UAB „SKAITMENINIO SERTIFIKAVIMO CENTRAS“

SERTIFIKAVIMO VEIKLOS NUOSTATAI

OID : 1.3.6.1.4.1.22501.1.2.0

Versija 1.0
(2007.12.28)

SKAITMENINIO
SERTIFIKAVIMO
CENTRAS

http://www.ssc.lt

TURINYS

1. ĮŽANGA

1.1. Apžvalga

Šie Sertifikavimo veiklos nuostatai apibrėžia kvalifikuotų SSC Sertifikavimo Tarnybų (toliau – „SSC QCA“) veiklą, sudarant Sertifikatus ir teikiant su tuo susijusias paslaugas.

Šie Sertifikavimo veiklos nuostatai (toliau – „CPS“, arba „Nuostatai“) skirti Sertifikatų naudojimo elektroninių parašų saugumui užtikrinti ir sertifikavimo tarnybų veiklos patikimumui garantuoti. CPS padeda sertifikatų naudotojams nustatyti, ar iš tikro sertifikatai atitinka numatomus naudojimo tikslus.

Šie Sertifikavimo veiklos nuostatai yra išsamios SSC QCA veiklos taisyklės, kuriomis SSC QCA vadovaujasi teikdamos sertifikavimo paslaugas. Šie CPS gali būti taikomi tik SSC QCA veiklos srityje[1]. Šie CPS taip pat apibrėžia santykį tarp SSC QCA sertifikavimo paslaugų gavėjų (Galutinių naudotojų), tiek fizinių, tiek ir juridinių asmenų.

Šie sertifikavimo veiklos nuostatai (CPS) yra skirti:

a) nustatyti detalias technines, procedūrines ir organizacines veiklos taisykles ir principus, kurie taikomi SSC QCA teikiant visas sertifikavimo paslaugas viso SSC QCA išduotų sertifikatų galiojimo laikotarpiu;
b) pateikti pagrindinę informaciją apie PCA funkcijas išduodant Sertifikatus;
c) įgyvendinti Sertifikavimo Tarnybos Sertifikato Taisykles (OID 1.3.6.1.4.1.22501.1.3.0);
d) apibrėžti SSC QCA ir RA funkcijas išduodant Sertifikatus.

Šie CPS taip pat nustato veiklos gaires visiems sertifikatais Pasitikintiems asmenims, įskaitant fizinius ir juridinius asmenis Lietuvoje ir užsienyje.

1.1.1. CPS funkcijos

Šie CPS yra tik vienas iš dokumentų, susijusių su SSC QCA sertifikavimo sistema. Kiti dokumentai, sudarantys SSC QCA sertifikavimo sistemos pagrindus:

- Pagalbiniai saugos ir veiklos dokumentai, papildantys CP ir CPS detalesniais reikalavimais, kaip antai:
    - SSC QCA apsaugos valdymo taisyklės (DID: AD.TSK.102) kuriame aprašomi detalūs reikalavimai SCC CA personalui, fizinei, telekomunikacijų, loginei ir kriptografinių raktų tvarkymo saugai.
    - SSC QCA privatumo ir asmens duomenų apsaugos taisyklės (DID: CA.TSK.189), kuriose nustatomos asmeninės informacijos rinkimo, panaudojimo bei teikimo aspektai, asmens duomenų savininkų teisės, o taip pat asmens duomenų apsaugos klausimai.
    - SSC QCA asmenų registravimo sertifikatams gauti ir asmenų konsultavimo taisyklės (DID: CA.TSK.190), kuriose nustatomos reikalavimai klientų ir pasirašančiųjų asmenų pateiktų prašymų registravimui.
- Pagalbinės sutartys, kurias sudaro SSC QCA. Šios sutartys privalomos SSC QCA klientams, Galutiniams Naudotojams, SSC RA ir kitiems SSC QCA sertifikavimo sistemos dalyviams.
- Bendrosios sertifikavimo paslaugų teikimo sąlygos (DID: CA.SLG.185). Šios sąlygos privalomos CA, RA ir Pasitikinčių Šalių sąntykiams.

[1] Sertifikavimo tarnybos veiklos sritis yra sritis, kurioje Sertifikavimo Tarnyba kompetentinga teikti sertifikavimo paslaugas. Pvz., į Sertifikavimo Tarnybos veiklos sritį nepatenka programinė įranga sertifikatų naudojimui ir t. t.

Šis dokumentas visiškai atitinka ir yra suderintas su šiais Lietuvos Respublikos teisės aktais:

a) 2000 m. liepos 11 d. Lietuvos Respublikos elektroninio parašo įstatymu Nr. VIII-1822 (pakeistu 2002 m. birželio 6 d. Nr. IX-934);
b) 1996 m. birželio 11 d. Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymu Nr. I-1374;
c) 2002 m. gruodžio 31 d. LR Vyriausybės nutarimu Nr. 2108 Dėl Reikalavimų kvalifikuotus Sertifikatus sudarantiems sertifikavimo paslaugų teikėjams, Reikalavimų elektroninio parašo įrangai, Kvalifikuotus Sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarkos ir Elektroninio parašo priežiūros reglamento patvirtinimo;
d) 2003 m. sausio 29 d. Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus įsakymu Nr. T-7 patvirtinta Asmenų registravimo sertifikatams gauti ir konsultavimo paslaugų teikimo tvarka;
e) 2003 m. sausio 29 d. Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus įsakymu Nr. T-8 patvirtintais reikalavimais elektroninio parašo tikrinimo procedūrai;
f) kitais taikytinais teisės aktais.

Šis dokumentas yra suderintas su SSC QCA Sertifikato Taisyklėmis (DID: CA.TSK.255).

Šie CPS yra suderinti su šiais standartais:

- RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
- RFC 3280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile;
- RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile;
- RFC 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP;
- ETSI TS 101 456: Policy requirements for certification authorities issuing qualified certificates;
- ETSI TS 101 862: Qualified certificate profile;
- ETSI TS 101 042: Policy requirements for certification authorities issuing public key certificates (Normalised level only);
- ETSI TS 101 456 v1.3.1 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates;
- ETSI TS 101 862 v1.3.2 Qualified Certificate profile
- ETSI TS 101 733 v1.6.3 Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES);
- LST CWA 14167-1 Saugos reikalavimai, keliami patikimoms elektroninių parašų sertifikatų valdymo sistemoms – 1 Dalis: Reikalavimai, keliami sistemų saugai CWA 14167-1:2003 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements (atnaujintas);
- LST CWA 14167-2 Saugos reikalavimai, keliami patikimoms elektroninių parašų sertifikatų valdymo sistemoms – 2 Dalis: Sertifikavimo paslaugų teikėjų pasirašymo operacijų kriptografinis modulis – Apsaugos profilis CWA 14167-2:2004 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 2: Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP (atnaujintas);
- LST CWA 14167-3 Saugos reikalavimai, keliami patikimoms elektroninių parašų sertifikatų valdymo sistemoms – 3 Dalis: Sertifikavimo paslaugų teikėjų raktų generavimo kriptografinis modulis – Apsaugos profilis CWA 14167-3:2002 Security Requirements for Trustworthy Systems Managing Certificates for

Electronic Signatures – Part 3: Cryptographic module for CSP key generation services protection profile CMCKG-PP (atnaujintas);

- LST CWA 14168 Saugi parašo formavimo įranga "EAL 4" CWA 14169:2004 Secure Signature-Creation Devices "EAL 4+" (atnaujintas);
- LST CWA 14170 Reikalavimai, keliami parašo formavimo taikomosioms sistemoms CWA 14170:2004 Security Requirements for Signature Creation Applications (atnaujintas);
- LST CWA 14171 Elektroninio parašo tikrinimo procedūros CWA 14171:2004 General guidelines for electronic signature verification (atnaujintas);
- ISO 1-7799 standard on security and infrastructure;
- LST ISO/IEC 15408-1:1999(E) Informacinės technologijos – Saugumo metodai – IT saugumo įvertinimo kriterijai – Dalis 1: Įvadas ir bendras modelis ISO/IEC 15408-1:1999(E) Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model;
- LST ISO/IEC 15408-2:1999(E) Informacinės technologijos – Saugumo metodai – IT saugumo įvertinimo kriterijai – Dalis 2: Saugumo funkciniai reikalavimai ISO/IEC 15408-2:1999(E) Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements;
- LST ISO/IEC 15408-3:1999(E) Informacinės technologijos – Saugumo metodai – IT saugumo įvertinimo kriterijai – Dalis 3: Saugumo užtikrinimo reikalavimai ISO/IEC 15408-3:1999(E) Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements.

Šie CPS atitinka *Internet Engineering Task Force* (IETF) RFC 3647 reikalavimus CPS formai ir turiniui. Kai kurie skyriai, kurių antraštės atitinka RFC 3647 struktūrą, nebūtinai taikomi teikiant SSC QCA sertifikavimo paslaugas. Tokie skyriai pažymėti tekstu "*Skyrius netaikomas*" arba „*Netaikoma*“. Nežymūs redakciniai RFC 3647 nuostatų pakeitimai buvo padaryti šiuose CPS, siekiant geriau pritaikyti RFC 3647 struktūrą konkrečiai taikymo sričiai, atsižvelgiant į SSC QCA veiklos ypatumus ir teikiamų paslaugų specifiką.

Atskirai SSC QCA teikiamai paslaugai gali būti išleistos ir atitinkamai paskelbtos papildomos CPS versijos.

Šie CPS yra viešai prieinami SSC QCA tinklalapyje internete adresu http://www.ssc.lt/cps .

SSC QCA priima pastabas ir komentarus dėl šių CPS adresu: UAB „Skaitmeninio sertifikavimo centras“, Jogailos g. 8-16, LT-01116, Vilnius, Lietuva.

Papildomos informacijos apie šiuos CPS ir SSC QCA galima gauti iš UAB „Skaitmeninio sertifikavimo centras“, Jogailos g. 8-16, LT-01116, Vilnius, Lietuva.

Šis dokumentas publikuojamas lietuvių kalbą.

1.2. Identifikavimas

Šis unikalus įregistruotas sertifikato taisyklių identifikatorius (OID) identifikuoja šiuos SSC QCA Sertifikavimo veiklos nuostatus:

1.3.6.1.4.1.22501.1.2.0

Atskiri OID komponentai yra šie:

Pavadinimas	Reikšmė	Paaiškinimas
Tarptautinė standartizacijos organizacija (ISO)	1	IANA priskirta reikšmė
Tarptautinė organizacija	3	IANA priskirta reikšmė
JAV gynybos departamentas	6	IANA priskirta reikšmė
Internetas	1	IANA priskirta reikšmė
Įmonė	4	IANA priskirta reikšmė
Registruota IANA	1	IANA priskirta reikšmė
Skaitmeninio sertifikavimo centras	22501	IANA priskirta reikšmė
SSC CP ir CPS dokumentacija	1	SSC QCA priskirta reikšmė
Šis dokumentas	2	SSC QCA priskirta reikšmė
Esamo dokumento redakcija (pradedant nuo „0“)	0	SSC QCA priskirta reikšmė

1.3. Sertifikatų klasės ir tipai

SSC QCA teikia trijų klasių (Klasės 1-3) sertifikavimo paslaugas. Sertifikavimo paslaugų klasės atitinka SSC QCA išduodamų sertifikatų klases.

Kiekviena sertifikato klasė atlieka specifines funkcijas ir pasižymi specialiais saugos elementaius ir atitinka skirtingą Pasirašančiojo parašo tikrinimo duomenų susiejimo su jo tapatybe, ir Pasirašančiojo tapatybės nustatymo ir patvirtinimo saugumo ir patikimumo lygį. SSC CA Sertifikavimo sistemos dalyviai patys pasirenka jiems reikalingas sertifikatų klases.

3-os klasės SSC QCA išduodami sertifikatai yra kvalifikuotieji sertifikatai, atitinkantys 2000 m. liepos 11 d. Lietuvos Respublikos Elektroninio parašo įstatymo (Nr. VIII-1822) 2 straipsnio 15 p. įtvirtintus reikalavimus ir RFC 3739 bei ETSI TS 101 862 nuostatas.

1-os klasės sertifikatai

1-os klasės sertifikatai suteikia žemiausią saugumo lygį SSC QCA Sertifikavimo sistemoje. Tai - fiziniams asmenims išduodami sertifikatai, kurių patikrinimas remiasi patikinimu, kad Galutinio naudotojo Sertifikatas yra unikalus ir neklaidinantis SSC QCA Sertifikavimo sistemoje, ir jame nurodytas elektroninio pašto adresas yra susietas su viešuoju raktu.

Tokiu būdu 1-os klasės sertifikatai įgalina Pasirašančiojo asmens duomenų susiejimą su parašo tikrinimo duomenimis ir netiesioginį tapatybės patvirtinimą. 1-os klasės sertifikatų atveju Pasirašančiojo tapatybės nustatymas neužtikrina tokio tapatybės nustatymo ir patvirtinimo patikimumo laipsnio, kaip 2-os ir 3-os klasės sertifikatai (t.y. to, kad Pasirašytojas yra būtent tas asmuo, kuriuo save nurodo). Įprastinis Pasirašytojo vardas ir pavardė yra netikrinamoji Pasirašytojo informacija. Tikrinant Pasirašytojo tapatybę, atliekama tik jo elektroninio pašto adreso paieška, siekiant užtikrinti, kad Galutinio naudotojo Sertifikatas būtų unikalus ir neklaidinantis CA Sertifikavimo sistemoje.

Į 1-os klasės funkciją taip pat įeina ribotas asmens, prašančio sudaryti Sertifikatą, elektroninio pašto adreso patvirtinimas.

1-os klasės sertifikatai tinkami elektroniniams parašams, patvirtinantiems **nekomercinio pobūdžio** elektroninius duomenų pranešimus, siunčiamus elektroniniu paštu, internetu ir / arba lygiavertėms individualioms komunikacijoms, kurias fiziniai asmenys naudoja ne savo amato, verslo ar profesijos tikslams, įskaitant jų naudojimą sutartims tarp tokių asmenų sudaryti.

2-os klasės sertifikatai

2-os klasės sertifikatai suteikia vidutinį saugumo lygį SSC QCA Sertifikavimo sistemoje. Šie sertifikatai išduodami:

1. fiziniams asmenims;
2. fiziniam asmeniui, besikreipiančiam juridinio asmens vardu (kai Galutinis naudotojas – juridinis asmuo);
3. fiziniam asmeniui, kurio sertifikatas bus naudojamas automatizuotose sistemose duomenų pasirašymui (Administratoriaus sertifikatas);
4. įvairioms automatizuotoms sistemoms bei tarnyboms (tokioms kaip OCSP, TimeStamping, SSL ir kt.);
5. programinio kodo autoriams (juridiniams bei fiziniams asmenims).

2-os klasės sertifikatų atveju Pasirašančiojo tapatybės nustatymo ir patikrinimo procedūros yra tapačios 1-os klasės patikrinimo procedūroms bei apima papildomas patikrinimo procedūras, kurių metu:

1. informacija, kurią pateikė asmuo, pateikęs paraišką sudaryti Sertifikatą, palyginama su informacija viešuosiuose registruose, verslo įrašuose ar duomenų bazėse ar SSC QCA priimtinos tapatybės nustatymo duomenų bazėse;
2. patikrinama, ar egzistuoja juridinis asmuo, kurio vardu kreipiasi fizinis asmuo;
3. patikrinami besikreipiančio fizinio asmens įgalinimai kreiptis juridinio asmens vardu;
4. automatizuotoms sistemoms ir tarnyboms yra nustatoma domeno nuosavybės teisę.

2-os klasės sertifikatams maksimalus SSC QCA materialinės atsakomybės dydis dėl netinkamai išduoto sertifikato **neviršija 10 000 (dešimt tūkstančių) litų**.

3-os klasės sertifikatai suteikia aukščiausią saugumo lygį SSC QCA Sertifikavimo sistemoje. 3-os klasės sertifikatai išduodami:

1. fiziniams asmenims;
2. fiziniam asmeniui, besikreipiančiam juridinio asmens vardu (kai Galutinis naudotojas – juridinis asmuo);
3. fiziniam asmeniui, kurio sertifikatas bus naudojamas automatizuotose sistemose duomenų pasirašymui (Administratoriaus sertifikatas).

3-os klasės sertifikatų tipai

Pagal paskirtį ir naudotojus 3-os klasės sertifikatai skirstomi į:

(a) Galutinių naudotojų sertifikatus (kai parašo formuotojas – Pasirašytojas arba juridinis asmuo, kurio vardu kreipėsi Pasirašytojas);
(b) Administratorių (arba automatizuoto duomenų pasirašymo sistemų) sertifikatus, kai parašus formuoja automatizuoto pasirašymo sistemos (šiuo atvėju sertifikatas išduodamas šios sistemos administratoriui).

3-os klasės sertifikatai tinkami bet kokiems elektroniniams parašams, įskaitant ir programas, reikalaujančias aukščiausio Pasirašančiojo parašo tikrinimo duomenų susiejimo su jo tapatybe, ir Pasirašančiojo tapatybės nustatymo ir patvirtinimo saugumo ir patikimumo lygio.

3-os klasės sertifikatams maksimalus SSC QCA materialinės atsakomybės dydis dėl netinkamai išduoto sertifikato **neviršija 100 000 (vienas šimtas tūkstančių) litų**.

3-os klasės sertifikatų panaudojimo ir taikymo paskirtis ribojamas sertifilkato sandaros pagalba sutinkant su tarptautiniais standatais.

Pareiškėjo tapatybės nustatymui ir patvirtinimui taikomos šių CPS 3.2.1 punkto nuostatos.

Lentelė Nr. 1 apibendrina sertifikatų tipus, kuriuos siūlo SSC QCA, sutinkamai su CP. Joje nustatomos kiekvienos sertifikato tipo savybės, tapatybės nustatymas bei taikymo sritys.

CP nurodytos sertifikatų klasių specifikacijos, apibendrintos šiuose CPS, nustato minimalų patikimumo lygį kiekvienai klasei. Pavyzdžiui, bet kuris 1-os klasės Sertifikatas gali būti naudojamas elektroniniams parašams, kodavimui, priėjimo kontrolei, kai aukšto patikimumo tapatybės nustatymas yra nereikalingas, t.y. žemo patikimumo lygio reikalaujančiai programinei įrangai. Tačiau sutarties pagrindu ar specifinėje aplinkoje (pavyzdžiui, aplinkoje tarp įmonių), SSC CA Sertifikavimo sistemos dalyviai turi teisę naudoti griežtesnes tikrinimo procedūras nei procedūros, nustatytos CP, arba naudoti Sertifikatus programinei įrangai, reikalaujančiai aukštesnio patikimumo lygio nei programinė įranga, aprašyta CPS. Šie Dalyviai atsako už bet kokią žalą, kurią sukelia toks Sertifikatų naudojimo būdas.

Lentelė Nr. 1. Sertifikatų tipai

Klasė	Galutinis naudotojas (parašo naudotojas)	Paraiškos teikėjo tapatybės nustatymas	TAIKYMO SRITYS
1-oji klasė	Fiziniai asmenys	Elektroninio pašto adreso paieška, siekiant užtikrinti, kad Galutinio naudotojo Sertifikatas yra unikalus ir neklaidinantis CA Sertifikavimo sistemoje.	Elektroninio pašto saugumo nedidelis sustiprinimas, naudojant šifravimą, elektroninį parašą, prieigos kontrolę internete, kai tapatybės įrodymas bereikalingas. Programos, reikalaujančios žemo saugumo lygio, pvz., **nekomercinio pobūdžio** naršyklės, paieškos varikliai, elektroninis paštas ir pan.
2-oji klasė	- Fiziniai asmenys; - Juridiniai asmenys; - Galutinių naudotojų sertifikatai; - Administratorių sertifikatai; - Sistemų bei tarnybų sertifikatai.	1-os klasės patvirtinimo priemonės ir vidinės dokumentacijos ir duomenų bazių patikrinimas, siekiant patvirtinti asmens, prašančio sertifikato, tapatybę, jo įgalinimus veikti juridinios asmens vardu ir tokio juridinio asmens egzistavimą	Elektroninio pašto saugumo sustiprinimas, naudojant konfidencialumo kodavimą, elektroninį parašą, priėjimo kontrolę internete. Programos, reikalaujančios vidutinio saugumo lygio, pvz., tapatybės patvirtinimas naudojant asmeninį elektroninį paštą, elektroninį paštą įmonės viduje ir tarp įmonių, tvarkant banko sąskaitas, patvirtinant sandorius.

Klasė	Galutinis naudotojas (parašo naudotojas)	Paraiškos teikėjo tapatybės nustatymas	TAIKYMO SRITYS
3-oji klasė	- Fiziniai asmenys; - Juridiniai asmenys; - Automatizuoto duomenų pasirašymo sistemų administratoriai.	Papildomai žr. CPS 3.2.1 punktą.	Tinkami bet kokiems elektroniniams parašams. Programos, reikalaujančios aukščiausio saugumo ir Pasirašytojo tapatybės patikrinio ir nustatymo patikimumo lygio.
3-oji klasė, Valstybinis sektorius	Valstybinio sektoriaus: - Juridiniai asmenys; - Automatizuoto duomenų pasirašymo sistemų administratoriai.	Papildomai žr. CPS 3.2.1 punktą.	Tinkami bet kokiems elektroniniams parašams. Programos, reikalaujančios aukščiausio saugumo ir Pasirašytojo tapatybės patikrinio ir nustatymo patikimumo lygio.

1.4. PKI sistemos dalyviai ir taikymo sritys

1.4.1. Sertifikavimo tarnybos

SSC PKI sistemos dalyviai, veikiantis pagal šias CPS, skirstomi į šias grupes:

a) Šakninės sertifikavimo tarnybos užtikrina pasitikėjimą CA. Šakninės sertifikavimo tarnybos išduoda Sertifikatus tik tokiems Sertifikatus sudarantiems paslaugų teikėjams (CA), kurie atitinka sertifikatų taisyklių reikalavimus, ir yra atsakingi už pastarųjų CA vadybą bei sertifikatų taisyklių įgyvendinimą. Šakninės sertifikavimo tarnybos yra:

   - SSC Root CA A,
   - SSC Root CA B,
   - SSC Root CA C.

   SSC Root CA B sertifikavimo tarnyba sudaro sertifikatus kaip CA, taip ir galutiniams vartotojams.

b) Sertifikatus sudarantis kvalifikuotas paslaugų teikėjas (QCA). Kiekviena QCA yra betarpiškai priskirta pirminei sertifikavimo tarnybai. Sudaro Sertifikatus tik Galutiniams naudotojams; SSC QCA užtikrina visų su sertifikatais susijusių paslaugų teikimą, įskaitant sertifikatų sudarymą, atšaukimą, statuso patvirtinimą, jei jas galima arba tampa privaloma taikyti konkrečiai programinei įrangai. SSC QCA prižiūrima pagal Lietuvos Respublikos elektroninio parašo įstatymo 14 straipsnį. SSC QCA yra įsteigta Lietuvoje. Su ja galima susisiekti adresu, nurodytu šiuose CPS. SSC QCA paslaugų teikimui, įskaitant sertifikatų sudarymą, sustabdymą, atšaukimą, atnaujinimą, statuso patvirtinimą, SSC QCA naudojasi saugia įranga ir avarinio atstatymo įranga. Žr. CPS 6.3. skyrių.

c) informacinė tarnyba - talpykla. Informacinė tarnyba realaus laiko (angl. *on-line*) režimu viešam naudojimui pateikia sertifikatų sąrašus, nebegaliojančių sertifikatų sąrašus (CRL), sertifikato

taisykles, visų CA, su kuriomis yra sudarytos atitinkamos sutartys, sertifikavimo veiklos nuostatus (CPS) ir kitą informaciją, susijusią su parašais ir sertifikavimo paslaugomis.

Šakninė sertifikavimo tarnyba praneša SSC PKI sistemos dalyviams apie kiekvieną įvykį, kuris gali turėti įtakos pasitikėjimui pačia Šaknine sertifikavimo tarnyba.

SSC QCA atsakomybės sritį sudaro visaapimantis sertifikatų tvarkymas visu jų galiojimo laikotarpiu.

1.4.2. Registravimo Tarnybos (RA)

SSC QCA kartu yra ir registravimo tarnyba (SSC RA). SSC QCA gali paskirti ar įgalioti naujas registravimo tarnybas, kurios gali būti arba savarankiški juridiniai asmenys arba struktūriniai SSC QCA padaliniai. SSC QCA kitiems juridiniams asmenims gali suteikti neišimtinę teisę vykdyti visas ar dalį SSC RA funkcijų. RA turi pasirašyti susitarimą su SSC QCA, prisiimdama pareigą laikytis reikalavimų, nustatytų šiame dokumente SSC RA.

Šio CPS nuostatos yra pilna apimtimi ir *mutatis mutandis* taikomos visoms SSC QCA paskirtoms SSC RA.

SSC RA pagrindinės funkcijos yra:

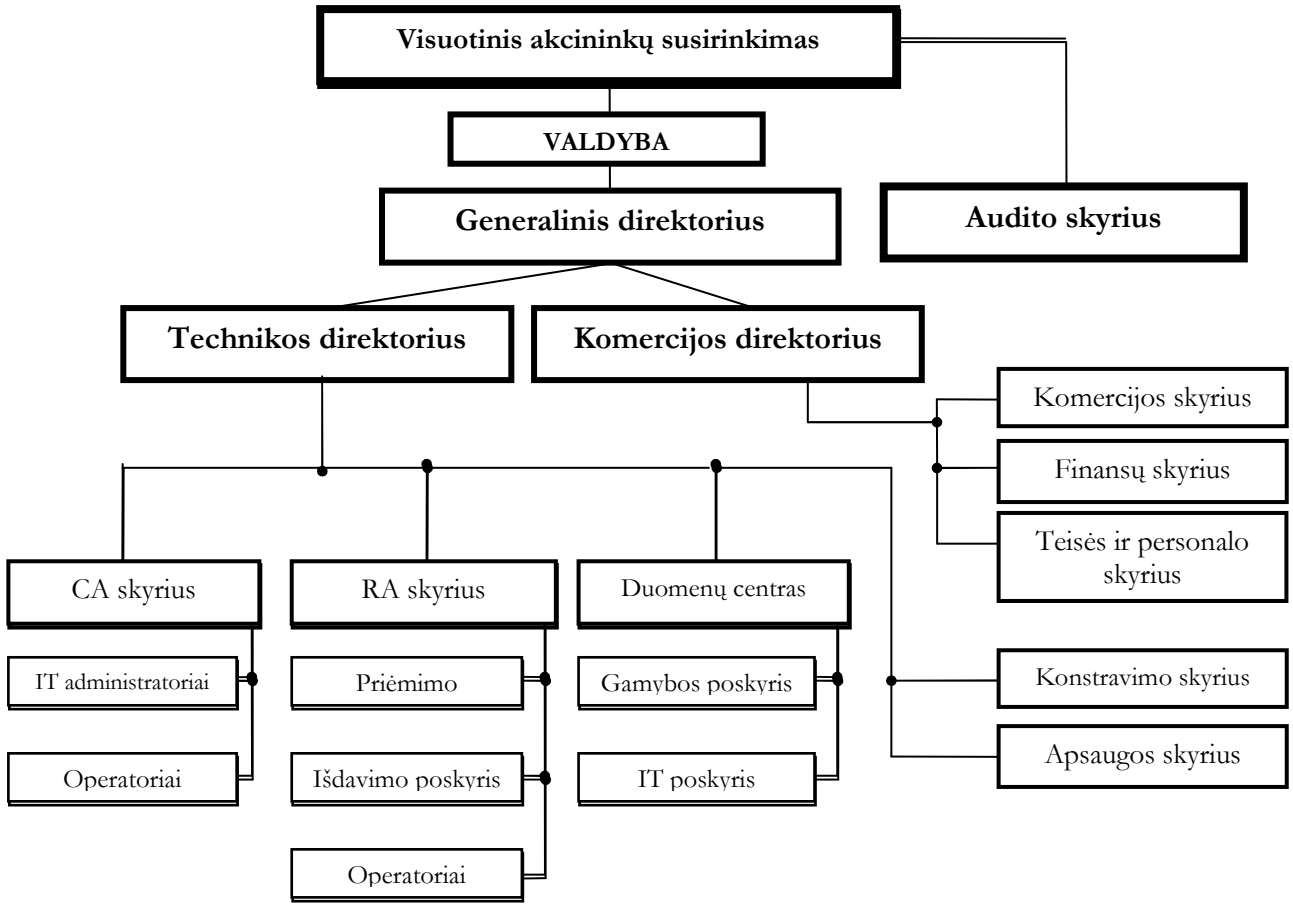
- pagalbos tarnybos įkurimas, kuriai sertifikato turėtojas galėtų pranešti apie jo privačiojo rakto (pasirašymo duomenų) ar sertifikato praradimą, vagystę ar sunaikinimą (toliau - "SSC RA pagalbos tarnyba“);
- asmenų paraiškų sertifikatams gauti bei atšaukti registravimas;
- asmenų, pageidaujančių įgyti, atšaukti ir sustabdyti Sertifikatus, tapatybės nustatymas;
- patvirtinus prašymą išduoti Sertifikatą, kreiptis į SSC QCA dėl sertifikato išdavimo;
- pradėti sertifikato galiojimo nutraukimo procedūrą, prašyti SSC QCA atšaukti ar sustabdyti sertifikato galiojimą.

SSC RA teikia SSC QCA duomenis, būtinus sertifikatams sudaryti, t.y. sertifikato turėtojo - Pasirašytojo asmens duomenis, taip pat elektroninio parašo tikrinimo duomenis, susietą su asmeniu, kuris bus nurodytas sertifikate.

Ryšys tarp SSC RA ir SSC QCA dėl bet kurios sertifikatų veikimo laikotarpio fazės (įskaitant prašymą išduoti Sertifikatą, sertifikato sudarymą, sustabdymą, sustabdymo panaikinimą ir galiojimo nutraukimą) yra apsaugotas PKI užšifravimu ir pasirašymo technologijomis, siekiant užtikrinti konfidencialumą ir abipusį tapatybės nustatymą ir patvirtinimą.

1.4.3. SSC QCA organizacinė struktūra

SSC PKI infrastruktūrą palaikančios organizacijos struktūra yra pavaizduota 1 pav.



Pav. 1. SSC QCA organizacijos struktūra.

1.4.4. Galutiniai naudotojai

Šiame dokumente Galutiniu naudotoju laikomi:

a) fiziniai asmenys;
b) juridiniai asmenys, kai pasirašytojas kreipiasi dėl sertifikato išdavimo, galiojimo nutraukimo ar sustabdymo ir pan. juridinio asmens vardu.

Šiame dokumente Administratoriais laikomi tarnybinių stočių, atliekančių automatizuotą informacijos pasirašymą, valdantis ir administratoruojantis fiziniai asmenis.

Šio CPS tikslais Galutinio naudotojo sąvoka atitinka Lietuvos Respublikos Elektroninio parašo įstatymo (2000 m. liepos 11 d. Nr. VIII-1822) 2 straipsnio 8 punkte įtvirtintą parašo naudotojo sąvoką („asmenys, kurie savo veikloje naudoja elektroninį parašą arba iš kitų asmenų gauna pasirašytus duomenis“). Bet kokiu atveju Pasirašytoju, tai yra asmeniu, sukuriančiu elektroninį parašą **gali būti tik veiksnus fizinis asmuo**, kuris turi parašo formavimo įrangą ir, veikdamas savo valia ir savo arba kito asmens, kuriam jis atstovauja, vardu, sukuria elektroninį parašą[2].

[2] Lietuvos Respublikos Elektroninio parašo įstatymo (2000 m. liepos 11 d. Nr. VIII-1822) 2 straipsnio 9 dalis.

1.4.5. Pasitikinčios šalys

Pasitikinčios šalys yra fiziniai ir juridiniai asmenys, kurie remiasi, pasitiki sertifikatu ir/ar elektroniniu parašu, kuriuos galima patikrinti, naudojant viešąjį raktą, nurodytą Galutinio naudotojo sertifikate.

Pasitikinti šalis, siekdama nustatyti, ar jos gautas Sertifikatas galioja, privalo kreiptis į SSC QCA galiojimo nustatymo tarnybą (pvz., CRL, OCSP, interneto sąsaja), ir tik po to vadovautis informacija, nurodyta Sertifikate.

1.4.6. Taikymo sritys

Pagal taikytiną teisę, elektroninis parašas arba sandoris su nuoroda į SSC QCA Sertifikatą galioja nepriklausomai nuo geografinės vietos, kurioje SSC QCA Sertifikatas buvo sudarytas, ar kurioje buvo sukurtas ar panaudotas elektroninis parašas, arba kurioje yra SSC QCA ar Galutinio naudotojo buveinė, gyvenamoji ar verslo vieta.

1.4.7. Teisinės sertifikatų naudojimo pasekmės

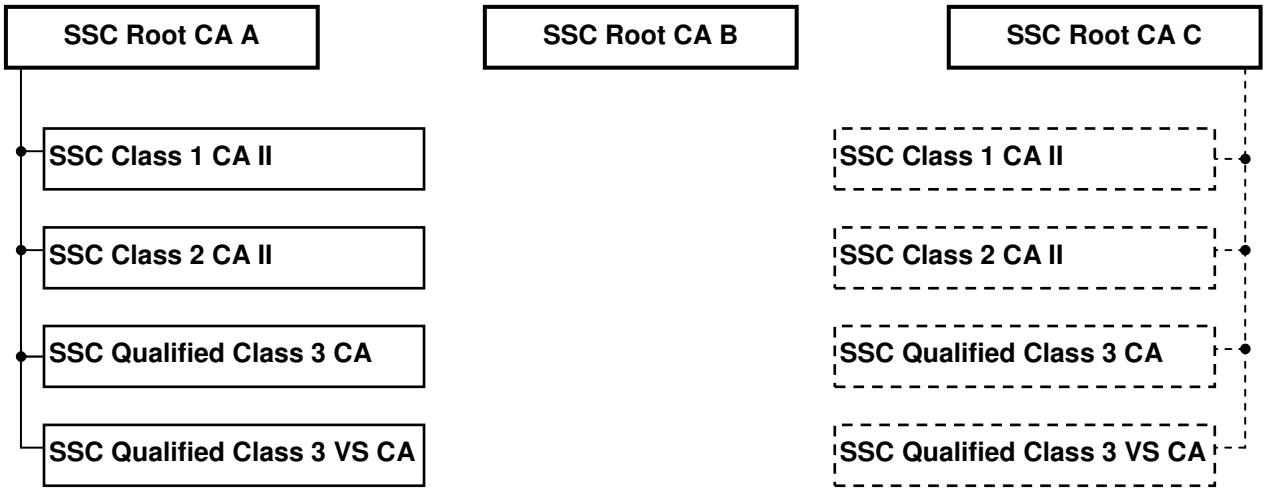
Nustatomi šie apribojimai SSC QCA sertifikatų naudojimui:

- 1-os klasės sertifikatai skirti tik Pasirašančiojo asmens susiejimui su elektroninio parašo tikrinimo duomenimis ir jo tapatybės patvirtinimui (tiesioginiam ar netiesioginiam) **nekomercinio pobūdžio sandoriuose, komunikacijose ar ryšio palaikyme**. Rekomenduojama nenaudoti 1-os klasės sertifikatų elektroniniam parašui, siekiant Lietuvos Respublikos Elektroninio parašo įstatymo 8 straipsnyje įtvirtintų teisinių pasekmių.
- 2-os ir 3-os klasės sertifikatai, kuriuos sudarė SSC QCA, atsižvelgiant į šių CPS 1.3 skyriuje numatytus maksimalius SSC QCA materialinės atsakomybės dydžius, gali būti naudojami visiems elektroniniams sandoriams, išskyrus tuos atvejus, kai pagal Lietuvos Respublikos teisės aktų reikalavimus negali būti pasirašomos elektroninės formos ir elektroniniai dokumentai.
- Tik 3-os klasės sertifikatai yra kvalifikuotieji. Tik 3–os klasės sertifikatu patvirtintas elektroninis parašas, suformuotas pagal šių CPS 6.1 skyrių, elektroniniams duomenims automatiškai ir *ex officio* įgyja ir turi tokią pat teisinę galią kaip ir parašas popieriniuose dokumentuose.
- Juridinio asmens atstovo elektroninio parašo, patvirtinto 3–os klasės sertifikatu, teisinė galia yra prilyginama juridinio asmens atstovo parašo, patvirtinto juridinio asmens antspaudu, galiai rašytiniuose dokumentuose.
- Draudžiama naudoti SSC QCA Sertifikatus srityse, kuriose klaida gali sukelti žmogaus žūtį, sužalojimą ar didelę žalą aplinkai, pvz., branduolinių jėgainių valdymui, laivų, orlaivių navigacijai ar komunikacijai, oro transporto kontrolės sistemoms, ginklų kontrolės sistemoms.

1.5. SSC sertifikatų vieta CA hierarchijoje

SSC QCA sudaryta iš kelių šakninių CA (Root CA) ir CA, išduodančių sertifikatus galutiniams vartotojams.

Sertifikavimo tarnybų hierarchinė struktūra šio dokumento sudarymo momentui:



Sertifikavimo tarnybos hierarchija gali būti keičiama, apie tai informuojant SSC QCA tvarkančios organizacijos tinklalapyje (žr. p. 1.6.2).

Sertifikavimo tarnybų hierarchijoje aukščiausias vietas užima Šakninės CA, kurios sertifikuoja visų SSC PKI CA grupės sertifikavimo tarnybų privačius raktus. Patvirtinant SSC PKI CA sukurto sertifikato galiojimą, tokia CA turi būti pasitikima taip, kaip pasitikima SSC Šakninėmis CA. Galutinio naudotojo sertifikatu turi būti taip pat pasitikima taip, kaip pasitikima SSC PKI CA.

SSC Šakninės CA veikia pagal SSC sertifikato taisyklės, versija 1.0, OID: 1.3.6.1.4.1.22501.1.3.0.

1.6. Kontaktinė informacija

1.6.1. Juridinis asmuo, administruojantis šiuos CPS

Šiuos CPS tvarko UAB "Skaitmeninio sertifikavimo centras", Jogailos 8-16, LT-01116, Vilnius, Lietuva (http://www.ssc.lt).

1.6.2. Kontaktinis asmuo

Su klausimais dėl šio dokumento kreiptis į:

UAB "Skaitmeninio sertifikavimo centras"
Jogailos 8-16, LT-01116 Vilnius, Lietuva
Tel.: +370-700-22722
Faks. : +370-700-22715
http://www.ssc.lt
e-mail: info@ssc.lt

1.7. CPS administravimas

CPS administruoja SSC QCA, UAB "Skaitmeninio sertifikavimo centras", Jogailos 8-16, LT-01116 Vilnius, Lietuva.

1.8. Sąvokos ir santrumpos

Sąvokų ir santrumpų sąrašas pateikiamas šių CPS pabaigoje .

2. BENDROSIOS NUOSTATOS

Šiame skyriuje numatytos SSC QCA, RA ir kitų SSC PKI sertifikavimo sistemos dalyvių pareigos, nuostatos dėl atsakomybės, finansinių/ekonominių klausimų, o taip pat informacijos skirstymas į konfidencialią informaciją ir viešai prieinamą informaciją, kurią galimą platinti. Skyriuje taip pat reglamentuojami SSC QCA veiklos patikrinimo principai.

2.1. PAREIGOS

2.1.1. SSC QCA pareigos

Sertifikatų išdavimas ir galiojimo nutraukimas. SSC QCA privalo užtikrinti, kad CA atitiktų jai keliamus reikalavimus.

CA privatieji raktai. SSC QCA privalo užtikrinti, kad jos privatieji raktai (raktai, naudojami sudaromiems sertifikatams pasirašyti) būtų apsaugoti tinkamomis infrastruktūrinėmis, organizacinėmis, personalo ir saugumo priemonėmis.

Informacijos skelbimas. SSC QCA yra atsakinga už šių dokumentų paskelbimą:

Sertifikato taisyklių (CP);
Sertifikavimo veiklos nuostatų (CPS);
SSC QCA sertifikatų.

SSC QCA yra atsakinga už sertifikavimo paslaugų teikimą laikantis SSC QCA Sertifikato taisyklių ir šių Sertifikavimo veiklos nuostatų, bei sudarytų sertifikatų tvarkymą, be kita ko, atsakant už šiuos veiksmus:

i. pagal pareiškėjų prašymus sudarant Sertifikatus;
ii. išsiunčiant pareiškėjams pranešimą apie sudarytą Sertifikatą;
iii. užtikrinant, kad sertifikatai būtų viešai skelbiami;
iv. viešai skelbiant CRL (Atšauktų sertifikatų sąrašą).

2.1.2. SSC RA pareigos

Registravimo tarnyba (SSC RA) veikia laikantis šių sertifikavimo veiklos nuostatų ir atlieka dėl sertifikato išdavimo, sustabdymo ar galiojimo nutraukimo besikreipiančio asmens tapatybės patikrinimo, nustatymo ir patvirtinimo funkcijas. Pagrindinės jos pareigos yra:

- identifikuoti prašymą dėl sertifikato sudarymo pateikiantį asmenį;
- patvirtinti ryšį tarp parašo tikrinimo duomenų ir pareiškėjo asmenybės;
- patvirtinti tokį ryšį sertifikavimo tarnybai/tarnyboje;
- sudaryti sutartį su sertifikavimo tarnyba ir laikytis šios sutarties nuostatų.

Be to, SSC RA yra atsakinga ir privalo:

a) priimti ir patvirtinti prašymus sudaryti Sertifikatus iš fizinių asmenų (pareiškėjų), prašančių sudaryti Sertifikatus, pagal procedūras, nustatytas Sertifikato taisyklėse (CP) ir šiuose Nuostatuose (CPS);
b) priimti ir tvirtinti prašymus nutraukti sertifikatų galiojimą iš to prašančių asmenų pagal procedūras, nustatytas Sertifikato taisyklėse (CP) ir šiuose Nuostatuose (CPS);

c) nustatyti asmenų, prašančių nutraukti sertifikatų galiojimą, tapatybę.

2.1.3. Galutinio naudotojo / Pasirašančiojo asmens pareigos

Pasirašantysis asmuo ar Galutinis naudotojas įsipareigoja laikytis šių CPS sąlygų. Tai apima:

- laikytis šių CPS;
- tinkamai saugoti savo privatųjį raktą, būnant vieninteliu turėtoju, jei pasirašymas liečia fizinį asmenį (jeigu Galutinis naudotojas – frizinis asmuo) ;
- sutikti su tuo, kad naudojant viešojo rakto Sertifikatus SSC QCA atsakomybė yra ribojama taip, kaip numatyta šių CPS 2.2 skyriuje;
- sutikti su tuo, kad galiojančių, sustabdyto ir nutraukto galiojimo sertifikatų duomenys būti ištisą parą teikiami viešai;
- leisti asmens duomenų (asmens kodas, darbovietė, gimimo data, gyvenamoji vieta (adresas), namų telefono numeris, pavardė, telefono numeris, vardas, kreipimosi dėl sertifikato išdavimo duomenys (data, laikas, būdas ir pan.), elektroninio pašto adresas, el.parašo formavimo ir tikrinimo duomenys, sisteminės įrašų bylos, kiti duomenys, kurie būtini teikiant sertifikavimo paslaugas, sertifikato galiojimo pradžios/pabaigos terminai, identifikatorius ir naudojimo paskirties apribojimai; parašo tikrinimo duomenys, pasirašančio asmens spec. atributai (suteikti įgalinimai ir kt.), sertifikavimo paslaugų teikėjo saugus elektroninis parašas) tvarkymą sertifikavimo paslaugų, susijusių su elektroninio parašo naudojimu, numatytų 2000 m. liepos 11 d. LR Elektroninio parašo įstatymo (Nr.VIII-1822) 9 straipsnyje, teikimui ir tiesioginei rinkodarai;
- nedelsiant pranešti SSC RA apie duomenų, nurodytų sertifikate, pasikeitimus, pateikdamas tai patvirtinančius dokumentus. Duomenų pasikeitimą patvirtinančių dokumentų nereikia pateikti, jei pranešama apie teisių, nurodytų sertifikate, apimties sumažėjimą;
- nedelsiant pranešti SSC RA apie privačiojo rakto (pasirašymo duomenų) ar sertifikato praradimą, vagystę ar sunaikinimą.

2.1.4. Sertifikatais Pasitikinčių šalių pareigos

Sertifikatu Pasitikinti šalis turi būti susipažinusi su šiais Nuostatais (CPS) ir Sertifikavimo taisyklėmis (CP) prieš darydama kokias nors išvadas dėl to, kiek galima pasitikėti sertifikatu, išduotu laikantis šių CPS.

Pasitikinti šalis, siekdama nustatyti, ar jos gautas Sertifikatas galioja, privalo:

(a) kreiptis į CRL, arba
(b) pasinaudoti OCSP paslauga, arba
(c) pasinaudoti interneto sąsajomis,

ir tik po to vadovautis informacija, nurodyta Sertifikate.

Sertifikatais Pasitikinčios šalys turi naudoti Sertifikatus tik pagal šiuose Nuostatuose apibrėžtas jų paskirtis (taikymo sritis).

2.1.5. Informacinės tarnybos pareigos

SSC QCA yra atsakinga už sertifikatų duomenų teikimą parašo naudotojams elektroniniams parašams tikrinti (Lietuvos Respublikos elektroninio parašo įstatymo (Žin., 2000, Nr. 61-1827; 2002, Nr. 64-2572) 9 str. 1 dalis).

SSC QCA skelbia informaciją apie Sertifikatus, kuriuos ji išduoda realiu laiku viešai prieinamoje talpykloje https://repository.ssc.lt . SSC QCA pasilieka sau teisę skelbti informaciją apie sertifikato statusą trečiųjų šalių talpyklose.

SSC QCA išlaiko realiu laiku veikiančią dokumentų talpyklą, kur ji atskleidžia tam tikrą informaciją apie jos veiklą, procedūras ir tam tikrų jos veiklos krypčių/strategijų turinį, įskaitant jos CPS, kuri bus prieinama adresu:

http://www.ssc.lt/cps .

SSC QCA pasilieka sau teisę padaryti prieinamą ir skelbti informaciją apie jos veiklos kryptis bet kokiomis jos manymu tinkamomis priemonėmis.

SSC QCA steigia ir išlaiko visų savo išduotų sertifikatų talpyklą. Ši talpykla taip pat nurodo išduoto sertifikato statusą.

SSC QCA turi naudoti viešai prieinamą talpyklą laikyti Sertifikatus ir Atšauktų sertifikatų sąrašus (CRL).

SSC QCA reguliariai publikuoja Atšauktų Sertifikatų Sąrašus (CRL)[3] adresu http://www.ssc.lt/crl, atsižvelgiant į šių CPS 4.4.9 punktą. Kiekviename naujame Sertifikatų Galiojimo nutraukimo Sąraše turi būti visi pakeitimai, kurie buvo iki tol publikuotuose Atšauktų Sertifikatų Sąrašuose.

SSC QCA adresu http://ocsp.ssc.lt padaro prieinamą Sertifikatų Statuso Realiu Laiku Protokolo (OCSP)[4] tarnybinę stotį, pagal kurios duomenis SSC QCA sutinkamai su standartu IETF RFC 2560 Pasitikinčioms šalims realiu laiku išduoda pažymėjimą apie sertifikato statusą konkrečiu laiko momentu.

SSC QCA sukuria ir išlaiko Atšauktų Sertifikatų Sąrašų paskirstymo tašką ir informuoja apie tinklo arba tarnybinės stoties adresą (URL) iki visų sertifikatų, kuriuose yra nurodytas tas Atšauktų Sertifikatų Sąrašų paskirstymo taškas, galiojimo pabaigos, o tokiai informacijai pakitus – nedelsiant informuoja ir apie tokius pokyčius. Publikuotini dokumentai, nurodyti CPS 1.1 punkte, internetu siunčiami į Talpyklą per 24 valandas nuo jų patvirtinimo momento. SSC QCA nedaro viešai prieinamų tam tikrų šių dokumentų elementų, pvz., tam tikrų saugos kontrolės elementų, procedūrų, susijusių su *inter alia* registravimo tarnybų funkcionavimu, vidinių saugumo taisyklių ir t.t. Tačiau tokie dokumentai ir dokumentuota praktika turi būti prieinami juose nurodytiems asmenims, kuriems SSC QCA yra įsipareigojusi pateikti minėtus dokumentus ir dokumentuotą praktiką, kad tie asmenys galėtų atlikti jų patikrinimą (auditą).

2.2. Atsakomybė

2.2.1. SSC QCA atsakomybė

SSC QCA atsakomybė bus ribojama garantija, kad bus imamasi visų priemonių, reikalingų jos privačiojo rakto apsaugai.

SSC QCA atsako už:

1) sudaryto sertifikato duomenų tikslumą;
2) tai, kad sudarytame sertifikate nurodytas asmuo yra parašo formavimo duomenų, atitinkančių sertifikate nurodytus parašo tikrinimo duomenis, turėtojas;
3) parašo formavimo duomenų ir parašo tikrinimo duomenų atitikimą, kai jis asmens prašymu sukuria šiuos abu duomenis;
4) sertifikato galiojimo sustabdymą ar nutraukimą laiku;
5) SSC QCA privataus rakto apsaugą.

[3] Sertifikatų Galiojimo nutraukimo Sąrašas (CRL) yra sąrašas, kurį išleidžia ir elektroniniu parašu pasirašo CA. Sertifikatų Galiojimo nutraukimo Sąraše (CRL) nurodomi atšaukti sertifikatai ir sertifikatai, kurių galiojimas sustabdytas. Pasitikinčios šalys privalo susipažinti su šiuo sąrašu prieš pasitikėdamos informacija, esančia sertifikate.

[4] Sertifikatų Statuso Internetinis Protokolas (IETF RFC 2560) naudojamas realiu laiku (nereikalaujant Sertifikatų Galiojimo nutraukimo Sąrašo) gauti informaciją apie skaitmeninio sertifikato statusą.

2.2.1.1. Sertifikavimo tarnybos garantijos Galutiniams naudotojams ir Sertifikatais pasitikinčioms šalims

Garantijos, garantijų atsisakymai ir SSC QCA bei atitinkamų jos Klientų atsakomybės ribojimai yra nustatyti tarp jų sudarytose Sutartyse ir reguliuojami jų nuostatų.

SSC QCA garantuoja Galutiniams naudotojams, kad:

- Nėra jokių Sertifikate esančios informacijos klaidų, kurios padarytos prašymą dėl sertifikato tenkinančių ar išduodančių Sertifikatą tarnybų dėl to, kad jos nebuvo tinkamai/pakankamai rūpestingos nagrinėjant prašymą dėl Sertifikato ar parengdamos Sertifikatą;
- Sertifikatai atitinka visus esminius šių Nuostatų reikalavimus, ir
- Sertifikatų panaikinimo paslaugos ir talpyklos naudojimas atitinka šiuos Nuostatus visais esminiais aspektais.

SSC QCA garantuoja Sertifikatais Pasitikinčioms šalims, kurios pagrįstai pasitiki Sertifikatu, kad:

- Visa informacija, esanti tokiame Sertifikate ar įtraukta į jį darant nuorodą, išskyrus Nepatikrintą Galutinio naudotojo informaciją, yra tiksli, kaip tai numatyta Nuostatų 3.1. ir 3.2. skyriuose;
- Sertifikatams esant SSC QCA talpykloje, kad Sertifikatas buvo išduotas asmeniui, nurodytam (nurodytai) Sertifikate kaip Galutinis naudotojas, ir kad Galutinis naudotojas priėmė Sertifikatą pagal Nuostatų 4.3 skyrių, ir
- Prašymą dėl sertifikato tenkinančios ir Sertifikatą išduodančios tarnybos laikėsi šių Nuostatų išduodamos Sertifikatą.

Tiek, kiek leidžia taikytina teisė, SSC QCA dėl jokios savo sertifikavimo veiklos nesuteikia jokios garantijos – nei tiesioginės, nei numanomos – pagal šią Sutartį suteikiamoms Paslaugoms, taip pat nesuteikia jokios netiesioginės garantijos.

2.2.1.2. Sertifikavimo tarnybos atsakomybės apribojimai

SSC QCA jokiais atvejais atsakomybė neapima jokių asmenų, įskaitant Galutinius naudotojus ir kitus SSC Sertifikavimo sistemos dalyvius, netiesioginių, specialiųjų ir šalutinių nuostolių, negautų pajamų ar pelno. SSC QCA atsakomybės už nuostolius, susijusius su tam tikru Sertifikatu, ribos detalizuojamos specialiose/atskirose Sutartyse.

2.2.1.3. Nenugalima jėga (*force majeure*)

SSC QCA atleidžiama nuo šiuose CPS numatytų įsipareigojimų vykdymo, jei jų nevykdymas yra force majeure aplinkybių, kurių SSC QCA negalėjo numatyti arba išvengti, pasitelkdama protingas priemones, pasekmė. Į *force majeure* aplinkybes įeina SSC QCA valios nekontroliuojami įvykiai, pvz. žemės drebėjimas, potvynis, gaisras, taip pat streikas, valstybės institucijų sprendimai arba valstybės institucijų administraciniai veiksmai. SSC QCA, besiremianti force majeure aplinkybėmis, privalo raštu pranešti visiems suinteresuotiems asmenims apie tokių aplinkybių atsiradimą. Pranešime turi būti nurodyta data ir aplinkybių pobūdis, taip pat jų poveikio SSC QCA įsipareigojimų vykdymui įvertinimas, jei tas yra įmanoma, bei laikas, kada įsipareigojimai buvo paveikti. Nustatant force majeure aplinkybes vadovaujamasi Lietuvos Respublikos civilinio kodekso (Žin., 2000, Nr. 74-2262) 6.212 straipsnis), kitų įstatymų ir teisės aktų nuostatomis.

Pasibaigus nurodytų aplinkybių poveikiui, SSC QCA turi nedelsiant raštu informuoti apie tai suinteresuotuosius asmenis.

2.2.1.4. Kiti SSC QCA atleidimo nuo atsakomybės pagrindai ir atvejai

SSC QCA atleidžiama nuo atsakomybės, susijusios su ar kylančios iš šiuose CPS numatytų įsipareigojimų vykdymo ar nevykdymo, jei toks vykdymas ar nevykdymas yra valstybės veiksmų pasekmė. Šios nuostatos prasme valstybės veiksmai suprantami kaip privalomi ir nenumatyti valstybės institucijų veiksmai (aktai), dėl kurių įvykdyti prievolę neįmanoma ir kurių SSC QCA neturėjo teisės ginčyti.

SSC QCA atleidžiama nuo atsakomybės ir kitais Lietuvos Respublikos įstatymų numatytais atvejais.

2.2.2. SSC RA atsakomybė

Registravimo tarnybos atsakomybė bus ribojama garantija, kad bus atlikti visi patikrinimai, reikalingi kiekvieno pareiškėjo tapatybės nustatymui.

Garantijos, garantijų atsisakymai ir atsakomybės ribojimai tarp SSC RA ir SSC QCA yra išdėstyti tarp jų sudarytose Sutartyse ir reguliuojami jų nuostatų.

2.2.3. Galutinio naudotojo atsakomybė

Galutiniai naudotojai privalo garantuoti, jog:

- Kiekvienas elektroninis parašas, sukurtas naudojant pasirašančios asmens privatųjį raktą, atitinkantį viešąjį raktą, nurodytą Sertifikate, yra Galutinio naudotojo elektroninis parašas ir Sertifikatas buvo patvirtintas ir yra veikiantis (jo galiojimas nepasibaigęs ir jis nebuvo panaikintas) elektroninio parašo sukūrimo metu,
- Joks neįgaliotas asmuo niekada neturėjo prieigos prie Galutinio naudotojo privačiojo rakto,
- Visi Galutinio naudotojo ar jo įgalioto asmens (jeigu Galutinis naudotojas – juridinis asmuo) padaryti pareiškimai Prašyme dėl sertifikato yra tikri, teisingi ir galiojantys,
- Visa Galutinio naudotojo ar jo įgalioto asmens (jeigu Galutinis naudotojas – juridinis asmuo) pateikta ir Sertifikate esanti informacija yra tikra, teisinga ir galiojanti,
- Sertifikatas naudojamas išimtinai tiems tikslams, dėl kurių buvo išduotas ir kurie yra teisėti ir suderinamiems su šiais Nuostatais, ir
- Galutinis naudotojas yra ne CA ir nenaudoja privačiojo rakto, atitinkančio kokį nors viešąjį raktą, nurodytą Sertifikate, siekiant pasirašyti bet kokį Sertifikatą skaitmeniniu būdu (ar bet kokiu kitokiu sertifikuoto viešojo rakto pavidalu/forma) ar CRL kaip CA.

Kitose Sutartyse taip pat turi būti įtvirtinti aukščiau nurodyti reikalavimai.

2.2.4. Sertifikatu pasitikinčios šalies atsakomybė

Sertifikatais Pasitikinčios šalys privalo garantuoti, (a) kad jos turi pakankamai informacijos, kad padarytų kompetentingą sprendimą dėl to, kiek jos pasitikės Sertifikate esančia informacija, (b) kad jos vienintelės yra atsakingos nuspręsti, ar pasitikėti tokia informacija, ar nepasitikėti, ir (c) kad jos prisiims visas teisines pasekmes, kylančias iš jų, kaip Sertifikatais Pasitikinčių šalių įsipareigojimų, numatytų Nuostatų 2.1 skyriuje.

2.3. Finansinė atsakomybė

SSC QCA neprisiima jokios finansinės atsakomybės už pagal šiuos Nuostatus išduotus Sertifikatus. Finansinių nuostolių atlyginimą garantuoja SSC QCA civilinės atsakomybės draudimas.

2.3.1. Kompensacija Galutiniams naudotojams ir Sertifikatais pasitikinčioms šalims

2.3.1.1. Galutinių naudotojų kompensacija

Tiek, kiek leidžia taikytina teisė, Galutiniai naudotojai privalo kompensuoti SSC QCA ar RA patirtus nuostolius (žalą) tais atvejais, kai:

- Pasirašytojas prašyme dėl Sertifikato nurodė netikslų ar neteisingą faktą,
- Pasirašytojas prašyme dėl sertifikato neatskleidė reikšmingo fakto,
- Pasirašytojas neapsaugojo privačiojo rakto, nenaudojo patikimos sistemos ar nesiėmė kitų atsargumo priemonių, būtinų siekiant užkirsti kelią Galutinio naudotojo privačiojo rakto (parašo formavimo duomenų) praradimui, netekimui, atskleidimui, pakeitimui ar neteisėtam naudojimui, ar
- Pasirašytojas naudojo vardą ar pavadinimą (įskaitant interneto domeno pavadinimą ar elektroninio pašto adresą, bet tuo neapsiribojant), kuris pažeidžia trečiosios šalies intelektinės nuosavybės teises.

2.3.1.2. Sertifikatais pasitikinčių šalių kompensacija

Sertifikatais pasitikinčioms šalims nėra kompensuojami nuostoliai (žala) tais atvejais, kai, jie atsirado dėl to, kad:

- Sertifikatu Pasitikinti šalis nevykdo savo pareigų;
- Sertifikatu Pasitikinti šalis be pakankamo pagrindo pasitikėjo sertifikatu, arba
- Sertifikatu Pasitikinti šalis nepatikrino tokio sertifikato statuso siekiant nustatyti, ar sertifikato galiojimas nepasibaigęs ir ar jis nėra atšauktas.

2.3.2. Pasitikėjimo santykiai

Netaikytina.

2.3.3. Administraciniai procesai

Netaikytina.

2.4. Aiškinimas ir vykdymas

2.4.1. Taikytina teisė

Atsižvelgiant į bet kokius ribojimus, esančius taikytinoje teisėje, turi būti vadovaujamasi Lietuvos Respublikos teise vykdant, aiškinant ir taikant šiuos Nuostatus ir nustatant jų galiojimą nepriklausomai nuo Sutarties ar kitų pasirinktos teisės nuostatų ir nepriklausomai nuo to, kad Pasitikinčioji šalis neturi buveinės, gyvenamosios ar verslo vietos Lietuvos Respublikoje.

Šiuo teisės pasirinkimu siekiama užtikrinti vieningas procedūras/tvarką ir aiškinimą visiems SSC QCA Sistemos Dalyviams, nepriklausomai nuo jų buvimo vietos.

Sutartyse, kuriose Nuostatai įtraukti darant nuorodą, gali būti tik joms taikytinos teisės nuostatų, su sąlyga, kad šiuo Nuostatų 2.4.1 punktu turi būti vadovaujamasi vykdant, taikant ir aiškinant Nuostatų sąlygas ir nustatant jų galiojimą atskirai, atsižvelgiant į bet kokius taikytinoje teisėje esančius apribojimus.

Pagal Lietuvos Respublikos elektroninio parašo įstatymą (2000 m. liepos 11 d., Nr. VIII – 1822, pakeistą 2002 m. birželio 6 d., Nr. IX – 934), SSC QCA yra sertifikavimo paslaugas turinti teisę teikti tarnyba, išduodanti **kvalifikuotus Sertifikatus**.

2.4.2. Atskiriamumas, išlikimas, sujungimas/atnaujinimas, pranešimas

Tiek, kiek yra leidžiama pagal taikytiną teisę, SSC QCA Sutartyse ir Bendrosiose sąlygose yra ir kitose Sutartyse turi būti numatytos atskiriamumo, išlikimo, atnaujinimo ir pranešimo sąlygos. Sutarties sąlyga dėl atskiriamumo užkerta kelią tam, kad dėl Sutarties nuostatos negaliojimo ar neįgyvendinamumo būtų įtakojamas likusios Sutarties dalies galiojimas ar vykdymas. Sąlyga dėl išlikimo nurodo Sutarties nuostatas, kurios lieka galioti, nepaisant Sutarties nutraukimo ar galiojimo pabaigos. Sąlyga dėl sujungimo/atnaujinimo patvirtina, kad visi susitarimai dėl Sutarties pagrindinio dalyko/esmės yra įtraukti į Sutartį. Sutarties sąlyga dėl pranešimo nustato, kaip šalys turi pateikti viena kitai pranešimus.

2.4.3. Ginčų sprendimo tvarka

Bet kokie ginčai dėl šio CPS ar su jo taikymu ar aiškinimu susiję nesutarimai ar prieštaravimai (įskaitant, bet neribojant prieš tai einančios nuostatos bendrumo, dėl CPS įsigaliojimo, galiojimo, vykdymo, nutraukimo ir jo pažeidimo) (toliau - Ginčas) sprendžiami geranoriškomis Šalių derybomis, konsultacijomis.

Jei tokie nesutarimai negali būti išspręsti derybų keliu, juos sprendžia kompetentingas SSC QCA buveinės vietos teismas.

2.5. Atlyginimas

2.5.1. Sertifikato išdavimo ar atnaujinimo mokestis

SSC QCA turi teisę nustatyti Galutiniams naudotojams mokesčius už Sertifikatų išdavimą, tvarkymą ir atnaujinimą, sustabdymą, atšaukimą.

2.5.2. Mokesčiai už Priėjimą prie Sertifikato

SSC QCA nenustato mokesčio kaip sąlygos padaryti Sertifikatą prieinamą talpykloje ar kitaip padaryti Sertifikatus prieinamus Sertifikatais Pasitikinčioms šalims.

2.5.3. Sertifikato galiojimo nutraukimo ar informacijos apie Sertifikato statusą suteikimo mokestis

SSC QCA nenustato jokio mokesčio kaip sąlygos suteikiant prieigą prie Atšauktų sertifikatų sąrašo (CRL), nurodyto šių Nuostatų 4.4.9 punkte, prieinamo talpykloje ar kitaip prieinamo Sertifikatais Pasitikinčioms šalims. Vis tik SSC QCA nustato mokestį už (a) užsakytų ir prie individualios naudotojo užklausos pritaikytų CRL pateikimą, (b) OCSP paslaugų teikimą ir (c) paslaugas už informacijos apie konkretaus Sertifikato statusą teikimą. SSC QCA viešai suteikia prieigą prie informacijos apie Sertifikato atšaukimą, statusą ar jo laiko žymos nustatymą.

2.5.4. Mokesčiai už kitas paslaugas

SSC QCA nenustato jokio mokesčio už priėjimą prie CP ar šių Nuostatų. Bet kokia nauda, gauta siekiant kitų tikslų nei tiesiog peržiūrėti šį dokumentą, tokių kaip atgaminimas, platinimas, viešas paskelbimas, pakeitimas ar neoriginalių versijų sukūrimas gali būti atliekamas tik sutarties su SSC QCA pagrindu.

2.5.5. Grąžinimo taisyklės/nuostatos

Netaikytina.

2.6. Prieigos prie talpyklų kontrolė

Prieiga prie SSC QCA Sertifikato Taisyklių, šių CPS ir CRL visada turi būti nemokama, tačiau pagal sutartis su Galutiniais naudotojais ar Pasitikinčiomis šalimis SSC QCA turi teisę imti mokestį už tokias paslaugas, kaip informacijos apie sertifikatų statusą publikavimas trečiųjų asmenų duomenų bazėse ar privačiose tarnybinėse stotyse ir/ar direktorijose (*private directory*) ir kt.

SSC QCA svetainėje internete viešai prieinami: (a) OCSP paslauga, (b) sertifikato statuso patikrinimo per interneto sąsają paslauga, (c) sertifikatų talpykla ir (d) Atšauktų Sertifikatų Sąrašai.

Prieiga prie šių SSC QCA paslaugų gali būti ribojama tokiais būdais (būdų sąrašas nėra baigtinis):

1. tik SSC RA ir Lietuvos Respublikos Vyriausybės įgaliotos teisėsaugos institucijos turi teisę pateikti sertifikatų talpyklai bendrąsias užklausas, kurių pateikimo rezultatas yra daugiau kaip vieno sertifikato (sertifikatų rinkinių) išdavimas;

2. viešai prieinančiam prie sertifikatų talpyklos naudotojui vienos užklausos metu išduodamas tik vienas Sertifikatas; šis ribojimas netaikomas, kai užklausą pateikia SSC RA ar Lietuvos Respublikos Vyriausybės įgaliotos teisėsaugos institucijos;

3. SSC QCA turi teisę imtis protingų priemonių užkertant kelią piktnaudžiavimui OCSP paslauga, sertifikato statuso patikrinimo per interneto sąsają paslauga, Atšauktų Sertifikatų Sąrašų parsisiuntimo internetu paslauga. Tokios priemonės gali būti, pvz.:

    a. SSC QCA turi teisę apriboti OCSP užklausų skaičių iki 10 užklausų vienam naudotojui per 24 valandas. Asmenims, kuriems dėl jų veiklos prigimties dažnas OCSP naudojimas yra būtinas, būtina sudaryti atskirą sutartį su SSC QCA;
    b. SSC QCA turi teisę apriboti sertifikato statuso patikrinimo per interneto sąsają užklausų skaičių iki 10 užklausų vienam naudotojui per 24 valandas;
    c. SSC QCA turi teisę apriboti Atšauktų Sertifikatų Sąrašų sėkmingų parsisiuntimų internetu skaičių iki 2 parsisiuntimų vienam naudotojui per 24 valandas.

2.7. Veiklos atitikimo patikrinimas

SSC QCA pati įvertina savo veiklos atitikimą Sertifikavimo veiklos nuostatams ir Sertifikavimo taisyklėms. Šios veiklos atitikimo išorinę kontrolę gali atlikti kompetentingos institucijos ar kiti subjektai Lietuvos Respublikos teisės aktų nustatyta tvarka.

Veiklos atitikimo patikrinimo ataskaitoje nustatoma ar SSC QCA laikosi sertifikato taisyklių, tikslų ir procedūrinių reikalavimų, SSC QCA įdiegta valdymo sistema atitinka standartų reikalavimus ir siekia tikslų, numatytų CA įgyvendinamose sertifikato taisyklėse.

Vertinimo ataskaitoje pateikiama:

1. SSC QCA organizacinės struktūros aprašas, jos patikimumo vertinimas
2. Peržiūrėtų dokumentų santrauka ir vertinimas;
3. SSC QCA informacijos saugumo rizikos analizė ir vertinimas;

4. Neatitikimų sąrašas, jeigu tokių yra;
5. Rekomendacijos ar SSC QCA atitinka kvalifikuotų sertifikatų išdavėjų reikalavimus.

2.7.1. Patikrinimų dažnumas

Netaikoma.

2.7.2. Kvalifikaciniai ir kiti reikalavimai tikrintojui

Netaikoma.

2.7.3. Tikrintojo santykis su tikrinamuoju asmeniu

Netaikoma.

2.7.4. Tikrinamos veiklos sritys

Netaikoma.

2.7.5. Priemonės, taikomos patikrinimo metu aptikus trūkumų

Netaikoma.

2.7.6. Pranešimas apie rezultatus

Netaikoma.

2.8. Konfidencialumas

Visa informacija, kurią SSC QCA surenka apie Galutinius naudotojus, yra apdorojama tokiais būdais, kurie užtikrina asmens duomenų ir privatumo apsaugą pagal Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymą (2003 m. sausio 21 d., Nr. IX-1296).

SSC QCA privatumo apsaugos taisykles publikuoja adresu https://repository.ssc.lt.

SSC QCA pagal Lietuvos Respublikos įstatymų reikalavimus yra įsiregistravusi kaip duomenų valdytojas viešajame Asmens duomenų valdytojų registre (Registracijos Nr. P-3069).

2.8.1. Informacijos, kuri laikoma konfidencialia, rūšys

Šių CPS tikslais konfidenciali yra laikoma visa informacija apie pasirašančiuosius asmenis, išskyrus informaciją, kuri įtraukta į viešus Sertifikatus ir CRL. Konkrečiai imant, bet neapsiribojant žemiau išdėstytu, ši informacija apie Galutinius naudotojus yra laikoma konfidenciali (toliau - "Konfidenciali/Privati Informacija") ir negali būti atskleista be aiškaus Galutinio naudotojo sutikimo, išskyrus Lietuvos Respublikos teisės aktų nustatytus atvejus:

- informacija apie prašymus, paduotus SSC QCA, nepriklausomai nuo to, ar prašymai buvo patenkinti;
- informacija apie prašymus sudaryti Sertifikatą;
- SSC QCA laikomi privatūs raktai (jeigu tokių yra) ir informacija, reikalinga tokių privačių raktų atstatymui;

- patikrinimų medžiaga (angl. *audit trail records*), parengta ar saugoma SSC QCA ar Kliento;
- SSC QCA patikrinimų ataskaitos, parengtos SSC QCA ar konkrečių tikrintojų (tiek išorės, tiek vidaus);
- informacija apie nenumatytų įvykių planavimą;
- informacijos atkūrimo stichinių nelaimių atvejais planai; ir
- informacija apie saugos priemones, skirtas SSC QCA kompiuterinės technikos ir programinės įrangos, sertifikavimo paslaugų teikimo administravimo, paraiškų sertifikatui gauti ir registravimo paslaugų kontrolei.

2.8.2. Viešai teikiami duomenys

SSC QCA Sertifikavimo sistemos Dalyviai patvirtina, kad galiojančių ir nutraukto galiojimo sertifikatų duomenys nebus laikoma konfidencialia informacija.

2.8.3. Informacijos apie sertifikatų atšaukimą/galiojimo sustabdymą atskleidimas

Sertifikato galiojimo nutraukimo, jo galiojimo sustabdymo priežastis *GALI* būti nurodoma Atšauktų Sertifikatų Sąraše. Duomenys apie tokią priežastį nėra laikomi konfidencialiais ir gali būti pateikti visiems kitiems Galutiniams naudotojams bei Pasitikinčioms šalims. Tačiau kiti duomenys apie sertifikato atšaukimą paprastai nėra atskleidžiami.

2.8.4. Informacijos atskleidimas teisėsaugos institucijoms

SSC QCA neturi teisės atskleisti Konfidencialios informacijos trečiosioms šalims, išskyrus atvejus, kai to reikalauja kompetentingų institucijų pareigūnai, atstovai, kuriems tokią teisę numato Lietuvos Respublikos teisės aktai ir/ar turintys teisės aktų reikalaujamą leidimą.

2.8.5. Informacijos atskleidimas kaip atskleidimo civiliniame procese dalis

Netaikoma.

2.8.6. Informacijos atskleidimas Pasirašytojui

SSC QCA neturi teisės trečiosioms šalims atskleisti Konfidencialios informacijos, išskyrus atvejus, kai to raštu reikalauja Pasirašytojas ir išskyrus Lietuvos Respublikos teisės aktų nustatytus atvejus.

2.8.7. Kitos aplinkybės, susijusios su informacijos atskleidimu

Netaikoma.

2.9. Intelektinės nuosavybės teisės

2.9.1. Intelektinės nuosavybės teisės į Sertifikatus ir į informaciją apie sertifikatų atšaukimą

SSC QCA išsaugo visas intelektinės nuosavybės teises į jos sudarytus Sertifikatus ir į informaciją apie jos sudarytų sertifikatų atšaukimą. SSC QCA ir Galutiniai naudotojai duoda leidimą atgaminti ir platinti Sertifikatus neatlygintinai, neišimtinai ir su sąlyga, kad Sertifikatas atgaminamas visa apimtimi ir su sąlyga, kad sertifikatai naudojami vadovaujantis Bendrosiomis sąlygomis, nurodytais sertifikate. SSC QCA ir Galutiniai naudotojai

duoda sutikimą naudoti informaciją apie sertifikatų atšaukimą tam, kad Pasitikinčios Šalys galėtų atlikti savo funkcijas vadovaudamosi taikytinomis Bendrosiomis sąlygomis, ar kitais susitarimais.

2.9.2. Intelektinės nuosavybės teisės į šiuos CPS

SSC QCA išsaugo visas intelektinės nuosavybės teises į šiuos CPS ir CP.

2.9.3. Intelektinės nuosavybės teisės į prekių (paslaugų) ženklą, pavadinimą

Asmuo, prašantis sudaryti Sertifikatą išsaugo visas teises, kurias jis turi į prekės ženklą, paslaugų ženklą, juridinio asmens pavadinimą, nurodytą prašyme sudaryti Sertifikatą, ir į turintį skiriamųjų požymių vardą (pseudonimą), nurodytą bet kuriame sertifikate, išduotame tokiam asmeniui, prašančiam sudaryti Sertifikatą.

2.9.4 Intelektinės nuosavybės teisės į parašo formavimo duomenis ir į jų medžiagą

Raktų poros, atitinkančios Galutinio Naudotojo Sertifikatus, yra Galutinio naudotojo nuosavybė, nepriklausomai nuo to, kokioje laikmenoje raktų poros yra laikomos ir saugomos. Visos intelektinės nuosavybės teisės į raktų poras, atitinkančias Galutinio Naudotojo Sertifikatus, priklauso Galutiniam naudotojui. Tačiau:

1) SSC QCA šakniniai viešieji raktai ir juos atitinkantys šakniniai sertifikatai, įskaitant visus SSC QCA viešuosius raktus ir savo pasirašytus (angl. *self-signed*) Sertifikatus, yra SSC QCA nuosavybė. SSC QCA išduoda licencijas programinės įrangos ir kompiuterinės technikos gamintojams atgaminti tokius šakninius Sertifikatus tam, kad šių kopijos būtų patalpinamos į patikimą programinę įrangą ir kompiuterinę techniką, įskaitant parašo formavimo ir tikrinimo įrangą;

2) SSC QCA privatusis raktas (parašo formavimo duomenys) yra SSC QCA nuosavybė; SSC QCA išsaugo visas intelektinės nuosavybės teises į jai priklausantį privatų raktą.

3. IDENTIFIKAVIMAS IR TAPATYBĖS NUSTATYMAS

Šiame skyriuje aprašomos procedūros, taikomos prieš sertifikato sudarymą, prieš kito rakto išdavimą, sertifikato galiojimo sustabdymą ar nutraukimą, siekiant nustatyti ir patvirtinti asmens, prašančio sudaryti Sertifikatą, tapatybę, o taip pat nustato taisykles, susijusias su vardų naudojimu.

3.1. Identifikavimas

3.1.1. Vardų (pseudonimų) tipai

SSC QCA sudaromuose sertifikatuose negali būti tuščių laukelių. SSC QCA privalo nurodyti papildomą identifikavimo informaciją Pasirašytojo alternatyviajame varde -elektroninio pašto adresą

Pasirašytojo vardo arba pseudonimo laukeliuose turi būti nurodomas skiriamųjų požymių turintis vardas (pseudonimas), kuris atitinka X.501 standartą, ir yra sudarytas iš komponentų, nurodytų žemiau pateikiamoje lentelėje Nr. 2.1.

Lentelė Nr. 2.1 – Pasirašytojo skiriamųjų požymių turinčio vardo atributai SSC QCA išduodamuose sertifikatuose

Atributas	Reikšmė		
	1-os klasės sertifikatas	2-os klasės sertifikatas	3-os klasės sertifikatas
Valstybė (*countryName*)	Lietuvos piliečiams bei asmenims, turintiems leidima nuolat gyventi Lietuvos Respublikoje - "LT", kitiems – pagal registracijos šalį, arba netaikoma.		
Organizacija (*organizationName*)	„fizinis asmuo"	Į juridinio asmens atributą įrašomas Galutinio Naudotojo juridinio asmens pavadinimas. Jeigu šio pavadinimo ilgis viršyja 64 simbolius, leidžiama trumpinti pavadinimą arba naudoti sutrumpinimus (lentelė 2.2). Į fizinio asmens atributą įrašoma „fizinis asmuo".	
Juridinio asmens struktūrinis padalinys/skyrius (*organizationalUnitName*)	Netaikomas.	Į juridinio asmens atributą įrašomas Galutinio Naudotojo juridinio asmens struktūrinio padalinio arba skyriaus pavadinimas. Fiziniam asmeniui šis atributas nenaudojamas.	
Vietovė (*localityName*)	Netaikomas.	Nurodoma vietovė, kurioje yra Galutinis Naudotojas, arba netaikoma.	
Adresas (*postalAddress*)	Netaikomas.	Nurodomas Galutinio naudotojo pašto adresas, arba netaikoma. Juridinio asmens atvėju Adresas yra organizacijos registracijos adresas.	
Įprastinis pavadinimas *(commonName)*	Šiame atribute įrašomi vardas(-ai) arba netaikomas, jei naudojamas pseudonimas („*pseudonym*" atributas).	Šiame atribute įrašoma: • juridinio asmens pavadinimas (jei atributas yra sertifikate, kuriuo pasirašomas programinis kodas/objektas); • vardas(-ai), pavardė, jei atributas yra asmens sertifikate; • tarnybinės stoties pavadinimas (tarnybinių stočių sertifikatams). Netaikomas, jei naudojamas pseudonimas („*pseudonym*" atributas).	Šiame atribute įrašomi asmens vardas(-ai) ir pavardė arba netaikomas, jei naudojamas pseudonimas („*pseudonym*" atributas).
Pseudonimas (*pseudonym*)	Netaikomas.	Pasirašytojo pseudonimas. Netaikomas, jeigu naudojamas įprastinis pavadinimas („*commonName*" atributas).	

Atributas	Reikšmė		
	1-os klasės sertifikatas	2-os klasės sertifikatas	3-os klasės sertifikatas
Sertifikato serijos numeris (*serialNumber*)	Unikalus ėsamo CA ribose sertifikato serijos numeris (arba netaikoma).		

Lentelė Nr. 2.2. Pasirašytojo skiriamųjų požymių turinčio vardo atributų sutrumpinimai SSC QCA išduodamuose sertifikatuose

Sutrumpinimas	Reikšmė
LR	Lietuvos Respublika(-os)
LRV	Lietuvos Respublikos Vyriausybė(-ės)

3.1.2. Reikalavimas, kad vardai (pseudonimai) būtų reikšminiai

Pasirašytojo vardas (pseudonimas) sertifikate turi būti reikšminis, t. y. sertifikavimo tarnyba privalo turėti tinkamą įrodymą, kad yra ryšys tarp to vardo (pseudonimo) ir subjekto, kuriam vardas priklauso.

Visų klasių Galutinio Naudotojo sertifikatuose esantys vardai, pavardės (pseudonimai) privalo turėti įprastinę semantinę reikšmę, kuri leistų nustatyti Pasirašytojo tapatybę.

3.1.3. Taisyklės įvairioms vardų (pseudonimų) formoms aiškinti

SSC QCA negali sertifikatuose naudoti vardų ir pavadinimų, kurie gali pažeisti žmonių grupių ar konkrečių asmenų teises (pvz., rasinę, tautinę, lytinę ar kitokio pobūdžio nesantaiką kurstančios juridinio asmens pavadinimas) ar prieštarauja viešajai tvarkai ar gerai moralei.

3.1.4. Vardų (pseudonimų) unikalumas

Kiekvieno subjekto, kurį sertifikavo SSC QCA (kaip tai nurodyta sertifikato sudarytojo pavadinimo laukelyje), skiriamųjų požymių turintis vardas turi būti unikalus.

3.1.5. Ginčų dėl vardo (pavadinimo) sprendimo procedūra

Asmenims, prašantiems sudaryti Sertifikatus, draudžiama prašymuose sudaryti Sertifikatus nurodyti vardus (pavadinimus), kurie pažeistų kitų asmenų intelektinės nuosavybės teises. Tačiau SSC QCA netikrina, ar asmuo, prašantis sudaryti Sertifikatą, turi intelektinės nuosavybė teises į vardą (pavadinimą), nurodytą prašyme sudaryti Sertifikatą, taip pat nearbitruoja, netarpininkauja ar kitaip nesprendžia ginčų, susijusių su nuosavybės teisėmis į interneto domeno pavadinimą, juridinio asmens pavadinimą, prekių ženklą ar paslaugų ženklą. SSC QCA turi teisę, esant tokiems ginčams, atmesti prašymą sudaryti Sertifikatą arba sustabdyti tokio prašymo nagrinėjimą, ir SSC QCA dėl to nekyla jokia atsakomybė nei prieš asmenį, prašantį sudaryti Sertifikatą, nei prieš trečiuosius asmenis.

3.1.6. Prekių ženklų pripažinimas, tapatybės nustatymas ir vaidmuo

Netaikoma.

3.1.7. Privataus rakto turėjimo įrodymo metodai

SSC QCA priima tik tuos prašymus sudaryti Sertifikatą, kuriuose yra tinkamų įrodymų apie atitinkamo privataus rakto (parašo formavimo duomenų) turėjimą. Toks įrodymas gali būti pasirašytas PKCS#10 prašymas sudaryti Sertifikatą, kurį SSC QCA siunčia SSC RA.

3.2. Tapatybės nustatymas

3.2.1. Pasirašytojo tapatybės nustatymas

1-os klasės sertifikatai

Norėdamas tapti SSC QCA sertifikavimo sistemos dalyviu, asmuo elektroniniu būdu (el. paštas, forma tinklalapyje) pateikia SSC RA užpildytą paraišką sertifikatui gauti.

Fizinių asmenų tapatybės nustatymas 1-os klasės sertifikatų atžvilgiu susideda iš įsitikinimo, kad Pasirašytojo vardas, turintis skiriamųjų požymių, yra unikalus ir vienareikšmis SSC QCA 1-os klasės CA sertifikavimo sistemoje.

1-os klasės tapatybės nustatymas neužtikrina tapatybės (t.y. to, kad Galutinis naudotojas yra būtent tas asmuo, kuriuo save nurodo). Įprastinis Galutinio naudotojo vardas ir pavardė yra netikrinamoji Galutinio naudotojo informacija. Tikrinant Pasirašytojo tapatybę, atliekama tik jo vardo ir elektroninio pašto adreso paieška, siekiant užtikrinti, kad Galutinio naudotojo Sertifikatas būtų unikalus ir neklaidinantis CA Sertifikavimo sistemoje.

Į 1-os klasės funkciją taip pat įeina ribotas asmens, prašančio sudaryti Sertifikatą, elektroninio pašto adreso patvirtinimas.

2-os klasės sertifikatai

Norėdamas tapti sertifikavimo sistemos dalyviu, asmuo raštu, faksu, elektroniniu paštu ar per tinklalapį pateikia SSC RA užpildytą paraišką sertifikatui gauti.

SSC RA įsitikina asmens, prašančio sudaryti fizinio asmens Sertifikatą, tapatybe reikalaudama, kad pareiškėjas pateiktų jo tapatybę identifikuojančius galiojančius dokumentus, kuriuose privalo būti šie duomenys:

- asmens, veikiančio savo arba kito fizinio asmens interesais:
- vardas ir pavardė;
- asmens kodas (taikoma Lietuvos Respublikos piliečiams ir užsieniečiams, turintiems leidimus nuolat gyventi Lietuvos Respublikoje);
- gimimo data;,
- leidimo laikinai apsigyventi Lietuvos Respublikoje numeris ir jo galiojimo laikas (taikoma asmenims, turintiems leidimus laikinai apsigyventi Lietuvos Respublikoje);
- gimimo data, paso arba jį atitinkančio kelionės dokumento numeris, jo išdavimo vieta ir data (taikoma užsienio valstybės piliečiams);
- gimimo data, leidimo nuolat gyventi užsienio valstybėje numeris ir galiojimo laikas, jo išdavimo vieta ir data (taikoma užsieniečiams, nuolat gyvenantiems užsienio valstybėje);
- Lietuvos Respublikos civilinio kodekso[5] reikalavimus atitinkantis įgaliojimas būtinas tuo atveju, kai asmuo veikia kito fizinio asmens vardu.

[5] Valstybės Žinios, 2000, Nr.: 74, Publikacijos Nr.: 2262; Valstybės Žinios, 2000, Nr.: 77; Valstybės Žinios, 2000, Nr.: 80; Valstybės Žinios, 2000, Nr.: 82.

SSC RA papildomai įsitikina asmens, prašančio sudaryti Sertifikatą juridinio asmens vardu, tapatybe patikrindamas šiuos duomenis:

- atstovaujamojo juridinio asmens pavadinimą;
- atstovaujamojo juridinio asmens teisinę formą;
- atstovaujamojo juridinio asmens buveinę;
- atstovaujamojo juridinio asmens įmonės kodą;
- atstovaujamojo juridinio asmens registravimo pažymėjimo numerį ir išdavimo datą;
- įgalinimus gauti ir naudoti Sertifikatą atstovaujamojo vardu;
- viešojo registro, trečiųjų asmenų duomenų bazių informaciją apie juridinį asmenį.

SSC RA patikrina, ar pateikti visi paraiškoje reikalaujami duomenys, o esant reikalui, pareikalauja papildomų dokumentų ir paaiškinimų. Surinkęs visus reikalaujamus dokumentus, SSC RA priima sprendimą, ar asmuo gali tapti sertifikavimo sistemos klientu.

2-os klasės tarnybinių stočių sertifikatai

Tarnybinių stočių (TS) sertifikatai yra skirti organizacijos arba fizinio asmens tarnybinės stoties tapatybės nustatymui. Specifiniai 2-os klasės TS sertifikatų tipai yra nurodyti šių CPS 1.3 skyriuje.

SSC RA apdoroja asmenų, prašančių sudaryti 2-os klasės TS sertifikatus, paraiškas šia tvarka:

- SSC RA pagal šių CPS 3.2 skyriaus nuostatas įsitikina, kad juridinis asmuo, kurioje dirba Pareiškėjas, ar kuri kitaip jį išlaiko, egzistuoja; SSC RA pagal šių CPS 3.2 skyriaus nuostatas patvirtina to juridinio asmens tapatybę;
- SSC RA įsitikina, kad Pareiškėjas dirba konkrečioje organizacijoje ir yra įgaliotas jos vardu užsakyti sertifikatą.

Papildomos procedūros atliekamos šiems sertifikatų tipams:

Sertifikato tipas	***Papildomos procedūros***
Visi tarnybinių stočių sertifikatai	SSC QCA įsitikina, kad asmuo prašantis sudaryti Sertifikatą, būtų tarnybinės stoties registruotas interneto domeno pavadinimo savininkas ar kitu pagrindu turėtų teisę naudotis interneto domenu.

3-os klasės Galutinių Naudotojų sertifikatai

Norėdamas tapti sertifikavimo sistemos dalyviu, asmuo raštu, faksu, elektroniniu paštu ar per tinklalapį pateikia SSC RA užpildytą paraišką sertifikatui gauti.

SSC RA įsitikina asmens, prašančio sudaryti fizinio asmens Sertifikatą, tapatybe reikalaudama, kad pareiškėjas pateiktų jo tapatybę identifikuojančius galiojančius dokumentus, kuriuose privalo būti šie duomenys:

- asmens vardas ir pavardė;
- asmens kodas (taikoma Lietuvos Respublikos piliečiams ir užsieniečiams, turintiems leidimus nuolat gyventi Lietuvos Respublikoje);
- gimimo data;
- leidimo laikinai apsigyventi Lietuvos Respublikoje numeris ir jo galiojimo laikas (taikoma asmenims, turintiems leidimus laikinai apsigyventi Lietuvos Respublikoje);

- paso arba jį atitinkančio kelionės dokumento numeris, jo išdavimo vieta ir data (taikoma užsienio valstybės piliečiams);
- leidimo nuolat gyventi užsienio valstybėje numeris ir galiojimo laikas, jo išdavimo vieta ir data (taikoma užsieniečiams, nuolat gyvenantiems užsienio valstybėje);
- Lietuvos Respublikos civilinio kodekso[6] reikalavimus atitinkantis įgaliojimas būtinas tuo atveju, kai asmuo veikia kito fizinio asmens vardu.

SSC RA papildomai įsitikina asmens, prašančio sudaryti Sertifikatą juridinio asmens vardu, tapatybe patikrindamas šiuos duomenis:

- atstovaujamojo juridinio asmens pavadinimą;
- atstovaujamojo juridinio asmens teisinę formą;
- atstovaujamojo juridinio asmens buveinę;
- atstovaujamojo juridinio asmens įmonės kodą;
- atstovaujamojo juridinio asmens registravimo pažymėjimo numerį ir išdavimo datą;
- įgalinimus gauti ir naudoti Sertifikatą atstovaujamojo vardu;
- viešojo registro, trečiųjų asmenų duomenų bazių informaciją apie juridinį asmenį.

SSC RA patikrina, ar pateikti visi paraiškoje reikalaujami duomenys, o esant reikalui, pareikalauja papildomų dokumentų ir paaiškinimų. Surinkęs visus reikalaujamus dokumentus, SSC RA priima sprendimą, ar asmuo gali tapti SSC QCA sertifikavimo sistemos dalyviu.

3-os klasės sertifikatai, sudaromi administratoriams

SSC RA autentifikuoja asmenų, prašančių sudaryti 3-os klasės Sertifikatus, išduodamus Administratoriams, tapatybę šia tvarka:

- SSC RA pagal šių CPS 3.2 skyriaus nuostatas įsitikina, kad juridinis asmuo, kurioje dirba Administratorius, ar kuri kitaip jį išlaiko, egzistuoja; SSC RA pagal šių CPS 3.2 skyriaus nuostatas patvirtina to juridinio asmens tapatybę;
- SSC RA įsitikina, kad asmuo, prašyme sudaryti Sertifikatą nurodytas kaip Administratorius, dirba konkrečioje organizacijoje ir yra įgaliotas veikti kaip Administratorius.

SSC RA taip pat patvirtina prašymus sudaryti Sertifikatą savo pačios Administratoriams. Administratoriai savo organizacijoje yra "Patikimi Asmenys" (žr. šių CPS 5.2.1 punktą). Šiuo atveju jų prašymų sudaryti Sertifikatą tapatybės nustatymas remiasi:

(i) įsitikinimu, kad jie dirba organizacijoje ar yra juridinio asmens samdomi kaip nepriklausoma sutarties šalis (žr. šių CPS 5.2.3 punktą);
(ii) patikrinimu, ar jie įgalinti veikti kaip Administratoriai.

3.3. Sutartys ir kiti dokumentai

Nusprendus patenkinti paraišką, ją pateikęs asmuo supažindinamas su sutarties projektu, CP, CPS, Bendrosiomis sąlygomis ir kitais viešais CPS 1.1.1 punkte nurodytais dokumentais.

Jeigu SSC QCA klientu pageidauja tapti UAB „Skaitmeninio sertifikavimo centras" struktūrinis padalinys, su juo sutartis nesudaroma.

[6] Valstybės Žinios, 2000, Nr.: 74, Publikacijos Nr.: 2262; Valstybės Žinios, 2000, Nr.: 77; Valstybės Žinios, 2000, Nr.: 80; Valstybės Žinios, 2000, Nr.: 82.

Jeigu abi šalys sutaria dėl sutarties sąlygų, ne vėliau kaip per 15 darbo dienų nuo visų pareikalautų dokumentų gavimo UAB „Skaitmeninio sertifikavimo centras“ su pareiškėju sudaro sutartį, kurioje abi šalys prisiima įsipareigojimus dėl sertifikato ir raktų poros tvarkymo ir naudojimo.

Sutartys dėl 1-os klasės sertifikatų gali būti sudaromos tiesiogiai internete pateikiant prašymą dėl sertifikato sudarymo (prisijungiant prie Internete esančių standartinių sutarties sąlygų).

3.4. Registravimas

1-os klasės sertifikatai

Kiekvienam SSC CA sistemos dalyvio statusą įgijusiam Pasirašytojui SSC RA suteikia registracijos kodą, kuris yra numeruojamas eilės tvarka. Pasirašytojas informuojamas apie jam suteiktą registravimo kodą. Užvedama sertifikavimo sistemos dalyvio byla.

2-os klasės sertifikatai

Kiekvienam SSC CA sistemos dalyvio statusą įgijusiam Pasirašytojui SSC RA suteikia registracijos kodą, kuris yra numeruojamas eilės tvarka. Pasirašytojas informuojamas apie jam suteiktą registravimo kodą. Užvedama sertifikavimo sistemos dalyvio byla.

3-os klasės sertifikatai

Kiekvienam SSC QCA sistemos dalyvio statusą įgijusiam Pasirašytojui SSC RA suteikia registracijos kodą, kuris yra numeruojamas eilės tvarka. Pasirašytojas informuojamas apie jam suteiktą registravimo kodą. Užvedama sertifikavimo sistemos dalyvio byla.

Sertifikavimo sistemos dalyvis sertifikatui juridinio asmens vardu gauti SSC QCA Skaitmeninio parašo sertifikatų skyriaus registratoriui pateikia užpildytą formą „Prašymas gauti Sertifikatą juridinio asmens vardu“ bei atitinkamo juridinio asmens įgaliojimą kontroliuoti privatųjį raktą. SSC QCA dalyvis sertifikatui gauti savo vardu pateikia užpildytą formą „Prašymas gauti Sertifikatą fizinio asmens vardu“.

Gavęs prašymą, SSC RA užpildo Sertifikavimo paslaugų paraiškų registracijos žurnalą, nurodydamas:

- prašymo gavimo datą;
- operaciją;
- prašymo pateikėją;
- prašymą sudaryti sertifikato klasę ir tipą;
- prašymo pateikimo būdą;
- prašymą, kad raktų porą sugeneruotų SSC QCA;
- prašymo pateikimo priežastį;
- prašymą priėmusį asmenį.

SSC RA patikrina, ar prašyme pateikti visi reikalaujami duomenys: iš juridinio asmens įgalioto asmens pareikalaujama pateikti dokumentus, patvirtinančius jo tapatybę, įgalinimus veikti juridinio asmens vardu ir juridinio asmens steigimo dokumentus. Pateiktas asmens dokumentas kopijuojamas ir kopija įsegama į bylą. SSC RA taip pat patikrina, ar pateikti duomenys ir prašymas yra teisingi.

Jeigu prašymas yra autentiškas, pereinama į sertifikato generavimo procedūrą. Jeigu SSC QCA registratorius atsisako sudaryti Sertifikatą, jis nedelsdamas apie tai praneša pareiškėjui arba jo įgaliotajam atstovui telefonu ir elektroniniu paštu, nurodydamas tokio sprendimo priežastį, ir Sertifikavimo paslaugų paraiškų registracijos žurnale užregistruoja pateikto prašymo atmetimą.

Dėl visų sertifikatų, sudarytų fiziniams asmenims, SSC RA įsitikina, kad:

- asmuo, prašantis sudaryti Sertifikatą, yra asmuo, nurodytas prašyme sudaryti Sertifikatą,
- asmuo, prašantis sudaryti Sertifikatą, valdo privatųjį raktą, atitinkantį viešąjį raktą, kuris bus nurodytas sertifikate pagal šių CPS 3.1.7 punktą, ir
- informacija, kuri bus nurodoma sertifikate yra tiksli, išskyrus netikrinamąją Galutinio naudotojo informaciją (angl. *Non-verified End User Information*).

3.5. Įprastinė sertifikato pratęsimo procedūra

Sertifikatas gali būti pratęstas tik remiantis atitinkamu Pasirašančio asmens prašymu. Sertifikatas negali būti pratęstas, jeigu ankstesnysis Sertifikatas buvo atšauktas arba pasibaigė jo galiojimo terminas.

Likus 30 dienų iki išduoto sertifikato galiojimo pabaigos, SSC QCA apie tai elektroniniu paštu arba kitokiu būdu praneša Pasirašytojui ir nurodo sertifikato pratęsimo procedūrą, terminus bei kainą.

Asmuo, prašydamas sertifikato pratęsimo, privalo, **prieš pasibaigiant ankstesniojo sertifikato galiojimo terminui**, SSC RA siųsti (PKCS#10 formatu, koduotu pagal PEM ar DES standartą, arba pasirašytą galiojančiu elektroniniu parašu) prašymą atnaujinti Sertifikatą. Sertifikatas gali būti atnaujintas tik jeigu Pasirašytojo vardas, turintis skiriamųjų požymių, išlieka nepakitęs. Sertifikavimo tarnyba turi teisę esant teisėtam pagrindui atsisakyti iš naujo sudaryti Sertifikatą.

Tapatybės nustatymas vykdomas pagal CPS 3.2 skyriaus nuostatas.

3.6. Naujo sertifikato išdavimo procedūra po sertifikato galiojimo nutraukimo

Sertifikatas negali būti sudarytas viešajam raktui, su kuriuo susietas ankstesnysis Sertifikatas buvo sertifikavimo tarnybos atšauktas (nutrauktas galiojimas) ar su kuriuo susietas privatusis raktas buvo prarastas ar atskleistas (angl. *compromise*). Šiuo atveju dėl sertifikato sudarymo turi būti kreipiamasi įprastine tvarka.

3.7. Prašymas nutraukti sertifikato galiojimą

Prašymas atšaukti Sertifikatą (nutraukti galiojimą) priimamas remiantis tapatybės nustatymo tvarka pagal šių CPS 3.2 punktą. Jei sertifikato galiojimo terminas nėra pasibaigęs ir Sertifikatas nėra atšauktas, šiuo sertifikatu gali būti pasirašytas prašymas atšaukti Sertifikatą. Kitais atvejais turi būti taikomos procedūros, nustatytos tapatybės nustatymui asmens pradinės registracijos metu pagal šių CPS 3.2 punktą.

Prieš atšaukiant 1-os klasės Sertifikatą, tapatybės nustatymui gali būti naudojamos šios procedūros:

- reikalauti, kad būtų pateikta Galutinio Naudotojo Atpažinimo Frazė (ar jos ekvivalentas), ir nutraukti sertifikato galiojimą automatiškai, jei pateiktoji Atpažinimo Frazė (ar jos ekvivalentas) sutampa su užfiksuotąja Atpažinimo Fraze (ar jos ekvivalentu);
- gauti pranešimą, kuriame teigiama, kad jį išsiuntė pasirašytojas ar asmuo, kuriam pagal sertifikate nurodytą informaciją pasirašantis asmuo turi teisę atstovauti, taip pat kuriame prašoma atšaukti Sertifikatą, ir kuriame yra elektroninis parašas, galimas patikrinti sertifikatu, kurį prašoma atšaukti.

4. REIKALAVIMAI VEIKLAI

Šiame CPS skyriuje įtvirtinti reikalavimai asmenims, dalyvaujantiems sertifikavimo ir sertifikatų galiojimo nutraukimo procese.

4.1. Prašymas sudaryti Sertifikatą

Asmuo, prašantis sudaryti Sertifikatą, privalo sutikti, kad bus veikiama pagal šiuos SSC QCA sertifikato veiklos nuostatus (CPS).

Pareiškėjo tapatybę nustato SSC RA. SSC RA turi teisę patvirtinti prašymo sudaryti Sertifikatą autentiškumą.

4.1.1. Galutinių naudotojų Sertifikatai

Visiems asmenims, prašantiems sudaryti Galutinio Naudotojo Sertifikatus, taikoma registravimo procedūra, susidedanti iš šių etapų:

- prašymą sudaryti Sertifikatą užpildymas ir reikalaujamos informacijos nurodymas;
- raktų poros pagal šių CPS 6.1 skyriaus nuostatas generavimas ar i jos generavimo organizavimas;
- jeigu pasirašytojas pats sugeneravo raktų porą, jis turi perduoti savo viešąjį raktą tiesiogiai SSC QCA pagal šių CPS 6.1.3 punktą;
- įrodytmas, kad pagal šių CPS 3.1.7 punktą asmuo, prašantis sudaryti Sertifikatą turi privatųjį raktą, kuris atitinka viešąjį raktą, perduotąjį SSC QCA, ir
- atitinkamos sutarties pasirašymas.

Prašymai sudaryti Sertifikatą paduodami SSC RA, kuri juos apdoroja ir patvirtina arba atmeta. Tarnyba, kuri apdoroja prašymą sudaryti Sertifikatą, ir tarnyba, kuri sudaro Sertifikatą pagal šių CPS 4.2 skyriaus nuostatas, gali nesutapti.

4.2. Sertifikato sudarymas

SSC QCA sudaro Sertifikatus vadovaudamasi sertifikato taisyklėmis (CP) ir šiais CPS. Sertifikatas gali būti sudaromas po pareiškėjo tapatybės nustatymo šių CPS 3.2 punkte nurodyta tvarka. Sutartyje turi būti nurodomas sertifikato galiojimo terminas. Pareiškėjui turi būti pranešama apie sertifikato sudarymą elektroniniu arba įprastų paštu.

Jeigu dėl kokių nors priežasčių sertifikavimo tarnyba nusprendžia nesudaryti sertifikato (net jei patikrinimų ir tapatybės nustatymo metu trūkumų nerasta), ji privalo pranešti apie tokio sprendimo priežastis pareiškėjui elektroniniu paštu arba įprastų paštu.

Visų klasių sertifikatai, kuriuos SSC QCA sudaro vadovaudamosi šiais CPS, atitinka X.509v3 standartą. Atskirais atvejais, sudarant vidiniam naudojimui skirtus sertifikatus (arba pagal susitarimą su kitą šalimi) gali būti naudojamas atitikimas X.509v1 standartui.

Sudaryti sertifikatai publikuojami LDAP duomenų bazėje arba HTTP, HTTPS priemonėmis.

4.3. Sertifikato priėmimas

Sugeneravusi Sertifikatą, SSC QCA praneša Pasirašytojui, kad jo Sertifikatas paruoštas, ir nurodo, kokiu būdu jis gali gauti Sertifikatą.

Sudarytas Sertifikatas perduodamas pareiškėjui naudojant specializuotas saugias laikmenas pagal reikalavimus, įtvirtintus sutartyje su Pasirašytoju arba numatytus LR teisės aktuose.

4.4. Sertifikato galiojimo sustabdymas ir galiojimo nutraukimas

SSC QCA sudaro CRL, skelbia jo pasirašytą versiją, o taip pat jį atnaujina, įtraukdama Sertifikatus, kurių galiojimas nutrauktas.

4.4.1. Pagrindai atšaukimui (galiojimo nutraukimui)

4.4.1.1. Galutinio Naudotojo sertifikato galiojimo nutraukimas

SSC QCA nutraukia sertifikato galiojimą:

1) pasirašančio asmens prašymu;
2) pasirašančiam asmeniui praradus Sertifikatą atitinkančių parašo formavimo duomenų kontrolę;
3) išaiškėjus, kad jam buvo pateikti klaidingi duomenys sertifikatui sudaryti;
4) remdamasis sertifikato galiojimo apribojimais, nurodytais sertifikate jį sudarant;
5) gavęs pranešimą, kad pasirašantis asmuo tapo neveiksnus;
6) gavęs pranešimą, kad pasirašantis asmuo mirė;
7) pasirašančiam asmeniui pažeidus elektroninio parašo naudojimą reglamentuojančius teisės aktus arba sutarties su sertifikavimo paslaugų teikėju sąlygas;
8) asmens, kuriam pagal sertifikate nurodytą informaciją pasirašantis asmuo turi teisę atstovauti, prašymu;
9) kitais Lietuvos Respublikos įstatymų numatytais atvejais.

4.4.2. Asmenys, galintys prašyti Sertifikato galiojimo nutraukimo

Šie asmenys turi teisę prašyti nutraukti Galutiniam Naudotojui išduoto Sertifikato galiojimą:

1. SSC QCA ir RA, kurie patvirtino prašymą sudaryti Galutinio Naudotojo Sertifikatą, turi teisę prašyti atšaukti bet kurį Galutinio Naudotojo ar Administratoriaus Sertifikatą pagal šių CPS 4.4.1.1 papunktį.
2. Pasirašytojai;
3. Asmenys, kuriems pagal sertifikate nurodytą informaciją Pasirašantis asmuo turi teisę atstovauti.

4.4.3. Prašymo atšaukti Sertifikatą procedūra

4.4.3.1. Prašymo atšaukti Galutinio Naudotojo Sertifikatą procedūra

Pasirašytojas privalo perduoti prašymą atšaukti Sertifikatą Galutinio Naudotojo prašymą sudaryti Sertifikatą patvirtinusioms CA arba RA, kurios privalo nedelsdamos inicijuoti sertifikato atšaukimą. Šiuo atveju taikoma tapatybės nustatymo ir patvirtinimo procedūra, analogiška įtvirtintai CPS 3.2.1 punkte.

Be to, SSC QCA turi priimti pranešimą, kuriuo prašoma sertifikato galiojimo nutraukimo, kuris yra pasirašytas elektroniniu parašu, atitinkančiu CP, kurio galiojimo terminas nėra pasibaigęs ir kurio galiojimas nėra nutrauktas. Taip pat gali būti reikalaujama, kad pasirašantis asmuo atvyktų pas CA arba RA ir pateiktų galiojantį tapatybės dokumentą.

4.4.3.2. Terminas, per kurį turi būti priimtas sprendimas dėl prašymo atšaukti Sertifikatą

SSC QCA turi priimti sprendimą dėl prašymo atšaukti Sertifikatą per vieną darbo dieną nuo prašymo gavimo.

4.4.3.3. Pagrindai sertifikato atšaukimui

Galutinio Naudotojo prašymu SSC QCA turi teisę laikinai nutraukti Galutinio Naudotojo sertifikato galiojimą. Informacija apie tai, kurių sertifikatų galiojimas yra nutrauktas, privalo būti prieinama specialiose talpyklose, valdomose sertifikavimo tarnybos.

4.4.3.4. Asmenys, kurie turi teisę prašyti nutraukti sertifikato galiojimą. Galiojimo nutraukimo pagrindai.

Prašymą dėl sertifikato galiojimo nutraukimo turi teisę pateikti:

1. Pasirašytojai.
2. Asmenys, kuriems pagal sertifikate nurodytą informaciją Pasirašantis asmuo turi teisę atstovauti.
3. Vyriausybės nustatytų teisėsaugos institucijos, siekiant užkirsti kelią nusikaltimams.

SSC QCA nutraukia sertifikato galiojimą ir tais atvejais, kai SSC QCA gauna informacijos, kad sertifikato duomenys yra neteisingi arba pasirašantis asmuo prarado jo Sertifikatą atitinkančių parašo formavimo duomenų kontrolę.

4.4.4. CRL sudarymo dažnumas

SSC QCA sudaro Atšauktų Sertifikatų Sąrašą (CRL) ne rečiau kaip kartą per savaitę. Šis sąrašas yra atnaujinamas kiekvieną kartą, kai atšaukiamas kuris nors šios sertifikavimo tarnybos sudarytas Sertifikatas. Sertifikavimo tarnyba savo elektroniniu parašu pasirašo atšauktų sertifikatų sąrašą.

Kiekviename sertifikate, kurį sertifikavimo tarnyba sudarė pagal šiuo CPS, turi būti nurodytas CRL pateikimo adresas (URL tipo adresas, kuriame prieinamas atšauktų sertifikatų sąrašai).

4.4.5. Reikalavimai CRL tikrinimui

Pasitikinčioji šalis, siekdama užtikrinti sertifikato naudojimo galimumą, privalo patikrinti Sertifikato statusą naudodamasi naujausiu CRL, sudarytu SSC QCA.

4.4.6. Galimybė patikrinti atšaukimą/sertifikato statusą realaus laiko (angl. *on-line*) režimu

Greta CRL publikavimo, SSC QCA privalo suteikti galimybę realiu laiku gauti informaciją apie sertifikatų statusą, užtikrindama atsakymus į internetu pateikiamas užklausas SSC QCA Talpyklai šiuo adresu:

http://ocsp.ssc.lt:2560

4.4.7. Reikalavimai galiojimo nutraukimo tikrinimui realaus laiko (angl. *on-line*) režimu

Jeigu Pasitikinčioji Šalis nepatikrina sertifikato, kuriuo nori pasitikėti, statuso naudodamasi naujausiu tinkamu CRL, Pasitikinčioji Šalis privalo patikrinti to sertifikato statusą naudodamasi:

(a) šių CPS 4.4.6 punkte nurodytu metodu; arba
(b) Sertifikato patikrinimu per interneto sąsają.

4.4.8. Kitos paskelbimo apie atšaukimą formos

Netaikoma.

4.4.9. Reikalavimui galiojimo nutraukimo patikrinimui, kai taikomos kitos paskelbimo apie atšaukimą formos

Netaikoma.

4.4.10. Specialūs reikalavimai dėl rakto praradimo, vagystės, sunaikinimo

Netaikoma.

4.5. Saugos tikrinimo procedūros

4.5.1. Fiksuojamų įvykių tipai

SSC QCA rankiniu ar automatiniu būdu fiksuoja šiuos reikšmingus įvykius:

SSC QCA rakto galiojimo laikotarpio tvarkymo įvykius, įskaitant:

- rakto generavimą, saugojimą, atstatymą (angl. *recovery*), archyvavimą, sunaikinimą ir atsarginių kopijų darymą (angl. *backup*);
- kriptografinės įrangos veikimo laikotarpio tvarkymo įvykius.

- SSC QCA ir Galutinio Naudotojo sertifikatų galiojimo laikotarpio tvarkymo įvykius, įskaitant:

  - prašymus sudaryti Sertifikatą, sertifikatų atnaujinimą, atšaukimą ir naujo rakto išdavimą (angl. *rekey*);
  - sėkmingą ir nesėkmingą prašymų apdorojimą;
  - sertifikatų ir CRL generavimą ir sudarymą.

- įvykius, susijusius su sauga, įskaitant:

  - sėkmingus ir nesėkmingus bandymus prieiti prie PKI sistemos;
  - veiksmus su PKI ir saugos sistema, atliktus SSC QCA personalo;
  - saugos atžvilgiu reikšmingų (angl. *security sensitive*) bylų ir įrašų nuskaitymą, įrašymą ar ištrynimą;
  - saugos profilių pokyčius;
  - sistemos avarijas (angl. *crash*), kompiuterinės technikos gedimus ir kitas anomalijas;
  - "ugnies sienos" (angl. *firewall*) ir maršrutizatoriaus veiklą;
  - SSC QCA patalpų lankytojų įėjimą/išėjimą.

Fiksavimo įrašuose turi būti šie elementai:

- įrašo data ir laikas;

- automatinio žurnalo įrašo serijinis ar eilės numeris;
- asmens, darančio įrašą žurnale, tapatybė;
- įrašo pobūdis.

SSC RA fiksuoja informaciją apie prašymus sudaryti Sertifikatus, įskaitant:

- identifikavimo dokumento (-ų), kurį pateikia asmuo, prašantis sudaryti Sertifikatą, pobūdį;
- įrašus apie identifikavimo dokumentuose esančią unikalią identifikavimo informaciją, numerius ar jų kombinacijas (pvz., asmens, prašančio sudaryti Sertifikatą, vairuotojo pažymėjimo numeris);
- prašymų ir identifikavimo dokumentų kopijų saugojimo vietą;
- asmens, priimančio prašymą, tapatybę;
- metodus, taikomus nustatyti identifikavimo dokumentų tikrumą, jei tokie metodai taikomi;
- gaunančiosios SSC QCA ar pateikiančiosios SSC RA pavadinimas.

4.5.2. Užfiksuotos informacijos apdorojimo dažnumas

Užfiksuota informacija tikrinama ne rečiau kaip kartą per savaitę, siekiant nustatyti reikšmingus saugai ir veiklai įvykius. Be to, SSC QCA privalo apžvelgti užfiksuotą informaciją, siekdama nustatyti įtartiną ar neįprastą veiklą, jeigu buvo pranešimų apie anomalijas ir incidentus SSC QCA ir SSC RA sistemose.

Užfiksuota informacija tikrinama apžvelgiant užfiksuotą informaciją ir dokumentus, siekiant nustatyti visus reikšmingus įvykius pagal užfiksuotos informacijos reziumė (angl. *audit log summary*), pvz., tikrinama, ar prie užfiksuotos informacijos nebuvo prieinama, tiriami visi užfiksuotos informacijos įrašai, ieškoma bet kokių įspėjimų ar anomalijų užfiksuotoje informacijoje. Veiksmai, kurių imamasi remiantis užfiksuotos informacijos patikrinimais, privalo būti dokumentuojami.

4.5.3. Užfiksuotos informacijos saugojimo laikotarpis

Užfiksuota informacija saugoma nearchyvuota ne trumpiau kaip du mėnesius po jos apdorojimo, o po to archyvuojama pagal šių CPS 4.6 skyriaus nuostatas.

4.5.4. Užfiksuotos informacijos apsauga

Užfiksuotos informacijos bylos (įrašai), sukurtos elektroniniu ar rankiniu būdu, nuo neteisėtos peržiūros, modifikavimo, ištrynimo ar kito priėjimo prie jų saugomos naudojant fizinio ar loginio priėjimo kontrolės priemones.

4.5.5. Užfiksuotos informacijos atsarginių kopijų darymo procedūra

Užfiksuotos informacijos tolydžio didėjančios (angl. *incremental*) atsarginės kopijos daromos kasdien. Pilnos atsarginės kopijos daromos kas savaitę.

4.5.6. Patikrinimų duomenų rinkimo sistema (vidinė ir išorinė)

Patikrinimų duomenys automatiškai generuojami ir įrašomi kompiuterio programos, tinklo ir operacinės sistemos lygmenyse. Rankiniu būdu generuojami patikrinimų duomenys įrašomi SSC QCA personalo.

4.5.7. Pranešimas subjektui, sukėlusiam įvykį

Apie tai, kad patikrinimų duomenų rinkimo sistema užfiksuoja įvykį, nėra privaloma pranešti fiziniam asmeniui,

juridiniam asmeniui, kurie sukėlė įvykį.

4.5.8. Pažeidžiamumo vertinimas

Patikrinimų metu įvykiai yra fiksuojami siekiant, be kita ko, stebėti sistemos pažeidžiamumą. Loginis saugos pažeidžiamumo vertinimas (angl. *logical security vulnerability assessments*, "LSVAs") atliekamas, apžvelgiamas ir peržiūrimas po stebėtų įvykių tyrimo. LSVA vertinimai atliekami kasdien, kas mėnesį ir kasmet naudojant realiu laiku automatiškai užfiksuotą informaciją pagal SSC QCA Saugos ir Audito reikalavimus. Metinis LSVA vertinimas yra metinio sertifikato taisyklių laikymosi patikrinimo dalis (angl. *Compliance Audit*).

4.6. Informacijos archyvavimas

4.6.1. Fiksuojamų įvykių tipai

Greta patikrinimams fiksuojamos informacijos nurodytos šių CPS 4.5 skyriuje, SSC QCA saugo, be kitos, šią dokumentaciją:

- dokumentaciją apie tai, kaip SSC QCA laikosi šių CPS ir kitų įsipareigojimų pagal sutartis su savo Galutiniais Naudotojais, ir
- dokumentaciją apie veiksmus ir informaciją, kurie yra esminiai prašymams sudaryti Sertifikatą.

SSC QCA fiksuoja, be kitų, šiuos sertifikato galiojimo termino įvykius:

- kiekviename sertifikate įvardinto Galutinio Naudotojo tapatybę (išskyrus 1 klasės Sertifikatus, dėl kurių fiksuojamas tik vienareikšmis Galutinio Naudotojo vardas (pavadinimas),
- asmenų, kurie prašo atšaukti Sertifikatą, tapatybę (išskyrus 1 klasės Sertifikatus, dėl kurių fiksuojamas tik vienareikšmis Galutinio Naudotojo vardas (pavadinimas),
- kitus faktus, nurodytus sertifikate,
- laiko žymas (angl. time stamps),
- tam tikrus įmanomus numatyti esminius faktus, susijusius su sertifikatų sudarymu, pvz., informaciją, reikšmingą sėkmingam sertifikato taisyklių laikymosi patikrinimui (Compliance Audit) pagal šių CPS 2.7 skyriaus nuostatas.

SSC QCA privalo archyvuoti:

- jau sudarytus Sertifikatus atitinkančius prašymus sudaryti Sertifikatus;
- sudarytus Sertifikatus;
- sudarytus CRL sąrašus;
- visus susitarimus, pasirašytus su kitais asmenimis (pvz., SSC RA);
- dokumentus, prašymo sudaryti Sertifikatą pateikimo procedūros metu gautus iš pareiškėjo;
- visus reikšmingus pranešimus, nusiųstus pareiškėjams ar SSC RA ar gautus iš jų.

SSC RA privalo archyvuoti:

- visą tapatybės patvirtinimo informaciją (validation information), gautą iš pareiškėjų;
- visus reikšmingus pranešimus, nusiųstus sertifikavimo tarnybai arba gautus iš jos.

Informacija gali būti archyvuojama elektronine ar materialia forma, tačiau turi būti klasifikuojama, laikoma, saugoma ir atgaminama išlaikant jos tikslumą, vientisumą ir išsamumą.

4.6.2. Archyvavimo laikotarpis

Minimalus archyvavimo laikotarpis yra penkeri metai.

4.6.3. Archyvo apsauga

SSC QCA saugo savo archyvuotą informaciją, surinktą pagal šių CPS 4.6.1 punktą, tokiu būdu, kad tik įgaliotiems patikimiems asmenims būtų leidžiama prie jos prieiti. Elektronine forma archyvuoti duomenys nuo neteisėto susipažinimo su jais, jų modifikavimo, ištrynimo ar kito priėjimo prie jų saugomi įdiegiant tinkamas fizines ir logines priėjimo kontrolės priemones. Laikmenos, kuriose yra archyvuoti duomenys, ir programinė įranga, reikalinga archyvuotų duomenų apdorojimui, laikomi tokiu būdu, kad būtų užtikrinta galimybė prieiti prie archyvuotų duomenų per laikotarpį, nurodytą šių CPS 4.6.2 punkte.

4.6.4. Archyvo atsarginių kopijų darymo procedūra

SSC QCA daro elektronine forma archyvuotos informacijos apie jos sudarytus Sertifikatus tolydžio didėjančias (angl. *incremental*) atsargines kopijas kasdien, o pilnas atsargines kopijas daro kas savaitę.

Informacijos, surinktos pagal šių CPS 4.6.1 punktą ir užfiksuotos popieriuje, kopijos laikomos pagal šių CPS 4.8 skyriaus nuostatas avarinio atstatymo įrangoje, esančioje ne CA patalpose (angl. *off-site disaster recovery facility*).

4.6.5. Reikalavimai įrašų laiko žymoms

Sertifikatuose, CRL sąrašuose ir kituose atšauktų sertifikatų duomenų bazės įrašuose nurodoma informaciją apie datą ir laiką.

4.6.6. Archyvo duomenų surinkimo sistema (vidinė ar išorinė)

Netaikoma.

4.6.7. Archyvinės informacijos įgijimo ir tikrinimo procedūros

Netaikoma.

4.7. Rakto pakeitimas

Žr. 4.8.2 punktą.

4.8. Parašo formavimo duomenų kontrolės praradimas ir avarinis atstatymas

4.8.1. SSC QCA privačiojo rakto pakeitimas

SSC QCA raktų pora negali būti naudojamos pasibaigus jų galiojimo laikotarpiui. SSC QCA sertifikatai gali būti atnaujinami tik neviršijant paties SSC QCA sertifikato galiojimo datos. SSC QCA raktų naujos poros turi būti generuojamos iškilus reikalui, pvz., siekiant pakeisti jomis CA raktų poras, kurių rengiamasi nebenaudoti, siekiant papildyti esančias aktyvias raktų poras, arba siekiant tinkamiau teikti naujas paslaugas pagal šių CPS 6.1 skyriaus nuostatas.

Prieš pasibaigiant SSC QCA sertifikato galiojimo terminui, vykdomos rakto pakeitimo procedūros, kurių tikslas yra užtikrinti aukštesniosios SSC QCA hierarchijoje esantiems asmenims sklandų perėjimą nuo aukštesniosios SSC QCA senosios raktų poros prie naujosios raktų poros (-ų).

4.8.2. Privačiojo rakto kompromitacija

Jeigu SSC QCA prarado privačiojo rakto kontrole, CA privalo:

- pranešti apie tai savo pareiškėjams, ir asmenims, naudojantiems Sertifikatus;
- liautis naudojus Kompromituotą privatųjį raktą teikiant sertifikavimo paslaugas ir sudarant atšauktų sertifikatų sąrašą;
- prašyti Sertifikatą sudariusią sertifikavimo tarnybą (PCA) atšaukti Sertifikatą;
- užtikrinti visų pasirašančių asmenų, turinčių Sertifikatus, pasirašytus CA sukompromituotu raktu, informavimą bei tų sertifikatų galiojimo nutraukimą;
- užtikrinti, kad bus nutrauktas sertifikatų/CRL, pasirašytų naudojant "sukompromituotą" privatų raktą, naudojimas.

Jeigu SSC RA prarado privačiojo rakto kontrolę, RA privalo:

- pranešti apie tai visiems suinteresuotiems asmenims;
- prašyti Sertifikatą sudariusią sertifikavimo tarnybą atšaukti Sertifikatą.

Jeigu Galutinio Naudotojo privatusis raktas buvo, ar įtariama, kad buvo, sukompromituotas, Galutinis Naudotojas privalo bent jau:

- pranešti apie tai visiems suinteresuotiems asmenims;
- prašyti SSC QCA atšaukti Sertifikatą.

4.8.3. Atvejai, kai pažeidžiama kompiuterinė įranga, programinė įranga ir/ar duomenys

Jeigu pažeidžiama kompiuterinė įranga, programinė įranga ir/ar duomenys, apie tai pranešama SSC QCA saugos tarnybai ir vykdomos SSC QCA incidentų valdymo procedūros, kurių metu turi būti adekvačiai pradedamas ir plečiamas incidento tyrimas bei adekvačiai reaguojama į incidentą. Prireikus turi būti vykdomos SSC QCA rakto Kompromitacijos ar avarinio atstatymo procedūros.

4.8.4. Atvejai, kai atšaukiamas viešasis raktas

Žr. CPS 4.4. skyrių.

4.8.5. Atvejai, kai raktas yra kompromituojamas

Žr. CPS 4.4. skyrių.

4.8.6. Saugi įranga stichinės nelaimės ar kitos avarijos atveju

Žr. CPS 4.4. skyrių.

4.9. SSC QCA veiklos nutraukimas

SSC QCA ne vėliau kaip prieš vieną mėnesį iki sertifikavimo paslaugų teikimo nutraukimo privalo apie tai informuoti visus pasirašančius asmenis, kurių Sertifikatus jis sudarė ir kurių sertifikatai yra galiojantys, SSC RA, su kuriais yra pasirašytos sutartys bei kitus sertifikavimo paslaugų teikėjus, su kuriais yra pasirašytos laidavimo sutartys.

SSC QCA paslaugų teikėjas gali nutraukti visų jo sudarytų sertifikatų galiojimą ne anksčiau kaip po vieno mėnesio nuo paskelbimo apie numatomą sertifikavimo paslaugų teikimo nutraukimą.

SSC QCA ne vėliau kaip prieš vieną mėnesį iki sertifikavimo paslaugų teikimo nutraukimo privalo apie tai informuoti elektroninio parašo priežiūros instituciją.

4.10. SSC QCA veiklos perdavimas

SSC QCA per vieną mėnesį po paskelbimo apie numatomą sertifikavimo paslaugų teikimo nutraukimą visus savo sudarytus kvalifikuotus Sertifikatus ir elektroninio parašo priežiūros institucijos nustatytą informaciją, susijusią su sertifikatų tvarkymu ir atsakymais į parašo naudotojų užklausas, privalo perduoti veiklos perėmėjui arba elektroninio parašo priežiūros institucijai. Veiklos perėmėjas arba elektroninio parašo priežiūros institucija privalo užtikrinti perimtų sertifikatų duomenų teikimą parašo naudotojams elektroniniams parašams tikrinti.

5. FIZINĖS APLINKOS, PROCEDŪRŲ ATLIKIMO IR DARBUOTOJŲ SAUGUMO KONTROLĖ

5.1. Fizinės aplinkos kontrolė

SSC QCA veikia tam tikslui skirtose ir pritaikytose patalpose, specialiai įrengtoje, saugioje vietoje. SSC QCA įdiegė SSC QCA Saugumo politiką, kuri patvirtina šių Nuostatų saugumo reikalavimus.

SSC QCA veikia ant atskiros tam skirtos ("*dedicated*") tarnybinės stoties, kuri yra fiziškai apsaugota.

5.1.1. Patalpų vieta ir konstrukcija

SSC QCA ir SSC RA veiksmai atliekami naudojant SSC QCA saugius įrenginius (įrangą), esančius adresu: Žvejų g. 14, Vilnius, atitinkančius reikalavimus saugumui ir auditui. Visi SSC QCA ir SSC RA veiksmai atliekami fiziškai saugomoje aplinkoje, sukurtoje siekiant apsaugoti nuo slapto ar atviro neteisėto patekimo, įsibrovimo ar suteikiančioje galimybę jį atskleisti.

SSC QCA rekomenduoja, kad klientai laikytųsi SSC QCA Saugumo politikoje numatytų rekomendacijų.

5.1.2. Fizinė prieiga

SSC QCA veiklai skirtose patalpose įrengta fizinės prieigos kontrolė. Tik asmenys, turintys patvirtintas teises veikti kaip SSC QCA operatoriai gali patekti į šias patalpas.

SSC QCA sistemos saugomos mažiausiai 4 fizinės apsaugos lygių, kai prieiga prie aukštesnės pakopos galima tik turint prieigą prie žemesnės pakopos.

Progresyviai ribojančios fizinę prieigą teisės skirtos kontroliuoti prieigą prie kiekvienos pakopos. Jautriai SSC QCA operacinei veiklai, bet kokiai su sertifikavimo proceso etapais susijusiai veiklai, tokiai kaip tapatybės nustatymas, patvirtinimas, tapatybės nustatymas, verifikavimas ir išdavimas, taikomos ypatingos fizinę prieigą ribojančios apsaugos pakopos. Prieigai prie kiekvienos pakopos reikalingas "SSC QCA leidimas". Fizinė prieiga automatiškai fiksuojama ir įrašoma video aparatūra. Papildomos pakopos užtikrina individualią prieigos kontrolę naudojant dviejų faktorių (angl. *two factors*) autentifikavimą, įskaitant biometrines priemones. Nelydimi darbuotojai, įskaitant neįgaliotus/nepatikimus darbuotojus ar lankytojus, neturi teisės patekti į jokias saugomas teritorijas.

Fizinės apsaugos sistema apima papildomas pagrindinio valdymo apsaugos pakopas, skirtas apsaugoti tiek realaus, tiek ir nerealaus laiko (angl. *offline*) CSU ir su raktais susijusios medžiagos saugojimą. Šifravimo medžiagą kurti ir laikyti naudojamos vietos užtikrina dvigubą kontrolę, naudojant dviejų faktorių (angl. *two factors*) autentifikavimą, įskaitant biometrines priemones. Realaus laiko CSU saugomos naudojant rakinamus kabinetus.Nerealaus laiko (angl. *offline*) CSU saugomi naudojant rakinamus seifus, kabinetus, talpyklas. Priėjimas prie CSU ir su raktais susijusios medžiagos ribojamas laikantis SSC QCA pareigų atskyrimo reikalavimų. Kabinetų ir talpyklų atidarymas ir uždarymas šiose pakopose fiksuojamas patikrinimo tikslais.

5.1.3. Elektros energija ir oro kondicionavimas

CA saugūs įrengimai yra pirmiausia aprūpinami ir sustiprinami:

- Elektros energijos sistema, užtikrinančia nuolatinį, nepertraukiamą elektros energijos tiekimą, ir
- Šildymo/vėdinimo/oro kondicionavimo sistemomis, skirtomis kontroliuoti temperatūrą ir santykinį oro drėgnumą.

5.1.4. Vandens buvimas

SSC QCA imasi pagrįstų apsaugos priemonių, skirtų sumažinti vandens poveikį.

5.1.5. Priešgaisrinė apsauga

SSC QCA imasi pagrįstų apsaugos priemonių, skirtų užkirsti kelią gaisrams ir juos gesinti ar apsaugoti nuo kitokio pavojingo ugnies ar dūmų poveikio. SSC QCA priešgaisrinės apsaugos priemonės kuriamos laikantis taikomų priešgaisrinės saugos reikalavimų/normų.

5.1.6. Laikmenų saugojimas

Visos gaminių, programinės įrangos ir duomenų, patikrinimų, archyvų laikmenos ar jų dublikatai yra laikomi SSC QCA įrenginiuose ar kitame saugiame laikymo įrenginyje, kurio priėjimui taikoma tinkama fizinė ir loginė prieigos kontrolė, skirta riboti priėjimą prie įgaliotų darbuotojų ir apsaugoti tokias laikmenas nuo atsitiktinio žuvimo rizikos (pvz., vandens, ugnies ir elektromagnetinės).

5.1.7. Atliekų naikinimas

Slapti dokumentai ir medžiaga prieš juos išmetant yra sunaikinami. Laikmenos, skirtos slaptos informacijos surinkimui ar perdavimui prieš jas panaikinant ar sunaikinant padaromos neperskaitomomis. Šifravimo įrenginiai prieš juos išmetant fiziškai sunaikinami ar neutralizuojami laikantis gamintojų nurodymų. Kitomis atliekomis atsikratoma laikantis SSC QCA įprastų atsikratymo atliekomis reikalavimų.

5.1.8. Atsarginių duomenų kopijų laikymas už juridinio asmens ribų

SSC QCA užtikrina kritinių sisteminių duomenų paprogrames, patikrinimų metu fiksuotų duomenų/informacijos ir kitos slaptos informacijos dublikatus.

5.2. Procedūrų kontrolė

5.2.1. Aukštos atsakomybės pareigos (angl. *trusted roles*)

Patikimi asmenys (t.y. užimantys Aukštos atsakomybės pareigas asmenys) apima visus darbuotojus, sutarties dalyvius ir konsultantus, kurie turi priėjimą prie šifravimo ar tapatybės nustatymo veiksmų, kurie gali iš esmės paveikti/įtakoti:

- Prašymuose sudaryti Sertifikatą esančios informacijos galiojimą;
- Prašymų sudaryti Sertifikatą priėmimą, atmetimą ar kitokį apiforminimą, prašymų panaikinti Sertifikatą ar prašymų atnaujinti sertifikato galiojimą arba informaciją apie sertifikatų įtraukimą į Atšauktų Sertifikatų Sąrašą;
- Sertifikatų išdavimą ar atšaukimą, įskaitant personalą, turintį prieigą prie ribotų talpyklų dalių (elementų); arba
- Galutinio naudotojo informacijos ar prašymų tvarkymą.

Aukštos atsakomybės asmenys apima įskaitant, bet nepasiribojant:

- klientus aptarnaujančius darbuotojus,
- šifravimo veiksmų darbuotojus,
- apsaugos darbuotojus,
- sistemos administracijos/valdymo darbuotojus,
- paskirtus inžinerijos darbuotojus.

SSC QCA laiko šiame skyriuje nurodytų darbuotojų kategorijas Patikimais asmenimis, užimančiais Aukštos atsakomybės pareigas. Asmenys, siekiantys tapti Patikimais asmenimis, užimdami aukštos atsakomybės pareigas turi atitikti peržiūros reikalavimus, nurodytus šių CPS 5.3 skyriuje.

5.2.2. Užduočiai atlikti reikalingas asmenų kiekis

SSC QCA laikosi veiklos taisyklių ir taiko griežtas kontrolės procedūras, siekdama užtikrinti pareigų atskyrimą, pagrįstą darbo įsipareigojimais. Atsakingiausi darbai, tokie kaip priėjimas prie SSC QCA kriptografinės kompiuterinės įrangos (kriptografinio pasirašymo vieneto arba CSU) ir su ja susijusios medžiagos apie raktus, bei jų tvarkymas, reikalauja daugiau kaip vieno asmens, užimančio aukštos atsakomybės pareigas, dalyvavimo.

Šios vidaus kontrolės procedūros yra skirtos užtikrinti, kad reikėtų mažiausiai dviejų darbuotojų, užimančių aukštos atsakomybės pareigas, norint gauti fizinį ar loginį priėjimą prie įrenginio. Priėjimas prie SSC QCA kriptografinės kompiuterinės įrangos visu jos veikimo laikotarpiu, nuo įeinančios informacijos priėmimo ir tyrimo iki Galutinio fizinio ir/ar loginio sunaikinimo galimas tik dalyvaujant daugiau kaip vienam asmeniui, užimančiam Aukštos atsakomybės pareigas. Jeigu modulis yra aktyvuotas veiklos raktais, turi būti pasitelkiamos priėjimo kontrolės priemonės tam, kad fizinio priėjimo kontrolė ir loginio priėjimo kontrolė būtų išlaikomos atskirtos. Asmenys, turintys fizinį priėjimą prie modulių, neturi Slaptųjų Dalių (angl. "*Secret Shares*") ir atvirkščiai. Reikalavimai SSC QCA privataus rakto atyvavimo duomenims ir Slaptosioms Dalims nurodyti šių CPS 6.2.7 punkte.

Kitos rankiniu būdu atliekamos operacijos, pvz., rankiniu būdu atliekamas 3 klasės sertifikatų galiojimo patikrinimas ir sudarymas reikalauja mažiausiai dviejų darbuotojų, užimančių Aukštos atsakomybės pareigas, dalyvavimo arba kombinacijos iš mažiausiai vieno darbuotojo, užimančio aukštos atsakomybės pareigas, ir sertifikato automatinio galiojimo patikrinimo ir sudarymo proceso.

5.2.3. Identifikavimas ir tapatybės nustatymas atskiroms pareigoms

Visų darbuotojų, siekiančių tapti darbuotojais, užimančiais aukštos atsakomybės pareigas, tapatybės patikrinimas atliekamas jiems asmeniškai (fiziškai) esant priešais darbuotojus, užimančius aukštos atsakomybės pareigas, kurie atlieka SSC QCA žmogiškųjų išteklių (HR) tvarkymo (ar panašias) arba saugos funkcijas, ir atliekant informatyvių identifikavimo formų ir dokumentų (pvz., asmens tapatybės kortelių, pasų ar vairuotojų pažymėjimų)

patikrinimą. Tapatybė papildomai patvirtinama atliekant biografijos patikrinimo procedūras, aprašytas šių CPS 5.3.1 punkte.

SSC QCA turi užtikrinti, kad darbuotojai būtų gavę Patikimų Asmenų Statusą (šis statusas suteikiamas darbuotojams, užimantiems aukštos atsakomybės pareigas) prieš tai, kai šiems darbuotojams yra:

- išduodami priėjimo įrenginiai ar leidžiama prieiti prie reikiamos įrangos;
- elektroniniu būdu išduodami įgaliojimai prieiti prie SSC QCA, SSC RA ir kitų informacinių technologijų (IT) sistemų bei atlikti jose specialiąsias funkcijas.

5.3. Personalo kontrolės priemonės

5.3.1. Biografiniai, kvalifikaciniai, patirties ir leidimų reikalavimai

Sertifikavimo tarnyba atsako už tinkamą jos operatorių, kuriems užtikrinta teisė prieiti prie visų priemonių, reikalingų sertifikavimo procese, paruošimą ir kvalifikaciją. Darbuotojai, siekiantys būti Patikimais Asmenimis, privalo pateikti įrodymus, kad jų biografija, kvalifikacija ir patirtis atitinka reikalavimus keliamus tam, kad jų būsimas darbas būtų atliktas kompetentingai ir patenkinamai, taip pat pateikti visus valstybės institucijų leidimus, kurie reikalingi sertifikavimo paslaugoms teikti. Patikimų Asmenų biografijos patikrinimai atliekami ne rečiau kaip vieną kartą per 5 metus.

5.3.2. Biografijos patikrinimo procedūros

Prieš įdarbindama asmenį atlikti Patikimo Asmens funkcijas, CA atlieka biografijos patikrinimą, kuriame, be kita ko, turi būti šie etapai:

- duomenys apie ankstesnį darbą, pareigas ir pan.;
- patikrinimas, ar asmuo turi profesinių rekomendacijų;
- aukščiausio ar labiausiai tinkamo išsilavinimo laipsnio nustatymas;
- teistumo patikrinimas (vietos ir valstybės mastu);
- kreditinės/finansinės informacijos patikrinimas;
- patikrinimas, ar asmuo turi vairuotojo pažymėjimą;
- valstybinio socialinio draudimo (SODRA) įrašų patikrinimas.

Biografijos patikrinimo metu atskleistos aplinkybės, kurių pagrindu leidžiama atmesti kandidatus į Patikimus Asmenis ar imtis priemonių prieš esamus Patikimus Asmenis, yra, pvz.:

- atvejai, kai kandidatas ar Patikimas Asmuo pateikė melagingą informaciją;
- nepalankios ar nepatikimos profesinės rekomendacijos;
- teistumas;
- duomenys apie finansinio atsakingumo trūkumą.

Tokią informaciją įvertina žmogiškųjų išteklių ir saugos specialistai, kurie nustato, kokių reikia imtis priemonių, atsižvelgdami į elgesio, atskleisto biografijos patikrinimo metu, pobūdį, mastą ir dažnumą. Griežčiausios iš tokių priemonių gali būti įdarbinimo pasiūlymų kandidatams galiojimo nutraukimas ir esamų Patikimų Asmenų atleidimas iš darbo.

Informacija, atskleista biografijos patikrinimo metu, naudojama įstatymų nustatyta tvarka.

5.3.3. Reikalavimai apmokymams

SSC QCA atlieka darbuotojų apmokymus iškart po įdarbinimo ir vėliau tam, kad darbuotojai kompetentingai ir patenkinamai vykdytų savo funkcijas. SSC QCA saugo informaciją apie šiuos apmokymus. SSC QCA periodiškai peržiūri savo apmokymų programas ir tobulina jas tiek, kiek tai yra reikalinga.

SSC QCA apmokymų programos derinamos prie konkrečių pareigybių ir jose gali būti, pvz., šios temos:

- Bazinės PKI koncepcijos,
- Darbo funkcijos,
- SSC QCA saugos ir veiklos nuostatai bei procedūros,
- Turimos kompiuterinės ir programinės įrangos naudojimas ir veikimas,
- Pranešimas apie incidentus ir kompromitacijos atvejus bei reagavimas į juos.
- Avarinio atstatymo ir veiklos tęstinumo užtikrinimo procedūros.

5.3.4. Kvalifikacijos kėlimo kursų dažnumas ir reikalavimai jiems

SSC QCA rengia kvalifikacijos kėlimo kursus ir aprūpina savo darbuotojus naujausia informacija tam, kad jie išlaikytų reikiamą darbo našumo lygį ir kompetentingai bei patenkinamai atliktų savo funkcijas. Saugos reikalavimų kursai turi būti vykdomi periodiškai.

5.3.5. Rotacijos darbe dažnumas ir eiliškumas

Netaikoma.

5.3.6. Sankcijos už neautorizuotus veiksmus

Už neautorizuotų veiksmų (t.y., tokių veiksmų, kuriems nebuvo gautas reikiamas leidimas, sutikimas ar pritarimas) atlikimą ir kitus SSC QCA veiklos taisyklių ir procedūrų pažeidimus turi būti taikomos adekvačios nuobaudos. Nuobaudos (įskaitant darbo santykių nutraukimą) turi būti proporcingos neautorizuotų veiksmų dažnumui ir jų pasekmių sunkumui.

5.3.7. Reikalavimai pagal sutartis dirbančiam personalui

Tam tikrais atvejais Patikimų Asmenų funkcijoms atlikti gali būti pasitelktos nepriklausomos sutarčių šalys ar konsultantai. Tokioms sutarčių šalims ar konsultantams taikomi tie patys funkcionalumo ir saugumo kriterijai, kurie taikomi SSC QCA darbuotojams, užimantiems adekvačias ar panašias pareigas.

Nepriklausomos sutarčių šalys ar konsultantai, kurių biografijų patikrinimai, numatyti šių CPS 5.3.2 punkte, nėra baigti ar kurie neišlaikė šių patikrinimų, turi teisę prieiti prie SSC QCA saugos įrangos tik tiek, kiek yra nuolat lydimi ir tiesiogiai prižiūrimi Patikimų Asmenų.

5.3.8. Dokumentacija, kuria aprūpinami darbuotojai

SSC QCA aprūpina savo darbuotojus apmokymų ir kita dokumentacija, reikalinga kompetentingai ir patenkinamai atlikti darbo funkcijas.

6. TECHNINĖS SAUGOS KONTROLĖS PRIEMONĖS

6.1. Raktų porų generavimas ir įdiegimas

Šis skyrius reglamentuoja raktų tvarkymą ir atitinkamas technines saugos kontrolės priemones.

6.1.1. Raktų porų generavimas

Raktai generuojami naudojant programinės įrangos paketą, pritaikytą darbui su sertifikatais.

Raktų pora, naudojama pasirašymui (nepaneigimo tikslams) ar šifravimui gali būti generuojama Galutinio naudotojo programine įranga. SSC RA taip pat turi teisę generuoti raktų porą registravimo (prašymo dėl sertifikavimo pateikimo) proceso metu.

6.1.2. Privataus rakto įteikimas Galutiniam naudotojui

Kai Galutinis Naudotojas pats sugeneruoja Galutinio Naudotojo raktų poras, privataus rakto įteikimas Galutiniam Naudotojui nereikalingas.

Tais atvejais, kai SSC QCA generuoja raktų porą pagal pareiškėjo prašymą, pareiškėjas turi gauti iš sertifikavimo ar registravimo tarnybos raktus (šifruotus ir išsaugotus laikmenoje, kurią gali nuskaityti kompiuteris) kartu su įėjimo fraze (slaptažodžiu) (angl. *pass phrase*), naudojama šifravimo algoritme.

Jeigu Galutinio Naudotojų raktų poras SSC QCA iš anksto generuoja kompiuterizuotuose laikmenuose (angl. *hardware tokens*) ar specialiose lustinuose kortelėse (angl. *smart cards*), šios laikmenos siunčiamos Galutiniam Naudotojui naudojant komercinio pristatymo paslaugas (įpakavimas turi būti toks, kad jį pažeidus, pažeidimai būtų akivaizdūs). Duomenys, reikalingi tokių laikmenų aktyvavimui, siunčiami RA ar Galutiniam Naudotojui. Tokių laikmenų platinimą fiksuoja SSC QCA.

Jeigu Galutinio Naudotojų raktų poras SSC QCA iš anksto generuoja ne kompiuterizuotuose laikmenuose ir ne specialiose lustinuose kortelėse, SSC QCA generuoja simetrinį sesijos raktą, šifruoja sugeneruotus raktus ir persiunčia pareiškėjui realaus laiko (angl. *on-line*) režimu arba perduoda fiziškai laikmenose.

6.1.3. Viešojo rakto įteikimas sertifikato sudarytojui

Galutiniai Naudotojai perduoda savo viešuosius raktus SSC QCA elektroniniu būdu, naudodami PKCS#10 ir SPKAC Prašymą Pasirašyti Sertifikatą (angl. *Certificate Signing Request (CSR*) ar kitą skaitmeniniu būdu pasirašytą paketą sesijos metu apsaugotos SSL *protokolu,* arba perduoda fiziškai laikmenose.

Jeigu Galutinio Naudotojo raktų poras generuoja SSC QCA, šis reikalavimas netaikomas.

6.1.4. SSC QCA viešojo rakto įteikimas naudotojams

SSC QCA padaro savo CA ir šakninių CA Sertifikatus prieinamus Galutiniams Naudotojams ir Pasitikinčioms Šalims šiais būdais:

a) CA Sertifikatus galima parsisiųsti internetu adresu www.ssc.lt;

b) įdiegia kompiuterizuotose laikmenose bei specialiose lustinėse kortelėse ir t.t.

SSC QCA viešasis raktas turi būti prieinamas per talpyklą (*repository*) standartiniais protokolais, tokiais kaip HTTP ar LDAP.

SSC QCA sertifikato išdavimo metu Galutiniam Naudotojui paprastai užtikrina pilną sertifikatų seką (įskaitant Sertifikatą sudarančią CA ir kitas CA šioje sekoje).

6.1.5. Raktų dydžiai

SSC QCA generuojamų raktų poros yra nuo 1024 iki 4096 bitų.

Kriptografiniai algoritmai ir raktų ilgiai turi užtikrinti elektroninį parašą patvirtinančio sertifikato galiojimo laikotarpiu praktinių galimybių nebuvimą atkurti parašo formavimo duomenis pagal parašo tikrinimo duomenis arba pagal elektroninį parašą.

SSC QCA raktų ilgiai turi būti ne mažiau nei 1024 bitų, o rekomenduojamas ilgis – ne mažiau 2048 bitų.

6.1.6. Duomenų santraukų algoritmai (angl. *hash*)

Duomenų santraukos algoritmai turi užtikrinti elektroninį parašą patvirtinančio sertifikato galiojimo laikotarpiu praktinių galimybių nebuvimą sukurti vienodą duomenų santrauką skirtingiems duomenims.

6.1.7. Viešųjų raktų parametrų generavimas

Šie CPS nenustato jokių reikalavimų šioje srityje, tačiau rekomenduojama, kad generuojant RSA ir DSA raktus būtų tenkinami minimalūs reikalavimai, aprašyti EESSI leidinyje "Saugių elektroninių parašų algoritmai ir parametrai[7]".

6.1.8. Parametrų kokybės patikrinimas

Netaikoma.

6.1.9. Raktų generavimas naudojant kompiuterinę įrangą/programinę įrangą

Galutinio Naudotojo raktų poros gali būti generuojamos tiek naudojant kompiuterinę įrangą, tiek programinę įrangą.

6.1.10. Tikslai, kuriems gali būti naudojami raktai (pagal X.509 v3 rakto naudojimo sritį)

X.509 trečiosios versijos sertifikatams CA paprastai nustato raktų naudojimo išplėtimą pagal standartą RFC 3280[8]: Interneto X.509 viešojo rakto infrastruktūros Sertifikatas ir CRL profilis, 2002 balandžio mėn.

[7] EESSI-SG, 2001 m. spalio 19 d..
[8] RFC 3280 pakeitė RFC 2459.

Lentelė Nr. 3. Rakto naudojimo išplėtimo nustatymai.

		Galutinių naudotojų sertifikatai	Parašas dviejų raktų porų pagrindu	Šifravimas dviejų raktų porų pagrindu
Kritiškumas		*būtina*	*būtina*	*būtina*
0	digitalSignature	1	1	0
1	nonRepudiation	1	0	0
2	keyEncipherment	1	0	1
3	dataEncipherment	0	0	0
4	keyAgreement	0	0	0
5	keyCertSign	0	0	0
6	CRLSign	0	0	0
7	encipherOnly	0	0	0
8	decipherOnly	0	0	0

Visi Galutinio Naudotojo sertifikatai turi palaikyti rakto naudojimo išplėtimą (*KeyUsage extension*), kuris turi būti nustatytas kaip *Critical*.

6.2. Privačiojo rakto apsauga

SSC QCA įdiegia fizinės, loginės ir procedūrinės kontrolės derinį, siekiant užtikrinti SSC QCA privačiųjų raktų saugumą. Loginė ir procedūrinė kontrolė aprašyta Nuostatų 6.2 skyriuje. Fizinės prieigos kontrolė aprašyta Nuostatų 5.1.2 punkte. Galutiniai naudotojai pagal Sutartį privalo imtis būtinų privačiųjų raktų apsaugos priemonių nuo praradimo, atskleidimo, pakeitimo ar nesankcionuoto jų naudojimo.

6.2.1. Kriptografinio modulio standartai

Privatieji raktai turi būti užkoduoti kompiuteriui įskaitomoje formoje, įskaitant specialiąsias (mikrolustines) korteles (angl. *smart cards)*. Raktą apsaugantis slaptažodis turi būti tinkamos kokybės.

Sąvoka "SSC QCA raktas" apjungia privataus rakto generavimo procedūrą ir saugojimą.

SSC QCA naudoja techninės įrangos kriptografinius modulius, kurie atitinka Lietuvos standartų LST CWA 14168 "Saugi parašo formavimo įranga EAL 4" ir LST CWA 14170 "Saugumo reikalavimus.

6.2.2. Privačiojo rakto daugiaasmenė kontrolė

Galutinio naudotojo privatusis raktas nepriklauso daugiaasmenei kontrolei. SSC QCA priklausantys privatieji raktai priklauso tokiai kontrolei.

SSC QCA įdiegia techninius ir procedūrinius mechanizmus, pagal kuriuos reikalaujama daugelio Aukštos atsakomybės asmenų dalyvavimo atliekant slaptas SSC QCA kriptografines operacijas.

CA naudoja "slaptą pasidalinimą dalimis", kad būtų padalinti atyvavimo duomenys, reikalingi SSC QCA privačiojo rakto panaudojimui, į atskiras dalis, vadinamas "Slaptomis dalimis", kurios laikomos kvalifikuotų ir Aukštos atsakomybės asmenų, vadinamų "Dalių turėtojais".

Pradinis Slaptų dalių skaičius, sukurtų ir paskirstytų konkretiems techninės įrangos kriptografiniams moduliams, reikalingas aktyvuoti modulyje, laikomą SSC QCA privatųjį raktą, yra 2. Pradinis dalių skaičius, reikalingas

pasirašyti CA Sertifikatą, yra 3. Pažymėtina, kad bendras dalių, paskirstytų avarinio atkūrimo kortelių ar kitų laikmenų skaičius gali būti mažesnis už paskirstytų mikroprocesorinių kortelių ar kitų laikmenų, skirtų eilinėms funkcijoms atlikti, bet reikalingų dalių skaičius lieka tas pats. Slaptos dalys saugomos laikantis Nuostatų 6.4.2 punkto.

Privačiojo rakto daugiaasmenė kontrolė atitinka Lietuvos standartų LST CWA 14168 "Saugi parašo formavimo įranga EAL 4" ir LST CWA 14170 "Saugumo reikalavimus.

6.2.3. Privačiojo rakto sąlyginis deponavimas *(escrow)*

SSC QCA nedeponuoja CA, RA ar Galutinio Naudotojo privačiųjų raktų jokiai trečiajai šaliai teisės normų įgyvendinimo tikslais. SSC QCA privačiojo parašo raktai neturi būti deponuojami trečiosios šalies.

6.2.4. Privačiojo rakto dubliavimas

SSC QCA kuria SSC QCA privačiojo rakto dublikatus einamojo atkūrimo ir avarinio atkūrimo tikslais. Tokie dublikatai laikomi kriptografine ar užšifruota forma techninės įrangos kriptografiniuose moduliuose ir susijusiuose rakto saugojimo prietaisuose.

Galutinių naudotojų privačiojo rakto laikymui naudojami kriptografiniai moduliai atitinka Nuostatų 6.2.1. punkto reikalavimus. 1-os ir 2-os klasės sertifikatų Galutinių naudotojų privatieji raktai kopijuojami į atsarginius techninės įrangos kriptografinius modulius laikantis Nuostatų 6.2.6 punkto.

3-os klasės Galutinių Naudotojų sertifikatų privatieji raktai nepasiliekami.

SSC QCA nelaiko RA privačiųjų raktų kopijų.

6.2.5. Privačiojo rakto archyvavimas

Kai baigiasi 1-os ir 2-os klasės sertifikatų Galutinių naudotojų raktų poros galiojimas, tokia raktų pora bus saugoma ne mažiau kaip 5 metų laikotarpį. Saugomos Galutinių naudotojų raktų poros bus saugiai laikomos naudojant techninės įrangos kriptografinius modulius, kurie atitinka Nuostatų 6.2.1. punkto reikalavimus. Procedūrų kontrolė apsaugo nuo saugomų Galutinių naudotojų raktų porų grąžinimo naudoti gaminimui. Saugojimo laikotarpio pabaigoje, saugomi Galutinių naudotojų privatieji raktai bus saugiai sunaikinti laikantis Nuostatų 6.2.9 punkto.

3-os klasės Galutinių Naudotojų sertifikatų privatieji raktai jokiais atvejais nėra saugomi.

6.2.6. Privačiojo rakto įvedimas į kriptografinį modulį

SSC QCA generuoja Galutinių naudotojų raktų poras techninės įrangos kriptografiniuose moduliuose, kuriuose raktai bus naudojami. Be to, SSC QCA daro 1-os ir 2-os klasės sertifikatų Galutinių naudotojų raktų porų kopijas einamojo ir avarinio atkūrimo tikslais.

Kai Galutinių naudotojų raktų porų atsarginės versijos yra išsaugotos kitame modulyje, tokios raktų poros perduodamos tarp modulių šifruota forma.

3-os klasės Galutinių Naudotojų sertifikatų privatieji raktai jokiais atvejais nėra saugomi.

6.2.7. Privačiojo rakto aktyvavimo metodas

Visi SSC QCA sertifikavimo sistemos dalyviai privalo saugoti privačiųjų raktų aktyvavimo duomenis nuo praradimo, vagystės, pakeitimo, neautorizuoto atskleidimo ar neautorizuoto panaudojimo.

Siekiant aktyvuoti privatų raktą specifiniai aktyvavimo duomenys turi būti įvedami į kriptografinį modulį. Aktyvavimo duomenis turi mažiausiai sudaryti PIN kodas arba slaptažodis (*passphrase*).

6.2.7.1. Galutinio naudotojo privatieji raktai

Šis skyrius nustato SSC QCA Galutinių naudotojų privačiųjų raktų aktyvavimo duomenų apsaugos standartus. Be to, Galutiniai naudotojai gali patys pasirinkti naudoti dar pažangesnius, patobulintus privačiųjų raktų apsaugos mechanizmus, įskaitant specialiąsias (mikrolustines) korteles (angl. *smart card*), biometrines prieigos įrangą, ir kitą techninę įrangą, skirtą saugoti privačiuosius raktus. Yra skatinamas/remiamas dviejų faktorių tapatybės nustatymo mechanizmų naudojimas (pvz., slaptažodžio, biometrinės priemonės ar pan.).

6.2.7.1.1. 1 klasės Sertifikatas

SSC QCA 1 klasės sertifikatų privačiųjų raktų apsaugos standartas pagrįstas Galutinių naudotojų komerciškai pagrįstomis priemonėmis garantuojant fizinę Galutinio naudotojo kompiuterinės įrangos, prijungto prie tinklo, apsaugą siekiant užkirsti kelią minėtos įrangos ir susijusio rakto panaudojimui be naudotojo sutikimo, leidimo. Be to, SSC QCA rekomenduoja Galutiniams naudotojams naudoti slaptažodžius sutinkamai su CPS 6.6.2 punktu ar ekvivalentiškas priemones, skirtas Galutinio naudotojo tapatybės nustatymui prieš privačiojo rakto panaudojimą..

6.2.7.1.2. 2 klasės sertifikatai

SSC QCA 2 klasės sertifikatų privačiųjų raktų apsaugos standartas pagrįstas Galutinių naudotojų:

- slaptažodžių naudojimu pagal šio CPS 6.6.2 punktą ar ekvivalentiškų priemonių, skirtų Galutinio naudotojo tapatybės nustatymui, pasitelkimu, kurios gali apimti, pvz., slaptažodį, būtiną privačiojo rakto panaudojimui;
- komerciškai pagrįstomis priemonėmis, užtikrinančiomis fizinę Galutinio naudotojo galinės įrangos ar kompiuterio, pajungto prie tinklo, apsaugą siekiant užkirsti kelią minėtos įrangos ir susijusio rakto panaudojimui be naudotojo sutikimo, leidimo.

Deaktyvuoti privatūs raktai bus laikomi tik užkoduotoje formoje.

6.2.7.1.3. 3 klasės sertifikatai, išskyrus Administratorių sertifikatai

SSC QCA 3 klasės Galutinių naudotojų sertifikatų privačiųjų raktų apsaugos standartas nustato Galutinių naudotojų:

- specialiųjų (mikrolustinių) kortelių (*smart card*), kitų kompiuterine įranga pagrįstų kriptografinių, biometrinių, ar ekvivalentiškų saugumo priemonių, kurių tikslas – pasirašytojo tapatybės patvirtinimas iki priėjimo prie privačiojo rakto, panaudojimą; ir
- komerciškai pagrįstas priemones, užtikrinančias fizinę Galutinio naudotojo galinės įrangos ar kompiuterio, pajungto prie tinklo, apsaugą siekiant užkirsti kelią minėtos įrangos ir susijusio rakto panaudojimui be naudotojo sutikimo, leidimo.

Privalomas slaptažodžio panaudojimas drauge su mokrolustine kortele (*smart card*) ar kitomis kompiuterine įranga pagrįstomis kriptografinėmis, biometrinėmis, ar ekvivalentiškomis saugumo priemonėmis sutinkamai su CPS 6.6.2 punktu.

6.2.7.2. 3-osios klasės Administratorių sertifikatai

SSC QCA standartai reikalauja, kad Administratoriai:

- Naudotų specialiąsias (mikrolustines) korteles (*smart card*), kitas kompiuterine įranga pagrįstas kriptografines, biometrines ar ekvivalentiškas saugumo priemones, kurių tikslas – Administratoriaus tapatybės patvirtinimas iki priėjimo prie privačiojo rakto; ir
- Imtųsi komerciškai pagrįstų priemonių, užtikrinančių fizinę Administratoriaus galinės įrangos ar kompiuterio, pajungto prie tinklo, apsaugą siekiant užkirsti kelią minėtos įrangos ir susijusio rakto panaudojimui be Administratoriaus sutikimo, leidimo.

Privalomas slaptažodžio panaudojimas drauge su specialiąja (mikrolustine) kortele (*smart card*) ar kitomis kompiuterine įranga pagrįstomis kriptografinėmis, biometrinėmis, ar ekvivalentiškomis saugumo priemonėmis sutinkamai su CPS 6.6.2 punktu.

6.3. Parašo formavimo įranga

SSC QCA užtikrina, kad privatieji raktai - parašo formavimo duomenys - būtų apsaugoti slaptažodžiu ir/arba biometriniais duomenimis.

SSC QCA užtikrina, kad parašo formavimo įranga:

1. užtikrina parašo formavimo duomenų apsaugą nuo nesankcionuotos prieigos;
2. būtų apsaugota nuo atkūrimo ir kopijavimo;
3. apsaugotų parašo formavimo duomenis nuo atkūrimo ir kopijavimo;
4. turėtų priemones, apsaugančias nuo slaptažodžio atskleidimo daugkartinių bandymų būdu.

3 klasės sertifikato atveju SSC QCA naudoja tik saugią parašo formavimo įrangą, atitinkančią Lietuvos standartų LST CWA 14168 "Saugi parašo formavimo įranga EAL 4" ir LST CWA 14170 "Saugumo reikalavimus.

Galutiniai naudotojai elektroninio parašo formavimui privalo naudoti tik saugią parašo formavimo įrangą, atitinkančią Lietuvos standartų LST CWA 14168 "Saugi parašo formavimo įranga EAL 4" ir LST CWA 14170 "Saugumo reikalavimus.

Parašo formavimo duomenų kūrimo mechanizmas turi užtikrinti, kad dviem pasirašantiems asmenims (arba daugiau pasirašančių asmenų) nebūtų suteikta tokia pati parašo formavimo duomenų ir parašo tikrinimo duomenų pora.

6.3.1. Privačiojo rakto deaktyvavimo metodika

Administratorių, Galutinių naudotojų privatieji raktai gali būti deaktyvuojami po kiekvienos operacijos, išsiregistruojant iš sistemos, arba pašalinant, išimant specialiąją (mikrolustinę) kortelę iš kortelių skaitytuvo, priklausomai nuo to, koks tapatybės nustatymo metodas yra naudojamas. Visais atvejais, Galutiniai naudotojai privalo adekvačiai apsaugoti savo privačiuosius raktus sutinkamai su šio CPS 2.1.3, 6.6.2 punktais.

6.3.2. Privačiojo rakto sunaikinimo metodika

Kai tai būtina, CA sunaikina Galutinių naudotojų privačiuosius raktus tokia tvarka, kuri protingai užtikrina, kad nelieka liekanų, likučių kurie gali būti panaudoti atstatant raktą. CA savo kompiuterinio kriptografinio modulio atžvilgiu naudoja „*neutralizavimo*“ funkciją (*zeroisation function*) ir kitas tinkamas priemones tam, kad būtų užtikrintas tinkamas CA raktų sunaikinimas.

6.4. Parašo tikrinimo įranga

SSC QCA užtikrina, kad parašo tikrinimo įranga:

1. patikimai patikrintų elektroninį parašą, teisingai ir tinkamai pateikti tikrinimo rezultatus parašo naudotojui;
2. teisingai pateiktų pasirašytus duomenis parašo naudotojui jam priimtinu būdu;
3. patikrintų pasirašančio asmens sertifikato galiojimo statusą (galiojantis, sustabdytas, nutrauktas);
4. patikrintų sertifikatų seką, visų sekos sertifikatų galiojimo statusą ir kitus duomenis pagal parašo taisyklėse ir sertifikatų taisyklėse nurodytus reikalavimus;
5. pasirašytų duomenų pakeitimus praneštų Galutiniam naudotojui;
6. teisingai ir Galutiniam naudotojui priimtinu būdu pateiktų elektroninio parašo ir sertifikatų sekos duomenis, naudojamus elektroniniam parašui tikrinti:
    i. apie pasirašantį asmenį;
    ii. pasirašančio asmens sertifikato galiojimo pradžią ir pabaigą;
    iii. sertifikato taisykles vienareikšmiškai pažymintį identifikatorių (jeigu toks yra);
    iv. pasirašančio asmens sertifikato naudojimo apribojimus (jeigu tokių yra);
    v. apie paslaugų teikėją;
    vi. pasirašančio asmens sertifikato galiojimo statusą;
    vii. sertifikatų seką;
    viii. parašo taisykles vienareikšmiškai pažymintį identifikatorių (jeigu toks yra);
    ix. sertifikato požymį (kad jis kvalifikuotas, jei tai – 3 –os klasės sertifikatas).

6.5. Kiti raktų poros tvarkymo aspektai

6.5.1. Viešojo rakto archyvavimas

Galutinio Naudotojo sertifikatų archyvavimas ir atsarginių kopijų kūrimas yra SSC QCA informacijos atsarginių kopijų kūrimo einamųjų procedūrų dalis.

Viešieji raktai turi būti visada archyvuojami.

6.5.2. Viešųjų ir privačiųjų raktų naudojimo laikotarpiai

Sertifikato veiklos laikotarpis baigiasi tada, kai baigiasi sertifikato galiojimo laikotarpis arba kai Sertifikatas atšaukiamas. Raktų porų veiklos laikotarpis yra toks pats, kaip su jais susijusių sertifikatų veiklos laikotarpis, išskyrus tai, kad privatūs raktai gali būti toliau naudojami dešifravimui, o viešieji raktai gali būti toliau naudojami parašo patikrinimui. Maksimalūs veiklos laikotarpiai sertifikatams, sudarytiems šių CPS galiojimo pradžios dieną ar vėliau, nurodyti žemiau pateikiamoje lentelėje.

Lentelė Nr. 4 – Sertifikatų galiojimo laikotarpiai

Sertifikatų tipai	***Galiojimo laikotarpis***
Galutinių Naudotojų sertifikatai	Paprastai iki 2 metų, bet neilgiau 5 metų
Administratorių sertifikatai	Paprastai iki 2 metų, bet neilgiau 5 metų

Išskyrus atvejus, nurodytus šiame skyriuje, SSC QCA sertifikavimo sistemos dalyviai privalo nustoti bet kokiu būdu naudoti savo raktų poras po to, kai šių naudojimo laikotarpis yra pasibaigęs.

Sertifikatai, kuriuos SSC QCA sudarė Galutiniams Naudotojams, gali turėti veiklos laikotarpius, kurie yra ilgesni nei dveji metai (iki penkerių metų), jeigu tenkinami šie reikalavimai:

- sertifikatai išduoti fiziniams asmenims,
- Galutinio Naudotojo raktų poros yra kompiuterizuotuose laikmenuose arba specialiose lustinuose kortelėse (angl. *smart cards*),
- Galutiniai Naudotojai kasmet privalo pereiti pakartotinio tapatybės nustatymo procedūras pagal šių CPS 3.2 skyriaus nuostatas, jei nori, kad raktas galiotų 5 metus;
- Galutiniai Naudotojai kasmet privalo įrodyti, kad turi privatųjį raktą, kuris atitinka viešąjį raktą, esantį sertifikate, jei nori, kad raktas galiotų 5 metus;
- jei Galutinis Naudotojas nesugeba sėkmingai pereiti pakartotinio tapatybės nustatymo procedūrų pagal šių CPS 3.2 skyriaus nuostatas, arba nesugeba įrodyti, kad turi privatųjį raktą, kuris atitinka viešąjį raktą, esantį sertifikate, kaip aptarta aukščiau, SSC QCA privalo automatiškai atšaukti Galutinio Naudotojo Sertifikatą.

6.6. Aktyvavimo duomenys

6.6.1 Aktyvavimo duomenų generavimas ir įdiegimas

Slaptažodžiai/įėjimo frazės, naudojami duomenų apsaugai sertifikavimo proceso metu turi būti parenkami pagal bendrąsias SSC QCA rekomendacijas dėl jų ilgumo ir netaisyklingumo (entropijos) laipsnio.

SSC QCA primygtinai rekomenduoja, kad ir Galutiniai Naudotojai parinkinėtų slaptažodžius, kurie atitinka aukščiau minėtus reikalavimus. SSC QCA taip pat rekomenduoja, kad privataus rakto aktyvavimui būtų naudojami du tapatybės nustatymo mechanizmai (pvz., laikmena ir įėjimo frazė, biometrija ir laikmena, biometrija ir įėjimo frazė).

6.6.2. Aktyvavimo duomenų apsauga

SSC QCA primygtinai rekomenduoja, kad Galutiniai Naudotojai saugotų savo privačiuosius raktus šifruotoje formoje, naudodami kompiuterizuotas laikmenas ir/ar saugias įėjimo frazes. Rekomenduojama naudoti du tapatybės nustatymo mechanizmus (pvz., laikmena ir įėjimo frazė, biometrija ir laikmena, biometrija ir įėjimo frazė). 3-os klasės sertifikatams tai privaloma.

6.6.3. Kiti aktyvavimo duomenų aspektai

Netaikoma.

6.7. Kompiuterinės saugos kontrolės priemonės

Sertifikavimo tarnyba privalo naudoti skirtą tik sertifikavimo tikslams ir neprijungtą prie viešųjų ryšių tinklų darbo stotį (angl. *dedicated workstation*).

6.7.1. Specifiniai techniniai reikalavimai kompiuterinei saugai

SSC QCA užtikrina, kad sistemos, kuriose laikoma SSC QCA programinė įranga ir duomenų bylos, yra Patikimos Sistemos, būtų apsaugotos nuo neteisėto priėjimo prie jų. Be to, SSC QCA leidžia prieiti prie gamybinių tarnybinių stočių (angl. *production servers*) tik tiems asmenims, kuriems tokio priėjimo pagrįstai reikia pagal Lietuvos Respublikos įstatymus. Kiti naudotojai neturi turėti paskyros (angl. *account*) produkcijos tarnybinėse stotyse.

SSC QCA sertifikatų gamybinis tinklas turi būti logiškai atskirtas nuo kitų komponentų. Toks atskyrimas užkerta kelią priėjimui prie tinklo išskyrus pasitelkiant aiškiai apibrėžtas priėjimo aplikacijas-priemones. SSC QCA turi

naudoti ugniasienes (angl. *firewall*), siekdama apsaugoti gamybini tinklą nuo įsiveržimo iš vidaus ir iš išorės bei apriboti priėjimo prie produkcijos sistemų galimybę.

SSC QCA turi reikalauti naudoti slaptažodžius, kurie atitinka minimalius simbolių skaičiaus bei raidžių, skaičių ir specialiųjų simbolių kombinuotumo reikalavimus. SSC QCA turi reikalauti, kad slaptažodžiai būtų periodiškai keičiami.

Tiesiogiai prieiti prie SSC QCA duomenų bazių, palaikančių SSC QCA talpyklą, leidžiama tik Patikimiems Asmenims iš SSC QCA operatyvinės grupės (angl. *operations group*), kuriems tokio priėjimo pagrįstai reikia verslo tikslais.

6.7.2. Kompiuterių saugos reitingas

Netaikoma.

6.8. Galiojimo laikotarpio techninės kontrolės priemonės

6.8.1. Sistemos vystymo kontrolės priemonės

SSC QCA kuria ir diegia savo programas pagal CA sistemų vystymo ir keitimo vadybos standartus.

SSC QCA užtikrina, kad sertifikatų valdymo sistema:

a) susidėtų tik iš informacinių technologijų priemonių ir komponentų, būtinų sertifikavimo paslaugoms atlikti būti apsaugota nuo nesankcionuotų pakeitimų, kontroliuoti, aptikti ir signalizuoti apie pakitimus, susijusius su galimu saugumo pažeidimu;
b) užtikrintų pakankamą techninį ir kriptografinį atliekamos funkcijos saugumą (įskaitant paslaugų teikėjo parašo formavimo duomenų apsaugą, įgalinančią išvengti sertifikatų klastočių), taip pat pasirašančio asmens parašo formavimo duomenų konfidencialumą jų kūrimo, tvarkymo ir perdavimo metu;
c) turėtų saugumo mechanizmus, užtikrinančius funkcijų atskyrimą taip, kad bent du asmenys vienu metu būtų įtraukti į parašo formavimo duomenų kūrimą ir tvarkymą ir kad tik įgalioti asmenys galėtų daryti pakeitimus sertifikatų valdymo sistemoje;
d) sudarytų galimybę kontroliuoti kiekvieną veiksmą, kuris gali turėti įtaką sertifikatų valdymo sistemos darbui, registruoti jų metu naudojamą informaciją, bet kuriuo metu patikrinti sertifikatų duomenų autentiškumą;
e) atitiktų EAL4 (pagal Lietuvos standartą LST ISO/IEC 15408 "Informacijos technologija. Saugumo metodai. Informacijos technologijų saugumo įvertinimo kriterijai") arba ekvivalentų saugumo įvertinimo lygį.

6.8.2. Saugos vadybos kontroliavimo priemonės

SSC QCA privalo turėti paruoštus mechanizmus ir/ar taisykles savo CA sistemų konfigūracijos kontrolei ir stebėjimui. SSC QCA sukuria visų programinės įrangos paketų ir CA programinės įrangos atnaujinimų santrauką (angl. *hash*). Ši santraukos funkcija naudojama mechaniškai įvertinant tokios programinės įrangos vientisumą, integralumą. SSC QCA turi patikrinti savo CA sistemų integralumą iš karto po įdiegimo, o vėliau – periodiškai.

6.8.3. Galiojimo laikotarpio saugos reitingai

Netaikoma.

6.9. Tinklo saugos kontrolės priemonės

SSC QCA atlieka visas savo CA ir RA funkcijas naudodama tinklus, apsaugotus pagal SSC QCA Saugos Politiką siekiant užkirsti kelią neteisėtam autorizuotam priėjimui prie jų ir kitai neteisėtai veiklai. SSC QCA saugo saugos reikalaujančią informaciją, naudodama šifravimą ir elektroninius parašus.

Kompiuteris, kuriame naudojamas kriptografinis modulis, skirtas SSC QCA veiklai, turi būti neprijungtas prie tinklo (*off-line*).

6.10. Kriptografinių modulių inžinerijos kontrolės priemonės

Kriptografiniai moduliai, kuriuos naudoja SSC QCA, turi atitikti reikalavimus, nurodytus šių CPS 6.2.1 skyriuje.

7. SERTIFIKATŲ IR CRL SĄRAŠŲ PROFILIAI

7.1. Sertifikato profilis

Šių CPS 7.1 skyrius apibrėžia SSC QCA sudarytų sertifikatų profilio ir sertifikato turinio reikalavimus sertifikatams, sudarytiems pagal šiuos CPS.

SSC QCA sudaryti sertifikatai turi atitikti:

(d) ITU-T rekomendaciją X.509 (1997): *Information Technology - Open Systems Interconnection - The Directory: Authentication Framework*, 1997 birželio mėn., ir
(e) RFC 3280: Interneto X.509 viešojo rakto infrastruktūros sertifikato ir CRL profilį, 2002 balandžio mėn. ("RFC 3280").

1-os klasės Sertifikatas

1-os klasės sertifikatų profiliai atitinka standartą RFC 32802459: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.

2-os klasės Sertifikatas

2-os klasės sertifikatų profiliai atitinka standartą RFC 32802459: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.

3-os klasės Galutinio Naudotojo Sertifikatas

3-os klasės sertifikatų profiliai atitinka standartą RFC 3280 „Internet X.509 Public Key Infrastructure: Certificate and CRL Profile" ir RFC 3739 „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile".

SSC QCA išduodamuose X.509 sertifikatuose turi būti bent pagrindiniai pirmosios versijos X.509 laukeliai ir iš anksto nustatytos vertės bei verčių apribojimai, nurodyti žemiau pateikiamose lentelėse Nr. 5.1 ir Nr.5.2

Sutrumpinimai:
P – privalomas;

N – nebūtinas;
D – dinaminė reikšmė;
F – fiksuota reikšmė;

Lentelė Nr. 5.1. 3-os klasės sertifikato sandara.

Kvalifikuotas 3-os klasės Sertifikatas					
Sertifikato parametrai	**Taikymas**				**Reikšmė**
	P	**N**	**D**	**F**	
Parašo algoritmas *signatureAlgorithm*	P			F	SHA-1 su RSA kodavimu.
Parašo vertė *signatureValue*	P		D		Sertifikavimo tarnybos suformuoas elektroninis subjekto sertifikato parašas (pagal RFC 3280).
Sertifikatas *tbsCertificate*	P				
Versija *version*	P			F	3 (0x02)
Serijinis numeris *serialNumber*	P		D		Suteikiamas CA.
Parašas *signature*	P		D		SHA-1 su RSA kodavimu.
Sertifikato išleidėjas *issuer*	P				
Valstybė *country*	P		D		„LT“.
Organizacija *organisation*		N	D		„UAB Skaitmeninio sertifikavimo centras“ arba „Skaitmeninio sertifikavimo centras“.
Organizacijos padalinys/skyrius *organisationalUnit*		N	D		„Sertifikavimo tarnyba“ arba „Certification Authority“.
Bendrasis pavadinimas *commonName*	P		D		Atitinkamos sertifikavimo tarnybos pavadinimas.
Serijos numeris *serialNumber*	P		D		Unikalus pasirinktos sertifikavimo tarnybos ribose sertifikato serijos numeris.
Galiojimas *validity*	P				
Ne iki *notBefore*	P		D		Sertifikato sukūrimo proceso data ir laikas.
Ne po *notAfter*	P		D		Sertifikato sukūrimo proceso data ir laikas + užsakomas sertifikato galiojimo periodas.
Subjektas (pasirašytojas) *subject*	P				
Valstybė	P		D		LR piliečiams – „LT“, kitiems – pagal registracijos vietą.

Kvalifikuotas 3-os klasės Sertifikatas					
Sertifikato parametrai	**Taikymas**				**Reikšmė**
	P	**N**	**D**	**F**	
country					
Atstovaujamas juridinis asmuo *organisation*		N	D		Juridinio asmens pavadinimas.
Atstovaujamo juridinio asmens padalinis/skyrius *organisationalUnit*		N	D		Atstovaujamo juridinio asmens padalinio/skyriaus pavadinimas.
Vardas, pavardė *commonName*		N	D		Šiame lauke įrašomi asmens vardas(-ai) ir pavardė arba netaikomas, jei užpildomas pseudonimo laukas („*pseudonym*“).
Pseudonimas *pseudonym*		N	D		Šiame lauke įrašomas asmens pseudonimas arba netaikomas, jei užpildomas vardo ir pavardės laukas („*commonName*“).
Serijos numeris *serialNumber*	P		D		Unikalus pasirinktos sertifikavimo tarnybos ribose sertifikato serijos numeris.
Subjekto viešojo rakto informacija *subjectPublicKeyInfo*	P				
Algoritmas *algorithm*	P			F	SHA-1 su RSA kodavimu.
Subjekto viešasis raktas *subjectPublicKey*	P		D		Subjekto sertifikato viešasis raktas.

Lentelė Nr. 5.2 – 3-os klasės sertifikato išplėtimų sandara

Kvalifikuotas 3-os klasės Sertifikatas						
Sertifikato išplėtimų parametrai	**Taikymas**					**Reikšmė**
	P	**O**	**D**	**F**	**K**	
Sertifikavimo tarnybos rakto identifikatorius *authorityKeyIdentifier*	P		D			Nurodomi: ▪ sertifikavimo tarnybos rakto identifikatorius; ▪ sertifikavimo tarnybos sertifikato leidėjo pavadinimas ir jo sertifikato serijos numeris.
Sertifikato turėtojo rakto identifikatorius *subjectKeyIdentifier*	P		D			Sertifikato turėtojo rakto identifikatorius yra generuojamas pagal RFC 3280 reikalavimus.
Raktų paskirtis *keyUsage*	P			F	K	Nustatomi šie keyUsage bitai: ▪ digital signature, ▪ key encipherment.

Kvalifikuotas 3-os klasės Sertifikatas						
Sertifikato išplėtimų parametrai	**Taikymas**					**Reikšmė**
	P	**O**	**D**	**F**	**K**	
Išplėstas raktų naudojimas *extendedKeyUsage*	P			F		Nustatomi šie extendedKeyUsage OID: ▪ 1.3.6.1.5.5.7.3.4 (id_kp_emailProtection), ▪ 1.3.6.1.5.5.7.3.2 (id_kp_clientAuth).
Sertifikatų taisyklės *certificatePolicies*	P			F		
Sertifikato taisyklių identifikatorius *certPolicyId*	P			F		Šių CPS identifikatorius – „1.3.6.1.4.1.22501.1.2.0“
Nuoroda į sertifikato taisykles *cPSuri*	P			F		Nuorodą į WEB resursą, iš kurio yra pasiekiamas šio CPS tekstas – „ http://www.ssc.lt/cps “
Papildomi subjektą identifikuojantis parametrai *subjectAlternativeName*		O				
Subjekto elektroninio pašto adresas *rfc822Name*		O	D			Įrašomas subjekto pateiktas paraiškoje el. pašto adresas.
Baziniai panaudojimo apribojimai *basicConstraints*	P					
Sertifikato turėtojo tipas *cA*	P			F		Galutinių vartotojų sertifikatams nustatoma reikšmė „FALSE“
Sertifikavimo grandinės ilgio apribojimas *pathLengthConstraints*		O		F		Galutinių vartotojų sertifikatams reikšmė nenustatoma arba nurodoma „None“
CRL paskirstymo taškai *cRLDistributionPoints*	P					
CRL paskirstymo taško adresas *distributionPoint*	P			F		URI tipo reikšmė į WWW resursą, iš kurio galima parsisiūsti atšauktų sertifikatų sąrašą
Priėiga prie sertifikavimo tarnybos informacijos *authorityInformationAccess*	P					Pasirinktinai arba kartu nurodomi: 1) priėjimo prie CA sertifikato adresas, 2) priėjimo prie OCSP tarnybos adresas.
Priėigos OID *oID*	P			F		1) OID = 1.3.6.1.5.5.7.48.2 (CA sertifikato adreso atvėju), 2) OID = 1.3.6.1.5.5.7.48.1 (OCSP tarnybos adreso atvėju)
Priėigos adresas *uRI*	P		D			URI tipo reikšmė(-ės).
Kvalifikuoto sertifikato pareiškimas *qcStatement*	P					

Kvalifikuotas 3-os klasės Sertifikatas						
Sertifikato išplėtimų parametrai	**Taikymas**					**Reikšmė**
	P	**O**	**D**	**F**	**K**	
qcStatement-1	P			F		*statementId* nustatoma reikšmė „0.4.0.1862.1.1“ (*id-etsi-qcs-QcCompliance*)
Sertifikato tipas Netscape suderinamai programinei įrangai *nsCertType*		O		F		Nustatomi šie nsCertType bitai: ▪ SSL Client Authentication, ▪ S/MIME.
Komentaras Netscape suderinamai programinei įrangai *netscapeComment*		O	D			„Kvalifikuotas sertifikatas“

3-os klasės Administratoriaus Sertifikatas

3-os klasės Administartoių sertifikatų profiliai atitinka standartą RFC 3280 „Internet X.509 Public Key Infrastructure: Certificate and CRL Profile“ ir RFC 3739 „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile“.

SSC QCA išduodamuose X.509 sertifikatuose turi būti bent pagrindiniai pirmosios versijos X.509 laukeliai ir iš anksto nustatytos vertės bei verčių apribojimai, nurodyti žemiau pateikiamose lentelėse Nr. 5.3 ir Nr.5.4

Sutrumpinimai:
P – privalomas;
N – nebūtinas;
D – dinaminė reikšmė;
F – fiksuota reikšmė;

Lentelė Nr. 5.3. 3-os klasės Administratoriaus sertifikato sandara.

Sertifikato parametrai	**Taikymas**				**Reikšmė**
	P	**N**	**D**	**F**	
Parašo algoritmas *signatureAlgorithm*	P			F	SHA-1 su RSA kodavimu.
Parašo vertė *signatureValue*	P		D		Sertifikavimo tarnybos suformuoas elektroninis subjekto sertifikato parašas (pagal RFC 3280).
Sertifikatas *tbsCertificate*	P				
Versija *version*	P			F	3 (0x02)
Serijinis numeris *serialNumber*	P		D		Suteikiamas CA.

Sertifikato parametrai	Taikymas				Reikšmė
	P	**N**	**D**	**F**	
Parašas *signature*	P		D		SHA-1 su RSA kodavimu.
Sertifikato išleidėjas *issuer*	P				
Valstybė *country*	P		D		„LT“.
Organizacija *organisation*		N	D		„UAB Skaitmeninio sertifikavimo centras“ arba „Skaitmeninio sertifikavimo centras“.
Organizacijos padalinys/skyrius *organisationalUnit*		N	D		„Sertifikavimo tarnyba“ arba „Certification Authority“.
Bendrasis pavadinimas *commonName*	P		D		Atitinkamos sertifikavimo tarnybos pavadinimas.
Serijos numeris *serialNumber*	P		D		Unikalus pasirinktos sertifikavimo tarnybos ribose sertifikato serijos numeris.
Galiojimas *validity*	P				
Ne iki *notBefore*	P		D		Sertifikato sukūrimo proceso data ir laikas.
Ne po *notAfter*	P		D		Sertifikato sukūrimo proceso data ir laikas + užsakomas sertifikato galiojimo periodas.
Subjektas (pasirašytojas) *subject*	P				
Valstybė *country*	P		D		LR piliečiams – „LT“, kitiems – pagal registracijos vietą.
Atstovaujamas juridinis asmuo *organisation*		N	D		Juridinio asmens pavadinimas.
Atstovaujamo juridinio asmens padalinis/skyrius *organisationalUnit*		N	D		Nurodomas administruojamos sistemos pavadinimas.
Vardas, pavardė *commonName*		N	D		Šiame lauke įrašomi asmens vardas(-ai) ir pavardė arba netaikomas, jei užpildomas pseudonimo laukas („*pseudonym*“).
Pseudonimas *pseudonym*		N	D		Šiame lauke įrašomas asmens pseudonimas arba netaikomas, jei užpildomas vardo ir pavardės laukas („*commonName*“).
Serijos numeris *serialNumber*	P		D		Unikalus pasirinktos sertifikavimo tarnybos ribose sertifikato serijos numeris.
Subjekto viešojo rakto informacija *subjectPublicKeyInfo*	P				

Sertifikato parametrai	Taikymas				Reikšmė
	P	**N**	**D**	**F**	
Algoritmas *algorithm*	P			F	SHA-1 su RSA kodavimu.
Subjekto viešasis raktas *subjectPublicKey*	P		D		Subjekto sertifikato viešasis raktas.

Lentelė Nr. 5.2 – 3-os klasės sertifikato išplėtimų sandara

Kvalifikuotas 3-os klasės Sertifikatas						
Sertifikato išplėtimų parametrai	**Taikymas**					**Reikšmė**
	P	**O**	**D**	**F**	**K**	
Sertifikavimo tarnybos rakto identifikatorius *authorityKeyIdentifier*	P		D			Nurodomi: ▪ sertifikavimo tarnybos rakto identifikatorius; ▪ sertifikavimo tarnybos sertifikato leidėjo pavadinimas ir jo sertifikato serijos numeris.
Sertifikato turėtojo rakto identifikatorius *subjectKeyIdentifier*	P		D			Sertifikato turėtojo rakto identifikatorius yra generuojamas pagal RFC 3280 reikalavimus.
Raktų paskirtis *keyUsage*	P			F	K	Nustatomi šie keyUsage bitai: ▪ digital signature, ▪ key encipherment.
Išplėstas raktų naudojimas *extendedKeyUsage*	P			F		Nustatomi šie extendedKeyUsage OID: ▪ 1.3.6.1.5.5.7.3.4 (id_kp_emailProtection), ▪ 1.3.6.1.5.5.7.3.2 (id_kp_clientAuth).
Sertifikatų taisyklės *certificatePolicies*	P			F		
Sertifikato taisyklių identifikatorius *certPolicyId*	P			F		Šių CPS identifikatorius – „1.3.6.1.4.1.22501.1.2.0“
Nuoroda į sertifikato taisykles *cPSuri*	P			F		Nuorodą į WEB resursą, iš kurio yra pasiekiamas šio CPS tekstas – „ http://www.ssc.lt/cps “
Papildomi subjektą identifikuojantis parametrai *subjectAlternativeName*		O				
Subjekto elektroninio pašto adresas *rfc822Name*		O	D			Įrašomas subjekto pateiktas paraiškoje el. pašto adresas.
Baziniai panaudojimo apribojimai	P					

Kvalifikuotas 3-os klasės Sertifikatas						
Sertifikato išplėtimų parametrai	**Taikymas**					**Reikšmė**
	P	**O**	**D**	**F**	**K**	
basicConstraints						
Sertifikato turėtojo tipas *cA*	P			F		Galutinių vartotojų sertifikatams nustatoma reikšmė „FALSE“
Sertifikavimo grandinės ilgio apribojimas *pathLengthConstraints*		O		F		Galutinių vartotojų sertifikatams reikšmė nenustatoma arba nurodoma „None“
CRL paskirstymo taškai *cRLDistributionPoints*	P					
CRL paskirstymo taško adresas *distributionPoint*	P			F		URI tipo reikšmė į WWW resursą, iš kurio galima parsisiūsti atšauktų sertifikatų sąrašą
Priėiga prie sertifikavimo tarnybos informacijos *authorityInformationAccess*	P					Pasirinktinai arba kartu nurodomi: 3) priėjimo prie CA sertifikato adresas, 4) priėjimo prie OCSP tarnybos adresas.
Priėigos OID *oID*	P			F		3) OID = 1.3.6.1.5.5.7.48.2 (CA sertifikato adreso atvėju), 4) OID = 1.3.6.1.5.5.7.48.1 (OCSP tarnybos adreso atvėju)
Priėigos adresas *uRI*	P		D			URI tipo reikšmė(-ės).
Kvalifikuoto sertifikato pareiškimas *qcStatement*	P					
qcStatement-1	P			F		*statementId* nustatoma reikšmė „0.4.0.1862.1.1“ (*id-etsi-qcs-QcCompliance*)
Sertifikato tipas Netscape suderinamai programinei įrangai *nsCertType*		O		F		Nustatomi šie nsCertType bitai: ▪ SSL Client Authentication, ▪ S/MIME.
Komentaras Netscape suderinamai programinei įrangai *netscapeComment*		O	D			„Kvalifikuotas Administratoriaus sertifikatas“

Veiksmų neatšaukiamumo (*nonRepudiation*) sertifikatų savybė yra nustatoma pagal nutylėjimą visiems kvalifikuotiems 3 klasės sertifikatams.

7.1.1. Versijos numeris (numeriai)

Galutinio Naudotojo sertifikatai turi būti X.509 trečiosios versijos sertifikatai

7.2. Sertifikato išplėtimai

SSC QCA sertifikatams suteikia išplėtimus, kurių reikalauja šių CPS 7.1.2.1-7.1.2.8 papunkčiai. Privačiųjų išplėtimų naudojimas leidžiamas, jeigu jis atitinka CA sertifikato taisykles ir šiuos CPS.

7.2.1. Key Usage ("Rakto naudojimas").

SSC QCA suteikia rakto naudojimo išplėtimą pagal šių CPS 6.1.9 punktą. Kritiškumo (angl. *criticality*) laukelis šiame išplėtime paprastai užpildomas verte „TRUE".

7.2.2. Certificate Policies („Sertifikato taisyklės")

PCA X.509 trečiosios versijos Galutinio Naudotojo sertifikatuose naudojamas sertifikato taisyklių išplėtimas. Sertifikato taisyklių išplėtime turi būti tinkamas objekto identifikatorius sertifikavimo taisyklėms (atributas „*Policy Identifier*") pagal sertifikato taisyklių 7.1.6 ir apibrėžiamaisiais žodžiais (atributas „*Qualifier*"), pateikiant nuorodą į šiuos SSC CPS (OID 1.3.6.1.4.1.22501.1.2.0 (Versija 1.0)). Kritiškumo laukelis šiame išplėtime užpildomas verte „FALSE".

7.2.3. Subject Alternative Name („Alternatyvūs vardai")

Rekomenduojama taikyti, kai reikia įtraukti elektroninio pašto adresą į Sertifikatą. Kritiškumo laukelis šiame išplėtime užpildomas verte „FALSE"

7.2.4. Basic Constrains („Pagrindiniai apribojimai")

X.509 trečiosios versijos Galutinio Naudotojo sertifikatuose taip pat naudojamas pagrindinių apribojimų išplėtimas, kurio laukelyje "Subject Type" nurodomas "End Entity". Kritiškumo laukelis šiame išplėtime užpildomas verte „FALSE"

7.2.5 Enhanced Key Usage („Išplėstas rakto naudojimas")

SSC QCA naudoja Enhanced Key Usage išplėtimą išduodamiems X.509 trečiosios versijos sertifikatams pagal lentelės Nr. 5.2, nustatymus.

7.2.6. CRL Distribution Points („CRL paskirstymo taškai")

Daugumoje SSC QCA X.509 trečiosios versijos Galutinių naudotojų sertifikatų naudojamas "*CRL Distribution Points*" išplėtimas, kuriame yra URL adresas, kuriuo Pasitikinčioji Šalis gali gauti CRL sąrašą ir pagal jį patikrinti sertifikato statusą. Kritiškumo laukelis šiame išplėtime užpildomas verte „FALSE".

7.2.7. Authority Key Identifier („Tarnybos rakto identifikatoriaus")

SSC QCA naudoja Authority Key Identifier išplėtimą X.509 trečiosios versijos Galutinio Naudotojo sertifikatuose. Kai Sertifikatą sudaranti CA naudoja *Subject Key Identifier* išplėtimą, *Authority Key Identifier* išplėtimas sudaromas iš Sertifikatą sudarančios CA 160 bitų SHA-1 viešojo rakto santraukos. Kitais atvejais, *Authority Key Identifier* išplėtime turi būti Sertifikatą sudarančios CA skiriamųjų požymių turintis pavadinimas ir serijos numeris. Kritiškumo laukelis šiame išplėtime užpildomas verte „FALSE".

7.2.8 Subject Key Identifier („Subjekto rakto identifikatorius")

Kai X.509 trečiosios versijos sertifikatuose SSC QCA naudoja S*ubject Key Identifier* išplėtimą, rakto identifikatorius generuojamas remiantis sertifikato subjekto viešuoju raktu. Kritiškumo laukelis šiame išplėtime užpildomas verte FALSE.

7.3. Algoritmo objekto identifikatoriai

SSC QCA X.509 sertifikatai pasirašomi naudojant vieną iš šių šifravimo algoritmų: "sha1WithRSAEncryption" (OID: 1.2.840.113549.1.1.5) arba "md5WithRSAEncryption" (OID: 1.2.840.113549.1.1.4) sutinkamai su RFC 3279.

7.4. Vardų (pseudonimų) formos

SSC QCA pagal šių CPS 3.1.1 punktą sertifikate naudoja Sertifikato sudarytojo ir pasirašytojo skiriamųjų požymių turintį vardą (pavadinimą), t.y. Issuer ir Subject laukus. Sertifikate visada nurodomas **pasirašytojo vardas ir pavardė arba slapyvardis.**

Be to, Galutinio Naudotojo sertifikatuose SSC QCA privalo naudoti laukelį "Organizacija", kai pasirašytojas pateikia prašymą Sertifikatą išduoti juridiniam asmeniui.

7.5. Apribojimai, taikomi vardams (pavadinimams)

Netaikoma.

7.6. Sertifikato taisyklių objekto identifikatorius

Kai naudojamas *Certificate Policies* išplėtimas, sertifikate turi būti sertifikato taisyklių, atitinkančių konkrečią sertifikato klasę pagal šių CPS 1.2. skyriaus nuostatas, objekto identifikatorius, pateikiant nuorodą į SSC Sertifikato taisykles OID 1.3.6.1.4.1.22501.1.3.0 (Versija 1.0).

7.7. Sertifikato taisyklių nustatomų apribojimų išplėtimo naudojimas

Netaikoma.

7.8. Sertifikato taisyklėse esančių apibrėžiamųjų žodžių sintaksė ir semantika

X.509 trečiosios versijos sertifikatuose SSC QCA naudoja sertifikato taisyklių apibrėžiamąjį žodį, padarydama jį "CertificatePolicies" išplėtimo dalimi. Tokiuose sertifikatuose taip pateikiama nuoroda į šiuos SSC QCA CPS, nurodant URL adresą (http://www.ssc.lt/cps).

7.9. Kritinio sertifikato taisyklių išplėtimo semantikos apdorojimas

Netaikoma.

7.10. CRL sąrašo profilis

SSC QCA sudaro CRL sąrašus, kurie atitinka RFC 3280. SSC QCA CRL sąrašuose turi būti bent jau tie pagrindiniai laukeliai ir jų turinys, kurie yra nurodyti Lentelėje Nr. 8, pateikiamoje žemiau:

Lentelė Nr. 8 – CRL profilio pagrindiniai laukeliai

Laukelis	***Vertė ar vertės apribojimas***
Version (Versija)	Žr. šių CPS 7.11. skyrių.
CRL number (CRL numeris)	Unikalus CRL sąrašo serijos numeris, vienintelis ir neklaidinantis šios sertifikavimo tarnybos infrastruktūroje.
Signature algorithm (Parašo algoritmas)	Algoritmas, naudojamas pasirašant CRL sąrašą. SSC QCA CRL sąrašai pasirašomi naudojant "sha1WithRSAEncryption" (OID: 1.2.840.113549.1.1.5)

Laukelis	*Vertė ar vertės apribojimas*
	arba "md5 WithRSAEncryption" (OID: 1.2.840.113549.1.1.4) sutinkamai su RFC 3279.
Issuer (Sudarytojas)	Subjektas, kuris pasirašė ir sudarė CRL sąrašą. CRL sąrašo sudarytojo pavadinimas turi atitikti skiriamųjų požymių turinčiam sudarytojo pavadinimui šių CPS 7.4 punkte keliamus reikalavimus.
Authority Key Identifier (Sudarytojo rakto identifikatorius)	CRL pasirašusios tarnybos privataus rakto identifikatorius.
Effective date (Sudarymo data)	CRL sąrašo sudarymo data. SSC QCA CRL sąrašai pradeda galioti nuo jų sudarymo.
Next update (Sekantis atnaujinimas)	Data, iki kurios turi būti sudarytas sekantis SSC QCA CRL sąrašas. CRL sąrašų sudarymo dažnumas turi atitikti šių CPS 4.4.9 punkto keliamus reikalavimus.
Revocation List (Galiojimo nutraukimo sarašas)	Atšauktų sertifikatų sąrašas, kuriame nurodomas atšaukto sertifikato serijos numeris ir galiojimo nutraukimo data.

SSC QCA OCSP atsakikliai atitinka RFC2560.

7.11. Versijų numeriai

SSC QCA išduoda tik CRL X.509 *2 versijos*.

SSC QCA OCSP atsakikliai įgyvendina OCSP specifikacijos, nurodytos RFC 2560 versiją 1.

7.12. CRL ir įtraukimas į CRL

Netaikomas.

8. NUOSTATŲ TVARKYMAS

8.1. CPS keitimo procedūros

Šie CPS gali būti pakeisti ar papildyti. Esminių pakeitimų atveju visiems Galutiniams naudotojams, pasirašytojams ir Pasitikinčioms šalims bus pranešta iš anksto. Pakeitimai bus daromi arba dokumentu, kuriuo pakeičiami CPS jas išdėstant nauja redakcija, arba papildant, atnaujinant. Pakeistos redakcijos ar atnaujinimai bus skelbiami: http://www.ssc.lt/cps . Atnaujinimai turės viršenybę prieš bet kokias prieštaraujančias CPS redakcijos nuostatas, į kurias daromos nuorodos.

SSC QCA pasilieka sau teisę keisti CPS nepranešdama apie pakeitimus, kurie yra neesminiai, įskaitant, bet neapsiribojant spausdinimo ar gramatinių klaidų, nuorodų, netikslumų taisymais, URL pakeitimais ir kontaktinės informacijos pakeitimais. Sprendimas laikyti pakeitimus esminiais ar neesminiais priklauso išimtinai SSC QCA nuožiūrai.

Išskyrus kaip paminėta aukščiau dėl neesminių pakeitimų, konsultacijų laikotarpis bet kokiems esminiams CPS pakeitimams yra penkiolika (15) dienų, pradedant nuo dienos, kurią pakeitimai gaunami SSC QCA Talpykloje. Bet kuris SSC QCA sertifikavimo sistemos dalyvis turi teisę pateikti pastabas SSC QCA iki konsultacijų laikotarpio pabaigos.

SSC QCA svarstys bet kokias gautas pastabas dėl siūlomų pakeitimų. SSC QCA arba (a) priima sprendimą, kad įsigaliotų SSC QCA siūlomi pakeitimai, arba (b) pakeis savo siūlomus pakeitimus ir paskelbs juos iš naujo kaip naują pakeitimą, arba (c) panaikins siūlomus pakeitimus. SSC QCA turi teisę panaikinti siūlomus pakeitimus paskelbdama viešą pranešimą. Išskyrus atvejus, kai siūlomi pakeitimai pakeičiami ar panaikinami, jie įsigalioja pasibaigus konsultacijų laikotarpiui.

8.2. Skelbimo ir pranešimų tvarka

8.2.1. CPS neskelbiami duomenys

SSC QCA ir susijusių asmenų konfidencialiais laikomi saugos dokumentai ir jie nėra atskleidžiami visuomenei/neskelbiami viešai.

8.2.2. CPS platinimas

Šie CPS skelbiami elektronine forma SSC QCA Talpykloje adresu http://www.ssc.lt/cps . CPS prieinami SSC QCA Talpykloje (Repozitoriume) Adobe Acrobat pdf formate.

8.2.3. CPS tvirtinimo procedūros

Netaikoma.

SĄVOKOS IR SANTRUMPOS

Santrumpos

Akronimas	***Sąvoka***
CA	Sertifikavimo tarnyba.
CP	Sertifikato taisyklės.
CPS	Sertifikavimo veiklos nuostatai.
CRL	Atšauktų sertifikatų sąrašas.
EAL	Įvertinimo Patikimumo lygis (angl. *Evaluation Assurance Level)*, pagal EAL4 (pagal Lietuvos standartą LST ISO/IEC 15408 "Informacijos technologija. Saugumo metodai. Informacijos technologijų saugumo įvertinimo kriterijai")
KRB	Rakto atstatymo blokas (angl. *Key Recovery Block*).
LSVA	Loginis saugos pažeidžiamumo įvertinimas.
OCSP	Sertifikatų Statuso Realiu Laiku Protokolas.
PCA	Pirminė sertifikavimo tarnyba.
PIN	Asmens identifikavimo numeris.
PKCS	Viešojo rakto kriptografinis standartas.
PKI	Viešojo rakto infrastruktūra.
PMA	Veiklos taisyklių valdymo institucija.
RA	Registravimo tarnyba.
RFC	Dokumentas, įtvirtinantis Interneto bendruomenės kuriamas taisykles.
S/MIME	Saugaus daugiatikslio interneto pašto išplėtimas (angl. *Secure multipurpose Internet mail extensions*).
SSL	Saugiosios jungties lygmens duomenų perdavimo protokolas.

Sąvokos

Sąvoka	***Apibrėžimas***
Asmuo	bet kuris fizinis ar juridinis asmuo
Administratorius	Tarnybinės stoties, OCSP atsakiklio administratroriai arba SSC QCA paslaugų centro Aukštos atsakomybės asmenys.
Administratoriaus Sertifikatas	Administratoriui išduotas Sertifikatas.
CA Talpykla	CA Sertifikatų ir kitos reikšmingos realiu laiku prieinamos CA informacijos duomenų bazė.
CA saugos politika (tvarka)	Aukščiausio lygmens dokumentas, aprašantis CA saugos tvarką
CA sertifikavimo sistemos dalyvis	Asmuo, kuris (kuri) yra vienas (viena) ar daugiau iš išvardintų CA sertifikavimo sistemos asmenų: CA, RA, Galutinis naudotojas ar Sertifikatu pasitikinčioji šalis.
Sertifikatas	elektroninis liudijimas, kuris susieja parašo tikrinimo duomenis su pasirašančiu asmeniu ir patvirtina arba leidžia nustatyti pasirašančio asmens tapatybę
Pareiškėjas	fizinis asmuo ar juridinis asmuo, kuris (kuri) prašo CA išduoti Sertifikatą.
Pasirašytojas	veiksnus fizinis asmuo, kuris turi parašo formavimo įrangą ir, veikdamas savo valia ir savo arba kito asmens, kuriam jis atstovauja, vardu, sukuria elektroninį parašą.
Parašo naudotojas	asmenys, kurie savo veikloje naudoja elektroninį parašą arba iš kitų asmenų gauna pasirašytus duomenis.
Sertifikavimo 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

Sąvoka	*Apibrėžimas*
	paslaugų teikėjų sertifikatų, pasibaigiantis paslaugų teikėjo, kuris pats sau sudaro ir pasirašo Sertifikatą, sertifikatu.
Sertifikato taisyklės (CP)	Taisyklių rinkinys, kuris nurodo sertifikato taikymą tam tikroms taikymo sritims, susijusioms bendrais saugumo reikalavimais.
Atšauktų Sertifikatų sąrašas (CRL)	Periodiškai (ar reikalui esant) išleidžiamas Sertifikatų, kurie atšaukti iki pasibaigiant jų galiojimo laikui, sąrašas, pasirašytas CA skaitmeniniu būdu. Sąrašas bendrai nurodo CRL leidėjo pavadinimą, išleidimo datą, kito planuojamo CRL datą, atšauktų Sertifikatų serijos numerius ir konkrečias galiojimo nutraukimo datas ir priežastis. CRL turi turėti laiko žymą.
Sertifikavimo tarnyba (CA)	asmuo, įgaliotas išduoti, tvarkyti, atšaukti ir atnaujinti Sertifikatus CA sertifikavimo sistemoje.
Sertifikavimo veiklos nuostatai (CPS)	Šis dokumentas, kuris nustato tvarką, kurią CA taiko patvirtindama ar atmesdama Prašymus išduoti Sertifikatą ir išduodama, tvarkydama ir atšaukdama Sertifikatus ar sustabdydama jų galiojimą.
Slaptažodžio frazė	Slapta frazė, pasirinkta Pareiškėjo registracijos dėl Sertifikato išdavimo metu. Išdavus Sertifikatą, Pareiškėjas tampa Galutiniu naudotoju ir CA ar RA gali naudoti Slaptažodžio frazę autentifikuoti Galutinį naudotoją, kai Galutinis naudotojas siekia panaikinti ar atnaujinti Galutinio naudotojo Sertifikatą.
Kompromitacija	Apsaugos tvarkos pažeidimas (ar įtariamas pažeidimas), kuriuo galėjo būti neteisėtai atskleista slapta informacija ar prarasta jos kontrolė. Privačiųjų raktų atžvilgiu, Kompromitacija yra tokio privačiojo rakto netekimas, vagystė, atskleidimas, pakeitimas, neautorizuotas panaudojimas ar kitokia tokio privačiojo rakto apsaugos kompromitacija.
Konfidenciali/privati informacija	Informacija, kuri turi būti laikoma konfidencialia ir privačia pagal šių CPS 2.8. skyriaus nuostatas.
Sutartis	sutartis, nustatanti sąlygas ir nuostatas, pagal kurias asmuo ar juridinis asmuo veikia kaip Galutinis naudotojas.
Galutinis naudotojas	fizinis asmuo, juridinis asmuo , kurie naudoja elektroninį parašą savo veikloje. Galutinis naudotojas gali ir yra įgaliotas naudoti privatųjį raktą, kuris atitinka viešąjį raktą, nurodytą Sertifikate.
Skubus auditas / tyrimas	CA atliekamas auditas ar tyrimas, kai CA turi priežastį manyti, kad CA neatitiko CA taikomų standartų, įvyko subjektui priskirtinas įvykis ar kompromitacija ar CA saugumui iškilo subjekto sukelta faktinė ar galima grėsmė.
Tarnybinės stoties ID sertifikatas	3 klasės Administratoriaus Sertifikatas, naudojamas palaikyti SSL sesijas tarp tinklo naršytojų ir tinklo tarnybinių stočių, kurie yra užkoduoti naudojant stiprią kriptografinę apsaugą, suderinamą su taikytinais eksporto įstatymais.
Infrastruktūros sertifikavimo tarnyba (Infrastruktūros CA)	CA rūšis, kuri išduoda Sertifikatus tam tikras CA paslaugas palaikantiems CA infrastruktūros komponentams. Infrastruktūros CA neišduoda CA, RA, ar Galutinių naudotojų Sertifikatų.
Intelektinės nuosavybės teisės	Teisės į vieną ar kelis iš išvardintų objektų: prekės ženklą, patentą, komercinę paslaptį ar bet kokį kitą intelektinės nuosavybės objektą.
Tarpinė sertifikavimo tarnyba (Tarpinė CA)	Sertifikavimo tarnyba, kurios Sertifikatas yra Sertifikatų sekoje tarp šakninės (pagrindinės) CA Sertifikato ir Galutinio naudotojo Sertifikatą išdavusios Sertifikavimo tarnybos Sertifikato.
Nepaneigiamumas	Komunikacijos dalis, kuri suteikia apsaugą prieš šalį, kuri nepagrįstai neigia pranešimo išsiuntimo šaltinį, neigia, kad pranešimas buvo išsiustas, arba neigia, kad pranešimas pasiekė adresatą. Išsiuntimo šaltinio neigimas apima neigimą, kad pranešimas išsiųstas iš to paties šaltinio, iš kurio išsiųsti vienas ar keli ankstesni pranešimai, net jei siuntėjo tapatybė nežinomas.
Netikrinama Galutinio naudotojo informacija	Informacija, pateikta Pareiškėjo CA ar RA ir įtraukta į Sertifikatą, kuri nebuvo patvirtinta CA ar RA ir kuriai atitinkama CA ir RA nesuteikia jokių garantijų, išskyrus garantiją, kad informaciją pateikė Pareiškėjas.

Sąvoka	*Apibrėžimas*
Sertifikatų Statuso Realiu Laiku Protokolas (OCSP)	Protokolas, skirtas realiu laiku pateikti Sertifikatu pasitikinčioms šalims informaciją apie sertifikato statusą.
Galiojimo laikotarpis	Laikotarpis, prasidedantis diena ir laiku, kai Sertifikatas išduotas (ar vėlesnę dieną ar laiku, jei nurodyta Sertifikate) ir pasibaigiantis dieną ir laiku, kai pasibaigia Sertifikato galiojimo laikas ar jis yra anksčiau atšaukiamas.
PKCS #10	Viešojo rakto kriptografinis standartas #10, nustatytas RSA Security Inc., kuris apibrėžia Prašymo pasirašyti Sertifikatą struktūrą.
PKCS #12	Viešojo rakto kriptografinis Standartas #12, nustatytas RSA Security Inc., kuris apibrėžia apsaugos priemones privačiųjų raktų perdavimui.
Pirminė sertifikavimo tarnyba (PCA)	CA, kuri veikia kaip pagrindinė CA konkrečiai Sertifikatų Klasei ir išduoda Sertifikatus CA pavaldžioms CA.
Duomenų apdorojimo centras	CA struktūrinis vienetas, kuris sukuria sąlygas saugoti, be kita ko, kriptografinius modulius, naudojamus Sertifikatų sudarymui. Klientų ir Interneto svetainės režimuose Duomenų apdorojimo centrai veikia kaip CA viduje esančios CA ir Sertifikato viso galiojimo laikotarpio metu atlieka visas Sertifikatų išdavimo, tvarkymo, galiojimo nutraukimo ir atnaujinimo paslaugas.
Viešojo rakto infrastruktūra (PKI)	Sertifikatu pagrįstos viešojo rakto kriptografinės sistemos įdiegimą ir veikimą kolektyviai palaikanti struktūra, juridinis asmuo, metodai, praktika ir procedūros. CA PKI susideda iš sistemų, kurios sąveikauja tam, kad būtų sukurta ir veiktų CA.
Registravimo tarnyba (RA)	Asmuo, įgaliotas CA aptarnauti Pareiškėjus dėl Sertifikato jiems kreipiantis dėl Sertifikato išdavimo ir tenkinti arba atmesti Prašymus išduoti Sertifikatą, atšaukti Sertifikatus ar atnaujinti Sertifikatus.
Sertifikatu pasitikinti šalis	Fizinis asmuo ar juridinis asmuo, kuris (kuri) veikia pasitikėdama Sertifikatu ir / ar skaitmeniniu parašu.
Bendrosios paslaugų sąlygos	CA naudojamos sąlygos ir terminai, išdėstantys nuostatas ir sąlygas, pagal kurias Asmuo veikia kaip Sertifikatu pasitikinčioji šalis.
RSA	Viešojo rakto kriptografinė sistema, išrasta Rivest, Shamir ir Adelman.
Slaptoji dalis	CA privačiojo rakto dalis ar aktyvacijos duomenų dalis, reikalinga naudoti CA privatųjį raktą pagal Slaptos dalies nustatymą.
Padalijimas į slaptąsias dalis	CA privačiojo rakto ar aktyvacijos duomenų padalijimo tvarka, naudotis CA privačiuoju raktu siekiant užtikrinti kelių asmenų vykdomą CA privačiojo rakto operacijų kontrolę pagal CPS 6.2.2 punktą.
Saugiosios jungties lygmuo (SSL)	Pramoninio standarto metodas, skirtas interneto komunikacijų apsaugai, sukurtas *Netscape Comunications* korporacijos. SSL saugos protokolas naudojamas Perdavimo kontrolės protokolo / Interneto protokolo ryšio duomenų kodavimui, tarnybinės stoties tapatybės nustatymui, pranešimų integralumui ir pasirinktiniam klientų tapatybės nustatymui užtikrinti.
Aukštos atsakomybės pareigas užimantis asmuo	CA darbuotojas, sutarties dalyvis ar patarėjas, atsakingas už institucijos infrastruktūrinį patikimumą, jos produktų, paslaugų, įrengimų ir / ar procesų valdymą, kaip nustatyta CPS 5.2.1 punkte.
Privatusis raktas	Elektroninio parašo formavimo duomenys.
Viešasis raktas	Elektroninio parašo tikrinimo duomenys.
Parašo formavimo įranga	Kompiuterių techninė ir (ar) programinė įranga, pritaikyta elektroniniam parašui sukurti.
Parašo tikrinimo įranga	Kompiuterių techninė ir (ar) programinė įranga, pritaikyta elektroniniam parašui tikrinti.
Biometriniai duomenys	Duomenys, išreiškiantys žmogaus individualias savybes, tokias kaip pirštų atspaudai, akies rainelė, balso tembras ir kitos, bei įgalinantys vienareikšmiškai nustatyti jo tapatybę.
Duomenų santraukų algoritmas	Algoritmas, įgalinantis įvairaus ilgio duomenis paversti fiksuoto ilgio duomenimis, t.y. padaryti duomenų santrauką, iš kurios neįmanoma atkurti

Sąvoka	***Apibrėžimas***
	pačių duomenų.
Patikima sistema	Kompiuterio techninė įranga, programinė įranga ir procedūros, kurios yra protingai apsaugotos nuo įsibrovimo ir netinkamo panaudojimo; yra protingai prieinamos, patikimos ir tinkamai veikia; yra tinkamai pritaikytos atlikti jų funkcijas ir įgyvendinti taikytiną saugos tvarką.

NUORODOS

[1] SSC Sertifikato taisyklės, Redakcija 1.0. OID: 1.3.6.1.4.1.22501.1.3.0