PATVIRTINTA
Valstybės įmonės Registrų centro
generalinio direktoriaus
2020 m. balandžio 23 d. įsakymu Nr. VE-282

REGISTRŲ CENTRO KVALIFIKUOTŲ SERTIFIKATŲ (ELEKTRONINIŲ PARAŠŲ IR ELEKTRONINIŲ SPAUDŲ) TAISYKLĖS

Unikalus objekto ID (OID): **1.3.6.1.4.1.30903.1.1.7**
Versija: 7.2
Galioja nuo: 2020-04-23

2020-04-23

TURINYS

Kvalifikuotų sertifikatų taisyklių keitimų istorija:

Versija	**Data**	**Aprašas**
0.1	2008-04-17	Projektas
1.0	2008-07-15	Pirma versija
2.0	2009-03-05	Antra versija
3.0	2010-11-24	Trečia versija
4.0	2017-01-25	Ketvirta versija
5.0	2017-04-28	Penkta versija
6.0	2017-07-11	Šešta versija
6.1	2017-11-24	Neesminiai pakeitimai.
7.0	2019-05-31	Pakeitimai po Lietuvos Respublikos ryšių reguliavimo tarnybos pastabų.
7.1	2019-12-16	Pakeitimai po Lietuvos Respublikos ryšių reguliavimo tarnybos pastabų.
7.2	2020-04-23	Pakeitimai.

Dokumento tvirtinimas:

Dokumento rengimas	**Pavardė**	**Data**	**Parašas**
Dokumentą tvirtino	Generalinis direktorius Saulius Urbanavičius	2020-04-23	

1. ĮVADAS

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

1.1. Apžvalga

Kvalifikuotų sertifikatų (elektroninių parašų ir elektroninių spaudų) taisyklės (toliau – **CP**) – tai taisyklių rinkinys, kuris atspindi patikimumo užtikrinimo paslaugų teikėjo – Registrų centro Sertifikatų centro (sertifikavimo tarnybos) – (toliau – **CA**) teikiamų kvalifikuotų elektroninių parašų ir kvalifikuotų elektroninių spaudų sertifikatų (toliau – sertifikatai) tinkamumą tam tikroms naudotojų grupėms ir taikymo sritims, turinčioms bendrus saugumo reikalavimus. Šio dokumento tikslas yra sutvirtinti pasitikėjimą CA sudaromais sertifikatais, kurie atitinka šių taisyklių reikalavimus. CP nustato patikimumo užtikrinimo paslaugų teikėjo ir sertifikatų savininkų, naudotojų ir jais pasitikinčių asmenų teises ir pareigas.

CP reikalavimai gali būti taikomi visiems pagal šias taisykles sudaromiems ir tvarkomiems sertifikatams, nepriklausomai ar jie kvalifikuoti ar ne.

CP išdėstyti reikalavimai nėra susieti su konkrečiais technologiniais sprendimais ar CA organizacine struktūra. CP reikalavimų įgyvendinimo techniniai sprendimai, procedūros ir personalo politika aprašyta Registrų centro Sertifikatų centro (toliau – RCSC) sertifikavimo veiklos nuostatuose (toliau – CPS).

CP paremtos šiais dokumentais:

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

b) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Bendrasis asmens duomenų apsaugos reglamentas) naujausia redakcija;

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

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

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

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

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

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

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

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

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

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

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

n) ETSI EN 319 412 Certificate Profiles;

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

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

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

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

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

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

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

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

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

CA sertifikatų sudarymo ir tvarkymo veikloje vykdo šias funkcijas:

a) registravimo funkcijos;

b) sertifikatų sudarymo funkcijos;

c) sertifikatų išdavimo ir informacijos apie sertifikatų naudojimą, apribojimus ir sąlygas teikimo funkcijos;

d) sertifikatų galiojimo ciklo valdymo funkcijos;

e) informacijos apie sertifikatų būseną teikimo funkcijos;

f) SSCD/QSCD parengimo ir teikimo funkcijos.

1.2. Identifikavimas

Šių CP unikalus identifikatorius (OID – Object identifier) yra:

1.3.6.1.4.1.30903.1.1.7

kurio laukų reikšmės nurodytos (*Lentelė Nr. 1*).

Lentelė Nr. 1. CP unikalaus identifikatoriaus laukų reikšmės

Pavadinimas	Reikšmė
ISO	1
ISO pripažinta organizacija	3
JAV Gynybos departamentas	6
Internetas	1
Privati įmonė	4
IANA registruota privati įmonė	1
Valstybės įmonė Registrų centras	30903
Padalinys (Registrų centro Sertifikatų centras - RCSC)	1
Dokumento tipas (sertifikatų taisyklės)	1
Dokumento versija	7

Naujausia CP versija pateikiama RCSC saugykloje (*repository*).

1.3. Sertifikatų naudotojai ir taikymo sritys

Pagal šias CP sudaromi ir tvarkomi:

a) kvalifikuoti elektroninio parašo sertifikatai, t. y. elektroninio parašo sertifikatai (elektroniniai liudijimai, kuriais elektroninio parašo patvirtinimo duomenys susiejami su fiziniu asmeniu ir kuriais patvirtinamas bent to asmens vardas ir pavardė arba slapyvardis), sudaryti pagal eIDAS ir kitus CP 1.1 d. nurodytus teisės aktus bei standartus;

b) kvalifikuoti elektroninio spaudo sertifikatai, t. y. elektroninio spaudo sertifikatai (elektroniniai liudijimai, kuriais elektroninio spaudo patvirtinimo duomenys susiejami su juridiniu asmeniu ir kuriais patvirtinamas to juridinio asmens pavadinimas), sudaryti pagal eIDAS ir kitus CP 1.1 d. nurodytus teisės aktus bei standartus;

c) kiti sertifikatai, sudaromi ir tvarkomi pagal šias CP ir kuriuose įrašomas šių CP OID.

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

Sertifikatų naudotojai:

a) abonentai;

b) sertifikatų savininkai;

c) sertifikatais pasitikinčios šalys.

Pagal šias CP elektroninio parašo sertifikatai juridiniams asmenims nėra išduodami, t. y. tik fizinis asmuo gali būti sertifikato savininkas. Spaudas gali būti išduodamas tik juridiniam asmeniui.

1.4. Organizacinė struktūra

Patikimumo užtikrinimo paslaugų teikėjo (toliau – **CSP**) funkcijas atlieka Registrų centras. CSP teikia sertifikatų sudarymo ir tvarkymo, laiko žymos kūrimo ir kitas patikimumo užtikrinimo paslaugas. Kvalifikuotų sertifikatų sudarymo ir tvarkymo paslaugas teikia CA.

CA dalį kvalifikuotų sertifikatų sudarymo ir tvarkymo funkcijų deleguoja patikimumo užtikrinimo paslaugų veiklos palaikymo (toliau – **Palaikymo tarnyba**) ir registravimo (asmenų atpažinties) tarnyboms (toliau – **RA**). RA funkcijas atlieka Registrų centro filialai ar kitos trečiosios šalys, su kuriomis sudarytos RA paslaugų teikimo sutartys.

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

1.5. Atitiktis

CA įrašydamas sudarytuose sertifikatuose unikalų identifikatorių, apibrėžtą 1.2 skyriuje, pažymi, kad sertifikatai atitinka šioms taisyklėms. Tokiu būdu CA turi prisiimti visus įsipareigojimus, apibrėžtus 2.1 skyriuje ir įgyvendinti visus 3 – 5 skyriuose nustatytus reikalavimus veiklai.

1.6. Kontaktinė informacija

CP administruoja:

Asmuo	Valstybės įmonės Registrų centro El. parašo sertifikatų skyriaus vadovas
Adresas	Lvovo g. 25-101, LT-09320 Vilnius, Lietuva
Tel.	+370 5 268 8202
URL:	http://www.registrucentras.lt
El. paštas:	*info@elektroninis.lt*

2. BENDROSIOS NUOSTATOS

Šiame skyriuje pateikiami CA ir su sertifikatų naudojimu susijusių šalių įsipareigojimai ir nuostatos teisiniais ir bendraisiais veiklos klausimais.

2.1. Įsipareigojimai

2.1.1 CA įsipareigojimai

CA turi užtikrinti, kad visi jam keliami reikalavimai, išdėstyti šio dokumento 3 – 5 skyriuose, būtų įgyvendinami.

CA turi užtikrinti vykdomų veiklos procedūrų atitikimą CP nustatytiems reikalavimams, netgi jei atskirų procedūrų vykdymas ar paslaugų teikimas yra perduotas trečiosioms šalims.

CA sertifikatų sudarymo ir tvarkymo paslaugas, turi teikti remdamasis CPS.

CA vykdydama savo funkcijas įsipareigoja:

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

b) užtikrinti informacijos išduotuosiuose kvalifikuotose sertifikatuose teisingumą;

c) užtikrinti tinkamą asmens, kuriam išduodamas sertifikatas identifikavimą;

d) užtikrinti prašymų išduoti sertifikatus priėmimą ir vykdymą:

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

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

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

f) priimti prašymus nutraukti ar sustabdyti sertifikato galiojimą:

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

g) priimti prašymus atšaukti sertifikatų galiojimo sustabdymą:

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

h) užtikrinti asmens duomenų apsaugą, reglamentuojamą Bendrojo asmens duomenų apsaugos reglamento, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo ir kitų Lietuvos Respublikos teisės aktų, tiek kiek jie neprieštarauja Bendrajam asmens duomenų apsaugos reglamentui;

i) kriptografiniams raktams generuoti ir saugoti bei su jais susietiems asmenims sudaromiems sertifikatams saugoti naudoti tik SSCD/QSCD atitinkančią eIDAS: elektroninio parašo sertifikatams – eIDAS 29 str. ir 30 str.; elektroninio spaudo sertifikatams: eIDAS 39 str. 1 d. ir 39 str.2 d.

2.1.2 RA įsipareigojimai

Registravimo tarnyba įsipareigoja:

a) atlikti asmens tapatybės nustatymą;

b) priimti prašymus sudaryti sertifikatus;

c) parengti SSCD/QSCD, sertifikatus bei juos įteikti asmenims;

d) priimti ir vykdyti prašymus nutraukti sertifikatų galiojimą;

e) priimti ir vykdyti prašymus sustabdyti sertifikatų galiojimą;

f) priimti ir vykdyti prašymus atšaukti sertifikatų galiojimo sustabdymą;

g) nutraukti bei sustabdyti RA išduotų sertifikatų galiojimą bei atšaukti sertifikatų galiojimo sustabdymą;

h) tvirtai laikytis su CA pasirašytos sutarties, veiklos delegavimo atveju, prisiimti visą atsakomybę už trečiosios šalies vykdomą veiklą.

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

a) viešai RA skelbiama informacija apie sertifikatų sudarymo sąlygas;

b) asmens, norinčio įsigyti sertifikatą identifikavimo procedūra;

c) RA personalo saugumas;

d) RA išduotų sertifikatų nutraukimo ar sustabdymo procedūra;

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

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

2.1.3 Palaikymo tarnybos įsipareigojimai

Palaikymo tarnyba įsipareigoja:

a) 7 (septynias) dienas per savaitę, 24 (dvidešimt keturias) val. per parą telefonu priimti prašymus sustabdyti sertifikatų galiojimą bei techniškai sustabdyti sertifikatų galiojimą ir teikti su patikimumo užtikrinimo paslaugų teikimo veikla susijusią informaciją.

2.1.4 Abonentų ir sertifikatų savininkų įsipareigojimai

CA, taikydama asmenų registravimo procedūras, turi užtikrinti, kad asmenys prisiimtų šiuos įsipareigojimus:

a) teikti tikslią ir pilną informaciją RA remiantis CP ir CPS reikalavimais;

b) leistų naudoti ir saugoti asmens duomenis, taip kaip tai apibrėžta CP ir CPS;

Sertifikatų savininkų įsipareigojimai:

c) naudoti viešojo ir privačiojo raktų porą tik pagal paskirtį, nurodytą sertifikate, laikantis detalizuotų apribojimų;

d) tinkamai pasirūpinti, kad kiti asmenys nepanaudotų jų privačiojo rakto ar nesužinotų aktyvavimo duomenų;

e) nedelsiant, bet ne vėliau kaip per 12 (dvylika) val. informuoti CA, jei iki sertifikatų galiojimo termino pabaigos įvyko bent vienas iš šių įvykių:

- asmens privatusis raktas buvo pamestas, pavogtas ar kitaip sukompromituotas;
- prarasta privačiojo rakto panaudojimo kontrolė aktyvavimo duomenų atskleidimo atveju;

- pastebėti sertifikatų netikslumai arba reikalingi pakeitimai jame;

f) privačiojo rakto sukompromitavimo atveju, nedelsiant ir visiškai nutraukti jo naudojimą.

2.1.5 Pasitikinčių šalių įsipareigojimai

Sertifikatais pasitikintys asmenys turi:

a) įsitikinti CA patikimumu;

b) įsitikinti, kad sertifikatai panaudoti pagal paskirtį;

c) įsitikinti sertifikatų galiojimu;

d) atlikti sertifikatų sekos patikrinimo procedūrą;

e) įsitikinti, kad naudojama programinė įranga yra pajėgi apdoroti visą sertifikatų informaciją, įskaitant ir papildomus laukus. Sertifikatais pasitikinčios šalys prieš nuspręsdamos apie sertifikatų patikimumo lygį turi būti susipažinusios su CP ir CPS. Pasitikinčios šalys turi naudoti sertifikatus tik pagal paskirtį ir žinoti draudžiamas sertifikatų naudojimo sritis.

2.2. Atsakomybė

Bendrąsias CA atsakomybės nuostatas reglamentuoja eIDAS reglamentas ir Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymas.

CA atsako už:

a) sudarytų sertifikatų duomenų tikslumą;

b) parašo formavimo duomenų ir parašo tikrinimo duomenų atitikimą;

c) tai, kad sudarytuose sertifikatuose nurodytas asmuo yra parašo formavimo duomenų, atitinkančių sertifikatuose nurodytus parašo tikrinimo duomenis, turėtojas;

d) sertifikatų galiojimo nutraukimą ar sustabdymą laiku;

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

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

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

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

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

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

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

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

2.3. Teisinės nuostatos ir interpretavimas

Elektroninio parašo kūrimą, tikrinimą, galiojimą, parašo naudotojų teises ir atsakomybę, patikimumo užtikrinimo paslaugas, įskaitant kvalifikuotų sertifikatų sudarymo ir tvarkymo paslaugas ir reikalavimus jų teikėjams, bei atsakomybę nustato eIDAS, kiti Europos Sąjungos bei nacionalinės teisės aktai, nurodyti CP 1.1 dalyje. Patikimumo užtikrinimo paslaugų teikimo sąlygos ir atsakomybės atvejai detaliai aprašomi CPS, įgyvendinančiuose šias CP.

2.4. Mokesčiai

CA gali imti mokesčius už sertifikatų sudarymo ir tvarkymo paslaugas.

CA negali reikalauti atlyginti už:

a) CRL pateikimą;

b) CP ir CPS skelbimą;

c) Sertifikatų galiojimo nutraukimą ar sustabdymą.

2.5. Informacijos teikimas ir saugyklos

CA turi palaikyti saugyklą, kuri laisvai pasiekiama viešaisiais telekomunikacijų tinklais, visą laiką be apribojimų. Saugykloje skelbiama:

a) aktualios CP ir CPS versijos;

b) CRL;

c) kita su patikimumo užtikrinimo paslaugų teikimo veikla susijusi aktuali informacija.

Informaciją apie sertifikatų statusą CA įsipareigoja teikti CRL. Be CRL, CA gali teikti OCSP atsakiklio paslaugą.

Prieš pasirašydamas sutartį, CA privalo informuoti sertifikatą sudaryti prašantį asmenį apie sertifikatų sudarymo ir tvarkymo sąlygas. Sąlygose CA privalo pateikti tokią informaciją:

a) leidžiamą sertifikatų naudojimą (naudojimo sritį, naudojimo srities apribojimus, maksimalią leidžiamos transakcijos vertę ir kitą);

b) komponentus ir procedūras, skirtas tikrinti elektroninį parašą bei jų galiojimo terminą;

c) sertifikatų savininko pareigas;

d) CA pareigas ir atsakomybę.

Sąlygose sertifikatais pasitikinčioms šalims privalo būti pateikta informacija apie:

a) leidžiamą sertifikatų panaudojimą (naudojimo sritį, naudojimo srities apribojimus, maksimalią leidžiamos transakcijos vertę ir kitą);

b) komponentus ir procedūras, skirtas tikrinti elektroninį parašą, bei jų galiojimo terminą;

c) pasitikinčių šalių pareigas.

2.6. Konfidencialumo nuostatos

a) CA privalo saugoti asmenų, prašančių sudaryti sertifikatus, duomenis laikydamasis Bendrojo asmens duomenų apsaugos reglamento bei kitų Lietuvos Respublikos teisės aktų, tiek kiek jie neprieštarauja Bendrajam asmens duomenų apsaugos reglamentui. Asmens duomenys saugomi tinkamą, reikiamą laikotarpį (CPS 4.3.2 str.) (įskaitant CA nutraukus veiklą), bet ne ilgiau nei to reikalauja duomenų tvarkymo tikslais, apie kurį asmuo, prašantis sudaryti sertifikatus yra

informuojamas, kad duomenis būtų galima panaudoti teismo procese bei taip būtų užtikrinamas veiklos tęstinumas;

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

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

2.7. Intelektinės nuosavybės teisės

CP ir jas įgyvendinantys CPS yra laisvai prieinami sertifikatų naudotojams. Naudojant šias CP ir CPS, yra būtina pateikti nuorodą į jų šaltinį.

CA netaiko nuosavybės teisių sudarytiems sertifikatams.

3. REIKALAVIMAI VEIKLAI

3.1. Veiklos nuostatai

CA veiklos procedūros, kontrolės mechanizmas ir techniniai reikalavimai infrastruktūrai yra detalizuoti CPS. CPS CA turi demonstruoti vykdomos patikimumo užtikrinimo paslaugų teikimo veiklos patikimumą:

a) turėti detaliai aprašytas veiklos taisykles ir procedūras, įgyvendinančias šių CP reikalavimus;

b) detalizuoti visų išorinių organizacijų, susijusių su patikimumo užtikrinimo paslaugų teikimo veikla, įsipareigojimus;

c) viešai publikuoti CPS ir kitą susijusią informaciją, kad būtų galima įsitikinti patikimumo užtikrinimo paslaugų veiklos atitikimu CP;

d) sertifikatų naudotojams teikti visą informaciją apie sertifikato naudojimo apribojimus ir sąlygas;

e) CA turi apibrėžti vykdomos veiklos peržiūros procedūrą ir nustatyti atsakomybę už CPS priežiūrą;

f) CA turi pateikti tinkamu laiku, tinkamos formos pranešimą apie pakeitimus, numatomus atlikti CPS, ir juos patvirtinus (punktas e) nedelsiant pateikti sertifikatų naudotojams ir pasitikinčioms šalims (punktas c).

CA valdytojas yra atsakingas, kad CA veikla atitiktų CPS.

3.2. Kriptografinių raktų gyvavimo ciklas

3.2.1 CA kriptografinių raktų generavimas

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

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

Visi asmenims sudaromų sertifikatų privatieji raktai yra generuojami aparatinėmis priemonėmis, todėl raktai yra apsaugoti nuo kopijavimo ar kitokio neteisėto panaudojimo. Elektroninio parašo sertifikatai sudaromi tik asmenims naudojantiems CA teikiamą SSCD/QSCD atitinkančią eIDAS 29 str. ir 30 str. reikalavimus. Elektroninio spaudo sertifikatams sudaryti naudojami kvalifikuoti elektroninio spaudo kūrimo įtaisai, atitinkantys eIDAS 39 str. 1 d. ir 39 str. 2 d. reikalavimus.

3.2.2 CA Kriptografinių raktų saugojimas

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

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

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

Kada CA privatieji raktai saugomi HSM, prieigos kontrolės priemonės turi užtikrinti, kad prieiga prie raktų nebūtų galima iš už HSM ribų.

3.2.3 CA privačių kriptografinių raktų atsarginių kopijų darymas ir atstatymas

CA privatieji raktai gali būti atstatomi ir jų kopijos saugomos tik naudojantis su kriptografine technine įranga susietomis sisteminėmis kortelėmis, kurių kiekvienoje saugomas fragmentas šifravimo rakto, kuriuo užšifruota CA privačiojo rakto kopija, duomenų. Privačiajam raktui atstatyti reikalingos bent 2 (dvi) iš minimaliai 4 (keturių) tokių sisteminių kortelių. Darant kopijas, saugant ir atstatant CA privatų raktą privalo dalyvauti bent 2 (du) ypatingo pasitikėjimo pareigas užimantys darbuotojai ir tai turi būti atliekama fiziškai saugioje aplinkoje.

3.2.4 CA viešųjų kriptografinių raktų skelbimas

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

3.2.5 CA raktų perdavimas trečioms šalims (*key escrow*)

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

3.2.6 CA privačiųjų kriptografinių raktų naudojimas

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

a) CA privatieji raktai naudojami asmenų sertifikatams tvirtinti bei asmenų CRL tvirtinti nebūtų naudojami jokiais kitais tikslais;

b) CA sertifikatų tvirtinimo privatieji raktai turi būti naudojami esant fiziškai saugiomis sąlygomis.

3.2.7 CA kriptografinių raktų gyvavimo ciklo pabaiga

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

3.2.8 Kriptografinės įrangos, naudojamos sertifikatams pasirašyti, gyvavimo ciklas

CA turi užtikrinti HSM saugumą viso jos gyvavimo ciklo metu.

CA turi užtikrinti, kad:

a) HSM nebuvo pažeistas iki jo pristatymo;

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

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

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

3.2.9 CA Asmenims išduotų kriptografinių raktų valdymas

CA turi užtikrinti, kad:

a) raktų poros būtų generuojamos naudojant algoritmus, atitinkančius kvalifikuoto elektroninio parašo reikalavimus;

b) generuojami raktų ilgiai būtų tinkami kvalifikuotam elektroniniam parašui;

c) elektroninio parašo raktų poros būtų generuojamos naudojant SSCD/QSCD atitinkančias eIDAS 29 str. ir 30 str. reikalavimus. Elektroninio spaudo raktų poros būtų generuojamos naudojant spaudo kūrimo įtaisus atitinkančius eIDAS 39 str. 1 d. ir 39str. .2 d. reikalavimus;

d) nebūtų daromos privataus rakto kopijos.

3.2.10 SSCD/QSCD parengimas ir perdavimas

CA turi užtikrinti saugų SSCD/QSCD parengimą ir perdavimą sertifikatų savininkams. CA turi užtikrinti, kad:

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

b) SSCD/QSCD būtų saugiai laikoma ir perduodama;

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

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

a) išduodama tik SSCD/QSCD atitinkanti eIDAS 39 str.1 d. ir 39 str. 2 d. ar eIDAS 29 str. ir , 30 str. nuostatas;

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

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

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

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

3.3. Sertifikatų valdymo ciklas

3.3.1 Sutarties sudarymas

CA turi užtikrinti, kad sertifikatus išduoti prašantys asmenys būtų tinkamai identifikuoti, t .y. turi būti tinkamai patikrinta šių asmenų tapatybė ir, jei taikytina, specifiniai jų požymiai, kaip tai reglamentuota Asmens tapatybės ir papildomų specifinių požymių tikrinimo išduodant kvalifikuotus elektroninio paraše, elektroninio spaudo, interneto svetainės tapatumo nustatymo sertifikatus tvarkos aprašo, patvirtintu Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2018 m. spalio 26 d. įsakymu Nr. 1V-1055, taip pat CA privalo užtikrinti pateiktų prašymų teisėtumą, pilnumą ir galiojimą.

RA privalo:

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

b) suteikti šią informaciją tvaria, nekintančia laike forma;

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

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

reikalauti, kad prašančiųjų sudaryti elektroninio spaudo sertifikatus **juridinių** asmenų atstovai asmeniškai pateiktų:

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

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

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

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

f) įvertinti, ar pateiktas galiojantis asmens tapatybės dokumentas;

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

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

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

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

k) dokumentuoti ir išsaugoti sudarytą sutartį, apimančią:

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

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

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

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

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

3.3.2 Sertifikatų atnaujinimas

Sertifikatų atnaujinimas, raktų pakeitimas nekeičiant sertifikatų ir sertifikatų informacijos keitimas pagal šias CP netaikomas. Pasikeitus sertifikatuose esantiems asmens duomenims ar esant kitoms aplinkybėms, tiksliai apibrėžtoms CPS, išduodami nauji sertifikatai.

3.3.3 Sertifikatų sudarymas

CA turi užtikrinti saugų sertifikatų sudarymą, leidžiantį išlaikyti autentiškus sertifikatus.

Sertifikatų sudarymo procesas ir sudaryti sertifikatai turi atitikti šiuos reikalavimus:

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

b) asmens raktų poros generavimo procedūra turi būti:

- saugiai susieta su sertifikato sudarymo procedūra;
- privatusis raktas turi būti generuojamas SSCD/QSCD;
- SSCD/QSCD turi būti saugiai perduodama sertifikatų savininkui.

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

d) būtų užtikrintas sertifikatų sudarymo duomenų konfidencialumas ir integralumas visą sertifikato gyvavimo ciklą;

e) CA turi užtikrinti, kad duomenų apsikeitimas su išorinėmis registravimo tarnybomis vyktų saugiai ir užtikrinti registravimo tarnybų patikimumą.

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

3.3.4 Informacijos apie sertifikatų sudarymo ir tvarkymo sąlygas teikimas

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

a) aiškiai nurodyti, kokios CP yra taikomos;

b) informuoti apie sertifikatų naudojimo ribojimus;

c) informuoti apie sertifikatų naudotojų įsipareigojimus;

d) teikti informaciją kaip tikrinti sertifikatų galiojimą;

e) informuoti apie CA prisiimamą atsakomybę ir jos ribojimus;

f) informuoti apie registravimo metu surinktos informacijos laikymo periodą;

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

h) informuoti apie ginčų sprendimo procedūras;

i) taikomus su veikla susijusius įstatymus.

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

3.3.5 Sertifikatų išdavimas

CA turi užtikrinti, kad:

a) po sertifikatų sudarymo, pilni ir tikslūs sertifikatai būtų perduoti jų savininkui;

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

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

CA išduotų sertifikatų sąrašų skelbimas ir sertifikatų paieška patikimumo užtikrinimo paslaugų teikimo veikloje netaikomi.

3.3.6 Sertifikatų galiojimo nutraukimas ir sustabdymas

CA užtikrina sertifikatų galiojimo nutraukimą. Gautas prašymas visais atvejais užregistruojamas sertifikatų duomenų bazėje. Sertifikatai nutraukiami, o informacija apie sertifikatų galiojimo nutraukimo statusą paskelbiama ne vėliau kaip per 24 (dvidešimt keturias) valandas po prašymo gavimo dienos. Sertifikatai netenka galios nuo jų nutraukimo momento, o nutraukimas įsigalioja nedelsiant po jo paskelbimo. Nutrauktų sertifikatų galiojimo statuso jokiomis aplinkybėmis negalima atkurti.

CA, išduodamas sertifikatus, privalo informuoti sertifikato savininką apie būdus ir komunikavimo priemones, kuriomis pasinaudojant, būtų galima nutraukti ar sustabdyti sertifikatų galiojimą.

CA nutraukia sertifikatų galiojimą:

a) abonento arba sertifikatų savininko prašymu;

b) paaiškėjus, kad sertifikatuose nurodyti duomenys nebėra teisingi;

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

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

e) sertifikatų savininkas nesilaiko sertifikatų naudojimosi sąlygų;

f) praradus sertifikatus atitinkančių parašo formavimo ar aktyvavimo duomenų kontrolę;

g) remdamasis sertifikatų galiojimo apribojimais, nurodytais sertifikatuose juos sudarant;

h) gavus pranešimą, kad sertifikatų savininkas tapo neveiksnus;

i) gavus pranešimą, kad sertifikatų savininkas mirė;

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

CA sustabdo sertifikatų galiojimą:

a) sertifikatų savininko prašymu;

b) teisėsaugos institucijų reikalavimu, siekiant užkirsti kelią nusikaltimams;

c) gavęs informacijos, kad sertifikatų duomenys yra neteisingi arba sertifikatų savininkas prarado jo sertifikatus atitinkančių parašo formavimo ar aktyvavimo duomenų kontrolę.

CA, siekdamas užtikrinti sertifikatų galiojimo nutraukimą ir sustabdymą laiku, remiantis patikrintu ir teisėtu prašymu, turi užtikrinti, kad:

a) CPS būtų nustatytos sertifikatų galiojimo nutraukimo, sustabdymo procedūros ir būtų nurodyta:

- kokiais atvejais ir kokioms aplinkybėms esant turi būti vykdomas sertifikatų galiojimo nutraukimas ir kokioms – sustabdymas;
- kas gali pateikti sertifikatų galiojimo nutraukimo ar sustabdymo prašymą;
- kaip gali būti pateiktas prašymas;
- kokie yra sertifikatų, galiojimo nutraukimo ir sustabdymo prašymo patvirtinimo reikalavimai;
- koks yra informacijos apie sertifikatus, kurių galiojimas sustabdytas ar nutrauktas skleidimo mechanizmas;

b) maksimalus laiko tarpas tarp sertifikatų galiojimo nutraukimo ir sustabdymo prašymo gavimo, iki informacijos apie sertifikatų statuso pasikeitimą pateikimo, būtų ne ilgesnis nei 1 (viena) darbo diena;

c) sertifikatų galiojimo nutraukimo ir sustabdymo prašymai būtų apdorojami nedelsiant juos gavus;

d) būtų tikrinamas sertifikatų galiojimo nutraukimo ir sustabdymo prašymų tikrumas, teisėtumas ir tai patvirtinama šias CP įgyvendinančiuose CPS nurodytais būdais;

e) Palaikymo tarnyba būtų prieinama bet kuriuo metu. Esant šios tarnybos prieinamumo sutrikimams, tiesiogiai nepriklausantiems nuo CA veiklos, CA turi imtis visų įmanomų priemonių, kad šios tarnybos neprieinamumo laikotarpis būtų ne ilgesnis nei nurodytas šias CP įgyvendinančiuose CPS;

f) kol sertifikatų galiojimo nutraukimas nėra patvirtintas, sertifikatams galėtų būti priskirtas galiojimo sustabdymo statusas, tačiau ši būsena neturėtų trukti ilgiau nei laikas, reikalingas sertifikatų statusui patvirtinti;

g) sertifikatų galiojimą sustabdžius ar nutraukus ne sertifikatų savininko prašymu, apie tai turi būti informuojamas sertifikatų savininkas.

Negalimas sertifikatų galiojimo nutraukimas ir sustabdymas atgaline data ar laiku. Sertifikatų galiojimo nutraukimas negali būti atšauktas.

3.3.7 Sertifikatų galiojimo tikrinimas

CA turi užtikrinti tokį jo sudarytų sertifikatų prieinamumą:

a) sudarius sertifikatus, visas ir tikslus sertifikatas turi būti prieinamas sertifikatų naudotojams. Informaciją apie sertifikatų statusus CA teikia:

- CRL, kuris atnaujinamas ne rečiau kaip kas 24 (dvidešimt keturias) val. CRL turi būti pasirašytas CA elektroniniu parašu, kiekviename CRL turi būti nurodytas kito CRL išleidimo laikas; arba (ir)

- OCSP atsakikliu, kuris nurodo sertifikatų statusą realiu laiku;

b) informacija aukščiau nurodytuose punktuose turi būti prieinama 24 (dvidešimt keturias) val. per parą, 7 (septynias) dienas per savaitę. Esant prieinamumo sutrikimams tiesiogiai nepriklausantiems nuo CA veiklos, CA turi imtis visų įmanomų priemonių, kad šios informacijos neprieinamumo laikotarpis būtų ne ilgesnis nei nurodytas šias CP įgyvendinančiuose CPS;

c) užtikrinti sertifikatų statuso informacijos integralumą ir autentiškumą;

d) aukščiau nurodyta informacija turi būti prieinama viešai ir tarptautiniu mastu.

3.4. CA valdymas ir veikla

3.4.1 Saugumo valdymas

CA turi užtikrinti, kad patikimumo užtikrinimo paslaugų teikimo veikloje būtų vykdomos pripažintos ir standartus atitinkančios saugumo valdymo ir administravimo procedūros.

CA privalo:

a) prisiimti visą atsakomybę už vykdomą patikimumo užtikrinimo paslaugų teikimo veiklą net jei dalis šios veiklos funkcijų yra perduodama trečiosioms šalims. CA turi tiksliai apibrėžti trečiųjų šalių atsakomybę ir įsipareigojimus bei užtikrinti, kad būtų laikomasi reikiamų veiklos ir saugumo procedūrų;

b) turėti saugumo valdymo grupę, kuri formuotų saugumo politiką ir ją skleistų CA darbuotojams;

c) palaikyti nuolatinę CA valdomos informacijos apsaugą, kiekvienas informacijos saugumo politikos pokytis turi būti derinamas su CA saugumo valdymo grupe;

d) užtikrinti, kad saugumo kontrolė ir procedūros, susijusios su CA įrenginiais, sistemomis ir informacija būtų apibrėžtos, vykdomos ir dokumentuojamos.

3.4.2 Turto inventorizacija ir valdymas

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

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

3.4.3 Personalo patikimumo kontrolė

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

a) Mokėti lietuvių kalbą;

b) Turėti reikalingą išsilavinimą arba kvalifikaciją;

c) Mokėti dirbti kompiuteriu ir kita organizacine technika;

d) Mokėti užsienio kalbą (jeigu reikalinga).

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

a) sudarantys ir tvarkantys sertifikatus turi aukštąjį išsilavinimą;

b) yra pasirašę susitarimą dėl pareigų vykdymo ir atsakomybės;

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

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

3.4.4 Biografijos tikrinimo procedūra

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

a) Asmens tapatybę patvirtinantį dokumentą;

b) Valstybinio socialinio draudimo pažymėjimą;

c) Teistumo (neteistumo) pažymą[1];

d) Išsilavinimą, profesinį parengimą patvirtinančius dokumentus;

e) Gyvenimo aprašymą;

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

f) Privalomojo sveikatos patikrinimo medicininę pažymą;

g) Neįgalaus asmens pažymėjimą, jei turi;

h) Vaiko (-ų) gimimo liudijimą (-us);

i) Santuokos ar ištuokos liudijimą.

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

3.4.5 Mokymo reikalavimai

CA darbuotojai turi būti išklausę mokymus ir susipažinę su:

a) CP ir CPS;

b) RA taisyklėmis;

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

d) CA ir RA sistemų programine įranga;

e) atsakomybe už sistemos atliekamų veiksmų sutrikimus;

f) galimais sistemos veikimo sutrikimais.

3.4.6 Fizinio saugumo kontrolė

CA turi užtikrinti fizinę kritinių CA sistemos vietų apsaugą ir minimizuoti patikimumo užtikrinimo paslaugoms naudojamo turto fizinio sunaikinimo riziką.

CA turi užtikrinti, kad:

Bendri reikalavimai

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

b) įgyvendintos priemonės leistų išvengti turto praradimo, sugadinimo ar sukompromitavimo ir veiklos pertraukimų;

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

Procedūrų, susijusių su sertifikatų generavimu, SSCD/QSCD teikimu, sertifikatų galiojimo nutraukimu ir sustabdymu fizinio saugumo valdymas:

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

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

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

3.4.7 Procedūrinio saugumo kontrolė

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

CA turi užtikrinti, kad:

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

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

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

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

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

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

3.4.8 Prieigos prie sistemų valdymas

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

CA turi užtikrinti:

Bendri reikalavimai:

a) vidinio CA kompiuterių tinklo nepasiekiamumą išoriniais tinklais;

b) svarbių duomenų apsaugą perdavimo nesaugiais tinklais metu;

c) naudotojų prieigos prie sistemos administravimą, saugumo palaikymą per naudotojų registracijos duomenų valdymą;

d) prieigos prie sistemos duomenų ir funkcijų ribojimą sutinkamai su prieigos kontrolės taisyklėmis. Turi užtikrinti itin ypatingo pasitikėjimo pareigų atskyrimą, atskiriant sistemos administravimo ir operavimo funkcijas;

e) personalo identifikavimą ir autentifikavimą prieš sertifikatų tvarkymo kritinių procedūrų atlikimą;

f) darbuotojų veiksmų su CA sistemomis apskaitą, pavyzdžiui fiksuojant ir išsaugant išrašus (*logs*) apie sistemų naudojimą;

Reikalavimai sertifikatų generavimui:

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

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

Reikalavimai sertifikatų išdavimui:

a) sertifikatų išdavimo sistemos kontrolę bandant pridėti, pašalinti ar pakeisti sertifikatus ir kitą susijusią informaciją;

Reikalavimai galiojimo nutraukimui ir sustabdymui:

a) kad būtų taikoma nuolatinio stebėjimo ir signalizavimo sistema, sudaranti sąlygas aptikti, registruoti ir laiku reaguoti į bandymus pakeisti sertifikato statusą;

Reikalavimai informacijos apie sertifikatų statusą teikimui:

a) informacijos apie sertifikatų statusą teikimo sistemos kontrolę bandant pridėti, pašalinti ar pakeisti sertifikatų statusą ir kitą susijusią informaciją ir savalaikę reakciją į tai.

3.4.9 Patikimų sistemų vystymas ir palaikymas

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

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

3.4.10 Veiklos sutrikimų ir tęstinumo valdymas

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

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

Minimalūs neatidėlioti veiksmai yra šie:

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

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

3.4.11 Patikimumo užtikrinimo paslaugų teikimo nutraukimas/ perdavimas

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

CA prieš nutraukdamas patikimumo užtikrinimo paslaugų teikimo veiklą įsipareigoja:

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

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

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

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

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

3.4.12 Įrašų kaupimas ir archyvavimas

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

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

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

Bendri reikalavimai:

a) palaikyti einamųjų ir archyvinių įrašų apie sertifikatus konfidencialumą ir integralumą;

b) užtikrinti, kad įrašai, susiję su sertifikatais, būtų archyvuojami ir saugomi, remiantis Lietuvos Respublikos dokumentų ir archyvų įstatymo naujausia redakcija;

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

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

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

f) fiksuojami įvykiai būtų saugomi taip, kad jų nebūtų galima pakeisti, ištrinti ar sunaikinti saugojimo laikotarpiu;

g) svarbūs ir išskirtiniai fiksuojami įvykiai ir duomenys turi būtų dokumentuojami;

Registracija:

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

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

- prašymuose sudaryti sertifikatą pateiktų dokumentų tipus;
- pateiktų dokumentų unikalius identifikacinius duomenis, tokius kaip numeris ir išdavimo data;
- prašymų, identifikacijai pateiktų dokumentų ir pasirašytos sutarties kopijų saugojimo vietą;
- specifinius pasirašančio asmens pasirinkimus sutartyje;
- prašymą priėmusio darbuotojo identifikacinius duomenis;
- taikomus tapatybės dokumentų patikrinimo metodus;

Sertifikatų generavimas:

a) fiksuoti visus CA valdomų raktų gyvavimo ciklo įvykius;

b) fiksuoti visus išduotų sertifikatų gyvavimo ciklo įvykius;

SSCD/QSCD parengimas ir išdavimas:

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

Sertifikato statuso keitimo valdymas:

d) fiksuoti visus įvykius, susijusius su sertifikatų statuso keitimu, įskaitant prašymus, ataskaitas ir iš to sekančius įvykius.

4. ORGANIZACINIAI KLAUSIMAI

CA turi užtikrinti savo veiklos patikimumą šiomis priemonėmis:

Bendrinės priemonės:

a) demonstruoti, kad patikimumo užtikrinimo paslaugų teikimo veikloje laikomasi CP ir CPS;

b) demonstruoti, kad CA veikia legaliai ir pagal Lietuvos Respublikos įstatymus;

c) turėti reikiamas kokybės ir informacijos valdymo sistemas;

d) turėti numatytus būdus, kaip įvykdyti įsipareigojimus, kylančius iš prisiimtos atsakomybės;

e) užtikrinti finansinį stabilumą ir turėti pakankamai kitų išteklių tinkamai įgyvendinti CP ir veikti pagal CPS;

f) įdarbinti personalą, turintį tinkamą išsilavinimą, patirties ir žinių, reikiamų patikimumo užtikrinimo paslaugų teikimo veiklai vykdyti;

g) turėti apibrėžtas procedūras skirtas spręsti su patikimumo užtikrinimo paslaugų teikimo veikla susijusiems ginčams;

h) turėti tinkamai teisiškai įformintas subrangos, samdos ir kitas sutartis.

Sertifikatų generavimas ir statuso valdymas

i) CA veikla, susijusi su sertifikatų generavimu, galiojimo sustabdymu ir nutraukimu turi būti nepriklausoma. Ypatingo pasitikėjimo pareigas užimantys darbuotojai turi būti apsaugoti nuo galimos išorinės finansinės ar komercinės įtakos, galinčios paveikti CA veiklos patikimumą;

j) Siekiant užtikrinti veiklos nešališkumą, objektyvumą ir skaidrumą, CA veikla, susijusi su sertifikatų generavimu, galiojimo sustabdymu ir nutraukimu turi būti griežtai dokumentuojama.

5. CP ADMINISTRAVIMAS

Šiame skyriuje pateikiami CP administravimo reikalavimai.

Naujai išleista CP versija panaikina ankstesnės CP versijos galiojimą. Naujos versijos galiojimo pradžia nurodyta CP dokumento viršelyje. Naujausia CP versija publikuojama saugykloje (*repository*) internete.

Naudotojai turi vadovautis CP redakcijos, kurios OID nurodytas elektroninio parašo sertifikate, vėliausiai išleista versija.

5.1. CP keitimo procedūros

CP gali būti keičiamos pastebėjus jose klaidas, iškilus reikalui jas atnaujinti arba gavus susijusių šalių pasiūlymus.

CP pakeitimai skirstomi į dvi kategorijas:

a) Esminiai pakeitimai, apie kuriuos turi būti pranešama naudotojams ir keičiamas CP OID,

b) Neesminiai pakeitimai, apie kuriuos CA neprivalo pranešti kitoms šalims, ir CP OID nėra keičiamas.

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

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

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

CP prižiūrimi, keičiami ir tvirtinami laikantis tokios procedūros:

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

b) CP pakeitimus inicijuoja CA arba sertifikatų naudotojai;

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

d) apie naują CP redakciją informuojama priežiūros įstaiga.

6. SĄVOKŲ APIBRĖŽIMAI IR SANTRUMPOS

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

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

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

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

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

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

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

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

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

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

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

Kriptografinis modulis – žiūr. Aparatinis saugumo modulis.

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

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

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

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

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

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

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

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

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

Naudotojai – sertifikatų savininkai ir sertifikatais pasitikinčios šalys.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sertifikato (el. spaudo) savininkas – juridinis asmuo kuriam (kurio vardu) sudaromas el. spaudo sertifikatas.

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

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

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

Spaudo kūrėjas – juridinis asmuo, kuris sukuria elektroninį spaudą.

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

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

CA – Sertifikavimo tarnyba (*Certification Authority)*

CP – Kvalifikuotų sertifikatų (elektroninių parašų ir elektroninių. spaudų) taisyklės *(Qualified Certificate (Electronic Signature and Electronic Seal) Policy)*

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

CSP - **Patikimumo užtikrinimo** paslaugų teikėjas (Certification Service Provider);

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

ETSI – Europos telekomunikacijų standartizavimo institutas *(European Telecommunication Standardisation Institute)*

FIPS – Jungtinių Amerikos Valstijų informacijos apdorojimo standartai *(Federal Information Processing Standards)*

LST – Lietuvos standartizacijos tarnyba;

OID – Unikalus objekto identifikatorius *(Object Identifier)*

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

QSCD – Kvalifikuotas elektroninio parašo arba elektroninio spaudo kūrimo įtaisas

PIN – Asmens identifikacinis skaičius *(Personal Identification Number)*

PKI – Viešojo rakto infrastruktūra *(Public Key Infrastructure)*

RA – Registravimo tarnyba *(Registration Authority)*

RCSC – Registrų centro Sertifikatų centras;

RSA – RSA asimetrinio šifravimo algoritmas *(Rivest-Shamir-Adleman algorithm)*;

SHA-1 – Saugus e. duomenų santraukos gavimo algoritmas 1 (*Secure Hash Algorithm 1)*;

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