RCSC KVALIFIKUOTŲ SERTIFIKATŲ TAISYKLĖS

Unikalus objekto ID (OID): **1.3.6.1.4.1.30903.1.1.3**
Versija: 3.0
Galioja nuo: 2010-11-24

2010-11-24

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

Dokumento tvirtinimas:

Dokumento rengimas	Pavardė	Data	Parašas
Dokumentą tvirtino	Kęstutis Sabaliauskas	2010-11-24	

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, kuria, įgyvendina, plėtoja ir tvarko su šiais bei kitais registrais susijusias informacines sistemas, tvarko registrų archyvus. Informacija apie įmonę pateikiama interneto svetainėje adresu: http://www.registrucentras.lt.

Registrų centras paskirtų funkcijų efektyviam vykdymui taiko modernias informacines technologijas ir teikia sertifikatų sudarymo ir tvarkymo paslaugas, remiantis Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimu Nr. 2108 „Dėl reikalavimų kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams, reikalavimų elektroninio parašo įrangai, kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarkos ir elektroninio parašo priežiūros reglamento patvirtinimo“ (Žin., 2003, Nr. 2-47), patvirtintais reikalavimais „Reikalavimai kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams“.

1.1. Apžvalga

Kvalifikuotų sertifikatų taisyklės (toliau – CP) – tai taisyklių rinkinys, kuris atspindi sertifikavimo tarnybos (toliau – CA) teikiamų sertifikatų 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 sertifikavimo paslaugų teikėjo ir sertifikatų 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. nutarimu Nr. 2108 „Dėl reikalavimų kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams, reikalavimų elektroninio parašo įrangai, kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarkos ir elektroninio parašo priežiūros reglamento patvirtinimo“ (Žin., 2003, Nr. 2-47);

b) LST ETSI TS 101 456 v1.2.1 „Reikalavimai, keliami kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams";

c) RFC 2527. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. March 1999 http://www.ietf.org/rfc/rfc2529.txt;

d) Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. April 2002 http://www.ietf.org/rfc/rfc3280.txt.

CP parengtos pagal bazines LST ETSI TS 101 456 standarte pateiktas viešai platinamų kvalifikuotų sertifikatų naudojamų su saugia parašo formavimo įranga (toliau - SSCD) taisykles, kurių OID yra 0.4.0.1456.1.1.

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 parengimo ir teikimo funkcijos.

1.2. Identifikavimas

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

1.3.6.1.4.1.30903.1.1.3

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	3

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

1.3. Sertifikatų 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 įstatymą (Žin., 2000, Nr. 61-1827, Žin., 2002, Nr. 64-2572);

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

Sertifikatų naudotojai:

a) abonentai;

b) sertifikatų savininkai;

c) sertifikatais pasitikinčios šalys.

Pagal šias CP sertifikatai juridiniams asmenims nėra išduodami, t.y. tik fizinis asmuo gali būti sertifikato savininkas.

1.4. Organizacinė struktūra

CA dalį vykdomų funkcijų (apibrėžtų 1.1 skyriuje) gali perduoti trečiosioms šalims, tačiau CA išlieka pilnai atsakinga už visas teikiamas paslaugas ir vykdomą sertifikavimo veiklą.

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	Saulius Kvedaravičius, Informacinių komunikacijų skyriaus vedėjas
Adresas	V. Kudirkos g. 18, LT-03105 Vilnius, Lietuva
Tel.	+370 5 2688 268
Faks.	+370 5 2688 311
URL:	http://www.registrucentras.lt
El.paštas:	*Saulius.Kvedaravicius@registrucentras.lt*

2. BENDROSIOS NUOSTATOS

Šiame skyriuje pateikiami CA ir su sertifikatų naudojimų 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 trečioms 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 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 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 sertifikato galiojimą kaip tai numatyta CP ir CPS;

- nutraukti sertifikato galiojimą pasibaigus sertifikato galiojimo sustabdymo laikotarpiui;

g) priimti prašymus atšaukti sertifikato galiojimo sustabdymą:

- priimti ir vykdyti prašymus atšaukti sertifikato 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 Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo (Žin., 1996, Nr. 63-1479; 2008, Nr. 22-804);

i) kriptografiniams raktams generuoti ir saugoti bei su jais susietiems asmenims sudaromiems sertifikatams 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) įsipareigoja tvirtai laikytis su CA pasirašytos sutarties, veiklos delegavimo atveju, prisiimti visą atsakomybę už trečiosios šalies vykdomą veiklą.

2.1.3 Palaikymo tarnybos įsipareigojimai

Palaikymo tarnyba įsipareigoja:

a) 7 dienas per savaitę 24 val. per parą telefonu priimti prašymus sustabdyti sertifikato galiojimą ir teikti su sertifikavimo veikla susijusią informaciją;

b) įsipareigoja tvirtai laikytis su CA pasirašytos sutarties.

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;

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

e) nedelsiant informuoti CA, jei iki sertifikato 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 netikslumai arba reikalingi pakeitimai jame;

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

2.1.5 Pasitikinčių šalių įsipareigojimai

Sertifikatu pasitikintys asmenys turi:

a) įsitikinti CA patikimumu;

b) įsitikinti, kad sertifikatas panaudotas pagal paskirtį;

c) įsitikinti sertifikato galiojimu;

d) atlikti sertifikato sekos patikrinimo procedūrą, aprašytą RFC 3280;

e) įsitikinti, kad naudojama programinė įranga yra pajėgi apdoroti visą sertifikato informaciją, įskaitant ir papildomus laukus taip, kaip to reikalauja RFC 3280.

Sertifikatu pasitikinčios šalys prieš nuspręsdamos apie sertifikato patikimumo lygį turi būti susipažinusios su CP ir CPS. Pasitikinčios šalys turi naudoti sertifikatus tik pagal paskirtį ir žinoti draudžiamas sertifikato naudojimo sritis.

2.2. Atsakomybė

CA atsako už:

a) sudaryto sertifikato duomenų tikslumą;

b) parašo formavimo duomenų ir parašo tikrinimo duomenų atitikimą;

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

d) sertifikato galiojimo nutraukimą ar sustabdymą laiku;

e) tinkamą nebenaudojamų kriptografinių raktų utilizavimą.

CA prisiima atsakomybę už žalą, padarytą asmenims, kurie naudojo arba pasitikėjo sertifikatu, jei nenustatoma, kad jie nesilaikė CP ir CPS apibrėžtų procedūrų, sertifikato naudojimo ribojimų ar naudojo sertifikatą ne pagal paskirtį, apibrėžtą CP ir CPS.

CA neatsako už asmenų nuostolius, patirtus dėl sertifikato naudojimo ne pagal paskirtį, taip pat, jei nebuvo laikomasi sertifikato naudojimo apribojimų ir procedūrų apibrėžtų CP ir CPS.

2.3. Teisinės nuostatos ir interpretavimas

Elektroninio parašo kūrimą, tikrinimą, galiojimą, parašo naudotojų teises ir atsakomybę, sertifikavimo paslaugas, įskaitant kvalifikuotų sertifikatų sudarymo ir tvarkymo paslaugas ir reikalavimus jų teikėjams, bei atsakomybę nustato Lietuvos Respublikos elektroninio parašo įstatymas. Sertifikavimo 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) sertifikato 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 statusą CA įsipareigoja teikti CRL. Be CRL, CA gali teikti OCSP atsakiklio paslaugą.

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

a) leidžiamą sertifikato 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 savininko pareigas;

d) CA pareigas ir atsakomybę.

Sąlygose sertifikatais pasitikinčioms šalims privalo būti pateikta informacija apie:

a) leidžiamą sertifikato 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

CA sertifikatų savininkų duomenis, surinktus sertifikatų sudarymui, privalo tvarkyti ir saugoti pagal Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo reikalavimus.

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 sertifikavimo veiklos patikimumą:

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

b) detalizuot 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 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 turi užtikrinti, kad:

a) CA raktai būtų generuojami fiziškai saugioje aplinkoje, dalyvaujant bent 2 ypatingo pasitikėjimo pareigas užimantiems darbuotojams;

b) CA raktai būtų generuojami naudojant įrangą, atitinkančią reikalavimus:

- FIPS PUB 140-1 trečio (*Level 3*) ar aukštesnio lygmens reikalavimus; arba
- reikalavimus nustatytus CEN Workshop Agreement 14167-2; arba
- ne žemesnio kaip ketvirtojo įvertinimo užtikrinimo lygmens (*EAL 4*) pagal ISO/IEC 15408 reikalavimus;

c) CA raktų generavimo algoritmas turi būti tinkamas išduodamiems sertifikatams tvirtinti;

d) CA generuojamų raktų ilgis ir CA sertifikato tvirtinimo algoritmas turi būti tinkamas išduodamiems sertifikatams tvirtinti.

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 3.2.1 skyriaus, b) punkto 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 iš minimaliai 4 tokių sisteminių kortelių. Darant kopijas, saugant ir atstatant CA privatų raktą privalo dalyvauti bent 2 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 trečioms 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 nebebūtų 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 sertifikavimo 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) raktų poros būtų generuojamos naudojant SSCD type 3, kurios saugumas pagal standartą ISO/IEC 15408 gavo ne žemesnį kaip EAL4 įvertinimą;

d) nebūtų daromos privataus rakto kopijos.

3.2.10 SSCD parengimas ir perdavimas

CA turi užtikrinti saugų SSCD parengimą ir perdavimą sertifikatų 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.

3.3. Sertifikatų valdymo ciklas

3.3.1 Asmenų registracija

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

Tapatybės nustatymas išduodant sertifikatą reikalauja, kad sertifikatą išduoti prašantis asmuo asmeniškai atvyktų į RA ir pateiktų asmens tapatybę leidžiantį nustatyti dokumentą.

CA registravimo tarnybos privalo:

a) prieš sudarant sutartį su sudaryti sertifikatą prašančiu asmeniu, informuoti jį apie sertifikatų sudarymo ir tvarkymo sąlygas, apribojimus, CA ir sertifikato naudotojo pareigas ir atsakomybę;

b) suteikti šią informaciją tvaria, nekintančia laike forma;

c) tinkamomis ir įstatymams neprieštaraujančiomis priemonėmis įsitikinti asmens tapatybe. Tapatybės įrodymai turi būti patikrinti sulyginat juos su pateikusiu asmeniu tiesiogiai arba kitais būdais, ekvivalenčiais tiesioginiam palyginimui;

d) reikalauti, kad išduotame sertifikate mažiausiai būtų nurodyti šie asmens duomenys: asmens vardas (vardai) ir pavardė, asmens kodas. CA kiekvienam sertifikatui suteikia vieną unikalų sertifikato numerį;

e) reikalauti, kad sertifikatą išduoti prašantis asmuo pateiktų kontaktinius duomenis, kuriais patikimai galima būtų su juo susisiekti;

f) dokumentuoti ir išsaugoti visą informaciją, naudojamą asmens tapatybei nustatyti, įskaitant panaudotų dokumentų nuorodas bei dokumentų galiojimo apribojimus;

g) dokumentuoti ir išsaugoti sudarytą su sutartį, apimančią:

   - sertifikato savininko įsipareigojimus;
   - sutikimą saugoti asmens registracijos, SSCD išdavimo ir kitą informaciją bei sutikimą šią informaciją pagal CP ir CPS numatytas procedūras perduoti trečioms šalims CA veiklos nutraukimo atveju;

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

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

3.3.2 Sertifikato atnaujinimas

Sertifikatų atnaujinimas, raktų pakeitimas nekeičiant sertifikato ir sertifikato informacijos keitimas pagal šias CP netaikomas. Pasikeitus sertifikate esantiems asmens duomenims ar esant kitoms aplinkybėms, tiksliai apibrėžtoms CPS, išduodamas naujas sertifikatas.

3.3.3 Sertifikato 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 būti generuojamas SSCD;
   - SSCD turi būti saugiai perduodama sertifikato savininkui.

c) sudarytame sertifikate 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 Lietuvos Respublikos elektroninio parašo įstatymo nustatytus reikalavimus elektroninio parašo kvalifikuotiems sertifikatams.

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 sertifikato naudojimo ribojimus;

c) informuoti apie sertifikato naudotojų įsipareigojimus;

d) teikti informaciją kaip tikrinti sertifikato 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 išdavimas

CA turi užtikrinti, kad:

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

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

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

d) b) punkte įvardinta informacija turi būti viešai prieinama tarptautiniu mastu.

CA išduotų sertifikatų sąrašų skelbimas ir sertifikatų paieška sertifikavimo veikloje netaikomi.

3.3.6 Sertifikato galiojimo nutraukimas ir sustabdymas

CA turi užtikrinti, kad sertifikatų galiojimo nutraukimas ir sustabdymas būtų vykdomi neatidėliotinai ir tik gavus įgaliotų asmenų tinkamai pateiktus prašymus.

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

Sertifikato galiojimo nutraukimo ir sustabdymo laikas turi būti fiksuojamas. Sertifikato galiojimo nutraukimas ir sustabdymas įsigalioja nuo to momento, kai galiojimo nutraukimo ar sustabdymo prašymas užregistruojamas reikiamoje duomenų bazėje.

CA nutraukia sertifikato galiojimą:

a) abonento arba sertifikato savininko prašymu;

b) paaiškėjus, kad sertifikato duomenys nebėra teisingi;

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

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

e) sertifikato savininkas nesilaiko sertifikato naudojimosi sąlygų;

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

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

h) gavus pranešimą, kad sertifikato savininkas tapo neveiksnus;

i) gavęs pranešimą, kad sertifikato savininkas mirė;

CA sustabdo sertifikato galiojimą:

a) sertifikato savininko prašymu;

b) teisėsaugos institucijų reikalavimu, siekiant užkirsti kelią nusikaltimams;

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

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

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

c) sertifikato 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 sertifikato galiojimo nutraukimas nėra patvirtintas, sertifikatui galėtų būti priskirtas galiojimo sustabdymo statusas, tačiau ši būsena neturėtų trukti ilgiau nei laikas, reikalingas sertifikato statusui patvirtinti;

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

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

3.3.7 Sertifikatų galiojimo tikrinimas

CA turi užtikrinti tokį jo sudarytų sertifikatų prieinamumą:

a) sudarius sertifikatą, visas ir tikslus sertifikatas turi būti prieinamas sertifikatų naudotojams. Informaciją apie sertifikato statusą CA teikia:

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

   - OCSP atsakikliu, kuris nurodo sertifikato statusą realiu laiku;

b) informacija aukščiau nurodytuose punktuose turi būti prieinama 24 val. per parą, 7 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 sertifikavimo veikloje būtų vykdomos pripažintos ir standartus atitinkančios saugumo valdymo ir administravimo procedūros.

CA privalo:

a) periodiškai atlikti rizikos analizę, kad nustatyti saugumo reikalavimus ir apibrėžti veiklos procedūras;

b) 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;

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

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

e) 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 pagal rizikos analizės rezultatus suklasifikuoti turto saugos reikalavimus.

3.4.3 Personalo patikimumo kontrolė

Dirbti CA turi būti priimami asmenys, turintys reikiamų žinių, įgūdžių bei patirties, reikalingos sertifikavimo veiklos funkcijoms vykdyti.

CA turi užtikrinti, kad:

Bendri reikalavimai

a) CA personalas turėtų aukštąjį išsilavinimą, reikalingų žinių, patirties bei kvalifikaciją, būtiną siūlomoms paslaugoms teikti ir atitinkančią darbo funkcijas;

b) saugumo užtikrinimo pareigos ir atsakomybės, nurodytos CA saugumo politikoje, būtų dokumentuotos pareigybių aprašymuose. Ypatingo pasitikėjimo pareigybės, nuo kurių tiesiogiai priklauso CA veikla ir saugumas, būtų tiksliai ir aiškiai apibrėžtos ir dokumentuotos;

c) CA personalas (tiek laikinas, tiek nuolatinis) turėtų pareigybių aprašymus, kurie būtų parengti atsižvelgiant į pareigų atskyrimą, nustatant pareigybės jautrumą priklausomai nuo pareigų ir prieigos lygio. Pareigybių aprašymuose turėtų būti nurodyti reikalavimai įgūdžiams ir patirčiai;

d) personalo vykdomos administracinės ir valdymo procedūros bei procesai atitiktų CA informacijos saugumo valdymo procedūras;

Reikalavimai su sertifikatų sudarymu ir tvarkymu susijusioms pareigoms

e) vadybinėms pareigoms priimami darbuotojai turėtų patirtį elektroninio parašo technologijų srityje ir būtų susipažinę su saugumo procedūromis bei turėtų patirties informacijos saugumo ir rizikos valdyme;

f) CA personalas, užimantis ypatingo pasitikėjimo pareigas, nebūtų paveikiamas bet kokių interesų konfliktų, galinčių paveikti CA operacijų objektyvumą;

g) asmenis ypatingo pasitikėjimo pareigoms skiria CA už saugumą atsakingas vadovas. Ypatingo pasitikėjimo pareigos apima:

- saugumo pareigūnus – bendra atsakomybė už saugumo politikos vykdymą;
- sistemos administratorius – įgalioti instaliuoti, konfigūruoti ir palaikyti CA sistemas naudojamas sertifikatų sudarymui ir tvarkymui;
- sistemos operatorius – atsakingi už kasdieninį CA sistemų naudojimą. Įgalioti atlikti sistemos atsargines kopijas bei atkūrimą;
- sistemos auditorius – įgalioti peržiūrėti CA sistemų archyvus bei audito įrašus.

CA neturi įdarbinti asmenų, kuriais nebūtų galima pasitikėti dėl teistumo ar kitokių kaltinimų nusikalstama veikla.

3.4.4 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 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 generavimu, SSCD teikimu, sertifikatų galiojimo nutraukimu ir sustabdymu fizinio suaugumo valdymas

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

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

f) būtų įgyvendintos fizinės ir kitokios apsaugos priemonės, apsaugančios patalpas, sertifikavimo paslaugų teikimo sistemą ir kitus paslaugų teikimo resursus nuo stichinių nelaimių, gaisro, elektros energijos tiekimo pertrūkių, komunikacijų tinklų veiklos sutrikimų;

3.4.5 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 minimizuojama;

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

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

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

f) CA saugumo procedūros būtų atskirtos nuo kitų procedūrų. Saugumo procedūros apima: veiklos procedūrų ir atsakomybių nustatymą, saugų sistemų plėtros planavimą, apsaugą nuo žalingų programų, patalpų priežiūrą, tinklo valdymą, aktyvią audito žurnalų stebėseną, įvykių analizę,

informacijos nešiklių valdymą ir apsaugą, duomenų ir programinės įrangos apsikeitimą. Šios operacijos turi būti valdomos ypatingo pasitikėjimo pareigas užimančio personalo, tačiau jas atlikti gali ir žemesnės kvalifikacijos specialistai jei tai aprašyta saugumo politikos ar kituose dokumentuose.

3.4.6 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 iš išsaugant išrašus (*logs*) apie sistemų naudojimą;

Reikalavimai sertifikatų generavimui

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

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

Reikalavimai sertifikatų išdavimui

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

Reikalavimai galiojimo nutraukimui ir sustabdymui

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

Reikalavimai informacijos apie sertifikatų statusą teikimui

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

3.4.7 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.

3.4.8 Veiklos sutrikimų ir tęstinumo valdymas

CA turi užtikrinti, kad gedimų atveju, įskaitant CA privačiojo rakto, skirto sertifikatams pasirašyti, kompromitaciją, bus 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 yra kitaip susiję su CA veikla;

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

3.4.9 Sertifikavimo paslaugų teikimo nutraukimas arba perdavimas

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

CA nutraukdamas sertifikatų sudarymo paslaugų teikimą turi atlikti šiuos veiksmus:

a) informuoti visus sertifikatų naudotojus ir kitus susijusius sertifikavimo paslaugų teikėjus;

b) nutraukti visų trečiųjų šalių įgaliojimus veikti CA vardu, teikiant sertifikavimo paslaugas;

c) perduoti įsipareigojimus kitiems asmenims saugoti ir teikti informaciją apie CA sudarytų sertifikatų statusą ir kitą archyvinę informaciją;

d) nutraukti savo privačiųjų raktų naudojimą ir juos sunaikinti.

CA savo CPS turi numatyti priemones, kurių imtųsi veiklos nutraukimo atveju. CPS turi būti detalizuota:

a) būdai, kuriais informuojami susiję asmenys;

b) įsipareigojimų perdavimas;

c) informacijos apie sertifikatų statusą teikimo funkcijų perdavimą.

3.4.10 Įrašų kaupimas ir archyvavimas

CA privalo kaupti įrašus apie visas operacijas, susijusias su jo išduotais sertifikatais, 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 patikrinti 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 įstatymu (Žin., 1995, Nr. 107-2389; 2004, Nr.57-1982);

c) pateikti einamuosius ir archyvinius įrašus apie sertifikatus 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 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 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 parengimas ir išdavimas

c) fiksuoti visus įvykius, susijusius su SSCD 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 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 spręsti su sertifikavimo 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) CA veikla, susijusi su sertifikatų generavimu, galiojimo sustabdymu ir nutraukim turi būti griežtai dokumentuojama, kad užtikrinti veiklos nešališkumą, objektyvumą ir skaidrumą.

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 atevejais, 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 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 elektroninio parašo priežiūros institucija.

6. SĄVOKŲ APIBRĖŽIMAI IR SANTRUMPOS

Abonentas (*subscriber*) – asmuo sudarantis sutartį su CA vieno ar daugiau asmenų, kuriems sudaromas 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 Revocation List)* – sertifikavimo centro periodiškai (arba neatidėliotinai) leidžiamas, jo pasirašomas sąrašas sertifikatų, 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 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.

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.

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 taisyklės *(CP - Qualified Certificate Policy)* – sertifikato taisyklės, kuriose įtraukti Europos Parlamento ir Tarybos direktyvos 1999/93/EB „Dėl Bendrijos elektroninių parašų reguliavimo sistemos" I ir II priedo 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.

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 savininkų pasirašytus duomenis ir sertifikatus bei siekiančios įsitikinti sertifikatų savininkų tapatybe bei kita sertifikatuose 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 ir kitos RCSC informacijos duomenų bazė, naudotojams prieinama tiesiogiai (*on-line*) bet kuriuo metu internete adresu www.rcsc.lt/repository/.

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 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.

Sertifikatų naudotojai – sertifikatų savininkai ir sertifikatais pasitikinčios šalys.

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 taisyklės *(Certificate Policy)* – sertifikato sudarymo ir naudojimo taisyklės, 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“.

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.

Sertifikavimo veiklos nuostatai *(CPS – Certification Practice Statement)* – kvalifikuotus sertifikatus 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 taisyklės *(Certificate Policy)*

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

CSP - Sertifikavimo paslaugų teikėjas (Certification Service Provider);

CRL – Atšauktų sertifikatų sąrašas *(Certificate 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 statusą gauti *Online Certificate 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)*