REGISTRŲ CENTRAS

RCSC LAIKO ŽYMOS TEIKIMO TAISYKLĖS

Unikalus objekto ID (OID): **1.3.6.1.4.1.30903.1.3.1**
Versija: 1.0
Galioja nuo: 2008-10-28

2008-10-28

TURINYS

RCSC laiko žymos teikimo taisyklių keitimų istorija:

Versija	Data	Aprašas
0.1	2008-06-07	Projektas
1.0	2008-10-28	Pirma versija

Dokumento tvirtinimas:

Dokumento rengimas	Pavardė	Data	Parašas
Dokumentą rengė	Jonas Kupinas Mindaugas Aputis	2008-09-10	
Dokumentą tikrino	Ieva Tarailienė Saulius Kvedaravičius	2008-10-10	
Dokumentą tvirtino	Rimantas Ramanauskas	2008-10-28	

1. ĮVADAS

Valstybės įmonė Registrų centras (toliau – Registrų centras) yra įsteigta 1997 m. Įmonės steigėjas – Lietuvos Respublikos Vyriausybė. Įmonės savininko teises ir pareigas įgyvendinanti institucija yra Lietuvos Respublikos teisingumo ministerija. Įmonė tvarko Nekilnojamojo turto kadastrą ir registrą, Adresų registrą, Juridinių asmenų registrą, 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 laiko žymos paslaugas pagal Lietuvos standarto LST ETSI TS 102 023 „Strateginiai reikalavimai, keliami laiko žymėjimo paslaugų teikėjams“ (versija V1.2.1 2003-01) nuostatas bei remiantis Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2003 m. sausio 29 d. įsakymu Nr. T-10 patvirtinta „Laiko žymos formavimo paslaugų teikimo tvarka“.

1.1. Apžvalga

Laiko žymos teikimo taisyklės (toliau – TSP) – tai taisyklių rinkinys, kuris atspindi Registrų centro laiko žymos teikimo tarnybos (toliau – TSA) sudaromų laiko žymų tinkamumą tam tikroms naudotojų grupėms ir taikymo sritims, turinčioms bendrus saugumo reikalavimus. Šio dokumento tikslas yra sutvirtinti pasitikėjimą TSA sudaromomis laiko žymomis, kurios atitinka šių taisyklių reikalavimus.

TSP išdėstyti reikalavimai nėra susieti su konkrečiais technologiniais sprendimais ar TSA organizacine struktūra. TSP reikalavimų įgyvendinimo techniniai sprendimai, procedūros ir personalo politika aprašyta RCSC laiko žymos teikimo veiklos nuostatuose (toliau – TSPS).

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

Šios taisyklės paremtos dokumentais:

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

b) LST ETSI TS 101 861 „Laiko žymos profilis“ standartu;

c) RFC 3628;

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

Šios taisyklės paremtos bazinėmis LST ETSI TS 102 023 standarte pateiktomis laiko žymos taisyklėmis, kurių OID yra 0.4.0.02023.1.1.

TSA teikdama laiko žymos paslaugas vykdo šias funkcijas:

- laiko žymos sudarymas
- laiko žymų tvarkymas

1.2. Identifikavimas

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

1.3.6.1.4.1.30903.1.3.1

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

Lentelė Nr. 1. TSP 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 taisyklės)	3
Dokumento versija	1

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

1.3. Naudotojai ir taikymo sritys

Šios taisyklės skirtos tenkinti laiko žymų, skirtų užtikrinti kvalifikuotų elektroninių parašų ilgalaikį galiojimą, reikalavimus (pagal ES direktyvos ir LR elektroninio parašo įstatymo reikalavimus). Laiko žymos skirtos elektroninių parašų naudotojams, siekiantiems įrodyti, kad elektroninis parašas buvo sukurtas iki žymoje nurodyto laiko. Laiko žymos paslaugų teikėjas gali teikti viešąsias paslaugas, taip pat, jis gali aptarnauti ir uždarąsias naudotojų grupes.

Pagrindinė TSA sudaromų laiko žymų taikymo sritis – teikti laiko žymos paslaugą saugiems elektroniniams parašams, sukurtiems saugia parašo formavimo įranga ir patvirtintiems kvalifikuotais sertifikatais. Tačiau šis dokumentas nenustato jokių laiko žymų naudojimo apribojimų. Šias TSP atitinkančios laiko žymos gali būti naudojamos vykdant elektronines transakcijas, elektroninių dokumentų archyvavime, elektroniniuose parašuose ir kt.

1.4. Atitiktis

TSA įrašydamas sukurtose laiko žymose unikalų identifikatorių, apibrėžtą 1.2 skyriuje pažymi laiko žymos atitikimą šioms taisyklėms. Tokiu būdu TSA turi prisiimti visus įsipareigojimus, apibrėžtus 2.1 skyriuje ir įgyvendinti visus 3 skyriuje nustatytus reikalavimus veiklai.

1.5. Kontaktinė informacija

Šias TSP tvarko valstybės įmonės Registrų centro padalinys - Registrų centro sertifikavimo centras (toliau – RCSC). RCSC kontaktiniai duomenys nurodyti žemiau (*Lentelė Nr. 2*).

Lentelė Nr. 2. RCSC kontaktinė informacija

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 TSA ir su juo susijusių šalių įsipareigojimai ir nuostatos teisiniais ir bendraisiais veiklos klausimais.

2.1. Įsipareigojimai

2.1.1 Bendri TSA įsipareigojimai

TSA turi užtikrinti, kad visi jam keliami reikalavimai, išdėstyti šio dokumento 3 skyriuje, būtų įgyvendinami.

TSA turi užtikrinti atliekamų procedūrų ir paslaugų atitikimą TSPS nustatytiems 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 teikti visas laiko žymos paslaugas laikydamasis TSPS ir užtikrinti TSPS atitikimą TSP.

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

2.1.2 TSA įsipareigojimai abonentams

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

2.1.3 Laiko žymos 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 laiko žymos taisyklėse, sutartyse su paslaugų teikėju arba kitur.

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

2.1.4 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 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 žymos teikimu, jeigu tai neprieštarauja galiojantiems įstatymams. Atsakomybės apribojimai nurodomi laiko žymos teikimo sąlygose.

2.3. Mokesčiai

TSA negali reikalauti atlyginti už TSP ir TSPS skelbimą.

TSA gali nustatyti kainas už laiko žymos paslaugų teikimą.

2.4. Informacijos teikimas ir saugyklos

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 sąrašas (toliau – CRL);

c) kita su laiko žymos teikimu susijusi aktuali informacija.

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

2.5. Intelektinės nuosavybės teisės

Šios TSP ir jas įgyvendinantys TSPS yra laisvai prieinami laiko žymų naudotojams. Naudojant šias TSP ir TSPS, yra būtina pateikti nuorodą į jų šaltinį.

3. TSA VEIKLOS REIKALAVIMAI

3.1. Veiklos nuostatai

TSA veiklos procedūros, kontrolės mechanizmas ir techniniai reikalavimai infrastruktūrai yra detalizuoti TSPS.

TSA privalo užtikrinti patikimą laiko žymos paslaugų teikimą:

a) TSA turi atlikti rizikos analizę įvertinant valdomą turtą ir grėsmes šiam turtui siekiant nustatyti būtinas saugumo priemones ir veiklos procedūras;

b) TSA turi turėti detaliai aprašytus veiklos nuostatus ir procedūras įgyvendinančias šių TSP reikalavimus;

c) TSPS turi detalizuoti visų išorinių organizacijų, prisidedančių prie sertifikavimo veiklos įsipareigojimus;

d) TSA privalo pateikti abonentams ir laiko žymomis pasitikinčioms šalims TSPS ir kitą susijusią informaciją, kad būtų galima įsitikinti sertifikavimo veiklos atitikimu šioms taisyklėms;

e) TSA privalo atskleisti abonentams ir laiko žymomis pasitikinčioms šalims laiko žymos paslaugų teikimo sąlygas;

f) TSA privalo turėti aukšto lygio valdymo organą, turintį atitinkamus įgaliojimus, kuris tvirtina TSPS;

g) TSA aukščiausioji vadovybė privalo užtikrinti, kad TSPS yra tinkamai įgyvendinami;

h) TSA turi apibrėžti vykdomos veiklos peržiūros procedūras ir nustatyti atsakomybę už TSPS priežiūrą;

i) TSA turi pateikti tinkamu laiko tinkamos formos pranešimą apie pakeitimus numatomus atlikti TSPS ir juos patvirtinus (punktas f) nedelsiant pateikti abonentams ir pasitikinčioms šalims (punktas d).

3.2. Laiko žymos 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 laiku;

f) laiko žymos paslaugų naudojimo apribojimus;

g) abonentų įsipareigojimus;

h) laiko žymomis pasitikinčiųjų pusių įsipareigojimus;

i) informaciją apie tai, kaip patikrinti laiko žymą tokiu būdu, kad būtų pakankamas pagrindas ja pasitikėti;

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.

3.3. Kriptografinių raktų valdymo ciklas

3.3.1 TSA kriptografinių raktų generavimas

TSA turi užtikrinti, kad bet kokie kriptografiniai raktai būtų generuojami kontroliuojamose ir saugiose sąlygose:

a) TSA privatusis raktas turi būti generuojamas fiziškai saugiose sąlygose, esant bent dviejų asmenų, kuriems priskirtos ypatingo pasitikėjimo pareigos, kontrolei. Konkrečios ypatingo pasitikėjimo pareigybės galinčios atlikti šią funkciją nurodytos TSPS;

b) kriptografinis modulis, kuriuo generuojamas privatusis raktas, turi atitikti: FIPS PUB 140-2 trečio ar aukštesnio lygio reikalavimus; arba reikalavimus nustatytus CEN Workshop Agreement 14167-2; arba EAL 4; arba aukštesniu pagal ISO/IEC 15408 reikalavimus;

c) privataus rakto generavimo algoritmas, rakto ilgis, pasirašymo algoritmas turi būti visuotinai arba kompetentingos nacionalinės institucijos pripažinti tinkamais tvirtinti laiko žymoms.

3.3.2 TSA privataus kriptografinio rakto apsauga

TSA turi užtikrinti TSA parašo formavimo duomenų (privačiojo rakto) konfidencialumą ir vientisumą (nepažeidžiamumą):

a) TSA privatus raktas turi būti laikomas ir naudojamas tik kriptografiniame modulyje, atitinkančiame: FIPS PUB 140-2 trečio ar aukštesnio lygio reikalavimus; arba reikalavimus nustatytus CEN Workshop Agreement 14167-2; arba EAL 4 arba aukštesniu pagal ISO/IEC 15408 reikalavimus;

b) TSA privatusis raktas gali būti atstatomas ir jo kopijos saugomos tik naudojantis su kriptografine techninę įranga susietomis sisteminėmis kortelėmis, kurių kiekvienoje saugomas fragmentas šifravimo rakto, kuriuo užšifruota TSA privačiojo rakto kopija. Privačiajam raktui atstatyti reikalingos bent 2 iš minimaliai 4 tokių sisteminių kortelių. Darant kopijas, saugant ir atstatant TSA privatų raktą privalo dalyvauti bent 2 ypatingo pasitikėjimo pareigas užimantys darbuotojai ir tai turi būti atliekama fiziškai saugioje aplinkoje;

c) TSA sertifikato gyvavimo ir atitinkamų parašo formavimo duomenų (privačiojo rakto) naudojimo trukmė turi būti ribota, atsižvelgiant į naudojamus duomenų santraukos apskaičiavimo ir parašo kūrimo algoritmus bei laiko žymoms tvirtinti naudojamo elektroninio parašo rakto ilgį.

3.3.3 TSA viešojo kriptografinio rakto skelbimas

Publikuodama savo viešąjį raktą pasitikinčioms šalims, TSA turi užtikrinti TSA parašo tikrinimo duomenų (viešojo rakto) ir susijusių parametrų autentiškumą ir vientisumą (nepažeidžiamumą). TSA viešasis raktas turi būti skelbiamas viešojo rakto sertifikate. Sertifikatas turi būti išduotas sertifikavimo paslaugų teikėjo, veikiančio panašaus arba aukštesnio saugumo lygmenyje koks nustatytas šiomis taisyklėmis.

3.3.4 TSA kriptografinių raktų keitimas (*rekey*)

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

3.3.5 TSA kriptografinių raktų poros gyvavimo ciklo pabaiga

TSA turi užtikrinti, kad TSA parašo formavimo duomenys (privatusis raktas) nebebūtų naudojami pasibaigus jų gyvavimo ciklui.

Nustatytos techninės ir valdymo procedūros turi užtikrinti, kad pasibaigus TSA raktų galiojimo terminui būtų sukurta ir naudojama nauja raktų pora, o anksčiau naudoti privatūs raktai (ar bet kokia jų dalis) būtų sunaikinti. Laiko žymų sudarymo sistema turi uždrausti išduoti laiko žymas, jei yra pasibaigęs TSA privataus rakto galiojimas.

3.3.6 Laiko žymas pasirašančio kriptografinio modulio gyvavimo ciklas

TSA turi užtikrinti kriptografinės techninės 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 TSA parašo formavimo duomenys (raktų pora) kriptografiniame modulyje instaliuojami ir aktyvuojami fiziškai saugioje aplinkoje, esant bent 2 ypatingo patikimumo pareigas einančių asmenų kontrolei;

d) kad laiko žymas pasirašantis kriptografinis modulis tinkamai funkcionuoja;

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

3.4. Laiko žymos sudarymas

3.4.1 Laiko žymos

TSA turi užtikrinti, kad laiko žymos išduodamos saugiai ir į jas įtraukiamas teisingas laikas. TSA privalo užtikrinti, kad:

a) laiko žymoje būtų nurodytas laiko žymos teikimo taisyklių identifikatorius;

b) kiekviena laiko žyma turėtų unikalų identifikatorių;

c) laiko žymoje būtų nurodytos datos ir laiko vertės;

d) laiko žymoje esančios laiko vertės būtų susietos su nors viena realaus laiko verte pateikta UTC laiko laboratorijos;

e) laiko žymoje nurodomo laiko vertė būtų sinchronizuota su UTC laiku, ne didesniu nei 1 sekundės, tikslumu;

f) jei nustatoma, kad TSA laikrodžio tikslumas nukrypo daugiau, nei deklaruojamas tikslumas, TSA neišduotų laiko žymos;

g) laiko žymoje būtų nurodyta laiko žyma pasirašomų duomenų santrauka (*hash*), kurią pateikia laiko žymą užsakantis asmuo;

h) laiko žyma būtų pasirašyta naudojant raktų porą, kuri buvo sukurta tik šiam tikslui ir negali būti naudojama kitoms reikmėms;

i) laiko žymoje būtų nurodyti TSA, TSA rezidavimo šalies ir laiko žymas išduodančio TSA padalinio identifikatoriai.

3.4.2 Sinchronizacija su UTC

TSA turi užtikrinti, kad jos naudojamas laikrodis būtų sinchronizuotas su UTC deklaruojamu tikslumu.

TSA naudojami laikrodžiai turi būti kalibruojami taip, kad nenukryptų nuo apsibrėžto tikslumo.

Laikrodžiai turi būti apsaugoti nuo grėsmių, galinčių sukelti nenustatytus laiko vertės pakeitimus ne kalibravimo metu.

TSA turi užtikrinti, kad bus pastebėti bet kokie laikrodžių sinchronizacijos su UTC poslinkiai ar nukrypimai.

TSA turi užtikrinti, kad laikrodžių sinchronizacija bus vykdoma korekcinės sekundės (UTC laiko korekcija pridedant ar atimant 1 sekundę UTC mėnesio pabaigoje) atveju gavus informaciją iš atitinkamos institucijos. Korekcinės sekundės pakeitimai TSA laikrodyje turi būti atlikti per paskutinę dienos, kurios metu numatyta UTC laiko korekcija, minutę. TSA turi saugoti įrašą, kuriuo laiku (sekundės tikslumu) buvo įvykdyti korekcinės sekundės pakeitimai TSA laikrodyje.

3.5. TSA valdymas ir veikla

3.5.1 Saugumo valdymas

TSA turi užtikrinti, kad bus vykdomos adekvačios administracinės ir valdymo procedūros kurios remiasi geriausia praktika.

TSA turi išlaikyti pilną atsakomybę teikiant laiko žymos paslaugas pagal šias TSP nepriklausomai nuo funkcijų delegavimo trečioms šalims. Trečių šalių atsakomybė turi būti aiškiai apibrėžta ir numatytos įsipareigojimų vykdymo užtikrinimo priemonės.

TSA vadovybė ar jos vadovaujama saugos grupė turi parengti informacijos saugumo politiką ir informuoti visus savo darbuotojus, kuriuos liečia ši informacijos saugumo politika.

TSA turi užtikrinti, kad jos informacijos saugumo infrastruktūra būtų visada tinkamai prižiūrima. Bet kokie pakeitimai, įtakojantys saugumo lygio pasikeitimus turi būti patvirtinti TSA vadovybės arba jos vadovaujamos saugos grupės.

TSA patalpų, sistemų ir informacijos saugumo kontrolės ir veiklos procedūros tiekiant laiko žymos paslaugas turi būti įgyvendinamos, prižiūrimos ir dokumentuojamos.

TSA turi užtikrinti, kad informacijos saugumas būtų išlaikomas kai TSA funkcijos yra deleguotos trečiosioms šalims.

3.5.2 Turto inventorizacija ir valdymas

TSA turi užtikrinti, kad jos informacija ir kitas turtas yra tinkamai apsaugoti.

TSA turi vykdyti viso turto inventorizaciją ir pagal rizikos analizės rezultatus turi suklasifikuoti turto saugos reikalavimus.

3.5.3 Personalo valdymo kontrolė

TSA yra atsakinga, kad samdomas personalas ir jo samdos procedūros užtikrintų ir keltų TSA veiklos patikimumą:

a) TSA personalas turi turėti aukštąjį išsilavinimą, reikalingų žinių, patirties bei kvalifikaciją, būtiną siūlomoms paslaugoms įgyvendinti, atitinkančią darbo funkcijas;

b) Saugumo užtikrinimo pareigos ir atsakomybės nurodytos TSA saugumo politikoje turi būti dokumentuotos pareigybių aprašymuose. Ypatingo pasitikėjimo pareigybės, nuo kurių stipriai priklauso TSA veikla ir saugumas, turi būti tiksliai ir aiškiai apibrėžtos ir dokumentuotos;

c) TSA personalas (tiek laikinas, tiek nuolatinis) turi turėti pareigybių aprašymus, kurie turi būti 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 turi atitikti TSA informacijos saugumo valdymo procedūras;

Laiko žymos paslaugų teikimo valdymui turi būti taikomos šios papildomos kontrolės priemonės:

e) vadovaujantis personalas turi:

- išmanyti laiko žymos technologijas;
- išmanyti skaitmeninio parašo technologijas;
- išmanyti TSA laikrodžių kalibravimo ar sinchronizavimo su UTC mechanizmus;
- žinoti saugumo procedūras, jei pareigos susijusios su atsakomybe už saugumą;
- turėti patirties informacijos saugumo ir rizikos vertinimo srityse.

f) TSA personalas, užimantis ypatingo pasitikėjimo reikalaujančias pareigas, neturi būti paveikiamas bet kokių interesų konfliktų, galinčių paveikti TSA operacijų objektyvumą;

g) ypatingo pasitikėjimo pareigos apima pareigas kurios apima šias atsakomybės sritis:

- saugumo pareigūnai – bendra atsakomybė už saugumo politikos vykdymą;
- sistemos administratoriai – įgalioti instaliuoti, konfigūruoti ir palaikyti TSA sistemas naudojamas laiko žymų valdymui;
- sistemos operatoriai – atsakingi už kasdienį TSA sistemų naudojimą. Įgalioti atlikti sistemos atsargines kopijas bei atkūrimą;
- sistemos auditoriai – įgalioti peržiūrėti TSA patikimumo sistemų archyvus bei audito įrašus.

h) į ypatingo pasitikėjimo TSA pareigas, darbuotojai skiriami vadovybės, atsakingos už saugumą, sprendimu;

i) TSA negali į ypatingo pasitikėjimo ar vadovybės pareigas skirti asmens, kuris buvo teistas už nusikaltimą ar kitą nusižengimą, galintį paveikti jo tinkamumą šioms pareigoms.

3.5.4 Fizinio saugumo kontrolė

TSA turi užtikrinti, fizinio priėjimo prie kritinių paslaugų kontrolę ir fizinės turto rizikos minimizavimą.

Fizinę prieigą prie patalpų, kuriuose vykdomos tiek laiko žymos sudarymo tiek tvarkymo funkcijos turi turėti tik autorizuotas personalas. Turi būti įdiegtos kontrolės priemonės siekiant išvengti turto netekties, žalos ir sukompromitavimo, bei veikos sustabdymo. Turi būti įdiegtos kontrolės priemonės siekiant išvengti informacijos ir jos apdorojimo įrangos vagystės ir sukompromitavimo.

Priėjimo prie kriptografinio modulio kontrolė turėtų būti realizuota atsižvelgiant į reikalavimus nustatytus 3.3.1. ir 3.3.2. skyriuose.

Laiko žymų valdymui turi būti įdiegtos šios papildomos kontrolės priemonės:

a) laiko žymų valdymo įranga turi būti aplinkoje, kuri fiziškai apsaugotų paslaugas nuo sukompromitavimo dėl nesankcionuotos prieigos prie sistemų ir duomenų;

b) fizinė apsauga turi būti pasiekta nustatant aiškius fizinius perimetrus. Bet kokios patalpos naudojamos kartu su kitomis organizacijomis turi būti už perimetro ribų;

c) turi būti įdiegtos fizinio ir aplinkos saugumo užtikrinimo priemonės apsaugančios sistemos resursus, įrangą, kurioje saugomi šie resursai ir

papildomą įrangą, užtikrinančią šios įrangos darbą. Fizinė sistemos, vykdančios laiko žymų valdymą, apsauga turi apimti fizinės prieigos kontrolę, apsaugą nuo stichinių nelaimių, priešgaisrinę saugą, apsaugą nuo palaikančios įrangos (telekomunikacijų, elektros energijos) sutrikimų, apsaugą nuo griučių, apipylimo, potvynio kitų nelaimingų atsitikimų ir vagysčių, bei atstatymo priemones;

d) turi būti įdiegtos kontrolės priemonės apsaugančios nuo techninės ir programinės įrangos, informacijos, informacijos nešiklių ir kaupiklių neautorizuoto išnešimo iš patalpų.

3.5.5 Procedūrinio saugumo kontrolė

Laiko žymos teikėjas turi užtikrinti, kad visi TSA sistemos komponentai yra valdomi tinkamai ir saugiai bei minimizuojant gedimų riziką:

a) laiko žymų sistemos ir informacijos integralumas turi būti apsaugotas nuo kompiuterinių virusų ar kitokio programinio pažeidimo;

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

c) TSA sistemose naudojami informacijos kaupikliai ir nešėjai turi būti apsaugoti nuo gedimų, vagystės, nesankcionuotos prieigos ar susidėvėjimo;

d) turi būti nustatytos procedūros visoms su laiko žymų sudarymu ir valdymu susijusioms pareigybėms, įskaitant ir ypatingo pasitikėjimo pareigybes;

e) TSA sistemose naudojami informacijos nešėjai turi būti suklasifikuoti ir nešėjai talpinantys ypatingo saugumo informaciją po panaudojimo turi būti sunaikinti;

f) TSA turi atlikti nuolatinį sistemos būklės monitoringa, kad būtų galima laiku prognozuoti, kada atlikti sistemos plėtrą ar padidinti galios ir atminties pajėgumus;

g) TSA privalo laiku ir nedelsiant reaguoti į incidentus ir sumažinti saugumo spragų įtaką. Apie visus incidentus turi būti nedelsiant informuojama;

h) vykdant laiko žymos valdymo funkcijas, TSA saugumo procedūros turi būti atskirtos nuo kitų procedūrų. Saugumo procedūros apima: veiklos procedūrų ir atsakomybių nustatymas, saugus sistemų planavimas, apsauga nuo žalingų programų, patalpų priežiūra, tinklo valdymas, aktyvi

audito žurnalų stebėsena, įvykių analizė ir veiksmai, informacijos nešiklių valdymas ir apsauga, duomenų ir programinės įrangos apsikeitimas. 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.

3.5.6 Sistemos prieigos valdymas

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

Vidinis TSA tinklas turi būti apsaugotas nuo neautorizuotos prieigos, įskaitant ir abonentus bei pasitikinčius asmenis. Ugniasienės turi drausti visus, su tiesiogine TSA veikla, nesusijusius protokolus ir prieigas.

TSA turi užtikrinti efektyvų vartotojų (operatorių, administratorių ir auditorių) prieigos saugumo užtikrinimui administravimą.

TSA turi užtikrinti, kad prieiga prie informacijos ir taikomosios sistemos funkcijų yra ribota ir atitinka prieigos kontrolės politiką. TSA sistema turi užtikrinti ypatingo pasitikėjimo rolių atskyrimą įskaitant sistemos administratoriaus ir operatoriaus funkcijas.

TSA personalas turi būti tinkamai autentifikuotas ir identifikuotas prieš naudojantis kritiniais laiko žymų sudarymo ir tvarkymo sistemos komponentais.

TSA turi užtikrinti darbuotojų veiksmų su TSA sistemomis apskaitą, pavyzdžiui fiksuojant iš išsaugant išrašus (*logs*) apie sistemų naudojimą.

Visi kompiuterinio tinklo komponentai (maršrutizatoriai ir t.t.) turi būti saugomi fiziškai saugioje aplinkoje, periodiškai atliekamas jų konfigūracijos ir jos atitikimas TSA reikalavimams patikrinimas.

Turi būti įdiegta nuolatinės stebėsenos ir signalizacijos įranga siekiant laiku nustatyti, registruoti ir reaguoti į nesankcionuotą ar neįprastą prieigą prie TSA resursų.

3.5.7 Patikimų sistemų vystymas ir palaikymas

TSA turi naudoti patikimas sistemas ir produktus, kurie yra apsaugoti nuo modifikacijos.

Bet kokios TSA sistemos projektavimo ir reikalavimų specifikavimo etapo metu turi būti atlikta saugumo reikalavimų analizė siekiant užtikrinti, kad IT sistemos yra saugios.

Veiklos procesams skirtos programinės įrangos pataisymams, atnaujinimams ir modifikacijoms turi būti vykdomos pakeitimų kontrolės procedūros.

3.5.8 TSA veiklos sukompromitavimas

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

TSA turi turėti atstatymo veiksmų planą kaip elgtis privataus rakto sukompromitavimo, galimo sukompromitavimo ar TSA laikrodžio kalibravimo neatitikimo atvejais.

Įvykus raktų sukompromitavimui ar galimam sukompromitavimui ar kalibravimo neatitikimui, TSA turi pateikti abonentams ir pasitikintiems asmenims 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 žymos teikėjas turi kaip įmanoma greičiau ir visom įmanomom priemonėm pranešti laiko žymos naudotojams ir pasitikintiems asmenims informaciją kaip identifikuoti laiko žymas, kurios yra pažeistos, nebent tai pažeistų privatumo susitarimams su abonentais ar sumažintų paslaugų saugą.

3.5.9 TSA veiklos nutraukimas

Laiko žymos paslaugų teikimo veiklos nutraukimo atveju TSA turi užtikrinti, kad būtų minimizuota potenciali abonentų ir pasitikinčių asmenų žala. Nutraukus laiko žymos 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 žymos abonentus ir pasitikinčius asmenis apie laiko žymos paslaugų teikimo nutraukimą;

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

c) TSA turi perduoti visus įsipareigojimus, susijusius su įvykiu žurnalizavimu ir audito archyvais, patikimam asmeniui protingam terminui, siekiant įrodyti, kad veikla buvo vykdoma pagal taisykles ir procedūras;

d) TSA turi perduoti patikimam asmeniui arba vykdyti įsipareigojimus teikti savo viešuosius raktus ar sertifikatus pasitikintiems asmenims protingą terminą;

e) TSA turi sunaikinti visus privačius raktus tokiu būdu, kad negalima būtų jų atstatyti.

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

TSA TSPS turi nurodyti atidėjimus padarytus paslaugų teikimo nutraukimo atveju, įskaitant: susijusių asmenų informavimą ir TSA įsipareigojimų perdavimą.

TSA turi atšaukti visus laiko žymos pasirašymui naudojamus sertifikatus.

Laiko žymos paslaugų teikimas nutraukiamas vadovaujantis Lietuvos Respublikos teisės aktais.

3.5.10 Atitikimas teisės aktų reikalavimams

TSA turi užtikrinti procedūrų ir veiklos atitikimą šių teisės aktų reikalavimams:

a) Europos duomenų apsaugos direktyvos reikalavimams;

b) Asmens duomenų teisinės apsaugos įstatymo reikalavimams.

3.5.11 Informacijos apie laiko žymos paslaugų teikimo veiklą kaupimas ir valdymas

TSA turi užtikrinti, kad visa informacija, susijusi su laiko žymos sudarymu ir tvarkymu, būtų registruojama ir archyvuojama TSPS apibrėžtą laikotarpį, kad būtų galima pateikti kaip įrodymo priemonę teisme.

Bendrieji reikalavimai:

a) TSA turi dokumentuoti kokie specifiniai įvykiai ir duomenys bus saugomi ir archyvuojami;

b) turi būti išlaikomas visų įrašų, susijusių laiko žymos teikimo veikla, konfidencialumas ir integralumas;

c) saugomi įrašai, esant būtinybei, gali būti panaudoti kaip teisingos veiklos įrodymai teisme;

d) turi būti dokumentuojamas tikslus pagrindinių TSA atliekamų operacijų laikas (raktų valdymo, laikrodžių sinchronizavimo ir t.t.);

e) pasibaigus TSA raktų galiojimo terminui, archyvuojami įrašai būtų saugomi paslaugų teikimo sąlygose nurodytą laikotarpį;

f) archyvuojami įrašai turi būti apsaugoti nuo ištrynimo ar kito sunaikinimo viso saugojimo laikotarpio metu;

g) visa su laiko žymos abonentais susijusi informacija turi būti konfidenciali, viešai naudoti ją galima tik turint abonento sutikimą.

TSA raktų valdymo reikalavimai:

h) visa informacija susijusi su TSA raktų poros valdymo ciklu turi būti žurnalizuojama ir archyvuojama;

i) visa informacija, susijusi su TSA sertifikatais turi būti žurnalizuojama ir archyvuojama;

TSA laikrodžio sinchronizacijos reikalavimai:

j) visa informacija, susijusi su TSA naudojamo laikrodžio sinchronizacijos su UTC laiku operacijomis, turi būti žurnalizuojama ir archyvuojama. Taip pat, informacija turi būti kaupiama ir apie kalibravimą ar sinchronizavimą TSA laiko žymoms išduoti naudojamų laikrodžių;

k) visi įrašai apie TSA laikrodžių sinchronizacijos sutrikimus turi būti dokumentuojami.

4. ORGANIZACINIAI KLAUSIMAI

TSA turi užtikrinti savo veiklos patikimumą šiomis priemonėmis:

a) TSA turi suteikti laiko žymos teikimo paslaugas visiems prašantiems, kurie patenka į TSA apibrėžtą laiko žymos taikymo sritį ir kurie sutinka su paslaugų teikimo sąlygomis;

b) TSA turi laiko žymos teikimui reikiamas kokybės ir informacijos valdymo sistemas;

c) TSA turi pakankamus resursus padengti savo atsakomybės įsipareigojimus tiekiant laiko žymos paslaugas;

d) TSA finansinis stabilumas ir veiklai reikalingi resursai atitinka šias taisykles;

e) TSA turi pakankamai žmogiškųjų išteklių su reikiamu išsilavinimu, mokymais, techninėmis žiniomis ir patirtimi reikalingų tinkamai teikti laiko žymos paslaugas;

f) TSA turi apibrėžtas procedūras spręsti su laiko žymos teikimo veikla susijusiems ginčams;

g) TSA turi turėti tinkamai teisiškai įformintas subrangos, samdos ir kitas sutartis.

5. TSP ADMINISTRAVIMAS

Šiame skyriuje nustatomi šių TSP administravimo ir priežiūros reikalavimai.

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

Naudotojai turi vadovautis vėliausiai išleista TSP versija.

5.1. TSP keitimo procedūros

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

TSP pakeitimai skirstomi į dvi kategorijas:

a) esminiai pakeitimai, apie kuriuos turi būti pranešama naudotojams ir keičiamas TSP OID;

b) neesminiai pakeitimai, apie kuriuos TSA neprivalo pranešti kitoms šalims, ir TSP OID nėra keičiamas.

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

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

Kitais atvejais pakeitimai yra esminiai ir po kiekvieno TSP pakeitimo keičiamas jų unikalus identifikatorius. Visais atevejais, jei pakeitimai įtakoja laiko žymos paslaugų saugumo lygio pasikeitimus, pakeitimai yra esminiai.

TSP prižiūrimi, keičiami ir tvirtinami laikantis tokios procedūros:

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

b) TSP pakeitimus inicijuoja TSA arba naudotojai;

c) TSA už saugumo politiką atsakingi darbuotojai rengia naują TSP redakciją;

d) Esminių pakeitimų atveju parengtos naujų TSP redakcijos projektas publikuojamas saugykloje internete 30 kalendorinių dienų siekiant gauti susijusių šalių pastabas. Atsižvelgus į per 30 dienų gautas pastabas, arba per 30 dienų negavus pastabų, TSP nauja redakcija teikiama tvirtinti. Neesminių pastabų atveju nauja redakcija teikiama tvirtinti iš karto po rengimo;

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

f) TSP naują redakciją tvirtina Registrų centro direktorius;

g) patvirtinta nauja TSP redakcija patalpinama į saugyklą, kur TSP yra laisvai prieinama visiems asmenims.

6. SĄVOKŲ APIBRĖŽIMAI IR SANTRUMPOS

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

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

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, tvarkymo ir tikrinimo 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.

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

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

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

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

OID – Objekto identifikatorius (*Object identifier*)

OCSP – Tiesioginis sertifikatų būsenos protokolas (*On-line cetificate status protocol*)

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

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

TSPS – Laiko žymos teikimo veiklos nuostatai (*Time stamping practice statement*)

CRL – Atšauktų sertifikatų sąrašas (*Certifcate revocation list*)

RCSC – Registrų centro sertifikavimo centras

UTC – Pasaulinis koordinuotas laikas (*Universal time coordinated*)