RCSC KVALIFIKUOTŲ SERTIFIKATŲ IR SPAUDŲ TAISYKLĖS

Unikalus objekto ID (OID): **1.3.6.1.4.1.30903.1.1.5**
Versija: 5.0
Galioja nuo: 2017-04-28

2017-04-28

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

Dokumento tvirtinimas:

Dokumento rengimas	Pavardė	Data	Parašas
Dokumentą tvirtino	Direktoriaus pavaduotojas turto vertinimui, atliekantis direktoriaus funkcijas Arvydas Bagdonavičius	2017-04-28	

1. ĮVADAS

Valstybės įmonė Registrų centras (toliau – Registrų centras) yra įsteigta 1997 m. Įmonės steigėjas – Lietuvos Respublikos Vyriausybė. Įmonės savininko teises ir pareigas įgyvendinanti institucija yra Lietuvos Respublikos teisingumo ministerija. Įmonė tvarko Nekilnojamojo turto kadastrą ir registrą, Adresų registrą, Juridinių asmenų registrą, 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.

Registrų centras paskirtų funkcijų efektyviam vykdymui taiko modernias informacines technologijas ir teikia sertifikatų. spaudų sudarymo ir tvarkymo paslaugas, remiantis Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimo 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“ aktualios redakcijos patvirtintais reikalavimais „Reikalavimai kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams“.

1.1. Apžvalga

Kvalifikuotų sertifikatų/ spaudų taisyklės (toliau – CP) – tai taisyklių rinkinys, kuris atspindi sertifikavimo tarnybos (toliau – CA) teikiamų sertifikatų/ spaudų tinkamumą tam tikroms naudotojų grupėms ir taikymo sritims, turinčioms bendrus saugumo reikalavimus. Šio dokumento tikslas yra sutvirtinti pasitikėjimą CA sudaromais sertifikatais/ spaudais, kurie atitinka šių taisyklių reikalavimus. CP nustato sertifikavimo paslaugų teikėjo ir sertifikatų/ spaudų naudotojų 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 sertifikavimo centro (toliau – RCSC) sertifikavimo veiklos nuostatuose (toliau – CPS).

CP paremtos šiais dokumentais:

a) Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimo 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“ aktualia redakcija;

b) Lietuvos Respublikos elektroninio parašo įstatymo naujausia redakcija;

c) 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 naujausia redakcija;

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

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

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

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

h) ETSI EN 319 412 Certificate Profiles;

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

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

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

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

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

n) ETSI TS 119 312 v1.1.1 Cryptographic Suites;

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

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

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

CA sertifikatų/ spaudų sudarymo ir tvarkymo veikloje vykdo šias funkcijas:

a) registravimo funkcijos;

b) sertifikatų/ spaudų sudarymo funkcijos;

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

d) sertifikatų/ spaudų galiojimo ciklo valdymo funkcijos;

e) informacijos apie sertifikatų/ spaudų būseną teikimo funkcijos;

f) SSCD parengimo ir teikimo funkcijos.

1.2. Identifikavimas

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

1.3.6.1.4.1.30903.1.1.5

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 sertifikavimo centras - RCSC)	1
Dokumento tipas (sertifikatų taisyklės)	1
Dokumento versija	5

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

1.3. Sertifikatų/ spaudų naudotojai ir taikymo sritys

Pagal šias CP sudaromi ir tvarkomi:

a) kvalifikuoti sertifikatai, skirti kvalifikuotiems elektroniniams parašams (saugus elektroninis parašas, sukurtas saugia parašo formavimo įranga ir patvirtintas galiojančiu kvalifikuotu sertifikatu) sudaryti pagal Lietuvos Respublikos elektroninio parašo įstatymo naujausią redakciją bei kitus CP 1.1 p. nurodytus teisės aktus bei standartus;

b) kvalifikuoti spaudai, patvirtinantys, kad elektroninį dokumentą išdavė juridinis asmuo, užtikrinant dokumento kilmę ir vientisumą.

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

Sertifikatų/ spaudų naudotojai:

a) abonentai;

b) sertifikatų/ spaudų savininkai;

c) sertifikatais/ spaudais pasitikinčios šalys.

Pagal šias CP sertifikatai juridiniams asmenims nėra išduodami, t. y. tik fizinis asmuo gali būti sertifikato savininkas, tačiau spaudas gali būti išduodamas ir juridiniam asmeniui.

1.4. Organizacinė struktūra

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

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

CA išlieka atsakinga už visas teikiamas sertifikavimo paslaugas ir vykdomą sertifikavimo veiklą, tačiau trečiųjų šalių teisės, pareigos bei atsakomybė visais atvejais detalizuojama sudaromose sutartyse bei CPS, CP.

1.5. Atitiktis

CA įrašydamas sudarytuose sertifikatuose/ spauduose unikalų identifikatorių, apibrėžtą 1.2 skyriuje, pažymi, kad sertifikatai/ spaudai 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 Sertifikatų centro vadovas
Adresas	Vinco Kudirkos g. 18, LT-03105 Vilnius, Lietuva
Tel.	+370 5 2688 388
Faks.	+370 5 2688 311
URL:	http://www.registrucentras.lt
El.paštas:	*info@elektroninis.lt*

2. BENDROSIOS NUOSTATOS

Šiame skyriuje pateikiami CA ir su sertifikatų/ spaudų 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/ spaudų 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 sertifikatuose/ spauduose teisingumą;

c) užtikrinti tinkamą asmens, kuriam išduodamas sertifikatas/ spaudas identifikavimą;

d) užtikrinti prašymų išduoti sertifikatus/ spaudus priėmimą ir vykdymą:

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

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

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

f) priimti prašymus nutraukti ar sustabdyti sertifikato/ spaudo galiojimą:

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

g) priimti prašymus atšaukti sertifikato/ spaudo galiojimo sustabdymą:

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

h) užtikrinti asmens duomenų apsaugą, reglamentuojamą Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo naujausios redakcijos, kuri įgyvendina 1995 m. spalio 24 d. Europos parlamento ir Tarybos direktyvą 95/46/EB dėl asmens apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo.

i) kriptografiniams raktams generuoti ir saugoti bei su jais susietiems asmenims sudaromiems sertifikatams/ spaudams saugoti naudoti tik SSCD.

2.1.2 RA įsipareigojimai

Registravimo tarnyba įsipareigoja:

a) atlikti asmens tapatybės nustatymą;

b) priimti prašymus sudaryti sertifikatus;

c) priimti prašymus nutraukti sertifikatų galiojimą;

d) priimti prašymus sustabdyti sertifikatų galiojimą;

e) priimti prašymus atšaukti sertifikatų galiojimo sustabdymą;

f) 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.

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 sertifikato/ spaudo galiojimą ir teikti su sertifikavimo veikla susijusią informaciją.

2.1.4 Abonentų ir sertifikatų/spaudų 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/ spaudų savininkų įsipareigojimai:

c) naudoti viešojo ir privačiojo raktų porą tik pagal paskirtį, nurodytą sertifikate/ spaude, 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 sertifikato/ spaudo 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 sertifikato/ spaudo netikslumai arba reikalingi pakeitimai jame;

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

2.1.5 Pasitikinčių šalių įsipareigojimai

Sertifikatu/ spaudu pasitikintys asmenys turi:

a) įsitikinti CA patikimumu;

b) įsitikinti, kad sertifikatas/ spaudas panaudotas pagal paskirtį;

c) įsitikinti sertifikato/ spaudo galiojimu;

d) atlikti sertifikato/ spaudo sekos patikrinimo procedūrą;

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

2.2. Atsakomybė

CA atsako už:

a) sudaryto sertifikato/ spaudo duomenų tikslumą;

b) parašo formavimo duomenų ir parašo tikrinimo duomenų atitikimą;

c) tai, kad sudarytame sertifikate/ spaude nurodytas asmuo yra parašo formavimo duomenų, atitinkančių sertifikate/ spaude nurodytus parašo tikrinimo duomenis, turėtojas;

d) sertifikato/ spaudo galiojimo nutraukimą ar sustabdymą laiku.

CA prisiima atsakomybę, už sertifikatų/ spaudų 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/ spaudų 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/ spaudų naudojimo sąlygos, apribojimai bei taisyklės nurodytos sudaromoje sutartyje bei viešai skelbiamuose CPS bei CP. Atsižvelgiant į tai, CA neatsako už neteisėtus sertifikatų/ spaudų naudotojų ir kitų su CA nesusijusių šalių veiksmus bei už sertifikatų/ spaudų 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 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/ spaudų naudojimo (pvz., kai jis yra negaliojantis arba kai pažeidžiami sertifikato/ spaudo 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, sertifikavimo paslaugas, įskaitant kvalifikuotų sertifikatų/ spaudų sudarymo ir tvarkymo paslaugas ir reikalavimus jų teikėjams, bei atsakomybę nustato Lietuvos Respublikos elektroninio parašo įstatymo aktuali redakcija, Europos parlamento ir tarybos reglamento Nr. 910/2014 dėl elektroninės atpažinties ir

elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB aktuali redakcija, kiti nacionalinės bei Europos sąjungos teisės aktai. Sertifikavimo paslaugų teikimo sąlygos ir atsakomybės atvejai detaliai aprašomi CPS, įgyvendinančiuose šias CP.

2.4. Mokesčiai

CA gali imti mokesčius už sertifikatų/ spaudų sudarymo ir tvarkymo paslaugas.

CA negali reikalauti atlyginti už:

a) CRL pateikimą;

b) CP ir CPS skelbimą;

c) Sertifikato/ spaudo 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 sertifikavimo veikla susijusi aktuali informacija.

Informaciją apie sertifikato/ spaudo statusą CA įsipareigoja teikti CRL. Be CRL, CA gali teikti OCSP atsakiklio paslaugą.

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

a) leidžiamą sertifikato/ spaudo 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) sertifikato/ spaudo savininko pareigas;

d) CA pareigas ir atsakomybę.

Sąlygose sertifikatais/ spaudais pasitikinčioms šalims privalo būti pateikta informacija apie:

a) leidžiamą sertifikato/ spaudo 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/ spaudus, duomenis laikydamasis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo, kuris įgyvendina 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvą 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. 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 sertifikatą/ spaudą 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/ spaudų naudotojams. Naudojant šias CP ir CPS, yra būtina pateikti nuorodą į jų šaltinį.

CA netaiko nuosavybės teisių sudarytiems sertifikatams/ spaudams.

3. REIKALAVIMAI VEIKLAI

3.1. Veiklos nuostatai

CA veiklos procedūros, kontrolės mechanizmas ir techniniai reikalavimai infrastruktūrai yra detalizuoti CPS. CPS CA turi demonstruoti vykdomos sertifikavimo veiklos patikimumą:

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

b) detalizuoti visų išorinių organizacijų, susijusių su sertifikavimo veikla, įsipareigojimus;

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

d) sertifikatų/ spaudų naudotojams teikti visą informaciją apie sertifikato/ spaudo 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/ spaudų 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/ spaudų privatieji raktai yra generuojami aparatinėmis priemonėmis, todėl raktai yra apsaugoti nuo kopijavimo ar kitokio neteisėto panaudojimo. Sertifikatai/ spaudai sudaromi tik asmenims naudojantiem CA teikiamą SSCD type 3, kurios saugumas pagal standartą ISO/IEC 15408 gavo ne žemesnį kaip EAL 4 ar aukštesnio lygio standartą pagal ISO/IEC 15408 ar lygiaverčius nacionaliniu arba tarptautiniu mastu pripažintus IT saugumo vertinimo kriterijus; arba ISO/IEC 19790 ar FIPS PUB 140-2 3 lygio 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/ spaudų 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/ spaudams tvirtinti bei asmenų CRL tvirtinti nebūtų naudojami jokiais kitais tikslais;

b) CA sertifikatų/ spaudų 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/ spaudams 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 sertifikavimo veiklai vykdyti;

c) Sertifikatams/ spaudams, 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) raktų poros būtų generuojamos naudojant SSCD type 3, kurios saugumas pagal standartą ISO/IEC 15408 gavo ne žemesnį kaip EAL 4 ar aukštesnio lygio standartą pagal ISO/IEC 15408 ar lygiaverčius nacionaliniu arba tarptautiniu mastu pripažintus IT saugumo vertinimo kriterijus; arba ISO/IEC 19790 ar FIPS PUB 140-2 3 lygio reikalavimus;

d) nebūtų daromos privataus rakto kopijos.

3.2.10 SSCD parengimas ir perdavimas

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

a) SSCD parengimas būtų kontroliuojamas ir atliekamas saugiai;

b) SSCD būtų saugiai laikoma ir perduodama;

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

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

a) išduodama tik SSCD atitinkanti FIPS standarto 140-2 standarto trečiojo SSCD tipo (SSCD type 3), arba SSCD saugumas yra ne žemesnio kaip EAL 4 ar aukštesnio lygio standartą pagal ISO/IEC 15408 ar lygiaverčius nacionaliniu arba tarptautiniu mastu pripažintus IT saugumo vertinimo kriterijus; arba ISO/IEC 19790 ar FIPS PUB 140-2 3 lygio reikalavimus.

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

c) priskyrus SSCD asmeniui arba sugeneravus SSCD viešojo rakto sertifikatą/ spaudą, 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 perdavimo asmeniui arba SSCD perdavimo asmeniui metu;

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

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

3.3. Sertifikatų/ spaudų valdymo ciklas

3.3.1 Asmenų registracija

CA turi užtikrinti, kad sertifikatą/ spaudą išduoti prašantys asmenys būtų tinkamai identifikuoti, taip pat, privalo užtikrinti pateiktų prašymų teisėtumą, pilnumą ir galiojimą.

RA privalo:

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

b) suteikti šią informaciją tvaria, nekintančia laike forma;

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

- pasą;

- asmens tapatybės kortelę;
- leidimą gyventi.

reikalauti, kad prašančiųjų sudaryti elektroninius spaudus **juridinių** asmenų atstovai pateiktų:

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

d) pagal nacionalinės teisės aktus įsitikinti prašančiųjų sudaryti sertifikatus/ spaudus asmenų tapatybe;

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

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

g) dokumentuoti ir išsaugoti sudarytą sutartį, apimančią:

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

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

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

3.3.2 Sertifikato/ spaudo atnaujinimas

Sertifikatų/ spaudų atnaujinimas, raktų pakeitimas nekeičiant sertifikato/ spaudo ir sertifikato/ spaudo informacijos keitimas pagal šias CP netaikomas. Pasikeitus sertifikate/ spaude esantiems asmens

duomenims ar esant kitoms aplinkybėms, tiksliai apibrėžtoms CPS, išduodamas naujas sertifikatas/ spaudas.

3.3.3 Sertifikato/ spaudo sudarymas

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

Sertifikatų/ spaudų sudarymo procesas ir sudaryti sertifikatai/ spaudai turi atitikti šiuos reikalavimus:

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

b) asmens raktų poros generavimo procedūra turi būti:

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

c) sudarytame sertifikate/ spaude nurodyti asmens identifikaciniai duomenys turi būti unikalūs visų CA sudarytų sertifikatų/ spaudų apimtyje ir nepriskiriami kitam asmeniui;

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

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

Sudaryti kvalifikuoti sertifikatai/ spaudai turi atitikti Lietuvos Respublikos elektroninio parašo įstatymo naujausios redakcijos nustatytus reikalavimus elektroninio parašo kvalifikuotiems sertifikatams.

3.3.4 Informacijos apie sertifikatų/ spaudų sudarymo ir tvarkymo sąlygas teikimas

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

a) aiškiai nurodyti, kokios CP yra taikomos;

b) informuoti apie sertifikato/ spaudo naudojimo ribojimus;

c) informuoti apie sertifikato/ spaudo naudotojų įsipareigojimus;

d) teikti informaciją kaip tikrinti sertifikato/ spaudo 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 Sertifikato/ spaudo išdavimas

CA turi užtikrinti, kad:

a) po sertifikato/ spaudo sudarymo, pilnas ir tikslus sertifikatas/ spaudas būtų perduotas sertifikato/ spaudo savininkui;

b) sertifikato/ spaudo naudotojams būtų pateiktos sertifikatų/ spaudų sudarymo ir tvarkymo sąlygos ir jas būtų galima lengvai identifikuoti konkretaus sertifikato/ spaudo 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/ spaudų sąrašų skelbimas ir sertifikatų/ spaudų paieška sertifikavimo veikloje netaikomi.

3.3.6 Sertifikato/ spaudo galiojimo nutraukimas ir sustabdymas

CA užtikrina sertifikato/ spaudo galiojimo nutraukimą ne vėliau kaip per 8 (aštuonias) darbo valandas po prašymo gavimo. Gautas prašymas visais atvejais užregistruojamas sertifikatų/ spaudų duomenų bazėje ir ne vėliau kaip per 24 (dvidešimt keturias) valandas paskelbiamas. Sertifikatas/ spaudas netenka galios nuo jo nutraukimo momento, o nutraukimas įsigalioja nedelsiant po jo paskelbimo. Nutraukto sertifikato/ spaudo galiojimo statuso jokiomis aplinkybėmis negalima atkurti.

CA, išduodamas sertifikatą/ spaudą, privalo informuoti sertifikato/ spaudo savininką apie būdus ir komunikavimo priemones, kuriomis pasinaudojant, būtų galima nutraukti ar sustabdyti sertifikato/ spaudo galiojimą.

CA nutraukia sertifikato/ spaudo galiojimą:

a) abonento arba sertifikato/ spaudo savininko prašymu;

b) paaiškėjus, kad sertifikato/ spaudo duomenys nebėra teisingi;

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

d) sertifikatą/ spaudą išduodantis CA nutraukia savo veiklą ir joks kitas CA neperima sertifikavimo veiklos;

e) sertifikato/ spaudo savininkas nesilaiko sertifikato/ spaudo naudojimosi sąlygų;

f) praradus sertifikatą/ spaudą atitinkančių parašo formavimo ar aktyvavimo duomenų kontrolę;

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

h) gavus pranešimą, kad sertifikato/ spaudo savininkas tapo neveiksnus;

i) gavus pranešimą, kad sertifikato/ spaudo savininkas mirė;

Sertifikato/ spaudo galiojimas, vadovaujantis nacionaliniais teisės aktais, sustabdomas per 4 (keturias) darbo valandas po prašymo gavimo. Sertifikato/ spaudo sustabdymas visais atvejais nurodomas sertifikatų/ spaudų duomenų bazėje, o tai, kad sertifikatas/ spaudas sustabdytas, matoma teikiant informaciją apie jo statusą. Sustabdytas sertifikatas/ spaudas netenka galios jo sustabdymo laikotarpiu.

CA sustabdo sertifikato/ spaudo galiojimą:

a) sertifikato/ spaudo savininko prašymu;

b) teisėsaugos institucijų reikalavimu, siekiant užkirsti kelią nusikaltimams;

c) gavęs informacijos, kad sertifikato/ spaudo duomenys yra neteisingi arba sertifikato/ spaudo savininkas prarado jo sertifikatą/ spaudo atitinkančių parašo formavimo ar aktyvavimo duomenų kontrolę.

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

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

   - kokiais atvejais ir kokioms aplinkybėms esant turi būti vykdomas sertifikato/ spaudo galiojimo nutraukimas ir kokioms – sustabdymas;
   - kas gali pateikti sertifikato/ spaudo galiojimo nutraukimo ar sustabdymo prašymą;
   - kaip gali būti pateiktas prašymas;

- kokie yra sertifikato/ spaudo galiojimo nutraukimo ir sustabdymo prašymo patvirtinimo reikalavimai;

- koks yra informacijos apie sertifikatus/ spaudus, kurių galiojimas sustabdytas ar nutrauktas skleidimo mechanizmas;

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

c) sertifikato/ spaudo galiojimo nutraukimo ir sustabdymo prašymai būtų apdorojami nedelsiant juos gavus;

d) būtų tikrinamas sertifikatų/ spaudų 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 sertifikato/ spaudo galiojimo nutraukimas nėra patvirtintas, sertifikatui/ spaudui galėtų būti priskirtas galiojimo sustabdymo statusas, tačiau ši būsena neturėtų trukti ilgiau nei laikas, reikalingas sertifikato/ spaudo statusui patvirtinti;

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

Negalimas sertifikato/ spaudo galiojimo nutraukimas ir sustabdymas atgaline data ar laiku. Sertifikato/ spaudo galiojimo nutraukimas negali būti atšauktas.

3.3.7 Sertifikatų/ spaudų galiojimo tikrinimas

CA turi užtikrinti tokį jo sudarytų sertifikatų/ spaudų prieinamumą:

a) sudarius sertifikatą/ spaudą, visas ir tikslus sertifikatas/ spaudas turi būti prieinamas sertifikatų/ spaudų naudotojams. Informaciją apie sertifikato/ spaudo statusą 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 sertifikato/ spaudo 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/ spaudų 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 sertifikavimo veikloje būtų vykdomos pripažintos ir standartus atitinkančios saugumo valdymo ir administravimo procedūros.

CA privalo:

a) prisiimti visą atsakomybę už vykdomą sertifikavimo veiklą net jei dalis sertifikavimo 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.

3.4.3 Personalo patikimumo kontrolė

Asmenys į darbą priimami vadovaujantis Lietuvos Respublikos darbo kodekso reikalavimais. Priėmimas į darbą įforminamas darbo sutartimi. Darbo tvarkos taisyklėje (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/ spaudus 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)Išsilavinimą, profesinį parengimą patvirtinančius dokumentus;

d) Gyvenimo aprašymą;

e) Privalomojo sveikatos patikrinimo medicininę pažymą;

f) Neįgalaus asmens pažymėjimą, jei turi;

g) Vaiko (-ų) gimimo liudijimą (-us);

h) 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 sertifikavimo paslaugoms naudojamo turto fizinio sunaikinimo riziką.

CA turi užtikrinti, kad:

Bendri reikalavimai

a) fizinis patekimas į patalpas, susijusias su sertifikatų/ spaudų sudarymu, SSCD 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/ spaudų generavimu, SSCD teikimu, sertifikatų/ spaudų galiojimo nutraukimu ir sustabdymu fizinio saugumo valdymas:

a) veiklos priemonės, susijusios su sertifikatų sudarymu, SSCD teikimu ir sertifikatų/ spaudų 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/ spaudų sudarymo, SSCD teikimo ir sertifikatų/ spaudų 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, sertifikavimo paslaugų teikimo sistemą ir kitus paslaugų teikimo resursus nuo stichinių nelaimių, gaisro, elektros energijos tiekimo pertrūkių, komunikacijų tinklų veiklos sutrikimų.

3.4.7 Procedūrinio saugumo kontrolė

CA turi užtikrinti sertifikavimo 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/ spaudų 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/ spaudų tvarkymo kritinių procedūrų atlikimą;

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

Reikalavimai sertifikatų/ spaudų 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/ spaudų išdavimui:

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

Reikalavimai galiojimo nutraukimui ir sustabdymui:

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

Reikalavimai informacijos apie sertifikatų/ spaudų statusą teikimui:

a) informacijos apie sertifikatų/ spaudų statusą teikimo sistemos kontrolę bandant pridėti, pašalinti ar pakeisti sertifikatų/ spaudų 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 sertifikavimo 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/ spaudams pasirašyti, kompromitaciją, butų 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/ spaudų naudotojai, pasitikinčios pusės ir kiti asmenys, su kuriais sudaryti susitarimai ar jie yra kitaip susiję su CA veikla;

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

3.4.11 Sertifikavimo paslaugų teikimo nutraukimas/ perdavimas

CA veiklos nutraukimo atveju turi būti minimizuojami sertifikatų/ spaudų naudotojų nepatogumai, užtikrinamas sukauptų sertifikavimo veiklos duomenų, kaip įrodymų teikimo tęstinumas teisminiams procesams.

CA prieš nutraukdamas sertifikavimo paslaugų teikimo veiklą įsipareigoja:

a) apie tai informuoti visus asmenis, kurių sertifikatus/ spaudus jis sudarė ir kurių sertifikatai/ spaudai yra galiojantys, bei kitus sertifikavimo paslaugų teikėjus su kuriais yra pasirašytos laidavimo sutartys, taip pat elektroninio parašo priežiūros instituciją ne vėliau kaip prieš 1 (vieną) mėnesį;

b) jei joks kitas sertifikavimo paslaugų teikėjas neperima veiklos, ne anksčiau kaip po 1 (vieno) mėnesio nuo paskelbimo apie numatomą sertifikavimo paslaugų teikimo nutraukimą, nutraukti visų jo sudarytų sertifikatų/ spaudų galiojimą;

c) parengti susitarimą su kitu sertifikavimo paslaugų tiekėju, o tokio neradus su elektroninio parašo priežiūros institucija dėl sukauptų duomenų perėmimo, saugojimo ir teikimo pasitikinčioms šalims;

d) nutraukti visų trečiųjų šalių įgaliojimus veikti CA vardu, teikiant sertifikavimo paslaugas.

3.4.12 Įrašų kaupimas ir archyvavimas

CA privalo kaupti įrašus apie visas operacijas, susijusias su jo išduotais sertifikatais/ spaudais, su tikslu turėti tinkamos sertifikavimo 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/ spaudus konfidencialumą ir integralumą;

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

c) pateikti einamuosius ir archyvinius įrašus apie sertifikatus/ spaudus kaip tinkamos sertifikavimo veiklos įrodymus teisiniuose procesuose;

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

e) su sertifikatais/ spaudais susiję įrašai turi būtų saugomi laikotarpį, kurį CA turi pateikti sertifikavimo 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/ spaudą 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/ spaudų generavimas:

a) fiksuoti visus CA valdomų raktų gyvavimo ciklo įvykius;

b) fiksuoti visus išduotų sertifikatų/ spaudų gyvavimo ciklo įvykius;

SSCD parengimas ir išdavimas:

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

Sertifikato/ spaudo statuso keitimo valdymas:

d) fiksuoti visus įvykius, susijusius su sertifikatų/ spaudų 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 sertifikavimo 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 sertifikavimo veiklai vykdyti;

g) turėti apibrėžtas procedūras skirtas spręsti su sertifikavimo veikla susijusiems ginčams;

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

Sertifikatų/ spaudų generavimas ir statuso valdymas

i) CA veikla, susijusi su sertifikatų/ spaudų 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/ spaudų 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.

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 sertifikavimo 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/ spaudų naudotojai;

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

d) apie naują CP redakciją informuojama elektroninio parašo priežiūros institucija.

6. SĄVOKŲ APIBRĖŽIMAI IR SANTRUMPOS

Abonentas (*subscriber*) – asmuo sudarantis sutartį su CA vieno ar daugiau asmenų, kuriems sudaromas sertifikatas/ spaudas (sertifikatų/ spaudų savininkų) vardu. Abonentas gali būti kartu ir sertifikato/ spaudo 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/ spaudų sąrašas *(CRL – Certificate/ Seal Revocation List)* – sertifikavimo centro periodiškai (arba neatidėliotinai) leidžiamas, jo pasirašomas sąrašas sertifikatų/ spaudų, kurių galiojimas sustabdytas arba nutrauktas. Tokiame sąraše paprastai nurodomas jį sudariusio sertifikavimo centro vardas, sąrašo sudarymo data, numatoma kitos sąrašo versijos išleidimo data, nebegaliojančių sertifikatų/ spaudų serijiniai numeriai, galiojimo sustabdymo ar nutraukimo laikas.

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

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

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

Elektroninis parašas (parašas) – duomenys, kurie įterpiami, prijungiami ar logiškai susiejami su kitais duomenimis pastarųjų autentiškumui patvirtinti ir pasirašančiam asmeniui identifikuoti.

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

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

Kriptografinis modulis – žiūr. Aparatinis saugumo modulis.

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

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

Kvalifikuotų sertifikatų/ spaudų taisyklės *(Qualified Certificate/ Seal Policy – CP)* – sertifikato/ spaudo taisyklės, kuriose įtraukti Europos parlamento ir tarybos reglamento Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB, reikalavimai.

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

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

Naudotojai – sertifikatų/ spaudų savininkai ir sertifikatais/ spaudais pasitikinčios šalys.

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

Pasirašantis asmuo – veiksnus fizinis asmuo, kuris turi parašo formavimo įrangą (privatųjį raktą) ir sukuria elektroninį parašą.

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

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

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

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

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

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

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

Saugos taisyklės – aukščiausios svarbos dokumentas, apibrėžiantis sertifikatų/ spaudų centro saugios veiklos taisykles.

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

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

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.

Sertifikato/ spaudo taisyklės *(Certificate/ Seal Policy)* – sertifikato/ spaudo sudarymo ir naudojimo taisyklės, nustatančios sertifikatų centro, sertifikato/ spaudo savininko bei pasitikinčių šalių teises ir pareigas. Kvalifikuotų sertifikatų/ spaudų taisykles renkasi parašo naudotojai, tvirtina ir įgyvendina sertifikatų centras. Kvalifikuotų sertifikatų/ spaudų 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“.

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

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

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

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/ spaudų taisyklės *(Certificate/ Seal Policy)*

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

CSP - Sertifikavimo paslaugų teikėjas (Certification Service Provider);

CRL – Atšauktų sertifikatų/ spaudų sąrašas *(Certificate/ Seal Revocation List)*

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

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/ spaudo statusą gauti *Online Certificate/ Seal Status Protocol)*

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

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

RA – Registravimo tarnyba *(Registration Authority)*

RCSC – Registrų centro sertifikavimo centras;

RFC – "Prašome komentarų" standartizavimo tarnyba *(Request For Comments)*;

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

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

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