RCSC LAIKO ŽYMOS TEIKIMO VEIKLOS NUOSTATAI

Unikalus objekto ID (OID): **1.3.6.1.4.1.30903.1.4.1**
Versija: 1.0
Galioja nuo: 2008-10-28

2008-10-28

TURINYS

RCSC laiko žymos teikimo veiklos nuostatų keitimų istorija:

Versija	Data	Aprašas
0.1	2008-06-19	Nuostatų projekto versija
1.0	2008-10-28	Pirma versija

Dokumento tvirtinimas:

Dokumento rengimas	Pavardė	Data	Parašas
Dokumentą rengė	Jonas Kupinas Mindaugas Aputis	2008-06-25	
Dokumentą tikrino	Ieva Tarailienė Saulius Kvedaravičius	2008-10-27	
Dokumentą tvirtino	Rimantas Ramanauskas	2008-10-28	

1. ĮVADAS

Valstybės įmonė „Registrų centras" (toliau – Registrų centras) įsteigta 1997 m. Teisingumo ministerija atlieka šios įmonės savininko pareigas. 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, registrų archyvus. Informaciją apie įmonę galima rasti internete adresu http://www.registrucentras.lt.

Registrų centras paskirtų funkcijų efektyviam vykdymui naudoja modernias informacines technologijas. Registrų centras yra įsteigęs Registrų centro sertifikavimo centrą (toliau – RCSC) – kvalifikuotų sertifikatų sudarymo ir laiko žymų teikimo paslaugų padalinį.

Šie laiko žymos teikimo veiklos nuostatai (toliau – TSPS) apibrėžia RCSC techninius, procedūrinius ir personalo politikos klausimus susijusius su laiko žymos sudarymo ir tvarkymo paslaugų teikimu.

TSPS atitinka Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2003 m. sausio 29 d. įsakymu Nr. T-10 patvirtintą Laiko žymos formavimo paslaugų teikimo tvarką.

1.1. Apžvalga

Šie TSPS detaliai apibrėžia RCSC veiklą teikiant laiko žymos sudarymo ir tvarkymo paslaugas, reikalingas užtikrinti kvalifikuotų elektroninių parašų ilgalaikį galiojimą.

TSPS apibrėžiami reikalavimai, formuojant vienos sekundės tikslumo laiko žymas, patvirtintas viešojo rakto sertifikatais.

TSPS struktūra atitinka šių dokumentų rekomendacijas:

a) LST ETSI TS 102 023 „Strateginiai reikalavimai, keliami laiko žymėjimo paslaugų teikėjams" standarto;

b) LST ETSI TS 101 861 „Laiko žymos profilis" standarto;

c) RFC 3628;

d) Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2003 sausio 29 d. įsakymo (Nr. T-10) „Dėl laiko žymos formavimo paslaugų teikimo tvarkos patvirtinimo".

1.2. Identifikavimas

Šie TSPS yra patvirtinti VĮ Registrų centras direktoriaus 2008 m. spalio 28 d. įsakymu Nr. v-245

TSPS talpinami saugykloje (repository) internete.

Unikalus TSPS identifikatorius (OID): **1.3.6.1.4.1.30903.1.4.1**.

Šiame identifikatoriuje taškais atskirtų skaičių reikšmės nurodytos žemiau (*Lentelė Nr. 1*)

Lentelė Nr. 1. TSPS 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 (laiko žymos teikimo veiklos nuostatai)	4
Dokumento versija	1

Šie TSPS parengti pagal laiko žymos teikimo taisykles (toliau – TSP), kurių unikalus OID yra **1.3.6.1.4.1.30903.1.3.1**.

1.3. Laiko žymų naudotojai ir taikymo sritys

1.3.1 Laiko žymų naudotojai

Laiko žymos skirtos elektroninių parašų naudotojams, siekiantiems įrodyti, kad elektroninis parašas buvo sukurtas iki žymoje nurodyto laiko. Laiko žymų paslaugų teikėjas gali teikti viešąsias paslaugas, taip pat, jis gali aptarnauti ir uždarąsias vartotojų grupes.

1.3.2 Laiko žymų taikymo sritys

Pagrindinė RCSC teikiamų laiko žymų taikymo sritis – teikti laiko žymų paslaugą saugiems elektroniniams parašams, sukurtiems saugia parašo formavimo įranga ir patvirtintiems kvalifikuotais sertifikatais. Tačiau, RCSC nenustato jokių laiko žymų naudojimo apribojimų. RCSC teikiamos laiko žymos gali būti naudojamos vykdant elektronines transakcijas, elektroninių dokumentų archyvavime ir kt.

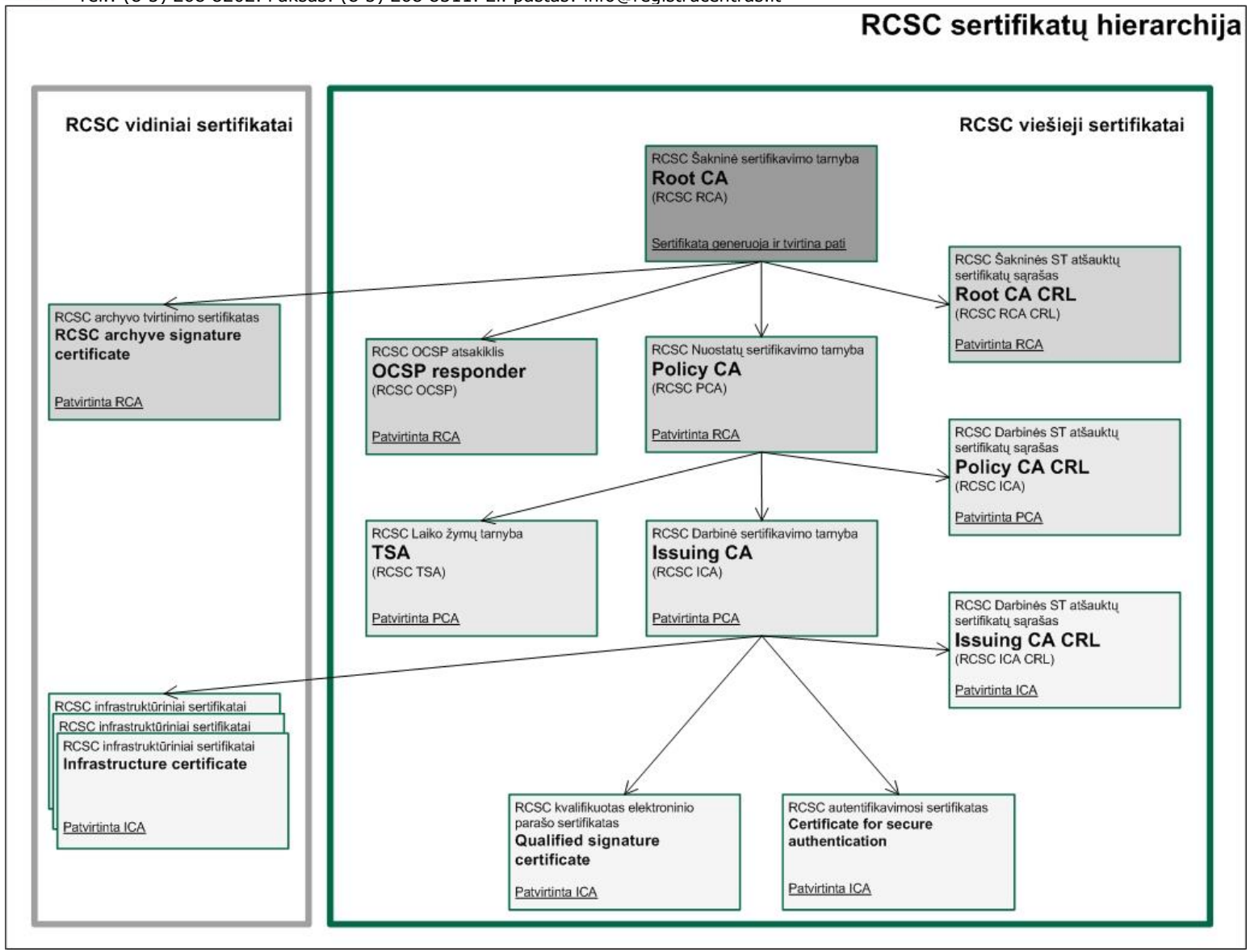
1.4. RCSC organizacinė struktūra

RCSC sudaro VĮ Registrų Centras patalpose įsikūrusi sertifikavimo tarnyba (toliau – CA), laiko žymų teikimo tarnyba (toliau – TSA) bei pagal sutartį su CA veikiančios ir CA pavaldžios sertifikavimo veiklos palaikymo (toliau – Palaikymo tarnyba) ir registravimo tarnybos (toliau – RA).

1.5. CA ir TSA sertifikatų seka

CA sertifikatų seka paremta 3 lygių CA struktūra. Pirmojo lygio šakninė CA naudos save pasirašantį sertifikatą (*self-signed certificate*), išduos sertifikatus nuostatų CA, OCSP pranešimų tvirtinimui, šakninio CA CRL tvirtinimui, archyvų tvirtinimui bei bus atjungta nuo tinklo (off-line) ir saugoma izoliuotoje aplinkoje. Nuostatų CA išduos sertifikatus darbinei CA, nuostatų CA CRL tvirtinimui ir TSA. Nuostatų CA taip pat laikoma atjungta nuo tinklo ir saugoma izoliuotoje aplinkoje. Darbinė CA išduos sertifikatus asmenims, darbinės CA CRL tvirtinimui ir infrastruktūros sertifikatus.

žemiau pateikiama CA sertifikatų sekos schema (*Pav. 1*).



Pav. 1. RCSC sertifikatų hierarchija

1.6. Kontaktinė informacija

1.6.1 Nuostatus išleidusi ir tvarkanti organizacija

Organizacija	Valstybės įmonė Registrų centras
Adresas	V. Kudirkos g. 18, LT-03105 Vilnius, Lietuva
Telefonas	+370 5 268 8202
Faksas	+370 5 268 8311
URL:	http://www.registrucentras.lt
El.paštas:	info@registrucentras.lt

1.6.2 Kontaktinis asmuo

Už TSPS atitikimą TSP ir TSPS administravimą atsakingas asmuo:

Saulius Kvedaravičius,

Valstybės įmonės Registrų centras informacinių komunikacijų skyriaus vedėjas,

V. Kudirkos g. 18, LT-03105 Vilnius, Lietuva,

Tel.: +370 5 2688 268,

Faks.: +370 5 2688 311,

E-paštas: *Saulius.Kvedaravicius@registrucentras.lt*.

2. BENDROSIOS NUOSTATOS

Šiame skyriuje pateikiami TSA ir su ja susijusių šalių įsipareigojimai, teisinės ir bendrosios veiklos nuostatos.

2.1. Įsipareigojimai

2.1.1 TSA įsipareigojimai

TSA turi teikti visas laiko žymos paslaugas laikydamasis šių TSPS ir užtikrinti TSPS atitikimą įgyvendinamoms TSP.

TSA turi laikytis laiko žymų teikimo sąlygose ir sutartyse su savo abonentais prisiimtų laiko žymos paslaugų teikimo įsipareigojimų, įskaitant teikiamų paslaugų prieinamumą, tinkamumą ir tikslumą.

TSA turi užtikrinti atliekamų procedūrų ir paslaugų atitikimą TSPS reikalavimams, netgi jei procedūras ar paslaugas atlieka TSA subrangovai.

TSA turi užtikrinti visų papildomų įsipareigojimų, tiesiogiai ar per nuorodas nurodytų laiko žymoje, įgyvendinimą.

TSA turi užtikrinti ne mažesnio nei 1 sekundės tikslumo TSA laikrodžių, naudojamų laiko žymoms formuoti, sinchronizaciją su UTC laiku.

TSA įsipareigoja skelbti naujausias TSPS ir TSP versijas saugykloje (*repository*) internete.

2.1.2 Laiko žymų abonentų įsipareigojimai

Gavę laiko žymą, abonentai turi patikrinti, ar paslaugų teikėjas ją pasirašė teisingai ir ar parašą atitinkantis sertifikatas pasirašymo metu buvo galiojantis.

Abonentai privalo atsižvelgti į laiko žymos naudojimo apribojimus ir atsargumo priemones, nurodytas TSP, TSPS, laiko žymos teikimo sąlygose, sutartyse su paslaugų teikėju arba kitur.

Abonento pareigos ir atsakomybė nustatomi abonento ir paslaugų teikėjo sudarytoje sutartyje.

2.1.3 Laiko žymomis pasitikinčių asmenų įsipareigojimai

TSA laiko žymos teikimo sąlygose, kurios turi būti laisvai prieinamos visoms susijusioms šalims, turi įtraukti įsipareigojimus laiko žymomis pasitikintiems asmenims, kurie pasitikėdami laiko žyma privalo:

a) įsitikinti, kad laiko žyma buvo teisingai pasirašyta, kad parašą atitinkantis sertifikatas pasirašymo metu buvo galiojantis bei, kad laiko žymos pasirašymui panaudotas privatus kriptografinis raktas (toliau – raktas) nebuvo sukompromituotas iki laiko žymos teisingumo patikrinimo;

b) atsižvelgti į TSP, TSPS, laiko žymos teikimo sąlygose, sutartyse su paslaugų teikėju arba kitur nurodytus laiko žymos taikymo apribojimus;

c) atsižvelgti į bet kurias kitas sutartyse ar kitur nurodytas atsargumo priemones.

Jei laiko žymos tikrinimo metu TSA sertifikato galiojimas yra pasibaigęs, asmuo turi įsitikinti:

a) ar TSA privatus raktas nebuvo sukompromituotas iki laiko žymos išdavimo;

b) ar tikrinimo metu TSA laiko žymai formuoti panaudoti duomenų santraukos (*hash*) algoritmai neturi jokių kolizijų;

c) ar tikrinimo metu TSA parašo algoritmas ir parašo rakto ilgis, kuriuo pasirašyti laiko žymos duomenys, vis dar yra technologiškai patikimi ir nepasiekiami kriptografinėmis atakomis.

2.2. Atsakomybė

TSA atsako už neteisėtus veiksmus ir padarytą žalą abonentams atlygina Lietuvos Respublikos įstatymų nustatyta tvarka.

TSA gali atsisakyti arba apriboti bet kokią atsakomybę, susijusią su laiko žymų teikimu, jeigu tai neprieštarauja galiojantiems įstatymams. Atsakomybės apribojimai nurodomi laiko žymų teikimo sąlygose.

2.3. Teisinės nuostatos ir interpretavimas

2.3.1 Pagrindiniai teisės aktai

Laiko žymų formavimą, teikimą, reikalavimus jų teikėjams bei atsakomybę, nustato:

a) Lietuvos Respublikos elektroninio parašo įstatymas (Žin., 2000, Nr. 61-1827; Žin., 2002, Nr. 64-2572);

b) Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2003 sausio 29 d. įsakymas (Nr. T-10) „Dėl laiko žymos formavimo paslaugų teikimo tvarkos patvirtinimo".

2.3.2 Ginčų sprendimo tvarka

Bet kurie ginčai tarp TSA ir galinių vartotojų sprendžiami geranoriškomis derybomis. Ginčo neišsprendus, kreipiamasi į Lietuvos teisėsaugos institucijas.

2.4. Mokesčiai

2.4.1 Laiko žymų teikimo mokestis

Laiko žymų teikimo įkainiai skelbiami Internete, adresu:

http://www.rcsc.lt/ikainiai.

2.4.2 TSP ir TSPS teikimo mokestis

TSP ir TSPS teikiami nemokamai. Internete jie laisvai prieinami adresu:

http://www.rcsc.lt/repository.

2.5. Informacijos teikimas ir saugyklos

2.5.1 TSA teikiama informacija

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

a) aktualios TSP ir TSPS versijos;

b) TSA atšauktų sertifikatų sąrašai (toliau – CRL);

c) kita su laiko žymos paslaugų teikimu susijusi aktuali informacija.

Informaciją apie TSA sertifikatų statusą TSA įsipareigoja teikti ir OCSP protokolu.

2.5.2 Teikiamos informacijos atnaujinimo dažnumas

TSA teikiama informacija atnaujinama tokiu laiku ar dažnumu:

a) TSP ir TSPS pakeitimai daromi kaip numatyta TSP ir TSPS;

b) TSA priklausančių sertifikatų duomenys, atlikus pakeitimus juose, skelbiami viešai nedelsiant;

c) kita skelbtina ir atnaujinta informacija skelbiama ją gavus.

2.6. Atitikties tikrinimas

TSA veiklos atitiktis TSP ir TSPS tikrinama TSA nustatyta vidaus tvarka.

2.6.1 TSA veiklos tikrinimo dažnumas

TSA veiklos atitiktis TSP ir TSPS turi būti tikrinama ne rečiau kaip kas vieneri metai.

2.6.2 Tikrintojai ir jų kvalifikacija

Išorinė tikrinimo organizacija turi būti nepriklausoma nuo TSA. Tikrinančioji organizacija turi turėti darbuotojus, išmanančius viešųjų raktų infrastruktūrą (toliau – PKI), informacinių technologijų saugumą ir turėti PKI arba su informacinių technologijų saugumu susijusių sričių tikrinimų patirtį.

Vidinį tikrinimą atlieka Registrų centro informacinių technologijų saugumo ir tvarkymo struktūros.

2.6.3 Tikrinamieji dalykai

TSA veiklai įvertinti yra tikrinama:

a) fizinis saugumas;

b) laiko žymų teikimo paslaugos ir jų teikimo galiniams vartotojams procedūros;

c) programinės įrangos ir sistemos prieigos kompiuterių tinklu saugumas;

d) TSA personalo patikimumas;

e) TSA sistemos operacijų ir veiklos registravimo žurnalai;

f) informacijos atsarginių kopijų darymas ir naudojimas;

g) archyvų tvarkymo procedūros;

h) įrašai apie TSA struktūros keitimus;

i) įrašai apie aparatinės ir programinės įrangos tikrinimą ir priežiūrą.

2.6.4 Veiksmai pastebėjus trūkumus

Vidinio ir išorinio tikrinimo protokolai įteikiami TSA saugumo pareigūnui. Per 30 kalendorinių dienų saugumo pareigūnas turi raštu parengti savo nuomonę dėl protokole išdėstytų trūkumų, numatyti veiksmus ir terminus trūkumams pašalinti. Informacija apie trūkumų pašalinimą pateikiama tikrinusiai organizacijai.

Jei pastebėti trūkumai kelia pavojų laiko žymų paslaugų teikimo procedūrų saugumui, saugumo pareigūnas gali priimti sprendimą laikinai sustabdyti TSA paslaugų teikimą. Tokiu atveju visi laiko žymų abonentai informuojami apie tai ir jiems pranešama apie numatomą veiklos atnaujinimo laiką.

2.6.5 Tikrinimo rezultatų skelbimas

TSA veiklos nepriklausomo tikrinimo išvados talpinamos TSA saugykloje ir skelbiamos viešai.

2.7. Intelektinės nuosavybės teisės

Naudojant TSP ar TSPS būtina pateikti nuorodą į šaltinį.

3. REIKALAVIMAI VEIKLAI

Šiame skyriuje dėstomi reikalavimai TSA veiklai teikiant laiko žymų sudarymo ir tvarkymo paslaugas.

3.1. Laiko žymų teikimo sąlygų skelbimas

TSA turi paskelbti visiems abonentams laiko žymos paslaugų teikimo sąlygas, įskaitant:

a) kontaktinę TSA informaciją;

b) TSP unikalų identifikatorių (OID);

c) duomenų, kuriems teikiama laiko žyma, bent vieną santraukos (*hash*) formavimo algoritmą;

d) parašo, naudojamo patvirtinti laiko žymai, tikėtiną gyvavimo trukmę;

e) laiko žymos tikslumą lyginant su UTC;

f) laiko žymos paslaugų naudojimo apribojimus;

g) abonentų įsipareigojimus;

h) laiko žymomis pasitikinčiųjų pusių įsipareigojimus;

i) informaciją kaip patikrinti laiko žymą;

j) laikotarpį, kurio metu TSA kaupia ir saugo įrašus apie įvykius;

k) taikomą šalies teisę;

l) atsakomybės apribojimus;

m) ginčų ir nesutarimų sprendimo tvarką;

n) ar buvo įvertintas TSA atitikimas šioms taisyklėms, ir kokia nepriklausoma institucija tai atliko.

Ši informacija turi būti prieinama įprastomis komunikacijos priemonėmis nekintančia laike forma, suprantama kalba, bei gali būti pateikta elektronine forma.

3.2. TSA kriptografinių raktų gyvavimo ciklas

3.2.1 TSA kriptografinių raktų generavimas

TSA raktų pora 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. TSA privatusis raktas turi būti generuojamas fiziškai saugiose sąlygose, esant bent dviejų asmenų, kuriems priskirtos ypatingo pasitikėjimo pareigos, kontrolei.

Raktų poros 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 (auditą) ir bendrąją sistemos peržiūrą.

3.2.2 TSA privačiojo rakto apsauga

TSA skaitmeniniam parašui, kuriuo pasirašomos laiko žymos, formuoti naudojamas aparatinis saugumo modulis (kriptografinis modulis) atitinka FIPS PUB 140-2 standarto trečiojo saugumo lygio (*Level3*) reikalavimus.

3.2.3 TSA viešojo rakto skelbimas

TSA viešasis raktas yra skelbiamas TSA sertifikate, OCSP atsakiklio pranešimuose ir oficialiame RCSC tinklapyje.

3.2.4 TSA privačiojo rakto atstatymas

TSA privatusis raktas atstatomas naudojant su kriptografine įranga susietomis sisteminėmis kortelėmis, kurių kiekvienoje saugoma dalis kriptografinio rakto, kuriuo užšifruota TSA privataus rakto kopija. TSA privačiųjų raktų atstatymo procedūra analogiška TSA raktų generavimo procedūrai (3.2.1 punktas).

3.2.5 Privačiojo rakto įvedimas į kriptografinį modulį

TSA privačiojo rakto įvedimo ir išvedimo į kriptografinį modulį procedūros taikomos tik privačiojo rakto atstatymo ir atsarginės kopijos darymo atvejais.

3.2.6 TSA kriptografinių raktų keitimas

TSA sertifikato galiojimas negali būti ilgesnis už TSA raktų poros galiojimo laikotarpį. TSA raktų keitimas išlaikant tą patį sertifikatą netaikomas.

3.2.7 TSA kriptografinių raktų poros gyvavimo ciklo pabaiga

Pasibaigus TSA raktų poros gyvavimo laikotarpiui, TSA turi užtikrinti, kad privatusis raktas būtų sunaikinamas, nebūtų daromos jo kopijos.

3.2.8 TSA kriptografinio modulio gyvavimo ciklas

TSA turi užtikrinti kriptografinės įrangos (kriptografinio modulio) saugumą viso jos gyvavimo ciklo metu. TSA turi užtikrinti:

a) kad laiko žymas pasirašantis kriptografinis modulis nebuvo sugadintas pristatymo (transportavimo) metu;

b) kad laiko žymas pasirašantis kriptografinis modulis nebuvo sugadintas saugojimo metu;

c) kad laiko žymas pasirašantis kriptografinis modulis tinkamai funkcionuoja;

d) kad laiko žymas pasirašančiame kriptografiniame modulyje esantys privatūs raktai bus ištrinti pasibaigus kriptografinio modulio gyvavimo ciklui.

3.3. Laiko žymų teikimas

3.3.1 Laiko žyma

Išduodamą laiko žymą TSA ją pasirašo savo skaitmeniniu parašu. Privatusis TSA raktas naudojamas tik išduodamoms laiko žymoms pasirašyti ir nenaudojamas jokiems kitiems tikslams.

Laiko žymoje daugiau parašų nenaudojama. RCSC TSA sertifikato identifikatorius yra įtrauktas kaip atributas pasirašančiame sertifikate. Jei nustatyta, kad TSA sisteminis laikrodis yra nukrypęs nuo deklaruojamo tikslumo, HSM automatiškai nustoja formuoti ir išduoti laiko žymas.

Laiko žymą sudaro:

a) laiko žyma tvirtinamų duomenų, kuriuos pateikė abonentas, santrauka (*hash*);

b) unikalus serijinis numeris, kuris naudojamas laiko žymų užsakymui ir identifikavimui;

c) TSP unikalus identifikatorius;

d) TSA identifikatorius, kurio reikšmė yra tokia pati kaip viena iš RCSC TSA sertifikato *subject* lauko reikšmių, naudojamų laiko žymai patikrinti;

e) iš pasirenkamų laukų tiktai *nonce* laukas yra palaikomas;

f) TSA sisteminio laiko vertės susietos su nors vienos UTC laboratorijos laiko verte.

Lauko pavadinimas	Reikšmė ir reikšmių ribos
Version	1
PolicyID	**1.3.6.1.4.1.30903.1.3.1**
messageImprint	Lauko reikšmė yra tokia pati kaip lauko, esančio laiko žymos užklausoje (*TimeStampReq)*, jei duomenų santraukos (*hash*) dydis atitinka duomenų santraukos formavimo algoritmo, nurodyto *hashAlgorithm* lauke, numatytą dydį.
serialNumber	Laiko žymų naudotojai turi palaikyti sveikuosius iki 160 bitų ilgio skaičius.
genTime	UTC laikas
Accuracy	1s
ordering	FALSE
nonce	Privalomas, jei toks laukas buvo laiko žymos užklausoje (*TimeStampReq).* Lauko reikšmė tokia pati kaip ir laiko žymos užklausoje (*TimeStampReq)*.
TSA	CN = VI Registru Centras RCSC (TSA) O = VI Registru Centras - I.k. 124110246 C = LT

3.3.2 Sinchronizacija su UTC

TSA užtikrina, kad jos naudojamas laikas yra 1 s. tikslumu sinchronizuotas su UTC. TSA tam pasiekti užtikrina:

a) TSA naudojamų sisteminių laikrodžių kalibravimą taip, kad nenukryptų nuo apsibrėžto tikslumo;

b) laikrodžių apsaugą nuo grėsmių, galinčių sukelti neaptinkamus laiko vertės pasikeitimus ne kalibravimo metu;

c) skirtumo tarp TSA laikrodžių ir UTC fiksavimą. Laikas skaičiuojamas laikantis BIPM ir NTP rekomendacijų; ir

d) laikrodžių sinchronizacijos palaikymą kai vykdoma korekcinės sekundės laiko korekcija gavus informacijos iš atsakingos institucijos. Du kartus per metus, per paskutinę birželio 30-osios ir gruodžio 31-osios dienos minutę, sureguliavimas yra atliekamas automatiškai, siekiant užtikrinti, kad iki sekančio planinio reguliavimo suminis skirtumas tarp UTC ir UT1 neviršytų 0,9 s. Turi būti formuojamas ir saugomas įrašas apie tikslų korekcijos vykdymo laiką.

3.4. Įrašų apie TSA operacijas kaupimas

3.4.1 Registruojamieji įvykiai

Svarbiausios TSA sistemos operacijos fiksuojamos saugiame operacijų žurnale. Fiksuojamos operacijos apima:

a) įvykius, susijusius su TSA valdomų kriptografinių raktų ir sertifikatų gyvavimo ciklu;

b) įvykius susijusius su TSA sisteminių laikrodžių kalibravimu ir sinchronizavimu;

c) užklausas laiko žymai sudaryti;

d) laiko žymos sudarymo faktus;

e) laiko žymų tarnybos sustabdymą ir paleidimą.

Kiekviename įraše turi būti ši informacija:

a) įvykio tipas;

b) įvykio identifikatorius;

c) įvykio data ir laikas;

d) identifikatorius arba kiti duomenys, įgalinantys nustatyti atsakingąjį už įvykį asmenį;

e) sprendimas, ar įvykis yra sietinas su sėkmingai ar klaidingai atlikta operacija.

Operacijų žurnalas apsaugomas prieigos valdymo sistema ir pasirašomas infrastruktūriniu RCSC parašu.

Be operacijų žurnalo, vedami ir TSA sistemos veiklos registravimo žurnalai, kurių pagalba galima stebėti sistemos darbą, gauti informaciją apie sistemos veiklos sutrikimus ir klaidas.

Diagnostikos žurnale fiksuojami detalūs sistemos veiksmai, kurie naudojami sistemos veikimo analizei, diagnostikai ir sutrikimų šalinimui. Pagrindiniai diagnostikos žurnalo naudotojai – sistemos kūrėjai ir administratoriai. Galima valdyti diagnostikos žurnalo įrašų detalumą, gaunant labiau detalią, arba mažiau detalią informaciją apie tam tikrus sistemos veiksmus.

Klaidų žurnalas (*Error Log*) fiksuojama informacija apie sistemos sutrikimus ir klaidas, nurodant sutrikimo laiką, šaltinį ir aprašymą.

Sistemos stebėsena gali būti atliekama ir standartinėmis programinėmis priemonėmis.

Formuojant įrašus apie sistemos veiklą įtraukiama ši informacija:

a) sistemos ugniasienių ir apsaugos nuo įsilaužimų sistemos (IDS) perspėjimai;

b) kiekvieno aparatinės ir programinės įrangos keitimo duomenys;

c) kompiuterių tinklo ir jo ryšių keitimo duomenys;

d) darbuotojų fizinio patekimo į saugias zonas ir pažeidimų duomenys;

e) slaptažodžių, PIN kodų ir darbuotojų pareigų keitimo duomenys;

f) sėkmingi ir nesėkmingi kreipiniai į TSA duomenų bazes ir serverių taikomąsias programas;

g) atsarginių kopijų, archyvinių įrašų, duomenų bazių kūrimo istorija.

3.4.2 Įrašų apie įvykius peržiūros dažnumas

TSA sistemos operacijų ir veiklos registravimo žurnalai peržiūrimi ne rečiau kaip kartą per mėnesį. Kiekvienas didesnės svarbos įvykis ar įvykis, atsitikęs dėl netinkamo sistemos funkcionavimo, turi būti aprašytas.

3.4.3 Įrašų saugojimo periodas

TSA sistemos operacijų ir veiklos registravimo žurnalai TSA saugomi 10 metų, tolesnį saugojimą reglamentuoja Lietuvos Respublikos dokumentų ir archyvų įstatymas.

3.4.4 Įrašų apsauga

TSA sistemos operacijų ir veiklos registravimo žurnalų atsarginės kopijos daromos kiekvieną savaitę. Viršijus konkrečiam žurnalui numatytą įrašų kiekį, žurnalo turinys perkeliamas į archyvą. Į archyvą rašomi duomenys užšifruojami naudojant AES algoritmą. Šifravimo raktą tvarko TSA saugumo pareigūnas.

TSA sistemos operacijų ir veiklos registravimo žurnalus peržiūrėti gali tik TSA saugumo pareigūnas, TSA administratorius ar auditorius. Kreipinio į žurnalą parametrai yra tokie, kad:

a) tik saugumo pareigūnas galėtų rašyti į archyvą arba ištrinti žurnalo failus;

b) būtų galimybė nustatyti bet kokį duomenų iškraipymo pažeidimą;

c) niekas neturėtų teisės pakeisti žurnalo turinio.

3.4.5 Įrašų rinkimo sistema

TSA naudoja vidinę įvykių įrašų registravimo sistemą. Kur galima, įrašai daromi automatiškai.

3.5. Duomenų archyvavimas

3.5.1 Į archyvą atiduodami duomenys

Į archyvą atiduodami šie duomenys:

a) TSA sistemos operacijų ir veiklos registravimo žurnalai;

b) laiko žymos abonentų duomenų bazė;

c) TSA priklausančių raktų ir sertifikatų istorija nuo jų sugeneravimo iki sunaikinimo.

3.5.2 Duomenų saugojimo archyve periodas

Elektroninės formos ar popieriuje užrašyti duomenys archyve saugomi 10 metų, tolesnį saugojimą reglamentuoja Lietuvos Respublikos dokumentų ir archyvų įstatymas.

3.5.3 Archyvo apsauga

TSA archyvas saugomas laikantis Registrų centro numatytos vidinės tvarkos ir Lietuvos Respublikos dokumentų ir archyvų įstatymo.

3.5.4 Archyvo atsarginių kopijų darymas

Atsarginės kopijos įgalina atstatyti sistemos darbą po sutrikimų. Tuo tikslu daromos tokios programinės įrangos ir duomenų failų kopijos:

a) instaliacinis diskas su TSA sistemos programine įranga;

b) instaliacinis diskas su TSA taikomosiomis programomis;

c) WWW serverio ir saugyklos instaliaciniai diskai;

d) saugyklos (*repository*) duomenų kopija.

Duomenų bazių atsarginės kopijos daromos kiekvieną dieną, o kitos informacijos – kartą per savaitę. TSA sistemos darbas po sutrikimų atstatomas ne vėliau kaip per 48 valandas.

3.6. TSA veiklos sukompromitavimas

TSA turi užtikrinti, kad laiko žymos paslaugų saugumui turinčių įtakos įvykių atveju, įskaitant privačiojo rakto sukompromitavimą ar nustatytą kalibravimo neatitikimą, atitinkama informacija bus pateikta TSA abonentams ir pasitikintiems asmenims.

TSA turi turėti veiklos atstatymo veiksmų planą kaip elgtis privataus rakto sukompromitavimo, galimo sukompromitavimo ar TSA laikrodžių kalibravimo sutrikimo atvejais.

Įvykus raktų sukompromitavimui, galimam sukompromitavimui ar TSA laikrodžių kalibravimo sutrikimams, TSA turi pateikti laiko žymų naudotojams įvykio aprašymą.

Įvykus TSA veiklos sukompromitavimui (pvz. raktų) ar galimam sukompromitavimui ar kalibravimo neatitikimui, laiko žymos neturi būti išduodamos, kol sistemos veikimas nėra atstatomas.

Įvykus svarbiam veiklos pažeidimui (privataus rakto sukompromitavimui arba sinchronizacijos su UTC praradimui), laiko žymų teikėjas turi kaip įmanoma greičiau ir visom įmanomom priemonėm pranešti laiko žymų naudotojams informaciją kaip identifikuoti laiko žymas, kurios yra pažeistos, nebent tai pažeistų privatumo susitarimams su abonentais ar sumažintų paslaugų saugą.

3.7. TSA veiklos nutraukimas

Laiko žymų teikimo veiklos nutraukimo atveju TSA turi užtikrinti, kad būtų minimizuota potenciali laiko žymų naudotojų žala. Nutraukus laiko žymų teikimo paslaugas, TSA turi užtikrinti, kad būtų nepertraukiamai teikiama informacija, reikalinga iki veiklos nutraukimo išduotų laiko žymų teisingumui patikrinti.

Prieš nutraukiant veiklą TSA turi minimaliai atlikti šias procedūras:

a) informuoti visus laiko žymų naudotojus apie laiko žymos paslaugų teikimo nutraukimą;

b) nutraukti bendradarbiavimą su visais laiko žymos teikimo paslaugų subkontraktoriais;

c) perduoti patikimam asmeniui teikti ir saugoti veiklos metu sukauptą informaciją;

d) sunaikinti visus privačius raktus;

e) atšaukti visus laiko žymų pasirašymui naudojamus sertifikatus.

TSA turi būti numačiusi lėšų šiems įsipareigojimams įvykdyti, jei bankrutuotų ar kitais nemokumo atvejais.

4. FIZINIO, PROCEDŪRINIO IR PERSONALO SAUGUMO KONTROLĖ

4.1. Fizinio saugumo kontrolė

TSA kompiuterių sistema, operatorių darbo vietos, informacijos resursai yra įrengti ir laikomi tam tikslui skirtoje vietoje, kuri yra fiziškai apsaugota nuo neleistino patekimo į ją, įrangos sunaikinimo ir veiklos sugriovimo. Prieiga prie kertinių sistemos elementų yra stebima. Kiekvienas asmenų patekimas į ją yra registruojamas, stebimas elektros energijos tiekimo stabilumas, temperatūra ir drėgmė.

4.1.1 Buveinės vieta

TSA buveinės adresas yra:

V. Kudirkos g. 18, LT-03105 Vilnius, Lietuva.

4.1.2 Fizinė prieiga

Fiziniam patekimui į TSA patalpas kontroliuoti yra stebėjimo sistema, veikianti ištisą parą. Veikia priešgaisrinė, apsaugos nuo užpylimo vandeniu, apsaugos nuo įsilaužimo ir atsarginė elektros energijos tiekimo sistemos.

TSA lankytojai priimami darbo dienomis Registrų centro direktoriaus įsakymu patvirtintomis darbo valandomis. Likusiu laiku (įskaitant nedarbo dienas) TSA buveinėje gali lankytis tik TSA vadovybės įgaliojimus turintys asmenys, kurių vardai ir pavardės yra žinomi apsaugos tarnybai.

Lankytojai patekti į TSA patalpas gali tik lydimi TSA įgaliotų asmenų.

Yra skiriamos 3 TSA patalpų saugumo zonos:

a) kompiuterinės sistemos zoną;

b) operatorių ir administratorių zoną;

c) projektuotojų ir programuotojų zoną.

Kompiuterinės sistemos zona yra įrengta bendroje Registrų Centro tarnybinių stočių saugykloje. Su laiko žymos teikimo paslaugomis susijusi įranga yra saugoma atskiroje tarnybinių stočių spintoje. Patekimą į tarnybinių stočių saugyklą reguliuoja elektroninių kortelių sistema, kurių atitinkamas skaitymo

įrenginys yra prie įėjimo durų. Kiekvienas įėjimas ir išėjimas iš šios zonos automatiškai registruojamas sistemos veiklos registravimo žurnale.

Patekimas į operatorių ir administratorių zoną kontroliuojamas elektroninėmis kortelėmis ir jų skaitymo įrenginiais. Įslaptintai informacijai saugoti naudojami seifai. Prieš naudojimąsi operatoriaus ir administratoriaus terminalais patikrinami darbuotojo įgaliojimai. Šioje zonoje gali būti tik leidimus turintys asmenys. Vienu metu zonoje turi būti ne mažiau kaip du asmenys.

Projektuotojų ir programuotojų zona yra saugoma panašiai, kaip ir operatorių bei administratorių zona. Nėra reikalavimo, kad joje vienu metu būtų bent du asmenys. Projektuotojai ir programuotojai neturi prieigos prie įslaptintos informacijos. Jei tai yra būtina, zonoje tuo metu turi būti saugumo pareigūnas. Įgyvendinamieji projektai ir jų programinė įranga bandomi naudojant sukurtos TSA sistemos bandomąją versiją ar jos modelį.

4.1.3 Elektros energijos tiekimas ir oro kondicionavimas

Registrų Centro tarnybinių stočių saugykloje yra įrengta moderni oro kondicionavimo sistema palaikanti reikiamą vienodą temperatūrą ir apsauganti įrangą nuo dulkių. Nutrūkus elektros energijos tiekimui iš tinklo, atsarginiai energijos šaltiniai (2 UPS ir 2 dyzeliniai elektros generatoriai) užtikrina normalų sistemos darbą 96 valandas.

4.1.4 Apsauga nuo užpylimo vandeniu

Kompiuterinės sistemos zonoje yra įdiegti drėgmės ir vandens jutikliai. Jie yra įjungti į visų Registrų centro patalpų apsaugos sistemą. Budėtojai yra informuoti apie galimus pavojus ir nelaimės atveju yra įpareigoti kreiptis į viešąsias miesto tarnybas, informuoti TSA saugumo pareigūną ir TSA administratorių.

4.1.5 Priešgaisrinė apsauga

RCSC patalpose yra įdiegta priešgaisrinės apsaugos sistema, atitinkanti priešgaisrinės apsaugos tarnybos nustatytus reikalavimus. Įdiegta automatinė gesinimo inertinėmis dujomis sistema.

4.1.6 Informacijos laikmenų saugojimas

Priklausomai nuo informacijos svarbos, laikmenos su archyvų duomenimis ir atsarginėmis duomenų kopijomis yra saugomos ugniai atspariuose seifuose, kurie stovi operatorių ir administratorių zonose.

4.1.7 Atliekų tvarkymas

Popieriai ir elektroninės laikmenos, kuriose yra TSA veiklos saugumui įtakos turinti informacija, pasibaigus tos informacijos saugojimo terminui sunaikinami specialiais plėšymo įrenginiais. Šifravimo raktų ir PIN kodų laikmenos yra naikinamos DIN3 klasės įrenginiais (taip naikinamos tik laikmenos, kuriose neįmanoma visiškai sunaikinti saugomos informacijos, pvz., kriptografinės kortelės).

4.1.8 Atsarginių kopijų saugojimas

Archyve saugomos sistemos sukurtos einamosios informacijos kopijos ir visų TSA taikomųjų programų instaliacinės kopijos. Gedimų atveju tai įgalina atstatyti bet kurios TSA funkcijos vykdymą per 48 valandas.

5. PROCEDŪRINIO SAUGUMO KONTROLĖ

5.1.1 Darbuotojų pareigos

TSA darbuotojų pareigos, kurias gali eiti vienas arba keli asmenys, yra šios:

a) **saugumo pareigūnas**. Jis inicijuoja TSA aparatinės (įskaitant kompiuterių tinklo) ir programinės įrangos diegimą ir tvarkymą; inicijuoja ir stabdo TSA paslaugas; vadovauja kitiems administratoriams, inicijuodamas raktų ir kitų slaptųjų duomenų generavimą; skiria TSA darbuotojams teises saugumo požiūriu ir prieigos prie sistemos privilegijas; teikia pradinius slaptažodžius vartotojams; peržiūri įvykių registracijos žurnalus; prižiūri paslaugų teikimą; prižiūri vidinio ir išorinio tikrinimo procedūras; priima patikrinimų protokolus ir rengia atsakymus į juos; prižiūri tikrinimo metu pastebėtų trūkumų šalinimą;

b) **TSA administratorius.** Jis prižiūri TSA operatorių darbą; instaliuoja naudojamą įrangą; nustato sistemos ir tinklo parametrus; paleidžia tinklo apsaugos priemones ir nustato apsaugos parametrus; kuria TSA vartotojų darbo laukus (*accounts*); peržiūri sistemos įrašus; daro atsargines duomenų kopijas gedimams likviduoti; keičia serverių vardus ir adresus; kuria ir atnaujina saugyklos katalogus; kuria saugyklos WWW puslapį ir tvarko sąsajas;

c) **TSA operatorius.** Jis atsakingas už kasdienes laiko žymų formavimo ir tvarkymo procedūras, pastoviai rengia duomenų atsargines kopijas ir tvarko duomenų bazių ir įvykių įrašų archyvą; tvarko duomenų bazes; bet neturi fizinės prieigos prie kitų sistemos resursų;

d) **TSA auditorius.** Jis yra atsakingas už įvykių registracijos žurnalų peržiūrą, vidinių patikrinimų atlikimą, TSPS laikymąsi.

Aprašytų pareigų paskirstymas užkerta kelią TSA sistemos naudojimo piktnaudžiavimams. Kiekvienam sistemos vartotojui yra leistini tik jo pareigose numatyti veiksmai.

5.1.2 Pareigų identifikacija ir autentiškumo tikrinimas

TSA darbuotojų pareigų identifikacija (atpažinimas) ir autentiškumo tikrinimas atliekami tokiais atvejais:

a) sudarant asmenų sąrašą, kuriems leidžiama patekti į TSA patalpas;

b) sudarant asmenų sąrašą, kuriems leidžiama fizinė prieiga prie TSA sistemos ir tinklo resursų;

c) skiriant vartotojų darbo laukus (*accounts*) ir slaptažodžius TSA informacinėje sistemoje.

Kiekvienas patvirtinimas ar paskyrimas:

a) yra unikalus ir betarpiškai susietas su konkrečiu asmeniu;

b) jais negali būti dalinamasi su bet kuriais kitais asmenims;

c) numato ribotas funkcijas (kylančias iš konkretaus asmens pareigų), susijusias tik su TSA sistemos programine įranga, operacine sistema ir kontrolės priemonėmis.

TSA operacijos, kurioms atlikti reikia paskirstytųjų (*shared*) tinklo resursų, apsaugomos griežtomis autentiškumo patvirtinimo ir siunčiamos informacijos šifravimo priemonėmis.

6. PERSONALO PATIKIMUMO KONTROLĖ

Garantuojama, kad TSA pavestas pareigas atliekantys asmenys:

a) turi aukštąjį išsilavinimą;

b) yra pasirašę susitarimą dėl pareigų vykdymo ir atsakomybės;

c) yra išklausę tobulinimo kursus, susijusius su jiems pavestų pareigų vykdymu;

d) yra išklausę mokymus, susijusius su asmens duomenų, konfidencialios ir privačiosios informacijos apsauga;

e) yra pasirašę susitarimą dėl TSA veiklos saugumui įtaką turinčios informacijos, konfidencialių ir asmenų, kuriems TSA teikia paslaugas, privačiųjų duomenų saugojimo.

6.1.1 Biografijos tikrinimo procedūra

Taikoma standartinė Registrų centro darbuotojų biografijos tikrinimo procedūra. Registrų centre negali dirbti teisti asmenys.

6.1.2 Mokymo reikalavimai

TSA atsakingieji darbuotojai yra išklausę mokymus ir susipažinę su:

a) TSP ir TSPS reikalavimais;

b) TSA saugumo reikalavimais ir jų laikymosi tikrinimo procedūromis;

c) atsakomybe už sistemos atliekamų veiksmų sutrikimus;

d) galimais sistemos veikimo sutrikimais ir TSA veiklos pažeidimais.

Mokymus praėję dalyviai yra pasirašę dokumentus, kad jie yra susipažinę su TSP ir TSPS, taip pat, sutinka su jiems keliamais reikalavimais ir nustatytomis pareigomis.

6.1.3 Reikalavimai samdomiems asmenims

Samdomi asmenys, atliekantys užduotis pagal sutartis (išorinių paslaugų tiekėjai, programinės įrangos kūrėjai ir kt.), tikrinami laikantis tokių pačių procedūrų,

kurios taikomos TSA darbuotojams. Be to, samdomus asmenis, atliekančius užduotis TSA patalpose, turi lydėti TSA darbuotojas.

6.1.4 Darbuotojams teikiami dokumentai

TSA užtikrina savo darbuotojams prieigą prie šių dokumentų:

a) TSP ir TSPS;

b) TSA sistemos naudotojų teisių ir pareigų aprašų.

7. TSA SERTIFIKATO IR CRL PROFILIAI

RCSC sudaromi sertifikatai atitinka LST ETSI 101 862 „Kvalifikuotų sertifikatų sandara" standarto reikalavimus.

7.1. Šakninio CA sertifikato profilis

X.509 V1 pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			*V3*
Serial number			*Automatiškai sudaromas šakninio CA*
Signature algorithm			*sha1RSA*
Issuer			*CN = VI Registru Centras RCSC (RootCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 16 metų*
Subject			*CN = VI Registru Centras RCSC (RootCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Public key			*RSA (4096 Bits)*
X.509 V3 Plėtiniai			
1.3.6.1.5.5.7.1.3	Taip		*Plėtinio OID reikšmė*
Subject Key Identifier	Ne		*Šakninio CA viešojo rakto hash reikšmė SHA1 algoritmu.*
CA Version	Ne		*V0.0*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.1*
		Policy Qualifier Id=User Notice	*No value.*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Key Usage	Taip		*Certificate Signing, Off-line CRL Signing, CRL Signing (06)*
Basic Constraints	Taip		*Subject Type=CA* *Path Length Constraint=None*
Properties			
Thumbprint algorithm			*sha1*
Thumbprint			*Šakninio CA sertifikato santrauka*

7.2. Nuostatų CA sertifikato profilis

X.509 V1 pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			*V3*
Serial number			*Automatiškai sudaromas šakninio CA*
Signature algorithm			*sha1RSA*
Issuer			*CN = VI Registru Centras RCSC (RootCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246*

			C = LT
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 8 metai*
Subject			*CN = VI Registru Centras RCSC (PolicyCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Public key			*RSA (2048 Bits)*
X.509 V3 Plėtiniai			
Subject Key Identifier	Ne	Key Identifier	*Nuostatų CA viešojo rakto hash reikšmė SHA1 algoritmu.*
1.3.6.1.5.5.7.1.3	Taip		*Plėtinio OID reikšmė*
CA Version	Ne		*V0.0*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.1*
		Policy Qualifier Id=User Notice	*No value.*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Certificate Template Name	Ne		*Sisteminis šablono identifikatorius*
Authority Key Identifier	Ne	Key Identifier	*Šakninio CA viešojo rakto hash reikšmė SHA1 algoritmu.*
CRL Distribution Points	Ne	Distribution Point Name	*URL=* *http://csp.rcsc.lt/CDP/VI%20Registru%20Centras%20RCSC%20(RootCA).crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*http://ocsp.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp.rcsc.lt/AIA/VI%20Registru%20Centras%20RCSC%20(RootCA).crt*
Basic Constraints	Taip		*Subject Type=CA* *Path Length Constraint=None*
Key Usage	Taip		*Certificate Signing, Off-line CRL Signing, CRL Signing (06)*
Properties			
Thumbprint algorithm			*sha1*
Thumbprint			*Nuostatų CA sertifikato santrauka*

7.3. TSA sertifikato profilis

X.509 V1 pagrindiniai laukai	Kritinis	Atributas	Reikšmė
Version			*V3*
Serial number			*Automatiškai sudaromas nuostatų CA*
Signature algorithm			*sha1RSA*
Issuer			*CN = VI Registru Centras RCSC (PolicyCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Valid from			*Išdavimo data*
Valid to			*Išdavimo data + 4 metai*
Subject			*CN = VI Registru Centras RCSC (TSA)* *OU = Registru Centro Sertifikavimo Centras (gali būti*

			papildytas TSU įrenginio serijiniu numeriu) *O = VI Registru Centras - I.k. 124110246* *C = LT*
Public key			*RSA (2048 Bits)*
X.509 V3 Plėtiniai			
Subject Key Identifier	Ne	Key Identifier	*TSA viešojo rakto hash reikšmė SHA1 algoritmu.*
Certificate Policies	Ne	Policy Identifier	*1.3.6.1.4.1.30903.1.1.1*
		Policy Qualifier Id=User Notice	*No value.*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Authority Key Identifier	Ne	Key Identifier	*Nuostatų CA viešojo rakto hash reikšmė SHA1 algoritmu.*
CRL Distribution Points	Ne	Distribution Point Name	*URL= http://csp.rcsc.lt/CDP/VI%20Registru%20Centras%20RCSC%20(PolicyCA).crl*
Authority Information Access	Ne	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*http://ocsp.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp.rcsc.lt/AIA/VI%20Registru%20Centras%20RCSC%20(PolicyCA).crt*
Extended Key Usage	Ne		*Time Stamping (1.3.6.1.5.5.7.3.8)*
Key Usage	Taip		*Digital Signature, Non-Repudiation (c0)*
Properties			
Thumbprint algorithm			*sha1*
Thumbprint			*TSA sertifikato santrauka*

8. TSPS ADMINISTRAVIMAS

Šiame skyriuje pateikiami TSPS administravimo reikalavimai.

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

Laiko žymų naudotojai turi vadovautis vėliausiai išleista TSPS versija.

8.1. TSPS keitimo procedūros

TSPS gali būti keičiami pastebėjus juose klaidas, iškilus reikalui atnaujinti juos arba gavus susijusių šalių pasiūlymus.

TSPS pakeitimai skirstomi į dvi kategorijas:

a) esminiai pakeitimai, apie kuriuos turi būti pranešama vartotojams ir keičiamas TSPS OID;
b) neesminiai pakeitimai, apie kuriuos RCSC neprivalo pranešti kitoms šalims, ir TSPS OID nėra keičiamas.

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

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

Kitais atvejais pakeitimai yra esminiai ir po kiekvieno TSPS pakeitimo keičiamas jų unikalus identifikatorius. Visais atvejais, jei pakeitimai įtakoja laiko žymų teikimo paslaugų saugumo lygio pasikeitimus, pakeitimai yra esminiai.

TSPS prižiūrimi, keičiami ir tvirtinami laikantis tokios procedūros:

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

b) TSPS keitimus inicijuoja TSA arba laiko žymų naudotojai;

c) už saugumo politiką atsakingi darbuotojai rengia naują TSPS redakciją;

d) esminių pakeitimų atveju parengtos naujos TSPS redakcijos projektas publikuojamas saugykloje (*repository*) internete prieš 30 dienų iki TSPS tvirtinimo siekiant gauti susijusių šalių pastabas. Atsižvelgus į per 30 dienų gautas pastabas, arba per 30 dienų negavus pastabų, nauja redakcija tvirtinama. Neesminių pastabų atveju nauja redakcija teikiama tvirtinti iš karto po rengimo;

e) sprendimą teikti tvirtinti naują TSPS redakciją priima RCSC saugumo politikos darbo grupė; esminių pakeitimų atveju suteikiamas naujas OID;

f) naują TSPS redakciją tvirtina RC administracijos vadovas;

g) patvirtinta nauja TSPS redakcija patalpinama į saugyklą (*repository*).

8.2. Skelbimo ir pranešimo procedūros

TSA neskelbia informacijos, galinčios turėti įtaką naudojamos sistemos saugai. Informacija prieinama tik saugumo pareigūnui, TSA administratoriui ir kontroliuojančioms institucijoms. Su šio tipo dokumentais susipažinti galima tik specialioje patalpoje. Kiekvienas prieigos prie slaptųjų dokumentų atvejis fiksuojamas.

TSA saugo visas savo TSPS versijas ir esant paklausimui, pateikia besidominčioms šalims.

Galiojanti TSPS versija ir TSP, kurias įgyvendina TSA, viešai prieinamos saugykloje (*repository*) internete.

9. SĄVOKŲ APIBRĖŽIMAI IR SANTRUMPOS

Abonentas (*subscriber*) – asmuo sudarantis sutartį su TSA ir kuriam yra teikiamos laiko žymos paslaugos.

Aktyvavimo duomenys – tai duomenys (pvz., PIN kodas, slaptažodis, 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 modulis) – aparatinė ir programinė įranga, kuri naudojama šifravimo raktų poroms – privatiesiems ir viešiesiems raktams generuoti arba/ir parašams kurti.

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

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

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

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 naudotojai - laiko žymos gavėjai, pasitikintys laiko žyma, įskaitant abonentus.

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

Laiko žymos taisyklės – laiko žymos sudarymo ir tvarkymo taisyklės, nustatančios paslaugų teikėjo, laiko žymos naudotojų teises ir pareigas. Laiko žymos taisykles renkasi laiko žymos naudotojai ir įgyvendina paslaugų teikėjas.

Laiko žymos teikimo nuostatai – paslaugų teikėjo patvirtintos laiko žymos paslaugų teikimo taisyklės.

Pasitikinčios šalys *(relying party)* – žr. laiko žymos naudotojai.

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

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

RSA – mokslininkų Rivest, Shamir ir Adelman sugalvota viešųjų raktų kriptografinė sistema.

Saugykla *(repository)* – sertifikatų ir kitos sertifikatų centro informacijos duomenų bazė, vartotojams prieinama tiesiogiai (*on-line*) bet kuriuo metu internete adresu www.rcsc.lt/repository/.

Saugos taisyklės – aukščiausios svarbos dokumentas, apibrėžiantis sertifikavimo 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.

UTC laikas – tarptautiniu mastu valdoma, vieninga atominių laikrodžių sistema.

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.

BIPM – Tarptautinis matų ir svorių biuras *(Bureau International des Poids*

et Mesures)

CA – Sertifikavimo tarnyba *(Certification Authority)*

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

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

DN – Asmens unikalus identifikacinis vardas *(Distinguished Name)*

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

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

IDS - Įsilaužimų atskleidimo sistema *(Intrusion Detection System)*

IETF – Interneto inžinierinių uždavinių sprendėjai *(Internet Engineering Task Force)*

LAN – Vietinis kompiuterių tinklas *(Local Area Network)*

LST – Lietuvos standartizacijos tarnyba

NTP – Susieto laiko protokolas *(Network Time Protocol)*

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)*

TSA – Laiko žymų teikimo tarnyba *(Time stamp authority)*

TSP – Laiko žymų teikimo taisyklės *(Time stamp policy)*

TSSP – Laiko žymų paslaugų teikėjas *(Time stamping service provider)*

UPS - Atsarginis energijos šaltinis *(Uninterrupted Power Supply)*

10. ŠALTINIAI

[1] ETSI TS 101 456 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates. http://portal.etsi.org/esi/el-sign.asp

[2] ETSI TS 101 862 Qualified Certificate Profile. http://portal.etsi.org/esi/el-sign.asp

[3] ETSI SR 002 176 Electronic Signatures and Infrastructures (ESI): Algorithms and Parameters for Secure Electronic Signatures. http://portal.etsi.org/esi/el-sign.asp

[4] CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements. http://www.uninfo.polito.it/WS_Esign/docs.htm#published

[5] CWA 14167-2 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP). http://www.uninfo.polito.it/WS_Esign/docs.htm#published

[6] CWA 14167-3 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP). http://www.uninfo.polito.it/WS_Esign/docs.htm#published

[7] CWA 14168 Secure Signature-Creation Devices, version 'EAL 4'. http://www.uninfo.polito.it/WS_Esign/docs.htm#published

[8] CWA 14170 Security Requirements for Signature Creation Applications. http://www.uninfo.polito.it/WS_Esign/docs.htm#published

[9] CWA 14171 — General Guidelines for Electronic Signature Verification. http://www.uninfo.polito.it/WS_Esign/docs.htm#published

[10] RFC 2459 — Internet X.509 Public Key Infrastructure Certificate and CRL Profile. http://www.ietf.org/rfc/rfc2459.txt

[11] RFC 3280 — Internet X.509 Public Key Infrastructure. Certificate and CRL Profile. http://www.ietf.org/rfc/rfc3280.txt

[12] RFC 3647 — Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework. http://www.ietf.org/rfc/rfc3647.txt

[13] RFC 3739 — Internet X.509 Public Key Infrastructure. Qualified Certificate Profile. http://www.ietf.org/rfc/rfc3739.txt

[14] RFC 3125 — Electronic Signature Policies. http://www.ietf.org/rfc/rfc3125.txt

[15] ISO/IEC 19790:2006 — Information Technology – Security Techniques – Security Requirements for Cryptographic Modules.

[16] FIPS PUB 140-2 — Security Requirements for Cryptographic Modules. http://www.nist.gov/cmvp

[17] FIPS 112 — Password Usage. http://csrs.nist.gov/fips/

[18] ITU-T — Recommendation X.509 – Information Technology – Open System Interconnection – The Directory: Authentication Framework, June 1997 (equivalent ISO/IEC9594-8).

[19] VeriSign CPS — VeriSign Certification Practice Statement. http://www.verisign.com

[20] Unizeto CERTUM — General Certification Authority – Certification Practice Statement. http://www.certum.eu/certum/cert,docs_certification_practise_statement.xml

[21] LST ISO/IEC 15408:1999(E) Information technology — Security techniques – Evaluation criteria for IT security.