VALSTYBĖS ĮMONĖS REGISTRŲ CENTRO SERTIFIKAVIMO VEIKLOS TAISYKLĖS

Unikalus objekto ID (OID): **1.3.6.1.4.1.30903.1.5.1**

Versija: 1.2

Galioja nuo: 2024-10-25

Registrų centro sertifikavimo veiklos taisyklių 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	Taisyklės papildytos informacija dėl kvalifikuotos elektroninės atpažinties paslaugų; atnaujinti kontaktiniai duomenys.

TURINYS

1. ĮVADAS 6
1.1. Apžvalga 6
1.2. Dokumento pavadinimas ir identifikavimas 8
1.3. Viešųjų raktų infrastruktūros dalyviai 8
1.3.1. Sertifikavimo tarnybos 8
1.3.2. Registravimo tarnybos 9
1.3.3. Abonentai ir sertifikatų savininkai 9
1.3.4. Pasitikinčios šalys 9
1.4. Sertifikatų naudojimas 9
1.4.1. Tinkamas sertifikatų naudojimas 9
1.4.2. Draudžiamas sertifikatų naudojimas 10
1.5. Šių taisyklių valdymas 11
1.5.1. CP patvirtinusi ir tvarkanti organizacija 11
1.5.2. Kontaktinis asmuo 11
1.5.3. Informacija apie CA teikiamas paslaugas 11
1.6. Apibrėžimai ir sutrumpinimai 11
2. SERTIFIKAVIMO INFORMACIJOS SKELBIMAS IR SAUGYKLOS 16
2.1. Saugyklos 16
2.2. Sertifikavimo informacijos skelbimas 16
2.3. Informacijos skelbimo terminai ir dažnumas 17
3. IDENTIFIKAVIMAS IR AUTENTIKAVIMAS 17
3.1. Vardai 17
3.2. Tapatybės patvirtinimas 17
3.2.1. Juridinio asmens tapatybės patvirtinimas 17
3.2.2. Fizinio asmens tapatybės patvirtinimas 18
3.2.3. Netikrinami abonento duomenys 19
3.3. Identifikavimas ir autentikavimas užsakant naują raktų porą (Re-key Requests) 19
3.4. Identifikavimas ir autentikavimas stabdant ar atšaukiant sertifikatų galiojimą 19
4. REIKALAVIMAI SERTIFIKATŲ GYVAVIMO CIKLUI 19
4.1. Prašymų išduoti sertifikatus teikimas 19
4.2. Prašymų išduoti sertifikatus apdorojimas 20
4.2.1. Identifikavimo ir autentikavimo funkcijų vykdymas 20
4.2.2. Informacijos apie sertifikatų sudarymo ir tvarkymo sąlygas teikimas 20

4.2.3. Prašymų išduoti sertifikatus priėmimas ir atmetimas 21
4.2.4. Prašymų išduoti sertifikatus apdorojimo terminai 22
4.3. Sertifikatų sudarymas 22
4.4. Sudarytų sertifikatų išdavimas 23
4.5. Kriptografinių raktų porų ir sertifikatų naudojimas 23
4.6. Sertifikatų atnaujinimas 24
4.7. Naujos raktų poros išduotam sertifikatui kūrimas (Certificate Re-key) 25
4.8. Išduoto sertifikato duomenų keitimas 25
4.9. Sertifikatų galiojimo sustabdymas ir atšaukimas 25
4.10. Sertifikatų galiojimo statuso patikrinimo paslaugos 26
4.11. Sertifikatų naudojimo terminai 26
4.12. Kriptografinių raktų saugojimas ir atkūrimas 26
5. ĮRANGOS, VALDYMO IR VEIKLOS PROCESŲ KONTROLĖ 27
5.1. Fizinės apsaugos kontrolė 27
5.1.1. Turto inventorizacija ir valdymas 27
5.2. Procedūrų kontrolė 27
5.2.1. Prieigos prie sistemų valdymas 28
5.2.2. Patikimų sistemų vystymas ir palaikymas 29
5.3. Personalo kontrolė 29
5.3.1. Personalo patikimumo kontrolė 29
5.3.2. Darbuotojų tikrinimo procedūra 30
5.3.3. Reikalavimai mokymams 30
5.4. Žurnalinių įrašų registravimas 30
5.5. Žurnalinių įrašų archyvavimas 31
5.6. Veiklos sutrikimų ir tęstinumo valdymas 32
5.7. CA veiklos nutraukimas 32
6. TECHNINĖS SAUGUMO KONTROLĖS PRIEMONĖS 33
6.1. Raktų porų generavimas ir diegimas 33
6.1.1. Kriptografinių raktų porų generavimas CA išduodamiems sertifikatams 33
6.1.2. CA kriptografinių raktų generavimas 33
6.1.3. Privataus rakto perdavimas sertifikato savininkui 33
6.1.4. Privataus rakto perdavimas sertifikatų išdavėjui 34
6.1.5. CA viešojo rakto perdavimas pasitikinčioms šalims 34
6.1.6. Kriptografinių raktų dydžiai 34
6.1.7. Kriptografinių raktų parametrų generavimas ir kokybės tikrinimas 35

6.1.8. Raktų naudojimo paskirtis 35
6.2. Privataus rakto apsauga ir kriptografinių modulių techninė kontrolė 35
6.2.1. Kriptografinių modulių standartai ir kontrolė 35
6.2.2. CA raktų perdavimas trečioms šalims (*key escrow*) 35
6.2.3. CA privačių kriptografinių raktų atsarginių kopijų darymas ir atstatymas 35
6.2.4. Privačių raktų archyvavimas 36
6.2.5. Privataus rakto perdavimas į kriptografinį modulį arba iš jo 36
6.2.6. CA privačiųjų kriptografinių raktų naudojimas 36
6.2.7. CA kriptografinių raktų gyvavimo ciklo pabaiga 36
6.2.8. Kriptografinės įrangos, naudojamos sertifikatams pasirašyti, gyvavimo ciklas 36
6.3. Kiti raktų poros valdymo aspektai 37
6.3.1. Viešųjų raktų archyvavimas 37
6.3.2. Sertifikatų ir juos atitinkančių raktų porų naudojimo terminai 37
6.4. Kriptografinių raktų aktyvavimo duomenys 37
6.5. Kompiuterių saugumo kontrolė 38
6.6. Kompiuterinių sistemų gyvavimo ciklo saugumo kontrolė 38
6.7. Kompiuterių tinklo saugumo kontrolė 38

7. SERTIFIKATŲ, CRL IR OCSP PROFILIAI 38
7.1. Sertifikatų profiliai 38
7.2. CRL profilis 38
7.3. OCSP profilis 38

8. ATITIKTIES AUDITAS BEI KITI VERTINIMAI 38

9. KITI TEISINIAI BEI VEIKLOS ASPEKTAI 39
9.1. Paslaugų kainos 39
9.2. Finansinė atsakomybė 39
9.2.1. Kompensacijos sertifikatų naudotojams 39
9.3. Veiklos informacijos konfidencialumas 39
9.4. Asmens duomenų apsauga 39
9.5. Intelektinės nuosavybės apsauga 40
9.6. Pareiškimai ir garantijos 40
9.6.1. CA pareiškimai ir garantijos 40
9.6.2. RA pareiškimai ir garantijos 41
9.6.3. Abonentų ir sertifikatų savininkų pareiškimai ir garantijos 42
9.6.4. Pasitikinčių šalių pareiškimai ir garantijos 42
9.6.5. Kitų šalių pareiškimai ir garantijos 42

9.7. Garantijų atsisakymas....42
9.8. Atsakomybės ribojimas....43
9.9. Nuostolių atlyginimas....43
9.10. Galiojimas....43
9.11. Individualūs pranešimai ir komunikavimas....44
9.12. CP pakeitimai....44
9.13. Ginčų sprendimo procedūros....45
9.14. Taikytina teisė....45
9.15. Atitiktis taikomai teisei....45
9.16. Kitos nuostatos....46
9.16.1. RA funkcijų delegavimo ir paslaugų teikimo sutartys....46
9.16.2. Baigiamosios nuostatos....46

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** sudarymo, tvarkymo bei **kvalifikuotų elektroninių laiko žymų** paslaugas.

Sertifikatai sudaromi ir tvarkomi bei kvalifikuotos elektroninės laiko žymos sudaromos Lietuvos Respublikos teritorijoje.

1.1. Apžvalga

Registrų centro sertifikavimo veiklos taisyklės (toliau – CP) – nustato pagrindinius reikalavimus, kurių turi būti laikomasi sudarant ir išduodant skaitmeninius sertifikatus. CP apibrėžia reikalavimus sudarant ir išduodant:

- Kvalifikuotą elektroninio parašo skaitmeninį sertifikatą **QSignC-ClS-QSCD**, kuris gali būti naudojamas tik su fiziniam asmeniui išduodamu kvalifikuoto elektroninio parašo kūrimo įrenginiu - QSCD, į kurį yra įrašytas privatus raktas, susietas su sertifikate esančiu viešu raktu. QSCD įrenginį savo valia pilnai valdo asmuo, kuriam jis yra išduotas. Reikalavimai sertifikato sudarymui ir išdavimui nustatyti vadovaujantis ETSI EN 319 411-2 standarto QCP-n-qscd taisyklėmis.

- 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 vadovaujantis ETSI EN 119 431-1 standarto EUCSP taisyklėmis.

- Autentikavimo elektroninėje erdvėje sertifikatą **QAuthC-ClS-QSCD**, kuris gali būti naudojamas tik su fiziniam asmeniui išduodamu kvalifikuoto elektroninio parašo kūrimo įrenginiu, į kurį yra įrašytas privatus raktas, susietas su sertifikate esančiu viešu raktu. QSCD įrenginį savo valia pilnai valdo asmuo, kuriam jis yra išduotas. Reikalavimai sertifikato sudarymui ir išdavimui nustatyti vadovaujantis ETSI EN 319 411-2 standarto QCP-n-qscd taisyklėmis.

- Autentikavimo elektroninėje erdvėje sertifikatą **QAuthC-ClS-SSCD**, kuris gali būti naudojamas tik su fiziniam asmeniui išduodamu saugiu kriptografiniu įrenginiu, į kurį yra įrašytas

privatus raktas, susietas su sertifikate esančiu viešu raktu. Saugų kriptografinį įrenginį savo valia pilnai valdo asmuo, kuriam jis yra išduotas. Reikalavimai sertifikato sudarymui ir išdavimui nustatyti vadovaujantis ETSI EN 319 411-1 standarto NCP + taisyklėmis.

- Kvalifikuotą elektroninio spaudo skaitmeninį sertifikatą **QSealC-ClS-QSCD**, kuris gali būti naudojamas tik su juridiniam asmeniui išduodamu kvalifikuoto elektroninio spaudo kūrimo įrenginiu QSCD, į kurį yra įrašytas privatus raktas, susietas su sertifikate esančiu viešu raktu. QSCD įrenginį savo valia pilnai valdo juridinis asmuo, kuriam jis yra išduotas. Reikalavimai sertifikato sudarymui ir išdavimui nustatyti vadovaujantis ETSI EN 319 411-2 standarto QCP-l-qscd taisyklėmis.

- Kvalifikuotą elektroninio spaudo skaitmeninį sertifikatą **QSealC-l**, kuris gali būti išduodamas tik juridiniam asmeniui ir naudojamas pažangiems elektroniniams spaudams kurti, kaip yra numatyta 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 reglamento (toliau – eIDAS) 36 ir 37 straipsniuose. Reikalavimai sertifikato sudarymui ir išdavimui nustatyti vadovaujantis ETSI EN 319 411-2 standarto QCP-l taisyklėmis.

- Kvalifikuotą elektroninio spaudo skaitmeninį sertifikatą **QSealC-R-QSCD**, kuris gali būti naudojamas tik su nuotolinio kvalifikuoto elektroninio spaudo kūrimo įrenginiu R-QSCD, į kurį yra įrašytas privatus raktas, susietas 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 vadovaujantis ETSI EN 119 431-1 standarto EUCSP taisyklėmis.

- 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 vadovaujantis ETSI EN 319 411-1 standarto OVCP taisyklėmis.

- Juridiniam asmeniui TSL/SSL sertifikatą **OVC**. Reikalavimai sertifikato sudarymui ir išdavimui nustatyti vadovaujantis ETSI EN 319 411-1 standarto OVCP taisyklėmis.

QSignC-ClS-QSCD, **QSignC-R-QSCD**, **QAuthC-ClS-QSCD**, **QSealC-ClS-QSCD, QSealC-R-QSCD** sertifikatai išduodami tik kvalifikuoto elektroninio parašo ir kvalifikuoto elektroninio spaudo kūrimo įrenginiams, atitinkantiems eIDAS nustatytus reikalavimus.

CP yra parengtos lietuvių ir anglų kalbomis. CP struktūra sudaryta vadovaujantis RFC 3647 standarte ,,Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework" nustatytais reikalavimais. CP apibrėžtų sertifikatų sudarymo ir išdavimo reikalavimų įgyvendinimas detalizuotas atskiruose Registrų centro sertifikavimo veiklos nuostatuose – CPS (Certification Practice Statement).

1.2. Dokumento pavadinimas ir identifikavimas

Šių CP unikalus identifikatorius (OID – Object identifier) yra **1.3.6.1.4.1.30903.1.5.1**.

CP unikalaus identifikatoriaus laukų reikšmės nurodytos lentelėje Nr. 1.

Lentelė Nr. 1. CP unikalaus identifikatoriaus laukų reikšmės

Pavadinimas	**Reikšmė**
ISO	1
ISO pripažinta organizacija	3
JAV Gynybos departamentas	6
Internetas	1
Privati įmonė	4
IANA registruota privati įmonė	1
Registrų centras	30903
Padalinys (RCSC)	1
Dokumento tipas (Sertifikavimo veiklos taisyklės)	5
Dokumento versija	1

Naujausia CP 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 elektroninėje 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".

[1] https://ltid.lt

1.3.2. Registravimo tarnybos

Registravimo tarnyba (RA) vykdo sertifikatų naudotojų identifikavimą ir autentifikavimą, priima jų prašymus išduoti ir atnaujinti sertifikatus, stabdyti jų galiojimą, gamina ir išduoda fizinius SSCD/QSCD įrenginius.

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

Registravimo tarnybos ir jų atliekamos funkcijos detalizuotos Registrų centro veiklos, sudarant ir išduodant 1.4.1. apibrėžtus skaitmeninius sertifikatus, nuostatuose – CPS. Kiekvieno skaitmeninio sertifikato ar jų grupės sudarymo ir išdavimo veiklą gali reglamentuoti atskiri CPS.

1.3.3. Abonentai ir sertifikatų savininkai

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

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

Galimi abonentai ir sertifikatų savininkai bei jų dalyvavimas sertifikatų sudarymo ir išdavimo procese detalizuotas atitinkamuose skaitmeninių sertifikatų CPS.

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 šį CP sudaromi ir tvarkomi:

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

b) **QAuthC-ClS-QSCD** ir **QAuthC-ClS-SSCD** autentifikavimo sertifikatai, skirti asmens tapatybei elektroninėje erdvėje nustatyti bei saugiam informacijos apsikeitimui elektroniniu paštu;

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

d) **QSealC-I** kvalifikuoti elektroninio spaudo sertifikatai, skirti pažangiems elektroniniams spaudams tvirtinti;

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

f) **OVC** TSL/SSL sertifikatai, skirti patvirtinti organizacijos tapatybę bei informacinių sistemų užklausų autentiškumą, organizuojant sąveiką tarp skirtingų organizacijų informacinių technologijų infrastruktūros.

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

QSignC-ClS-QSCD, **QSignC-R-QSCD**, **QAuthC-ClS-QSCD**, **QAuthC-ClS-SSCD**, **QSealC-ClS-QSCD**, **QSealC-R-QSCD** sertifikatai sudaromi į:

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

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

c) HSM tipo QSCD įtaisas;

d) CA valdomą nuotolinio kvalifikuoto elektroninio parašo ir spaudo kūrimo įrenginį (remote electronic signature and seal creation device) .

QSealC-l , **OVC** TSL/SSL bei **R_SIC** sertifikatai C gali būti išduodami ir į nekvalifikuotus įtaisus.

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:

- bet kokiai neteisėtai veiklai (įskaitant kibernetines atakas, bandymus klastoti asmens tapatybę ir pan.);
- išduoti (patvirtinti) kitus naujus skaitmeninius sertifikatus;
- patvirtinti informaciją apie šio ar kitų sertifikatų galiojimą;
- netikrų dokumentų ar informacijos (pvz., dokumentų skirtų sistemų ar procesų testavimui) elektroninių parašų patvirtinimui.

QSealC-l, OVC TSL/SSL bei **R-SIC** sertifikatai negali būti naudojami elektroninių dokumentų, duomenų ar transakcijų tvirtinimui kvalifikuotu elektroniniu parašu ar spaudu.

Autentifikavimo sertifikatai, skirti asmens tapatybei elektroninėje erdvėje nustatyti, negali būti naudojami kvalifikuotiems elektroniniams parašams kurti.

1.5. Šių taisyklių valdymas

1.5.1. CP 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 CP administravimą atsakingas asmuo:

Valstybės įmonės Registrų centro El. 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, CPS, TSP bei TSPS versijos.

1.6. Apibrėžimai ir sutrumpinimai

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

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

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

Atšauktų sertifikatų sąrašas (CRL – Certificate / Seal Revocation List) – Registrų centro periodiškai (arba neatidėliotinai) leidžiamas, jo pasirašomas sąrašas sertifikatų, kurių galiojimas nutrauktas ar sustabdytas. 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.

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

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

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

Kriptografinis modulis – 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.

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

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

Kvalifikuotas elektroninio parašo arba elektroninio spaudo kūrimo įtaisas (SSCD/QSCD – Qualified Signature (Seal) Creation Device) – elektroninio parašo arba elektroninio spaudo kūrimo įtaisas (sukonfigūruota programinė arba aparatinė įranga, naudojama elektroniniam parašui arba elektroniniam spaudui kurti), atitinkantis eIDAS nustatytus reikalavimus kvalifikuotiems elektroninio parašo arba elektroninio spaudo kūrimo įtaisams.

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

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

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

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

Kvalifikuotų sertifikatų (elektroninių parašų ir elektroninių spaudų) taisyklės (Qualified Certificate / Seal Policy – CP) – sertifikatų sudarymo ir naudojimo taisyklės, parengtos pagal eIDAS reikalavimus, nustatančios 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".

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

Naudotojai – sertifikatų savininkai ir sertifikatais pasitikinčios šalys.

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

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

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

Privatusis raktas – unikalūs duomenys, kuriuos asmuo naudoja kurdamas elektroninį parašą / 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.

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

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

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).

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

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).
CDB	Sertifikatų duomenų bazė
CP	Registrų centro kvalifikuotų sertifikatų (elektroninių parašų ir elektroninių spaudų) taisyklės (Qualified Certificate (Electronic Signature and Electronic Seal) Policy)
CPS	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)
LAN	Vietinis kompiuterių tinklas (Local Area Network)
LST	Lietuvos standartizacijos tarnyba
OID	Unikalus objekto identifikatorius (Object Identifier)
OCSP	Tiesioginės prieigos protokolas informacijai apie sertifikato statusą gauti (Online Certificate Status Protocol)
QSCD	Kvalifikuotas elektroninio parašo arba elektroninio spaudo kūrimo įtaisas
PIN	Asmens identifikacinis skaičius (Personal Identification Number)
PKI	Viešojo rakto infrastruktūra (Public Key Infrastructure)

RA	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	Komentarų standartizavimo tarnyba (Request For Comments)
RSA	RSA asimetrinio šifravimo algoritmas *(Rivest-Shamir-Adelman algorithm)*
SHA-1	Saugus elektroninių duomenų santraukos gavimo algoritmas 1 *(Secure Hash Algorithm 1)*
SHA-256	Saugus elektroninių duomenų santraukos gavimo algoritmas 256 *(Secure Hash Algorithm 2561)*
UPS	Atsarginis energijos šaltinis *(Uninterrupted Power Supply)*
TSP	Laiko žymos teikimo taisyklės (*Time-Stamping Policy*)
TSPS	Laiko žymos teikimo veiklos nuostatai (*Time-Stamping Practice Statement*)

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:

- Šakninės sertifikavimo tarnybos (Root CA), Darbinės sertifikavimo tarnybos (Issuing CA), laiko žymų tarnybos (TSA) sertifikatus;
- CA išduotų ir atšauktų sertifikatų duomenis;
- Registrų centro kvalifikuotų sertifikatų (elektroninių parašų ir elektroninių spaudų) taisykles – CP (Certificate Policy), Registrų centro sertifikavimo veiklos nuostatus – CPS (Certification Practice Statement) – elektroninio parašo sertifikatų sudarymo, išdavimo ir naudojimo bei e. spaudo sertifikatų sudarymo, išdavimo ir naudojimo sąlygas;
- instrukcijas naudotojams;
- įgaliotų institucijų parengtos CA veiklos tikrinimo ataskaitų santraukas.

CP ir CPS skelbiama 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, elektroninio parašo sertifikatų sudarymo ir išdavimo bei elektroninio parašo sertifikatų sudarymo, išdavimo ir naudojimo sąlygos 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 10 darbo dienų.

3. Identifikavimas ir autentikavimas

3.1. Vardai

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 ITU-T X.500 ir ETSI EN 319 412 standartų rekomendacijų.

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

3.2. Tapatybės patvirtinimas

CA turi patikrinti abonento pateiktų duomenų tapatumą, lyginant juos su Gyventojų ir Juridinių asmenų registre arba kitos Europos Sąjungos (toliau – ES) šalies narės, Islandijos, Lichtenšteino ar Norvegijos, verslo registre (toliau - ES šalių verslo registrai) esančia informacija. Taip pat CA turi užtikrinti, kad užsakymas išduoti skaitmeninį sertifikatą būtų pateiktas autorizuoto tai atlikti asmens, bei užsakyme būtų pateikti visi duomenys (įrodymai), reikalingi asmens tapatybės patvirtinimui.

Asmens tapatybės patvirtinimas gali būti atliekamas priimant užsakymą išduoti sertifikatą arba išduodant elektroninio parašo ar spaudo kūrimo įrenginį. Asmens tapatybės patvirtinimas turi būti atliekamas laikantis ETSI TS 119 461 specifikacijos reikalavimų.

3.2.1. Juridinio asmens tapatybės patvirtinimas

Užsakant QSealC-I, QSealC-ClS-QSCD ir QSealC-R-QSCD kvalifikuotus elektroninio spaudo sertifikatus Juridinių asmenų registre arba ES šalių verslo registruose turi būti pateikiamas juridinio

asmens pavadinimas ir kodas, juridinio asmens vadovo ar kito fizinio asmens, turinčio teisę atstovauti šį juridinį asmenį, duomenys – vardas, pavardė, asmens identifikacinis numeris, asmens tapatybės dokumento numeris, įgaliojimo duomenys (jei užsakymą teikia ne organizacijos vadovas), elektroninio pašto adresas bei mobilaus telefono numeris. Išduodant šiuos sertifikatus yra tikrinama juridinio asmens tapatybė bei užsakyme pateikti duomenys, taip pat yra tikrinama juridinį asmenį atstovaujančio fizinio asmens tapatybė bei jo teisė atstovauti įmonę užsakant ir atsiimant sertifikatus.

Juridinį asmenį atstovaujančio fizinio asmens tapatybė patvirtinama vienu iš šių būdų:

- asmeniui fiziškai atvykus į RA padalinį;
- nuotoliniu būdu, užsakymą išduoti sertifikatą patvirtinus galiojančiu kvalifikuotu elektroniniu parašu.

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

Juridinių asmenų, juos galinčių atstovauti fizinių asmenų tapatybė ir jų įgaliojimų duomenys tikrinami pagal LR Juridinių asmenų registre esančią informaciją.

Užsakant **OVC** sertifikatus Juridinių asmenų registre turi būti pateikiamas juridinio asmens pavadinimas ir kodas. Juridinio asmens tapatybė patikrinama pagal bankinio pavedimo, kurio apmokama išankstinės sąskaita, duomenis. Juridinį asmenį atstovaujančio fizinio asmens, teikiančio užsakymą, tapatybė patvirtinama pagal jo viešai skelbiamą elektroninio pašto domeno atitiktį.

3.2.2. Fizinio asmens tapatybės patvirtinimas

Užsakant **QSignC-ClS-QSCD** ir **QSignC-R-QSCD** kvalifikuotus elektroninio parašo bei **QAuthC-ClS-QSCD** ir **QAuthC-ClS-SSCD** autentifikavimo sertifikatus turi būti pateikiama fizinio asmens vardas, pavardė, asmens identifikacinis numeris, asmens tapatybės dokumento numeris, elektroninio pašto adresas bei mobilaus telefono numeris. Išduodant šiuos sertifikatus yra tikrinama fizinio asmens, kurio vardu sudaromi sertifikatai, tapatybė bei užsakyme pateikti duomenys. Fizinio asmens tapatybė patvirtinama vienu iš šių būdų:

- asmeniui fiziškai atvykus į RA padalinį;
- nuotoliniu būdu, užsakymą išduoti sertifikatą patvirtinus galiojančiu kvalifikuotu elektroniniu parašu;
- nuotoliniu būdu, asmens tapatybę patvirtinat banko transakcijos autentikacijos TAN (TAN – transaction authentication number) kodu;
- nuotoliniu būdu, naudojant asmens veido biometrinius duomenis. Šis būdas gali būti naudojamas tik tuo atveju, jeigu tam yra naudojama ETSI TS 119 461 specifikacijos reikalavimus atitinkanti asmens tapatybės patvirtinimo programinė, techninė ir organizacinė infrastruktūra;

- nuotoliniu būdu, pasinaudojant išorinio asmens tapatybės patvirtinimo paslaugų tiekėjo, užtikrinančio pakankamą arba aukštą saugumo lygį, kuris yra numatytas eIDAS reglamento 8 straipsnyje, paslaugomis;
- nuotoliniu būdu, panaudojant asmens elektroninės atpažinties priemones, kurios užtikrina pakankamą arba aukštą saugumo lygį pagal eIDAS reglamento 8 straipsnį.

Asmens duomenys tikrinami pagal Gyventojų ir Užsieniečių registre esančią informaciją.

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

3.2.3. Netikrinami abonento duomenys

Užsakant OVC sertifikatus prisijungimui prie Registrų centro tvarkomų informacinių sistemų abonento duomenys nėra tikrinami.

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

Taikomi 3.2 papunktyje nustatyti reikalavimai.

3.4. Identifikavimas ir autentikavimas stabdant ar atšaukiant sertifikatų galiojimą

CA turi užtikrinti prašymų sustabdyti ar nutraukti sertifikato galiojimą autentiškumo patikrinimą. CA išduotų sertifikatų sustabdymo ir atšaukimo procedūros apibrėžtos atitinkamo tipo sertifikatų CPS.

Šio skyriaus reikalavimai taikomi tik QSealC-I, QSignC-ClS-QSCD, QSignC-R-QSCD, QSealC-ClS-QSCD, R-SIC ir QSealC-R-QSCD sertifikatų galiojimo ir sustabdymo atvejais.

4. Reikalavimai sertifikatų gyvavimo ciklui

4.1. Prašymų išduoti sertifikatus teikimas

Prieš pateikiant 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.

Prašymą išduoti **QSealC-I**, **QSealC-ClS-QSCD**, **QSealC-R-QSCD** ir **OVC** sertifikatus gali pateikti ne jaunesnis kaip 18 metų, o **QSignC-ClS-QSCD**, **QSignC-R-QSCD**, **QAuthC-ClS-QSCD**, **QAuthC-ClS-SSCD** sertifikatus ne jaunesnis kaip 14 metų amžiaus fizinis asmuo.

Užsakymą išduoti **QSealC-I**, **QSealC-ClS-QSCD**, **QSealC-R-QSCD** tipo sertifikatus gali pateikti tik Juridinių asmenų registre ar ES šalių verslo registruose įregistruotos įmonės įgaliotas atstovas.

Prašymas išduoti sertifikatus gali būti pateiktas atvykus į RA arba elektroniniu būdu. Abonentas prašyme turi pateikti pakankamą kiekį duomenų, leidžiančių CA ir RA vienareikšmiškai nustatyti jo tapatybę. Visais atvejais CA ir RA turi užtikrinti prašyme pateiktų duomenų autentiškumo patikrinimą pagal informaciją, esančią Lietuvos Respublikos valstybės registruose ar asmens elektroninės atpažinties priemonėje, kuri užtikrina pakankamą arba aukštą saugumo lygį pagal eIDAS reglamento 8 straipsnyje esančias nuostatas. Elektroniniu būdu priimant prašymą išduoti sertifikatą, turi būti patikrintas prašyme nurodyto mobilaus telefono numerio ir / ar elektroninio pašto adreso priklausymas abonentui bei jo gebėjimas valdyti šiuos įrenginius.

CA turi užtikrinti, kad sudarytame sertifikate esantys duomenys pilnai atitiktų prašyme esančius.

4.2. Prašymų išduoti sertifikatus apdorojimas

4.2.1. Identifikavimo ir autentikavimo funkcijų vykdymas

CA turi užtikrinti, kad sertifikatus išduoti prašantys asmenys būtų tinkamai identifikuoti, t .y. turi būti tinkamai patikrinta šių asmenų tapatybė ir, jei taikytina, specifiniai jų požymiai, taip pat CA privalo užtikrinti pateiktų prašymų teisėtumą, pilnumą ir autentiškumą.

Patikimam abonento asmens tapatybės patvirtinimui ir prašymo duomenų autentiškumui užtikrinti CA ir RA turi turėti kvalifikuotą personalą, saugias taikomąsias sistemas bei prieigą prie Lietuvos Respublikos valstybės registruose saugomos informacijos, būtinos vienareikšmiškai identifikuoti asmenį, kuriam prašoma išduoti sertifikatą.

Užsakant **QSignC-R-QSCD** ir **QSealC-R-QSCD** sertifikatus fizinio asmens tapatybė tikrinama jam teikiant prašymą, visais kitais atvejais tapatybės patikrinimas gali būti atliekamas teikiant prašymą arba išduodant elektroninio parašo ar spaudo įrenginį. **R-SIC** sertifikatai išduodami patvirtinus asmens tapatybę **QSignC-R-QSCD** ir **QSealC-R-QSCD** sertifikatų išdavimo proceso metu.

Detaliau asmens tapatybės patvirtinimo ir prašymų duomenų autentiškumo užtikrinimo procedūros apibrėžtos atitinkamo tipo sertifikatų CPS.

Šio skyriaus reikalavimai netaikomi abonentui užsakant ir išduodant **OVC** sertifikatus.

4.2.2. Informacijos apie sertifikatų sudarymo ir tvarkymo sąlygas teikimas

CA turi užtikrinti, kad sertifikatų naudotojai būtų informuoti apie sertifikatų sudarymo ir tvarkymo sąlygas. CA privalo:

a) aiškiai nurodyti, kokios CP ir CPS yra taikomos;

b) informuoti apie sertifikatų naudojimo ribojimus;

c) informuoti apie sertifikatų naudotojų įsipareigojimus;

d) teikti informaciją, kaip tikrinti sertifikatų galiojimą;

e) informuoti apie CA prisiimamą atsakomybę ir jos ribojimus;

f) informuoti apie registravimo metu surinktos informacijos laikymo periodą;

g) informuoti apie laikotarpio, kurį laikomi CA veiklos duomenys, trukmę;

h) informuoti apie ginčų sprendimo procedūras;

i) taikyti su veikla susijusius teisės aktus.

Visa ši informacija turi būti teikiama visiems prieinama forma, pateikiama aiškiai ir suprantamai.

4.2.3. Prašymų išduoti sertifikatus priėmimas ir atmetimas

Prašymas išduoti sertifikatą yra atmetamas jeigu:

- prašymą išduoti **QSealC-l**, **QSealC-ClS-QSCD**, **QSealC-R-QSCD** ir **OVC** sertifikatus pateikė jaunesnis negu 18 metų amžiaus fizinis asmuo;
- prašymą išduoti **QSignC-ClS-QSCD**, **QSignC-R-QSCD, QAuthC-ClS-QSCD, QAuthC-ClS-SSCD** sertifikatus pateikė jaunesnis negu 14 metų amžiaus fizinis asmuo;
- prašyme yra pateikti ne visi privalomi duomenys;
- asmuo nepatvirtino susipažinimo ir sutikimo su sertifikatų užsakymo, išdavimo ir naudojimo sąlygomis;
- fizinis asmuo, prašantis išduoti **QSignC-ClS-QSCD**, **QAuthC-ClS-QSCD**, **QAuthC-ClS-SSCD** ar **QSealC-ClS-QSCD** sertifikatą, neturi galiojančio Lietuvos Respublikos ar užsienio valstybės išduoto asmens tapatybę patvirtinančio dokumento;
- prašymą išduoti **QSealC-l**, **QSealC-ClS-QSCD** ar **QSealC-R-QSCD sertifikatą** teikiantis asmuo neturi galiojančių įmonės įgaliojimų jos vardu užsakyti ir gauti šiuos sertifikatus;
- prašyme pateikti duomenys neatitinka Lietuvos Respublikos valstybės registruose esančių asmens duomenų;
- prašyme nurodyto asmens tapatybė nėra patvirtinta vienu iš šiame CP nustatytų būdų;
- prašyme nurodyti asmens duomenys nesutampa su asmens duomenimis, gautais asmens tapatybės patvirtinimo metu.

Prašymų išduoti **QSealC-ClS-QSCD** ar **QSealC-R-QSCD** priėmimo ir apdorojimo procesas turi užtikrinti, kad tik abonentas gali kontroliuoti CA išduodamą nuotolinio kvalifikuoto elektroninio parašo bei nuotolinio kvalifikuoto elektroninio spaudo kriptografinių raktų aktyvavimo priemonę, jos sugeneruotą privatų raktą, susietą su privačiu raktu, kuris pateikiamas CA kartu su šios sistemos užklausa išduoti **R-SIC** sertifikatą.

Visais atvejais asmuo turi būti tinkamai informuotas apie jo teikto parašymo atmetimo priežastis.

4.2.4. Prašymų išduoti sertifikatus apdorojimo terminai

Sertifikatų sudarymo ir išdavimo terminai nustatyti atitinkamų paslaugų CPS.

4.3. Sertifikatų sudarymas

CA turi užtikrinti saugų sertifikatų sudarymą, leidžiantį išlaikyti autentiškus sertifikatus. Sertifikatų sudarymo procesas ir sudaryti sertifikatai turi atitikti šiuos reikalavimus:

a) sertifikatų sudarymo procedūra turi būti saugiai susieta su kitomis susijusiomis sertifikatų gyvavimo ciklo procedūromis;

b) asmens raktų poros generavimo procedūra turi būti saugiai susieta su sertifikato sudarymo procedūra;

c) **QSignC-ClS-QSCD**, **QAuthC-ClS-QSCD**, **QAuthC-ClS-SSCD** ar **QSealC-ClS-QSCD** sertifikatai sudaromi į SSCD/QSCD, atitinkančius eIDAS 29– 30 straipsniuose, 39 straipsnio 1–2 dalyse ir 51 straipsnio nustatytus reikalavimus;

d) sertifikatų savininkams sudaryti **QSignC-R-QSCD** ir **QSealC-R-QSCD** išsaugomi CA valdomame R-QSCD įrenginyje, kurį valdo kvalifikuotas patikimumo užtikrinimo paslaugos teikėjas pasirašančio asmens, kuriam sertifikatas yra išduotas, vardu ir kuris turi būti susietas su asmeniui išduotomis jų aktyvavimo nuotoliniu būdu priemonėmis ir joms išduotu R-SIC sertifikatu;

e) išduodant **QSignC-ClS-QSCD**, **QAuthC-ClS-QSCD**, **QAuthC-ClS-SSCD** ar **QSealC-ClS-QSCD** sertifikatus parengti SSCD/QSCD turi būti saugiai perduodami sertifikatų savininkui;

f) **R-SIC** sertifikatai sudaromi tik išduodant **QSignC-R-QSCD** ir **QSealC-R-QSCD** sertifikatus, raktų pora generuojama ir CA išduotoje nuotolinio parašo / spaudo kriptografinių raktų aktyvavimo priemonėje, o sertifikatai saugomi CA valdomame R-QSCD įrenginyje.

g) sudarant **OVC** ir **QSealC-l** sertifikatus kriptografinių raktų pora generuojama CA valdomoje infrastruktūroje, sertifikatas ir raktų pora sertifikato savininkui perduodama saugiu, su juo suderintu būdu;

h) sudarytuose sertifikatuose nurodyti asmens identifikaciniai duomenys turi būti unikalūs visų CA sudarytų sertifikatų apimtyje ir nepriskiriami kitam asmeniui;

i) turi būti užtikrintas sertifikatų sudarymo duomenų konfidencialumas ir integralumas visą sertifikato gyvavimo ciklą;

j) CA turi užtikrinti registravimo tarnybų patikimumą ir saugų duomenų apsikeitimą su išorinėmis registravimo tarnybomis.

Sudaryti sertifikatai turi atitikti eIDAS bei Lietuvos Respublikos teisės aktų, reglamentuojančių patikimumo užtikrinimo paslaugas (tiek, kiek neprieštarauja eIDAS), reikalavimus.

4.4. Sudarytų sertifikatų išdavimas

CA turi užtikrinti, kad:

a) po sertifikatų sudarymo pilni ir tikslūs sertifikatai būtų perduoti jų savininkui arba suteikta autorizuota prieiga prie jų;

b) sertifikatų naudotojams būtų pateiktos sertifikatų sudarymo ir tvarkymo sąlygos ir jas būtų galima lengvai identifikuoti konkretaus sertifikato atveju;

c) punkte b) įvardintą informaciją teikti 24 (dvidešimt keturias) valandas per parą, 7 (septynias) dienas per savaitę. Esant veiklos sutrikimams, CA turi dėti visas įmanomas pastangas veiklai atstatyti.

CA viešai neskelbia sertifikatų savininkams išduotų sertifikatų duomenų.

Naujai sugeneruotų **QSealC-I**, **QSignC-ClS-QSCD**, **QAuthC-ClS-QSCD**, **QAuthC-ClS-SSCD** ar **QSealC-ClS-QSCD** sertifikatų galiojimas turi būti sustabdytas ir jie turi būti įtraukti į atšauktų sertifikatų sąrašą. Jų galiojimas turi būti aktyvuojamas iš karto po to, kai sertifikato savininkas sutinka su sertifikatų užsakymo, išdavimo ir naudojimo sąlygomis, ir jam perduodamas elektroninio parašo / spaudo kūrimo įrenginys. Prieš perduodant elektroninio parašo / spaudo kūrimo įrenginį RA papildomai patikrinamas išduodame sertifikate įrašytų duomenų teisingumas. CA turi užtikrinti saugų kriptografinių raktų aktyvavimo kodų perdavimą sertifikatų savininkui.

Kai sugeneruojami nauji **QSignC-R-QSCD** ir **QSealC-R-QSCD** sertifikatai, apie tai sertifikatų savininkui turi būti pranešta, o jis nedelsdamas naudodamasis CA išduotų nuotolinio parašo / spaudo kriptografinių raktų aktyvavimo priemonėmis turi patvirtinti sertifikatų duomenų teisingumą ir sutikimą su sertifikatų užsakymo, išdavimo ir naudojimo sąlygomis. Priešingu atveju naujai sugeneruotų sertifikatų galiojimas yra atšaukiamas.

CA turi užtikrinti sertifikatų savininkų sutikimų su sertifikatų užsakymo, išdavimo ir naudojimo sąlygomis saugojimą. Saugojimo terminas apibrėžiamas atitinkamo tipo sertifikatų CPS.

Naujai sugeneravus **OVC** sertifikatą, CA apie tai informuoja sertifikatų savininką ir sutartu būdu jį perduoda.

4.5. Kriptografinių raktų porų ir sertifikatų naudojimas

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

- užsakant sertifikatus CA teikti aktualius ir teisingus duomenis, reikalingus sertifikato išdavimui;
- pasikeitus įrašytiems į sertifikatą duomenims nedelsiant apie tai informuoti CA;
- išduotą sertifikatą ir atitinkamas kriptografinių raktų poras naudoti pagal paskirtį ir apribojimus, apibrėžtus sertifikato naudojimo sąlygose;

- apsaugoti CA išduotus elektroninio parašo / spaudo kūrimo įrenginius nuo trečių šalių neteisėto naudojimosi jais;
- apsaugoti CA išduotas nuotolinio elektroninio parašo / spaudo kriptografinių raktų aktyvavimo priemones nuo trečių šalių neteisėto naudojimosi jomis;
- neatskleisti CA išduotų kriptografinių raktų aktyvavimo kodų trečiosioms šalims;
- nustoti naudotis išduotais sertifikatais bei raktų pora ir nedelsiant parnešti CA jeigu:
    - buvo prarasta CA išduoto elektroninio parašo / spaudo kūrimo įrenginio kontrolė ar trečiosioms šalims tapo žinomi kriptografinių raktų aktyvavimo kodai;
    - buvo prarasta CA išduotos nuotolinio elektroninio parašo / spaudo kriptografinių raktų aktyvavimo priemonės kontrolė ar trečiosioms šalims tapo žinomi prieigos prie jos kodai.

Jeigu abonentas ir sertifikato savininkas yra skirtingi asmenys, su abonentu turi būti sudaryta papildoma sutartis, kurioje be kitų sąlygų jis turi įsipareigoti:

- neperduoti elektroninio parašo įrangos ir joje esančio privataus kriptografinio rakto aktyvavimo kodų kitiems asmenims, negu ji yra skirta ir išduota;
- užtikrinti, kad abonento valdomose ir tvarkomose IT sistemose elektroninio parašo kūrimo įrenginio privatus kriptografinis raktas būtų aktyvuojamas tik asmens, kuriam šis įrenginys buvo išduotas, laisva valia surinkus PIN kodą;
- organizacinėmis ir techninėmis priemonėmis užtikrinti, kad išduotame elektroninio parašo įtaise esantis privatus kriptografinis raktas būtų naudojamas tik šiame įtaise kriptografinėms funkcijoms atlikti;
- CA nedelsiant pranešti, įvykus bent vienam iš šių įvykių:
    - asmeniui išduota elektroninio parašo ar spaudo įranga buvo pamesta, pavogta, sugadinta ar asmuo kaip nors kitaip prarado jos kontrolę (pvz.: asmuo grąžino įtaisą nutrūkus ar pasikeitus darbiniams santykiams ir pan.);
    - atskleistas ar kaip nors kitaip sukompromituotas įtaise esantis privatus raktas;
    - kitiems asmenis tapo prieinamas ar kitaip buvo atskleistas elektroninio parašo savininkui išduotas elektroninio parašo įrangos aktyvavimo PIN arba PUK kodas;
    - pasikeitė išduotame sertifikate įrašyti asmens duomenys.

4.6. Sertifikatų atnaujinimas

Yra leidžiamas tik išduotų **QSignC-R-QSCD** ir **QSealC-R-QSCD** tipo sertifikatų atnaujinimas. Sertifikatai gali būti atnaujinami jeigu:

- sertifikato galiojimas yra nepasibaigęs, nėra sustabdytas ar atšauktas;
- sertifikato savininkas prašymą atnaujinti sertifikatą pasirašo kvalifikuotu elektroniniu parašu ar spaudu, patvirtintu šiuo sertifikatu;
- sertifikato savininko duomenys įrašyti į prašomą atnaujinti sertifikatą yra nepasikeitę;

- kvalifikuotas elektroninio parašo arba elektroninio spaudo kūrimo įtaisas, kuriame saugomi sertifikato savininko kriptografiniai raktai, užtikrina saugių kriptografinių algoritmų naudojimą;
- 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 galiojimas nutraukiamas tokias atvejais:

1. Sertifikato savininko iniciatyva pateikus CA prašymą nutraukti sertifikatų galiojimą;
2. CA iniciatyva:

a) paaiškėjus, kad sertifikatų duomenys daugiau nėra teisingi;

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

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

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

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

f) vadovaudamasis 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 arba spaudo sertifikatų savininkas likviduojamas, išregistruojamas;

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) SSCD/QSCD nebeatitinka eIDAS reikalavimų;

l) kai abonentas, sertifikato savininkas neatsiima pagamintų sertifikatų per 90 kalendorinių dienų nuo sertifikatų įrašymo į SSCD/QSCD dienos. Sertifikatų užsakymas ir pagaminti sertifikatai – atšaukiami.

3. Teisėsaugos institucijų motyvuotu reikalavimu, siekiant užkirsti kelią nusikalstamoms veikoms.

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

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

- sertifikato savininko, savo iniciatyva teikiant prašymą nutraukti;
- CA savo iniciatyva priėmus sprendimą nutraukti sertifikato galiojimą.

Informacija apie sertifikato galiojimo sustabdymą ar nutraukimą Pasitikinčioms šalims turi būti prieinama ne vėliau kaip per 60 minučių nuo CA ar RA sprendimo sustabdyti ar nuo priėmimo momento nutraukti sertifikato galiojimą.

4.10. Sertifikatų galiojimo statuso patikrinimo paslaugos

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

CA turi sudaryti ir viešai internete skelbti CRL, kuris atnaujinamas ne rečiau kaip kas 24 (dvidešimt keturias) valandas. CRL turi būti pasirašytas CA kvalifikuotu elektroniniu parašu, kiekviename CRL turi būti nurodytas kito CRL išleidimo laikas. Taip pat CA realiu laiku turi teikti sertifikatų galiojimo atšaukimo arba sustabdymo patikrinimo paslaugas OCSP atsakikliu.

Šios paslaugos turi būti prieinamos viešai 24 (dvidešimt keturias) valandas per parą, 7 (septynias) dienas per savaitę. Esant prieinamumo sutrikimams, tiesiogiai nepriklausantiems nuo CA veiklos, CA turi imtis visų įmanomų priemonių, kad šios informacijos neprieinamumo laikotarpis būtų ne ilgesnis nei nurodytas šias CP įgyvendinančiuose CPS.

CA turi užtikrinti skelbiamos informacijos apie išduotų sertifikatų galiojimo sustabdymo ar atšaukimo integralumą bei autentiškumą.

4.11. Sertifikatų naudojimo terminai

Sertifikatų savininkas nutraukia CA išduotų sertifikatų naudojimą, kai 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 straipsnio 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 turi užtikrinti fizinę kritinių CA sistemos vietų apsaugą ir minimizuoti patikimumo užtikrinimo paslaugoms naudojamo turto fizinio sunaikinimo riziką.

CA turi užtikrinti, kad:

a) fizinis patekimas į patalpas, kuriose vykdomos veiklos, susijusios su sertifikatų sudarymu, SSCD/QSCD teikimu ir sertifikatų galiojimo nutraukimu ar sustabdymu, būtų ribojamas ir įmanomas tik įgaliotiems asmenims;

b) įgyvendintos priemonės leistų išvengti turto praradimo, sugadinimo ar sukompromitavimo bei veiklos pertraukimo;

c) įgyvendintos priemonės leistų išvengti informacijos ar informacijos apdorojimo priemonių kompromitacijos ar vagystės;

d) veiklos priemonės, susijusios su sertifikatų sudarymu, SSCD/QSCD teikimu ir sertifikatų galiojimo nutraukimu bei sustabdymu, būtų naudojamos fiziškai apsaugotoje aplinkoje ir būtų apsaugotos nuo kompromitacijos bei neteisėtos prieigos prie sistemos ar duomenų;

e) būtų užtikrinta fizinė apsauga, sukuriant saugias sertifikatų sudarymo, SSCD/QSCD teikimo ir sertifikatų galiojimo nutraukimo bei sustabdymo operacijų atlikimo zonas. Bet kokios patalpos, naudojamos bendrai CA ir kitų padalinių veiklai, būtų šių zonų išorėje;

f) būtų įgyvendintos fizinės ir kitokios apsaugos priemonės, apsaugančios patalpas, patikimumo užtikrinimo paslaugų teikimo sistemą ir kitus paslaugų teikimo resursus nuo stichinių nelaimių, gaisro, vagysčių, elektros energijos tiekimo pertrūkių, komunikacijos tinklų veiklos sutrikimų.

5.1.1. Turto inventorizacija ir valdymas

CA turi užtikrinti, kad jos valdoma informacija ir kitas turtas būtų tinkamai apsaugoti.

CA turi vykdyti viso turto inventorizaciją ir suklasifikuoti turto saugos reikalavimus atsižvelgiant į rizikos veiksnius.

5.2. Procedūrų kontrolė

CA turi užtikrinti patikimumo užtikrinimo paslaugų teikimo sistemos saugų ir tinkamą veikimą bei 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 minimali;

c) CA sistemose naudojami informacijos kaupikliai ir nešėjai būtų apsaugoti nuo gedimų, vagystės, nesankcionuotos prieigos ar susidėvėjimo;

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.

5.2.1. Prieigos prie sistemų valdymas

CA turi užtikrinti prieigą prie CA sistemų tik tinkamai autorizuotam personalui.

CA turi užtikrinti šių bendrųjų prieigos prie sistemų valdymo reikalavimų vykdymą:

a) vidinio CA kompiuterių tinklas neturi būti pasiekiamas išoriniais tinklais;

b) svarbūs duomenys turi būti apsaugoti juos perduodant nesaugiais tinklais;

c) naudotojų prieiga prie sistemų turi būti administruojama (prieigos saugumas palaikymas per naudotojų registracijos duomenų valdymą);

d) prieiga prie sistemų duomenų ir funkcijų yra ribojama atsižvelgiant į prieigos kontrolės taisykles (turi būti užtikrinta ypatingo pasitikėjimo pareigų atskyrimas, atskiriant sistemos administravimo ir operavimo funkcijas);

e) turi būti užtikrintas personalo identifikavimas ir autentifikavimas prieš sertifikatų tvarkymo kritinių procedūrų atlikimą;

f) turi būti užtikrinta darbuotojų veiksmų su CA sistemomis apskaita, pavyzdžiui, fiksuojant ir išsaugant išrašus (*logs*) apie sistemų funkcionalumo naudojimą;

Reikalavimai, keliami sertifikatų generavimui: CA turi užtikrinti, kad:

a) vietinio kompiuterių tinklo komponentai būtų fiziškai apsaugoti ir jų konfigūracija periodiškai audituojama;

b) būtų taikoma nuolatinio stebėjimo ir signalizavimo sistema, sudaranti sąlygas aptikti, registruoti ir laiku reaguoti į bandymus prieiti prie sistemos resursų;

Reikalavimai, keliami sertifikatų išdavimui: CA turi užtikrinti sertifikatų išdavimo sistemos kontrolę bandant pridėti, pašalinti ar pakeisti sertifikatus ir kitą susijusią informaciją.

Reikalavimai, keliami galiojimo nutraukimui ir sustabdymui: CA turi užtikrinti, kad būtų taikoma nuolatinio stebėjimo ir signalizavimo sistema, sudaranti sąlygas aptikti, registruoti ir laiku reaguoti į bandymus pakeisti sertifikato statusą;

Reikalavimai, keliami informacijos apie sertifikatų statusą teikimui: CA turi užtikrinti informacijos apie sertifikatų statusą teikimo sistemos kontrolę bandant pridėti, pašalinti ar pakeisti sertifikatų statusą ir kitą susijusią informaciją bei tinkamą / greitą reakciją į tai.

5.2.2. Patikimų sistemų vystymas ir palaikymas

Įgyvendinant bet kokį sistemos plėtros projektą, saugumo reikalavimų analizė yra atliekama projektavimo ir poreikių specifikavimo etape. CA turi užtikrinti saugumo valdymo priemonių realizavimą kiekvienoje su patikimumo užtikrinimo paslaugų teikimo veikla susijusioje IT sistemoje.

Turi būti nustatytos pokyčių, susijusių su programinės įrangos modifikavimu ar tobulinimu, valdymo procedūros.

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 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 kurią 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) RA taisyklėmis;

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

d) CA ir RA sistemų programine įranga;

e) atsakomybe už sistemos atliekamų veiksmų sutrikimus;

f) galimais sistemos veikimo sutrikimais.

5.4. Žurnalinių įrašų registravimas

CA privalo kaupti įrašus apie visas operacijas, susijusias su išduotais sertifikatais, siekdama turėti tinkamus patikimumo užtikrinimo paslaugų teikimo veiklos įrodymus teisminiuose procesuose. Incidentų bei specifinių operatyvinių įvykių faktai ir aplinkybės turi būti dokumentuojamos ir archyvuojamos.

Dokumentavimo forma turi užtikrinti, kad duomenys, duomenų autentiškumas ir įrašymo data galėtų būti patikrinta bet kuriuo laiku.

Duomenys turi būti saugomi CPS nustatytą laiką, būti pasiekiami ir saugomi nuo praradimo bei sugadinimo.

Bendri reikalavimai, keliami žurnalinių įrašų kaupimui: CA turi:

a) pateikti einamuosius ir archyvinius įrašus apie sertifikatus kaip tinkamos patikimumo užtikrinimo paslaugų teikimo veiklos įrodymus teisminiuose procesuose;

---

[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.

b) užtikrinti, kad būtų fiksuojamas tikslus laikas svarbių įvykių, susijusių su CA veikla, sertifikatų ar raktų gyvavimo ciklu;

c) užtikrinti, kad su sertifikatais susiję įrašai būtų saugomi laikotarpį, per kurį CA turi pateikti patikimumo užtikrinimo paslaugų teikimo veiklos teisinius įrodymus kvalifikuotų elektroninių parašų tikrumui paremti;

d) užtikrinti, kad fiksuojami įvykiai būtų saugomi taip, kad jų nebūtų galima pakeisti, ištrinti ar sunaikinti per saugojimo laikotarpį;

e) dokumentuoti svarbius ir išskirtinai fiksuojamus įvykius bei duomenis ;

Reikalavimai, keliami naudotojų ir jų prašymų registracijos žurnalinių įrašų kaupimui: CA turi:

a) užtikrinti, kad visi įvykiai, susiję su registracijos procedūra, būtų fiksuojami;

b) užtikrinti, kad visa registracijos metu gauta informacija būtų fiksuojama ir dokumentuojama. Ši informacija turi apimti:

- prašymuose sudaryti sertifikatą pateiktų dokumentų tipus;
- pateiktų dokumentų unikalius identifikacinius duomenis – numeris ir išdavimo data;
- prašymų, identifikacijai pateiktų dokumentų ir pasirašytos sutarties saugojimo vietą;
- prašymą priėmusio darbuotojo identifikacinius duomenis;
- taikomus tapatybės dokumentų patikrinimo metodus;
- tapatybės patvirtinimo nuotoliniu būdu įvykių duomenis.

Reikalavimai, keliami sertifikatų generavimo žurnalinių įrašų kaupimui: CA turi:

a) fiksuoti visus CA valdomų raktų gyvavimo ciklo įvykius;

b) fiksuoti visus išduotų sertifikatų gyvavimo ciklo įvykius.

Reikalavimai, keliami SSCD/QSCD parengimo ir išdavimo žurnalinių įrašų kaupimui: CA turi:

a) fiksuoti visus įvykius, susijusius su SSCD/QSCD parengimu ir išdavimu;

b) fiksuoti visus įvykius, susijusius su nuotolinio parašo / spaudo kriptografinių raktų aktyvavimo priemonių registravimu.

Reikalavimai, keliami sertifikato statuso keitimo žurnalinių įrašų kaupimui: CA turi fiksuoti visus įvykius, susijusius su sertifikatų statuso keitimu, įskaitant prašymus ir iš to kylančius įvykius.

5.5. Žurnalinių įrašų archyvavimas

CA turi užtikrinti kriptografinių raktų tvarkymo įvykių žurnalinių įrašų bei dokumentų, įrodančių CA sugeneruoto sertifikato perdavimą sertifikato savininkui bei sutikimą su sertifikatų užsakymo, išdavimo ir naudojimo sąlygomis, archyvavimą ir saugojimą ne trumpiau kaip 7 metus nuo sertifikato galiojimo pabaigos.

CA turi užtikrinti, kad dokumentai, susiję su sertifikatų išdavimu, būtų archyvuojami ir saugomi, vadovaujantis Lietuvos Respublikos dokumentų ir archyvų įstatymo reikalavimais.

5.6. Veiklos sutrikimų ir tęstinumo valdymas

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. CA turi sudaryti veiklos tęstinumo planą, kuriame būtų apibrėžti veiklos atstatymo ir pratęsimo veiksmai, įvykus arba įtariant privačiojo rakto kompromitaciją. Minimalūs neatidėlioti veiksmai yra šie:

a) informuojami visi sertifikatų naudotojai, pasitikinčios pusės ir kiti asmenys, su kuriais sudaryti susitarimai ar jie yra kitaip susiję su CA veikla;

b) nurodoma, kad sudaryti sertifikatai ir atšauktų sertifikatų sąrašai, pasirašyti sukompromituotu privačiuoju raktu, gali būti pripažinti negaliojančiais.

5.7. CA veiklos nutraukimas

CA veiklos nutraukimo atveju turi būti minimizuojami sertifikatų naudotojų nepatogumai, užtikrinamas sukauptų patikimumo užtikrinimo paslaugų teikimo veiklos duomenų kaip įrodymų teikimo tęstinumas teisminiams procesams. CA prieš nutraukdamas patikimumo užtikrinimo paslaugų teikimo veiklą įsipareigoja:

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 kvalifikuotų patikimumo užtikrinimo paslaugų teikimo veiklos nutraukimo planą;

c) užtikrinti asmenims išduotų sertifikatų gyvavimą jų galiojimo laikotarpiu bei visos surinktos (teikiant patikimumo užtikrinimo paslaugas) informacijos saugojimą, kad ją būtų galima panaudoti teismo procese kaip įrodymą. Šis įsipareigojimas vykdomas tuomet, jei nusprendus nutraukti kvalifikuotų patikimumo užtikrinimo paslaugų teikimą, veikla nėra perduodama trečiajai šaliai. Siekiant įgyvendinti šį įsipareigojimą, CSP užtikrins OCSP ir CRL generavimo funkcijų vykdymą iki visų išduotų kvalifikuotų sertifikatų galiojimo pabaigos įskaitant prašymų sustabdyti / atšaukti sertifikatų galiojimą priėmimą ir įvykdymą;

d) neturint galimybės užtikrinti asmenims išduotų sertifikatų gyvavimo ciklą, 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 kvalifikuotų patikimumo užtikrinimo paslaugų teikimo veiklos nutraukimo plane;

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

6. Techninės saugumo kontrolės priemonės

6.1. Raktų porų generavimas ir diegimas

6.1.1. Kriptografinių raktų porų generavimas CA išduodamiems sertifikatams

CA turi užtikrinti privačiojo rakto slaptumą ir kad CA kriptografiniai raktai būtų generuojami kontroliuojamose, saugiose sąlygose.

Visi asmenims sudaromi kvalifikuoto elektroninio spaudo ir kvalifikuoto elektroninio parašo privatieji raktai yra generuojami aparatinėmis priemonėmis, todėl raktai yra apsaugoti nuo kopijavimo ar kitokio neteisėto panaudojimo. Kvalifikuoto elektroninio parašo kriptografiniai raktai sudaromi SSCD/QSCD įrenginiuose, atitinkančius eIDAS 29–30 straipsniuose ir 51 straipsnyje nustatytus reikalavimus. Kvalifikuoto elektroninio spaudo kriptografiniai raktai sudaromi kvalifikuoto elektroninio spaudo kūrimo įtaisuose, atitinkančiuose eIDAS 39 straipsnio 1–2 dalyse ir 51 straipsnio nustatytus reikalavimus.

Sudarant **QSignC-R-QSCD** ir **QSealC-R-QSCD** sertifikatus kriptografinių raktų pora generuojama CA valdomoje infrastruktūroje ir turi būti susieta su asmeniui išduotomis jų aktyvavimo nuotoliniu būdu priemonėmis ir joms išduotu **R-SIC** sertifikatu.

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

Sudarant **OVC bei QSealC-I** sertifikatus kriptografinių raktų pora generuojama CA valdomoje infrastruktūroje.

6.1.2. CA kriptografinių raktų generavimas

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

6.1.3. Privataus rakto perdavimas sertifikato savininkui

Su **QSignC-ClS-QSCD**, **QAuthC-ClS-QSCD**, **QAuthC-ClS-SSCD**, **QSealC-ClS-QSCD** sertifikatais susieti privatūs raktai sertifikatų savininkui perduodami SSCD/QSCD įrenginiuose. CA turi užtikrinti saugų SSCD/QSCD parengimą ir perdavimą sertifikatų savininkams. CA turi užtikrinti, kad:

a) SSCD/QSCD parengimas būtų kontroliuojamas ir atliekamas saugiai;

b) SSCD/QSCD būtų saugiai laikoma ir perduodama;

c) SSCD/QSCD aktyvavimas ir deaktyvavimas turi būti kontroliuojamas ir atliekamas saugiai.

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

a) išduodamas tik SSCD/QSCD, atitinkantis eIDAS 39 straipsnio 1i –2 dalyse ir 51 straipsnio ar eIDAS 29–30 straipsniuose ir 51 straipsnio nustatytus reikalavimus;

b) iki SSCD/QSCD priskyrimo asmeniui ir sertifikato generavimo iniciavimo, SSCD/QSCD yra saugiai sandėliuojamas;

c) priskyrus SSCD/QSCD asmeniui arba sugeneravus SSCD/QSCD viešojo rakto sertifikatą, privataus rakto aktyvavimo duomenys (PIN) ir SSCD/QSCD atblokavimo duomenys (PUK) yra pateikiami apsauginiame voke, kuris negali būti fiziškai įplėštas ar kitaip pažeistas (taip užtikrinama, kad aktyvavimo ir atblokavimo duomenų nesankcionuotos peržiūros atvejai būtų aptinkami iki SSCD /QSCD perdavimo asmeniui arba SSCD/QSCD perdavimo asmeniui metu);

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

e) SSCD/QSCD RA išduodamas tik fiziškai dalyvaujant asmeniui, SSCD/QSCD nėra siunčiamas ar perduodamas naudotojui kitais kanalais.

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

Su **OVC** ir **QSealC-I** sertifikatais susieta kriptografinių raktų pora sertifikato savininkui perduodama saugiu, su juo suderintu būdu.

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 turi viešai publikuoti savo viešuosius raktus pasitikinčioms šalims. Publikuodama savo viešąjį raktą, CA turi užtikrinti viešojo rakto ir kitų susijusių duomenų vientisumą ir autentiškumą.

6.1.6. Kriptografinių raktų dydžiai

Raktų dydžiai nustatomi atitinkamo tipo sertifikatų CPS apibrėžtame profilyje.

6.1.7. Kriptografinių raktų parametrų generavimas ir kokybės tikrinimas

Laikomasi ETSI EN 319 411-1 ir ETSI EN 319 411-2 standartų nustatytų reikalavimų.

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.

Privatūs raktai **QSignC-ClS-QSCD**, **QAuthC-ClS-QSCD**, **QAuthC-ClS-SSCD** ir **QSealC-ClS-QSCD** sertifikatams generuojami SSCD/QSCD įrenginiuose, atitinkančiuose eIDAS 29–30 straipsniuose, 39 straipsnio 1–2 dalyse ir 51 straipsnio nustatytus reikalavimus.

Privatūs raktai **QSignC-R-QSCD** ir **QSealC-R-QSCD** sertifikatams generuojami CA valdomame R-QSCD įrenginyje, atitinkančiame eIDAS 29–30 straipsniuose ir 39 straipsnio 1–2 dalyse nustatytus reikalavimus.

Kriptografinių raktų pora **OVC** ir **QSealC-I** sertifikatams generuojama CA valdomoje infrastruktūroje.

6.2.2. CA raktų perdavimas trečioms šalims (*key escrow*)

CA negali turėti jokių galimybių perduoti CA ir sertifikatų savininkų privačius raktus trečiosioms šalims.

6.2.3. CA privačių kriptografinių raktų atsarginių kopijų darymas ir atstatymas

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

6.2.4. Privačių raktų archyvavimas

CA 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

CA privačiųjų raktų saugumui užtikrinti turi būti naudojamos techninės priemonės bei procedūros, patikimai saugančios nuo privačiojo rakto atskleidimo ar neautorizuoto panaudojimo, leidžiančios išlaikyti privataus rakto konfidencialumą ir integralumą.

Tinkamos techninės priemonės bei procedūros turi užtikrinti, kad privatus raktas būtų laikomas ir naudojamas tik su įranga, atitinkančia saugumo reikalavimus.

Kai CA privatieji raktai saugomi ar laikomi ne saugioje kriptografinėje įrangoje, raktai turi būti šifruojami. Šifravimui naudojamas rakto ilgis ir algoritmas turi užtikrinti CA privačiųjų raktų saugumą ir atsparumą kriptografinėms atakoms visą raktų galiojimo laikotarpį.

Kai CA privatieji raktai saugomi saugioje kriptografinėje įrangoje (toliau – HSM), prieigos kontrolės priemonės turi užtikrinti, kad prieiga prie raktų nebūtų galima iš už HSM ribų.

6.2.6. CA privačiųjų kriptografinių raktų naudojimas

CA turi užtikrinti, kad CA priklausantys privatieji raktai būtų naudojami tinkamai. CA turi užtikrinti, kad:

a) CA privatieji raktai, naudojami asmenų sertifikatų bei asmenų CRL tvirtinimui , nebūtų naudojami jokiais kitais tikslais;

b) CA sertifikatų tvirtinimo privatieji raktai turi būti naudojami esant fiziškai saugioms sąlygoms.

6.2.7. CA kriptografinių raktų gyvavimo ciklo pabaiga

CA turi užtikrinti, kad CA privatieji raktai nebūtų naudojami pasibaigus jų gyvavimo ciklui. Nustatytos techninės ir valdymo procedūros turi užtikrinti, kad pasibaigus CA raktų galiojimo terminui būtų naudojama nauja raktų pora, o anksčiau naudoti privatieji raktai būtų sunaikinti.

6.2.8. Kriptografinės įrangos, naudojamos sertifikatams pasirašyti, gyvavimo ciklas

CA turi užtikrinti HSM saugumą viso jos gyvavimo ciklo metu. CA turi užtikrinti, kad:

a) HSM nebuvo pažeistas iki jo pristatymo;

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

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

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

6.3. Kiti raktų poros valdymo aspektai

6.3.1. Viešųjų raktų archyvavimas

CA sugeneruoti vieši raktai su atitinkamais sertifikatais turi būti archyvuojami ir saugomi atitinkamame CPS nustatytą laikotarpį.

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

Raktų porų galiojimo laikas turi būti lygus juos atitinkančių sertifikatų galiojimo laikui. Root CA ir Issuing CA sertifikatų galiojimo laikas turi būti ilgesnis negu jais patvirtintų CA išduodamų sertifikatų galiojimo terminas.

Jeigu elektroninio parašo arba elektroninio spaudo kūrimo įtaisas, į kurį yra išduotas elektroninio parašo ar spaudo sertifikatas ir jį atitinkanti raktų pora, netenkina eIDAS nustatytų reikalavimų, sertifikatų galiojimas turi būti atšaukiamas.

Jeigu CA elektroniniams parašams, kuriais tvirtinami CA išduodami sertifikatai, kurti naudojami kriptografiniai algoritmai ir / ar kriptografinių raktų ilgiai neatitinka ETSI TS 119 312 standarto reikalavimų, šiais CA parašais patvirtintų sertifikatų galiojimas turi būti atšauktas.

CA išduodamų sertifikatų galiojimo terminai nustatomi atitinkamo tipo sertifikatų CPS apibrėžtame profilyje.

6.4. Kriptografinių raktų aktyvavimo duomenys

CA sertifikatų raktų aktyvavimo duomenys yra sukuriami CA raktų poros generavimo procedūros metu ir saugomi specialiame seife.

QSignC-ClS-QSCD, **QAuthC-ClS-QSCD**, **QAuthC-ClS-SSCD**, **QSealC-ClS-QSCD** sertifikatų privačių raktų aktyvavimui SSCD/QSCD įrenginių personalizacijos metu kuriami PIN kodai. Šie PIN kodai sertifikatų savininkui yra pateikiami apsauginiame voke.

QSignC-R-QSCD ir **QSealC-R-QSCD** sertifikatų privatūs raktai aktyvuojami **R-SIC** viešuoju raktu, kuris sukuriamas CA išduotos nuotolinio parašo / spaudo kriptografinių raktų

aktyvavimo priemonės registracijos CA valdomoje infrastruktūroje proceso metu. **R-SIC** privataus rakto aktyvavimo PIN kodą **QSignC-R-QSCD** ir **QSealC-R-QSCD** sertifikatų savininkai sudaro CA jiems išduotoje nuotolinio parašo / spaudo kriptografinių raktų aktyvavimo priemonėje. **R-SIC** privataus rakto aktyvavimo PIN kodai nėra saugomi nuotolinio parašo / spaudo kriptografinių raktų aktyvavimo priemonėje, juos sertifikatų savininkai turi įsiminti.

OVC ir **QSealC-I** sertifikatų privačių raktų aktyvavimo duomenis kuria CA ir saugiu būdu perduoda sertifikatų savininkams.

6.5. Kompiuterių saugumo kontrolė

Turi būti užtikrintas ETSI EN 319 411-1 standarto reikalavimų vykdymas.

6.6. Kompiuterinių sistemų gyvavimo ciklo saugumo kontrolė

Turi būti užtikrintas ETSI EN 319 411-1 standarto reikalavimų vykdymas.

6.7. Kompiuterių tinklo saugumo kontrolė

Turi būti užtikrintas ETSI EN 319 411-1 standarto reikalavimų vykdymas.

7. Sertifikatų, CRL ir OCSP profiliai

7.1. Sertifikatų profiliai

QSignC-ClS-QSCD, **QAuthC-ClS-QSCD**, **QAuthC-ClS-SSCD**, **QSignC-R-QSCD** sertifikatų profiliai atitinka ETSI EN 319 412-2 standarto reikalavimus.

QSealC-ClS-QSCD ir **QSealC-R-QSCD** sertifikatų profiliai atitinka ETSI EN 319 412-3 standarto reikalavimus.

Visi kiti CA generuojami sertifikatai atitinka ITU-T X.509 standarto reikalavimus.

Detaliau profiliai apibrėžti atitinkamų sertifikatų CPS.

7.2. CRL profilis

CRL profilis sudaromas laikantis ITU-T X.509 standarto reikalavimų.

7.3. OCSP profilis

OCSP atsakiklio veikimas atitinka RFC 6960 arba RFC 5019 standarto reikalavimus.

8. Atitikties auditas bei kiti vertinimai

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

CA veiklos atitiktis CP ir CPS tikrinama CA nustatyta vidaus tvarka.

9. Kiti teisiniai bei veiklos aspektai

9.1. Paslaugų kainos

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

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).

9.2. Finansinė atsakomybė

Finansinės atsakomybės įsipareigojimams užtikrinti CA savo veiklą draudžia ne mažesne kaip Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymo 10 straipsnio 2 dalyje nustatyta suma.

9.2.1. Kompensacijos sertifikatų naudotojams

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

a) prašantysis sudaryti sertifikatus pateikė klaidingus duomenis;
b) sertifikatų savininkas neapsaugojo savo privačiojo rakto nuo kompromitacijos;
c) pasirašantysis asmuo pažeidė su CA sudaryto susitarimo dėl sertifikato naudojimo sąlygas.

9.3. Veiklos informacijos konfidencialumas

Konfidencialia informacija yra laikoma CA valdoma informacija, kuriai pagal Lietuvos Respublikoje galiojančius teisės aktus ar CA sudarytus sandorius taikomas konfidencialios informacijos statusas. Taip pat konfidencialia informacija yra laikoma informacija, numatyta Registrų centro konfidencialios, komercinę (gamybos) paslaptį sudarančios informacijos sąraše, patvirtintame Registrų centro valdybos 2018 m. rugpjūčio 21 d. sprendimu (2018 m. rugpjūčio 31 d. protokolas Nr. VPP-20).

9.4. Asmens duomenų apsauga

Asmens duomenys tvarkomi vadovaujantis 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), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymu.

CA renka ir tvarko tik tiek asmens duomenų, kiek tai yra būtina užtikrinti teikiamų patikimumo paslaugų saugumą ir patikimumą. Prieš teikiant prašymą išduoti sertifikatą asmuo turi būti supažindinamas su renkamais asmens duomenimis bei jų tvarkymo apimtimi ir tikslu, asmens duomenų rinkiniu, kuris bus įtrauktas į išduodamą sertifikatą, sertifikatų užsakymo, išdavimo ir naudojimosi sąlygomis.

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

9.5. Intelektinės nuosavybės apsauga

CP ir CPS yra CA intelektinė nuosavybė, tačiau laisvai prieinama 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

Įsipareigojimų, garantijos ir atsakomybių pasidalijimas tarp CA, RA, abonento ir sertifikatų savininko bei pasitikinčių šalių yra aprašomi šalių tarpusavio susitarimuose.

9.6.1. CA pareiškimai ir garantijos

CA įsipareigoja:

a) teikti sertifikatų sudarymo ir išdavimo paslaugas vadovaujantis šiame CP ir atitinkamų sertifikatų CPS nustatytomis procedūromis ir reikalavimais;

b) užtikrinti 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 Respublikoje galiojančiais teisės aktais, kurie nustato asmens duomenų saugumo reikalavimus;

d) užtikrinti Registrų centro privačiųjų kriptografinių raktų saugumą;

e) užtikrinti sudaromuose sertifikatuose informacijos teisingumą;

f) užtikrinti 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 patikimumo užtikrinimo paslaugas tiek, kiek neprieštarauja eIDAS, reikalavimams;

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

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

k) užtikrinti, kad šiame CP aprašytos patikimumo užtikrinimo paslaugų teikimo sąlygos atitiktų eIDAS bei Lietuvos Respublikos teisės aktų reikalavimus;

l) užtikrinti, kad šie CP bei sertifikatų užsakymo, išdavimo ir naudojimo sąlygos ir taisyklės būtų viešai prieinamos internete;

m) viešai internete, šiame CP nustatytu periodiškumu, skelbti CRL;

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

CA atsako už:

a) sudarytuose sertifikatuose 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 galiojimo sustabdymą ar nutraukimą laiku;

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

9.6.2. RA pareiškimai ir garantijos

RA, veikdama pagal šiuos CP, įsipareigoja:

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

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

c) sustabdyti, atšaukti sertifikatų galiojimą ar atšaukti sustabdymą;

d) patikrintus ir visus reikalavimus atitinkančių 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) laikytis su CA pasirašytos sutarties, jei RA funkcijas atlieka trečia šalis.

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 šioje 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;

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

c) tinkamai pasirūpinti išduotų sertifikatų ir kriptografinių raktų bei jų aktyvavimo kodų saugumu;

d) sertifikatą naudoti tik atitinkame CPS nurodytais tikslais;

e) nedelsiant kreiptis į Registrų centrą dėl sertifikato galiojimo sustabdymo ar atšaukimo šiais atvejais, kai:

- pametama ar kaip nors kitaip prarandama įtaisų, į kuriuos yra išduoti sertifikatai ir kriptografiniai raktai, kontrolė;
- pavagiamas ar kitaip sukompromituojamas privatus raktas, susietas su CA išduotu sertifikatu ar jo aktyvavimo duomenys (PIN kodas, PUK kodas ir kt.);
- pastebimi netikslumai sertifikate arba jame prireikia daryti pakeitimus;
- pasikeičia asmens tapatybės duomenys;

f) CA išduotų sertifikatų 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 atitinkamais CPS.

Pasitikinčios šalys privalo įsitikinti, kad sertifikatas buvo galiojantis 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

Kitų asmenų, dalyvaujančių sertifikatų išdavimo procesuose, įsipareigojimai ir atsakomybės apibrėžtos atitinkamuose CPS.

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 sudaromuose susitarimuose 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 eIDAS 13 straipsnyje 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, jei nuostoliai buvo patirti dėl:

- trečiųjų šalių ir galimų vartotojų naudojamos CA neautorizuotos aparatinės ir programinės įrangos kriptografiniams raktams generuoti, duomenims šifruoti, elektroniniams parašams kurti;
- neleistino sertifikatų naudojimo;
- teikiamų paslaugų prieinamumo ir kokybės, jei sutrikimai fiksuojami ne Registrų centro veikimo ribose, kurios detalizuotos atitinkamame sertifikatų CPS;
- sertifikato atšaukimo CPS nustatytais atvejais.

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

9.10. Galiojimas

Ši CP įsigalioja nuo jos patvirtinimo Registrų centro generalinio direktoriaus įsakymu momento ir galioja iki naujos šios CP versijos išleidimo. Naujos versijos galiojimo pradžia nurodyta CP dokumento viršelyje. Naujausia CP versija publikuojama saugykloje (repository) internete.

9.11. Individualūs pranešimai ir komunikavimas

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

Visi pranešimai ir paklausimai, susiję su sertifikatų išdavimu ir naudojamu, turi būti teikiami elektroniniu paštu pagalba@registrucentras.lt. CA individualūs pranešimai sertifikatų savininkams siunčiami elektroniniu paštu, kurį jie nurodė teikdami prašymus išduoti sertifikatus.

9.12. CP pakeitimai

Šie CP gali būti keičiami pastebėjus juose netikslumų, 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 kai keičiamas nuostatų OID;

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

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

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

Kitais atvejais pakeitimai yra esminiai ir po kiekvieno CP pakeitimo keičiamas jų unikalus identifikatorius. Visais atvejais, jei pakeitimai daro įtaką patikimumo užtikrinimo paslaugų saugumo lygio pasikeitimams, pakeitimai yra esminiai.

CP prižiūrimi, keičiami ir tvirtinami laikantis tokios procedūros:

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

b) CP pakeitimus inicijuoja CA arba sertifikatų naudotojai;

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

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

9.13. 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

Šios CP reglamentuojamos, aiškinamos ir interpretuojamos pagal Lietuvos Respublikos įstatymus bei eIDAS.

9.15. Atitiktis taikomai teisei

Šios CP parengtos 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;

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

d) Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

e) 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";

f) 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";

g) 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";

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

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

j) ETSI EN 319 412 Certificate Profiles;

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

l) ETSI TS 119 312 Cryptographic Suites;

m) ETSI TS 119 612 Trusted Lists.

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.

Šios CP yra Registrų centro vidaus teisės 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 naudojimų susijusios sąlygos.

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

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

9.16.2. Baigiamosios nuostatos

CP neaptarti klausimai nagrinėjami pagal Lietuvos Respublikoje galiojančius teisės aktų nustatytus reikalavimus. Jei CP nuostatos tampa prieštaraujančiomis Lietuvos Respublikoje galiojančių teisės aktų reikalavimams, taikomos Lietuvos Respublikoje galiojančių teisės aktų nuostatos.