



RCSC LAIKO ŽYMOŠ TEIKIMO TAISYKLĖS

Unikalus objekto ID (OID): **1.3.6.1.4.1.30903.1.3.2**
Versija: 2.5
Galioja nuo: 2020-04-23

2020-04-23

TURINYS

1. ĮVADAS	4
1.1. APŽVALGA	4
1.2. IDENTIFIKAVIMAS	5
1.3. NAUDOTOJAI IR TAIKYMO SRITYS.....	6
1.4. ATITIKTIS.....	6
1.5. KONTAKTINĖ INFORMACIJA.....	6
2. BENDROSIOS NUOSTATOS	7
2.1. ĮSIPAREIGOJIMAI	7
2.1.1 <i>Bendri TSA įsipareigojimai</i>	7
2.1.2 <i>TSA įsipareigojimai abonentams</i>	7
2.1.3 <i>Laiko žymos abonentų įsipareigojimai</i>	7
2.1.4 <i>Laiko žymomis pasitikinčių asmenų įsipareigojimai</i>	7
2.2. ATSAKOMYBĖ	8
2.3. MOKESČIAI	8
2.4. INFORMACIJOS TEIKIMAS IR SAUGYKLOS.....	8
2.5. INTELEKTINĖS NUOSAVYBĖS TEISĖS.....	8
3. TSA VEIKLOS REIKALAVIMAI	9
3.1. VEIKLOS NUOSTATAI	9
3.2. LAIKO ŽYMOŠ TEIKIMO SĄLYGŲ SKELBIMAS.....	9
3.3. KRIPTOGRAFINIŲ RAKTŲ VALDYMO CIKLAS	10
3.3.1 <i>TSA kriptografinių raktų generavimas</i>	10
3.3.2 <i>TSA privataus kriptografinio rakto apsauga</i>	11
3.3.3 <i>TSA viešojo kriptografinio rakto skelbimas</i>	11
3.3.4 <i>TSA kriptografinių raktų keitimas (rekey)</i>	11
3.3.5 <i>TSA kriptografinių raktų poros gyvavimo ciklo pabaiga</i>	11
3.3.6 <i>Laiko žymas pasirašančio kriptografinio modulio gyvavimo ciklas</i>	12
3.4. LAIKO ŽYMOŠ SUDARYMAS	12
3.4.1 <i>Laiko žymos</i>	12
3.4.2 <i>Sinchronizacija su UTC</i>	13
3.5. TSA VALDYMAS IR VEIKLA.....	13
3.5.1 <i>Saugumo valdymas</i>	13
3.5.2 <i>Turto inventorizacija ir valdymas</i>	14
3.5.3 <i>Personalo patikimumo kontrolė</i>	14
3.5.3.1 <i>Biografijos tikrinimo procedūra</i>	14
3.5.4 <i>Fizinio saugumo kontrolė</i>	16
3.5.5 <i>Procedūrinio saugumo kontrolė</i>	17
3.5.6 <i>Sistemos prieigos valdymas</i>	18
3.5.7 <i>Patikimų sistemų vystymas ir palaikymas</i>	18
3.5.8 <i>TSA veiklos sukompromitavimas</i>	18
3.5.9 <i>TSA veiklos nutraukimas</i>	19
3.5.10 <i>Atitikimas teisės aktų reikalavimams</i>	20
3.5.11 <i>Informacijos apie laiko žymos paslaugų teikimo veiklą kaupimas ir valdymas</i>	20
4. ORGANIZACINIAI KLAUSIMAI	22
5. TSP ADMINISTRAVIMAS	23
5.1. TSP KEITIMO PROCEDŪROS.....	23
6. SAVOKŲ APIBRĖŽIMAI IR SANTRUMPOS	25

RCSC laiko žymos teikimo taisyklių keitimų istorija:

Versija	Data	Aprašas
0.1	2008-06-07	Projektas
1.0	2008-10-28	Pirma versija
2.0	2017-04-28	Antra versija
2.1	2017-07-11	Neesminiai pakeitimai
2.2	2017-11-08	Pakeitimai
2.3	2017-11-24	Korekciniai pakeitimai
2.4	2019-12-16	Pakeitimai po Lietuvos Respublikos ryšių reguliavimo tarnybos pastabų.
2.5	2020-04-23	Pakeitimai

Dokumento tvirtinimas:

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

1. ĮVADAS

Valstybės įmonė Registrų centras (toliau – Registrų centras) yra įsteigta 1997 m. Įmonės steigėjas – Lietuvos Respublikos Vyriausybė. Įmonės savininko teises ir pareigas įgyvendinanti institucija yra Lietuvos Respublikos teisingumo ministerija. Įmonė tvarko Nekilnojamojo turto kadastrą ir registrą, Adresų registrą, Juridinių asmenų registrą, Gyventojų registrą, Hipotekų registrą, Turto arešto registrą, Testamento registrą, Vedybų sutarčių registrą, Įgaliojimų registrą, Neveiksnių ir ribotai veiksnių asmenų registrą, Sutarčių registrą, kuria, įgyvendina, plėtoja ir tvarko su šiais bei kitais registrais susijusias informacines sistemas, tvarko registrų archyvus. 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 remiantis Lietuvos Respublikos teisės aktais, reglamentuojančiais patikimumo užtikrinimo paslaugų teikimą.

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 1 (vienos) sekundės tikslumo laiko žymas patvirtintas viešojo rakto sertifikatais.

Šios taisyklės paremtos dokumentais:

- a) ETSI EN 319 421 v1.1.1: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;
- b) ETSI EN 319 422 v1.1.1 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and electronic time-stamp token profiles;
- c) RFC 3628;
- d) RFC 3161;
- e) Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymo naujausia redakcija;

- f) Europos parlamento ir tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB naujausia redakcija;
- g) Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2018 m. spalio 26 d. įsakymas Nr. 1V-1055 „Dėl asmens tapatybės ir papildomų specifinių požymių tikrinimo išduodant kvalifikuotus elektroninio parašo, elektroninio spaudo, interneto svetainės tapatumo nustatymo sertifikatus tvarkos aprašo patvirtinimo“;
- h) Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2019 m. birželio 4 d. įsakymas Nr.1V-594 „Dėl Pranešimų apie patikimumo užtikrinimo paslaugų saugumo ir (ar) vientisumo pažeidimus teikimo tvarkos aprašo patvirtinimo“.

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:

1.3.6.1.4.1.30903.1.3.2

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

Lentelė Nr. 1. TSP unikalios 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	2

Naujausia TSP versija pateikiama valstybės įmonės Registrų centro Sertifikatų centro saugykloje (*repository*).

1.3. Naudotojai ir taikymo sritys

Šios taisyklės skirtos tenkinti laiko žymų, skirtų užtikrinti kvalifikuotų elektroninių parašų ilgalaikį galiojimą, reikalavimus (pagal Europos Sąjungos bei nacionalinius teisės aktus). 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, vadovaujantis CP ir CPS. 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 priimti visus įsipareigojimus, apibrėžtus 2.1 skyriuje ir įgyvendinti visus 3 skyriuje nustatytus reikalavimus veiklai.

1.5. Kontaktinė informacija

Šias TSP tvarko RCSC, kurios kontaktiniai duomenys nurodyti žemiau (*Lentelė Nr. 2*).

Lentelė Nr. 2. RCSC kontaktinė informacija

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

2. BENDROSIOS NUOSTATOS

Šiame skyriuje pateikiami TSA ir su juo susijusių šalių įsipareigojimai ir nuostatos teisiniais bei 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. Detalus funkcijų bei atsakomybės pasiskirstymas, kuomet dalis TSA teikiamų paslaugų ar procedūrų perduodamos subrangovams, aprašytas sudaromose sutartyse.

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 priimtų 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 ar sutartyse su paslaugų teikėju.

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 atlygina padarytą žalą abonentams Lietuvos Respublikos įstatymų nustatyta tvarka.

TSA gali atsisakyti arba apriboti bet kokią atsakomybę, susijusią su laiko žymos teikimu, jeigu tai neprieštaruoja 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 pasiekama 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 įsipareigojimų;
- 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 tinkamos formos pranešimą apie pakeitimus numatomus atlikti TSPS ir juos patvirtinus (punktas f) nedelsiant pateikti abonentams ir pasitikinčioms šalims (punktas d). Pranešimai teikiami vadovaujantis TSP 5.1 skyriaus nuostatomis.

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 ne žemesnį EAL 4 ar aukštesnio lygio standartą pagal ISO/IEC 15408 ar lygiaverčius nacionaliniu arba tarptautiniu mastu pripažintus IT saugumo vertinimo kriterijus; arba ISO/IEC 19790 ar FIPS PUB 140-2 3 lygio reikalavimus.
- 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 EAL 4 ar aukštesnio lygio standartą pagal ISO/IEC 15408 ar lygiaverčius nacionaliniu arba tarptautiniu mastu pripažintus IT saugumo vertinimo kriterijus; arba ISO/IEC 19790 ar FIPS PUB 140-2 3 lygio reikalavimus;
- b) TSA privatusis raktas gali būti atstatomas ir jo kopijos saugomos tik naudojantis su kriptografinė technine įranga susietomis sistemėmis 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 (du) 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 parametru 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 privatus 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 (dviejų) 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. Laikos žymos sudarymas

3.4.1 Laikos 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 (vienos) 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 (pasauliniu koordinuotu laiku) deklaruojamu tikslumu. TSA tam pasiekti užtikrina, jog:

- a) TSA naudojami laikrodžiai turi būti kalibruojami taip, kad nenukryptų nuo apibrėžto tikslumo;
- b) laikrodžiai turi būti apsaugoti nuo grėsmių, galinčių sukelti nenustatytus laiko vertės pakeitimus ne kalibravimo metu;
- c) bus pastebėti bet kokie laikrodžių sinchronizacijos su UTC poslinkiai ar nukrypimai;
- d) TSA turi užtikrinti, kad laikrodžių sinchronizacija bus vykdoma korekcinės sekundės (UTC laiko korekcija pridedant ar atimant 1 (vieną) 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 trečiosioms šalims, tačiau trečiųjų šalių atsakomybė visais atvejais aiškiai apibrėžta sudaromose sutartyse. Taip pat numatytos ir įsipareigojimų įvykdymo 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 patikimumo kontrolė

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

- a) Mokėti lietuvių kalbą;
- b) Turėti reikalingą išsilavinimą arba kvalifikaciją;
- c) Mokėti dirbti kompiuteriu ir kita organizacine technika;
- d) Mokėti užsienio kalbą (jeigu reikalinga).

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

- e) sudarantys ir tvarkantys sertifikatus turi aukštąjį išsilavinimą;
- f) yra pasirašę susitarimą dėl pareigų vykdymo ir atsakomybės;
- g) yra išklauseę vidinius mokymus, susijusius su jiems pavestų pareigų vykdymu;
- h) yra išklauseę mokymus, susijusius su asmens duomenų ir konfidencialios informacijos apsauga, susipažinę su saugos dokumentais bei yra pasirašę pasižadėjimą dėl konfidencialios informacijos saugojimo jog yra susipažinę su saugos dokumentais.

3.5.3.1 Biografijos tikrinimo procedūra

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

- a) Asmens tapatybę patvirtinantį dokumentą;
- b) Valstybinio socialinio draudimo pažymėjimą;
- c) Teistumo (neteistumo) pažymą¹;

¹ Pagal Valstybės įmonės Registrų centro generalinio direktoriaus 2019 m. rugpjūčio 30 d. įsakymą Nr. VE-421 (1.3 E) „Dėl Korupcijos prevencijos priemonių įgyvendinimo tvarkos aprašo ir Pareigybių, tikrinamų valstybės

- d) Išsilavinimą, profesinį parengimą patvirtinančius dokumentus;
- e) Gyvenimo aprašymą;
- f) Privalomojo sveikatos patikrinimo medicininę pažymą;
- g) Neįgalaus asmens pažymėjimą, jei turi;
- h) Vaiko (-ų) gimimo liudijimą (-us);
- i) Santuokos ar ištuokos liudijimą.

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

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

- a) 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;
- b) 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;
- c) 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:

- d) vadovaujantis personalas turi:
 - išmanyti laiko žymos technologijas;
 - išmanyti elektroninio 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.

- e) TSA personalas, užimantis ypatingo pasitikėjimo reikalaujančias pareigas, neturi būti paveikiamas bet kokių interesų konfliktų, galinčių paveikti TSA operacijų objektyvumą;
- f) ypatingo pasitikėjimo pareigos apima pareigas kurios apima šias atsakomybės sritis:
 - o saugumo pareigūnai – bendra atsakomybė už saugumo politikos vykdymą;
 - o sistemos administratoriai – įgalioti instaliuoti, konfigūruoti ir palaikyti TSA sistemas naudojamas laiko žymų valdymui;
 - o sistemos operatoriai – atsakingi už kasdienį TSA sistemų naudojimą. Įgalioti atlikti sistemos atsargines kopijas bei atkūrimą;
 - o sistemos auditoriai – įgalioti peržiūrėti TSA patikimumo sistemų archyvus bei audito įrašus.
- g) į ypatingo pasitikėjimo TSA pareigas, darbuotojai skiriami vadovybės, atsakingos už saugumą, sprendimu;
- h) 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 griūčių, apipylimo, potvynio, kitų nelaimingų atsitikimų ir vagysčių, bei atstatymo priemonės;

- 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 monitoringą, 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 incidentus informuojama vadovaujantis Europos parlamento ir tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB 19 str. 2 d. bei nacionalinės teisės aktais.
- 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 stebėseną, įvykių analizę ir veiksmus, 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. Informacija pranešama vadovaujantis Europos parlamento ir tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB 19 str. 2 d. bei nacionalinės teisės aktais.

TSA turi turėti atstatymo veiksmų planą kaip elgtis privataus rakto sukompromitavimo, galimo sukompromitavimo ar TSA laikrodžio kalibravimo neatitikimo atvejais. Minėtais TSA veiklos sukompromitavimo atvejais, vadovaujamosi bendru veiklos nutraukimo planu bei CPS detalizuotais veiksmais.

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 visomis įmanomomis priemonėmis 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) Ne vėliau kaip prieš 3 (tris) mėnesius iki veiklos nutraukimo dienos informuoti priežiūros įstaigą apie numatomą veiklos nutraukimą ir ne vėliau kaip prieš 1 (vieną) mėnesį informuoti visus laiko žymos abonentus, pasitikinčius asmenis bei patikimumo užtikrinimo paslaugų priežiūros įstaigą apie laiko žymos paslaugų teikimo nutraukimą;
- b) TSA turi nutraukti bendradarbiavimą su visais laiko žymos paslaugų teikimo subkontraktorais;
- c) TSA per 1 (vieną) mėnesį turi perduoti visus įsipareigojimus, susijusius su įvykiu žurnalizavimu ir audito archyvais, patikimam veiklos perėmėjui ar priežiūros įstaigai 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 numachiusi lėšų šiems įsipareigojimams įvykdyti, jei bankrutuotų ar kitais nemokumo atvejais. TSA draudžia savo civilinę atsakomybę ne mažesne kaip patikimumo užtikrinimo paslaugų priežiūros įstaigos nustatyta suma.

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 elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymo naujausioje redakcijoje numatyta tvarka bei sąlygomis.

3.5.10 Atitikimas teisės aktų reikalavimams

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

- a) Europos duomenų apsaugos direktyvos naujausios redakcijos reikalavimams;
- b) Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo naujausios redakcijos reikalavimams;
- c) Lietuvos Respublikos elektroninio elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymo naujausios redakcijos reikalavimams;
- d) Europos parlamento ir tarybos reglamento Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB 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 abonto 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 TSP redakcijos, kurios OID nurodytas elektroninėje laiko žymoje, vėliausiai išleista 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 atvejais, 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 (vienerius) 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 (trisdešimt) kalendorinių dienų siekiant gauti susijusių šalių pastabas. Atsižvelgus į per 30 (trisdešimt) dienų gautas pastabas, arba per 30

(trisdešimt) 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. SAŲOKŲ 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 – privatesiems ir viešiesiems raktams generuoti, saugoti ir/arba elektroniniams parašams kurti.

Atšauktų sertifikatų/ spaudų sąrašas (*CRL – Certificate/ Seal Revocation List*) – sertifikavimo centro periodiškai (arba neatidėliotinai) leidžiamas, jo pasirašomas sąrašas sertifikatų/ spaudų, kurių galiojimas nutrauktas ar sustabdytas. Tokiame sąrašė paprastai nurodomas jį sudariusio sertifikavimo centro vardas, sąrašo sudarymo data, numatoma kitos sąrašo versijos išleidimo data, nebegaliojančių sertifikatų/ spaudų 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 taisyklės renkasi laiko žymos naudotojai ir įgyvendina paslaugų teikėjas.

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

Pasitikinčios šalys (*relying parties*) – 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 – pasaulinis koordinuotasis laikas. Tarptautinių mastu valdoma, vieninga atominių laikrodžių sistema.

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

CP - Kvalifikuotų sertifikatų/ spaudų taisyklės (*Qualified Certificate/ Seal Policy*)

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

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

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

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

OCSP – Tiesioginis sertifikatų/ spaudų būsenos protokolas (*On-Line Certificate/ Seal Status Protocol*)

OID – Objekto identifikatorius (*Object Identifier*)

RCSC – Registrų centro sertifikavimo centras

TSA – Laiko žymų teikimo tarnyba (*Time-Stamping Authority*)

TSP – Laiko žymų teikimo taisyklės (*Time-Stamping Policy*)

TSPS – Laiko žymų teikimo veiklos nuostatai (*Time-Stamping Practice Statement*)

UTC – Pasaulinis koordinuotas laikas (*Coordinated Universal Time*)