartuose, reglamentuojančiuose elektroninės atpažinties ir patikimumo užtikrinimo paslaugų teikimą, nustatytiems reikalavimams vertinimą.

8.5. Atitikties ataskaitos vertinimas ir trūkumų šalinimas

Elektroninės atpažinties ir patikimumo užtikrinimo paslaugų teikimo priežiūrą vykdo Lietuvos Respublikos Vyriausybės įgaliota priežiūros įstaiga. Atlikus atitikties vertinimą audito ataskaita yra pateikiama Lietuvos Respublikos Vyriausybės įgaliotai priežiūros įstaigai. Audito ataskaitos ir joje įvardintų trūkumų vertinimas bei šalinimo procesai atliekami Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2018 m. birželio 21 d. įsakymu Nr. 1V-588 patvirtinta Kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų ir kvalifikuotų patikimumo užtikrinimo paslaugų statuso suteikimo ir jų įrašymo į nacionalinį patikimą sąrašą bei kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų veiklos ataskaitų teikimo tvarka.

8.5.1. Atitikties rezultatų skelbimas

CA atitikties vertinimo išvados dedamos į saugyklą (*repository*) ir skelbiamos viešai.

9. Kiti teisiniai bei veiklos aspektai

9.1. Paslaugų kainos

9.1.1. Sertifikatų išdavimo ir atnaujinimo mokesčiai

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

9.1.2. Prieigos prie sertifikatų mokesčiai

Prieiga prie viešai skelbiamų CA sertifikatų yra nemokama.

Trečių šalių prieiga prie CA išduotų abonentų sertifikatų yra negalima.

9.1.3. Sertifikatų atšaukimo bei informacijos apie sertifikatų galiojimą teikimo mokesčiai

CRL ir OCSP atsakiklio paslaugų teikimas nėra apmokestinamas.

CA, gavusi sertifikatų savininko prašymą, sertifikato galiojimą nutraukia ir stabdo nemokamai. CP ir CPS skelbiami nemokamai saugykloje (*repository*).

9.1.4. Mokesčiai už kitas paslaugas

Mokestis už elektroninio parašo ir elektroninio spaudo kūrimo transakcijų aptarnavimą bei kitų CA teikiamų elektroninės atpažinties ir patikimumo užtikrinimo paslaugų kainos yra skelbiamos viešai Registrų centro paslaugų kainoraštyje.

9.1.5. Pinigų grąžinimo tvarka

Sertifikatų savininkui pateikus motyvuotą prašymą gali būti grąžinamos jo sumokėtos sumos už Registrų centro nesuteiktas paslaugas. Bet kokie nesutarimai ar ginčai, kylantys tarp CA ir sertifikatų naudotojų, sprendžiami derybų būdu, o jeigu tokiu būdu ginčų išspręsti nepavyksta, jie sprendžiami Lietuvos Respublikos teisme, vadovaujantis Lietuvos Respublikoje galiojančiais įstatymais ar kitais teisės aktais.

9.2. Finansinė atsakomybė

9.2.1. Draudimo aprėptis

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

9.2.2. Sertifikatų naudotojų kompensacijos

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

a) prašantysis sudaryti sertifikatus pateikė klaidingus duomenis;

b) sertifikatų savininkas, praradęs kvalifikuotą sertifikatą atitinkančių elektroninio parašo, elektroninio spaudo kūrimo duomenų kontrolę iš karto, kai jam tapo žinoma apie tai, neinformavo CA;

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

9.3. Veiklos informacijos konfidencialumas

CA valdoma informacija, kuriai pagal Lietuvos Respublikos teisės aktus ar CA sudarytus sandorius, taikomas konfidencialios informacijos statusas. Taip pat konfidencialia informacija yra laikoma informacija, numatyta Registrų centro valdybos patvirtintame Registrų centro konfidencialios, komercinę (gamybinę) paslaptį sudarančios informacijos sąraše.

9.4. Asmens duomenų apsauga

Asmens duomenys tvarkomi laikantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo, Lietuvos Respublikos bei Bendrojo asmens duomenų apsaugos reglamento reikalavimų.

CA renka ir tvarko tik tiek asmens duomenų, kiek tai yra būtina norint užtikrinti teikiamų elektroninės atpažinties ir patikimumo paslaugų saugumą ir patikimumą. Prieš teikiant prašymą išduoti sertifikatą asmuo yra supažindinamas su renkamais asmens duomenimis bei jų tvarkymo apimtimi ir tikslu, asmens duomenų rinkiniu, kuris bus įtrauktas į išduodamą sertifikatą, sertifikatų užsakymo, išdavimo ir naudojimo sąlygomis. Abonento bei juridinio asmens atstovo sutikimas su šiomis sertifikatų užsakymo, išdavimo ir naudojimo sąlygomis yra privalomas.

Bet kokie duomenys, gauti iš abonento ar juridinio asmens atstovo jam teikiant prašymą, kurie nėra viešai prieinami sertifikato saugykloje ir CRL, yra laikomi privačiais asmens duomenimis. Visi duomenys, viešai prieinami CA išduotame sertifikate, nėra laikomi privačiais asmens duomenimis, kiek tai neprieštarauja Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo, Lietuvos Respublikos bei Bendrojo asmens duomenų apsaugos reglamento nuostatoms.

CA tvarkomi privatūs asmens duomenys trečiosioms šalims be asmens sutikimo gali būti atskleisti tik Lietuvos Respublikos teisės aktų numatytais atvejais.

9.5. Intelektinės nuosavybės apsauga

CP ir CPS yra CA intelektinė nuosavybė, tačiau jie laisvai prieinami sertifikatų naudotojams. Naudojant CP ir CPS būtina pateikti nuorodą į šaltinį.

Kriptografinių raktų pora yra sertifikato savininko nuosavybė. CA netaiko nuosavybės teisių sudarytiems sertifikatams.

9.6. Pareiškimai ir garantijos

Šiame skyriuje yra apibrėžiama įsipareigojimų / garantijos ir atsakomybių pasidalijimas tarp CA, RA, abonento / sertifikatų savininko bei pasitikinčių šalių. Šie įsipareigojimai bei atsakomybės yra aprašomi šalių tarpusavio susitarimuose.

9.6.1. CA pareiškimai ir garantijos

CA įsipareigoja:

a) teikti elektroninės atpažinties, nuotolinio elektroninio parašo ir nuotolinio elektroninio spaudo sertifikatų sudarymo ir išdavimo bei nuotolinio elektroninio parašo ir nuotolinio elektroninio spaudo kūrimo paslaugas laikantis CP ir šiuose CPS nustatytų procedūrų ir reikalavimų;

b) užtikrinti elektroninės atpažinties ir patikimumo užtikrinimo paslaugų teikimo metu gautos informacijos konfidencialumą ir apsaugą nuo neteisėtos prieigos;

c) užtikrinti asmens duomenų apsaugą, vadovaujantis Bendruoju asmens duomenų reglamentu bei kitais Lietuvos Respublikos teisės aktais, kurie nustato asmens duomenų saugumo reikalavimus;

d) užtikrinti Registrų centro privačiųjų kriptografinių raktų saugumą;

e) užtikrinti informacijos sudaromuose sertifikatuose teisingumą;

f) užtikrinti prašymų išduoti sertifikatus priėmimą ir vykdymą vadovaujantis šiais CPS bei tinkamą abonento asmens tapatybės identifikavimą;

g) abonentams teikti informaciją sertifikatų įsigijimo ir naudojimo klausimais;

h) sudaryti sertifikatus, kurie atitiktų eIDAS ir kitų teisės aktų, reglamentuojančių elektroninės atpažinties ir patikimumo užtikrinimo paslaugas tiek, kiek neprieštarauja eIDAS, reikalavimus;

i) šiuose CPS nustatytomis sąlygomis R-QSCD saugoti sertifikatų savininkams CA išduotus sertifikatus ir su jais susijusių kriptografinių raktų poras bei užtikrinti jų saugumą;

j) šiuose CPS nustatytomis sąlygomis R-QSCD saugoti sertifikatų savininkams išduotų nuotolinio parašo / spaudo aktyvavimo priemonių viešuosius raktus ir su jais susijusius CA išduotus sertifikatus bei užtikrinti jų saugumą;

k) sertifikatų savininkams išduoti saugias, jiems išduotų nuotolinio parašo / spaudo kriptografinių raktų aktyvavimo autorizacijos priemones bei užtikrinti nepertraukiamą jomis teikiamų kriptografinių raktų aktyvavimo autorizacijos užklausų apdorojimą;

l) užtikrinti nepertraukiamą kvalifikuoto elektroninio parašo bei kvalifikuoto elektroninio spaudo duomenų kūrimo R-QSCD įrenginyje pagal sertifikatų savininko autorizuotas užklausas paslaugų teikimą;

m) užtikrinti, kad R-QSCD atitiktų kvalifikuotiems elektroninio parašo bei kvalifikuotiems elektroninio spaudo įtaisams eIDAS nustatytus reikalavimus;

n) priimti ir vykdyti prašymus nutraukti ar sustabdyti sertifikatų galiojimą;

o) priimti ir vykdyti prašymus atšaukti anksčiau pateiktus prašymus sustabdyti sertifikatų galiojimą;

p) užtikrinti, kad šiuose CPS aprašytos elektroninės atpažinties ir patikimumo užtikrinimo paslaugų teikimo procedūros atitiktų eIDAS bei Lietuvos Respublikos teisės aktų reikalavimus;

q) užtikrinti, kad šie CPS bei tipinės sutarčių su abonentais formos būtų viešai prieinamos internete;

r) viešai internete šiuose CPS nustatytu periodiškumu skelbti CRL;

s) užtikrinti 24 val. per parą ir 7 dienas per savaitę CA išduotų sertifikatų statuso tikrinimo OCSP atsakikliu viešos paslaugos teikimą.

CA atsako už:

a) sudarytų sertifikatų, juose esančių duomenų tikslumą;

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

c) sertifikatų savininkui išduodamų elektroninio parašo bei elektroninio spaudo kūrimo duomenų ir atitinkamų sertifikatų duomenų vienareikšmį tarpusavio susiejimą ir saugojimą;

d) sutartyse su pasitikinčiomis šalimis nustatytos struktūros elektroninio parašo bei elektroninio spaudo duomenų kūrimą pagal sertifikatų savininko teikiamas autorizuotas užklausas;

e) sertifikatų galiojimo sustabdymą ar nutraukimą laiku;

f) tinkamą informacijos apie išduotų sertifikatų galiojimo, atšaukimo skelbimą.

9.6.2. RA pareiškimai ir garantijos

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 įgaliojimus teikti tokius prašymus;

c) sustabdyti, atšaukti sertifikatų galiojimą ar atšaukti sustabdymą;

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

e) suinteresuotiems asmenims teikti informaciją nuotolinio elektroninio parašo bei nuotolinio elektroninio spaudo kūrimo duomenų bei sertifikatų sudarymo ir išdavimo klausimais;

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

RA atsako už:

a) asmens, pateikusio prašymą išduoti sertifikatą, tapatybės, jam fiziškai dalyvaujant, nustatymą bei prašymo duomenų autentiškumo patvirtinimą;

b) juridinio asmens atstovo įgaliojimo įmonės vardu užsakyti elektroninio spaudo sertifikatą duomenų patikrinimą ir šios teisės patvirtinimą;

c) asmens, teikiančio prašymus sustabdyti ar atšaukti galiojimą, tapatybės nustatymą, prašymų priėmimą ir jų vykdymą šiuose CPS nustatytais terminais;

d) teisingos informacijos nuotolinio elektroninio parašo bei nuotolinio elektroninio spaudo kūrimo priemonių išdavimo klausimais teikimą.

9.6.3. Abonentų ir sertifikatų savininkų pareiškimai ir garantijos

Abonentai ir sertifikatų savininkai įsipareigoja:

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

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

c) tinkamai pasirūpinti, kad elektroninės atpažinties, nuotolinio parašo / spaudo aktyvavimo priemonės privačiuoju raktu nepasinaudotų kiti asmenys;

d) sertifikatą naudoti tik elektroniniams parašams / spaudams patvirtinti bei asmens identifikavimui ir autentikavimui elektroninėje erdvėje bei el. pašto apsaugai. Elektroninis parašas negali būti naudojamas jokiems kitiems tikslams;

e) nedelsiant kreiptis į Registrų centrą dėl sertifikato galiojimo sustabdymo ar atšaukimo šiais atvejais, kai sertifikato galiojimo laikotarpiu atsitinka bent vienas iš šių įvykių:

- pametama ar kaip nors kitaip parandama nuotolinio parašo / spaudo aktyvavimo priemonės kontrolė;
- pavagiamas ar kitaip sukompromituojamas nuotolinio parašo / spaudo aktyvavimo priemonės privatusis raktas;
- atskleidžiami nuotolinio parašo / spaudo aktyvavimo priemonės privačiojo rakto panaudojimui reikalingi identifikavimo duomenys (autentikavimo kodas ir pan.);
- pastebimi netikslumai sertifikate arba jame prireikia daryti pakeitimus;
- pasikeičia asmens tapatybės duomenys;

f) nuotolinio parašo / spaudo aktyvavimo priemonės privataus rakto kompromitacijos atveju nedelsiant ir visiškai nutraukti jo naudojimą.

9.6.4. Pasitikinčių šalių pareiškimai ir garantijos

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

Pasitikinčios šalys privalo įsitikinti, kad sertifikatai buvo galiojantys parašo sudarymo metu. Sertifikato statusas tikrinamas naudojant OCSP protokolą arba saugykloje (*repository*) esantį CRL.

Sertifikatas tikrinamas vadovaujantis sertifikatuose esančia informacija. Parašo tikrintojai turi atkreipti dėmesį į tai, ar nepažeisti sertifikatų naudojimo apribojimai.

9.6.5. Kitų šalių pareiškimai ir garantijos

9.6.6. Palaikymo tarnybos įsipareigojimai

Palaikymo tarnyba įsipareigoja 7 (septynias) dienas per savaitę 24 (dvidešimt keturias) valandas per parą telefonu priimti prašymus sustabdyti sertifikato galiojimą bei techniškai sustabdyti sertifikato galiojimą.

9.6.7. Konsultacijų centro įsipareigojimai

Konsultacijų centras – atsakingas už klientų konsultavimą:

a) nuotolinio elektroninio parašo bei nuotolinio elektroninio spaudo kūrimo priemonių išdavimo bei sertifikatų sudarymo ir tvarkymo klausimais;

b) elektroninio parašo bei elektroninio spaudo duomenų kūrimo pagal sertifikatų savininko teikiamas autorizuotas užklausas paslaugų teikimo klausimais.

9.6.8. Tapatybės patvirtinimo nuotoliniu būdu paslaugų tiekėjo įsipareigojimai

Tapatybės patvirtinimo nuotoliniu būdu paslaugų tiekėjas yra atsakingas už asmens, pateikusio prašymą išduoti sertifikatą, tapatybės nustatymą bei prašymo duomenų autentiškumo patvirtinimą nuotoliniu būdu asmeniui fiziškai nedalyvaujant.

Tapatybės patvirtinimo nuotoliniu būdu paslaugų tiekėjas turi užtikrinti pakankamą arba aukštą asmens identifikavimo ir tapatybės patvirtinimo nuotoliniu būdu saugumo lygį, kaip yra numatyta eIDAS reglamento 8 straipsnyje. Paslaugų tiekėjo asmens tapatybės patvirtinimui naudojama infrastruktūra turi atitikti ETSI TS 119 461 specifikacijos reikalavimus.

9.7. Garantijų atsisakymas

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

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

a) nenugalimos jėgos (*force majeure*), kurios kontroliuoti, numatyti ar užkirsti jai kelią iš anksto buvo neįmanoma;

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

9.8. Atsakomybės ribojimas

Aukščiausia atsakomybės už bet kokį reikalavimą riba yra 30 000 (trisdešimt tūkstančių) eurų vienam draudžiamajam įvykiui ir 90 000 (devyniasdešimt tūkstančių) eurų suma visiems draudžiamiesiems įvykiams per metus.

9.9. Nuostolių atlyginimas

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

CA prisiima atsakomybę už sertifikatų naudotojų patirtus nuostolius, kuriuos sukėlė trečiosios šalys (RA), kurioms CA delegavo dalį savo funkcijų.

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

CA neatsako, jei nuostoliai buvo patirti dėl:

a) trečiųjų šalių ir galimų vartotojų naudojamos CA neautorizuotos aparatinės ir programinės įrangos kriptografiniams raktams generuoti, duomenims šifruoti, elektroniniams parašams kurti;

b) neleistino sertifikatų naudojimo;

c) teikiamų paslaugų prieinamumo ir kokybės, jei sutrikimai fiksuojami ne Registrų centro veikimo ribose, kurios detalizuotos CPS bei CP;

d) sertifikato atšaukimo šiuose CPS nustatytais atvejais.

Žalos atlyginimo sąlygos detalizuojamos dvišaliuose susitarimuose dėl elektroninės atpažinties ir patikimumo užtikrinimo paslaugų teikimo.

9.10. Galiojimas

Šie CPS įsigalioja nuo jų patvirtinimo Registrų centro generalinio direktoriaus įsakymu momento ir galioja iki naujos šių CPS versijos išleidimo. Naujos versijos galiojimo pradžia nurodyta CPS dokumento viršelyje. Naujausia CPS versija publikuojama saugykloje (*repository*) internete.

9.11. Individualūs pranešimai ir komunikavimas

Visi pasiūlymai keisti sertifikatų išdavimo procesus bei šiuos CPS turi būti pateikti Registrų centrui elektroniniu ar popieriniu dokumentu, patvirtintu asmens parašu.

CA pranešimai sertifikatų savininkui teikiami elektroniniu paštu, kuris buvo nurodytas teikiant prašymą išduoti elektroninio parašo ar elektroninio spaudo sertifikatą. Visi pranešimai ir paklausimai, susiję su sertifikatų išdavimu ir naudojamu, turi būti teikiami elektroniniu paštu pagalba@registrucentras.lt.

9.12. Pakeitimai

Šie CPS gali būti keičiami pastebėjus juose netikslumus, 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 turi įtakos elektroninės atpažinties ir patikimumo užtikrinimo paslaugų saugumo lygio pasikeitimui, pakeitimai yra esminiai.

CPS prižiūrimi, keičiami ir tvirtinami laikantis tokios procedūros:

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

b) CPS pakeitimus inicijuoja CA arba sertifikatų naudotojai;

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

d) visais atvejais apie naują CPS redakciją bei apie bet kokius CA teikiamų paslaugų pasikeitimus informuojama priežiūros įstaiga: 1) apie bet kokius kvalifikuotos elektroninės atpažinties ir kvalifikuotų patikimumo užtikrinimo paslaugų teikimo pakeitimus – nedelsiant, bet ne vėliau kaip per 3 darbo dienas nuo šių pakeitimų dienos; 2) apie numatomą veiklos nutraukimą – ne vėliau kaip prieš 9 mėnesius iki veiklos nutraukimo dienos.

9.13. Ginčų sprendimo procedūros

Bet kokie nesutarimai ar ginčai, kylantys tarp CA ir sertifikatų naudotojų sprendžiami derybų būdu, o jeigu tokiu būdu ginčų išspręsti nepavyksta, jie sprendžiami Lietuvos Respublikos teisme, vadovaujantis Lietuvos Respublikoje galiojančiais įstatymais ar kitais teisės aktais.

9.14. Taikytina teisė

Šie CPS reglamentuojami, aiškinami ir interpretuojami pagal Lietuvos Respublikos įstatymus bei eIDAS reglamentą.

9.15. Atitiktis taikomai teisei

Šie CPS parengti vadovaujantis šiais teisės aktais:

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

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

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

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

e) Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymu;

f) Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

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

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

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

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

k) Lietuvos Respublikos teisės aktais, reglamentuojančiais patikimumo užtikrinimo paslaugas tiek, kiek neprieštarauja a) punkte nurodytam teisės aktui;

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

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

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

o) ETSI EN 319 412 Certificate Profiles;

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

r) ETSI EN 319 422 Time-stamping protocol and electronic time-stamp profiles;

s) ETSI TR 119 100 on Guidance on the use of standards for signatures creation and validation;

t) ETSI TS 119 101 Policy and security requirements for applications for signature creation and signature validation;

u) ETSI TR 119 300 Guidance on the use of standards for cryptographic suites;

v) ETSI TS 119 312 Cryptographic Suites;

y) ETSI TR 119 600 Guidance on the use of standards for trust service status lists providers;

z) ETSI TS 119 612 Trusted Lists.

CPS įgyvendina sertifikavimo veiklos politiką (toliau – CP), kurios OID yra 1.3.6.1.4.1.30903.1.5.1.

9.16. Kitos nuostatos

9.16.1. RA funkcijų delegavimo ir paslaugų teikimo sutartys

RA funkcijų vykdymą užtikrina Registrų centro klientų aptarnavimo centrai bei išorinės RA, su kuriomis yra sudarytos atitinkamos funkcijų delegavimo sutartys. Šiomis sutartimis išorės RA yra įpareigojamos laikytis šių CPS.

Šie CPS yra Registrų centro vidaus tesės aktas, kurio privalo laikytis Registrų centro klientų aptarnavimo centrai vykdydami RA funkcijas.

Kiekviena šalis, pageidaujanti pasinaudoti Registrų centrui priklausančiais produktais bei teikiamomis paslaugomis, privalo sudaryti atitinkamą susitarimą, kuriame būtų apibrėžiamos su produktų ar paslaugų naudojimu susijusios sąlygos.

Jei susitarime yra nuostatų, kurios skiriasi nuo šių CPS, pirmenybė teikiama su ta šalimi sudarytam susitarimui, tačiau tik tos šalies atžvilgiu. Trečiosios šalys negali remtis tokia sutartimi ar pareikšti ieškinio dėl jos vykdymo.

Pagal šiuos CPS veikiantys subjektai negali perleisti savo teisių ar įsipareigojimų be išankstinio raštiško Registrų centro sutikimo.