# BALTSTAMP
# LAIKO ŽYMŲ TEIKIMO VEIKLOS NUOSTATAI

Unikalus objekto ID (OID): **1.3.6.1.4.1.38424.1.4.1**
Versija: 1.1

Galioja nuo 2013-02-06

**2013**

# TURINYS


1 ĮVADAS ....4
1.1 Apžvalga ....4
1.2 Identifikavimas ....4
1.3 Laiko žymų naudotojai ir taikymo sritys ....5
1.4 Atitiktis. Jos patvirtinimas ir tikrinimas ....5
1.5 Kontaktinė informacija ....5
2 ĮSIPAREIGOJIMAI IR ATSAKOMYBĖ ....5
2.1 TSA įsipareigojimai ....5
2.1.1 Bendroji dalis ....5
2.1.2 TSA įsipareigojimai abonentams ....6
2.2 Laiko žymų abonentų įsipareigojimai ....6
2.3 Laiko žymomis pasitikinčių asmenų įsipareigojimai ....6
2.4 Atsakomybė ....6
2.5 Teisinės nuostatos ir interpretavimas ....6
2.5.1 Pagrindiniai teisės aktai ....6
2.5.2 Ginčų sprendimo tvarka ....7
2.6 Mokesčiai ....7
2.7 Intelektinės nuosavybės teisės ....7
3 TSA VEIKLA ....7
3.1 Veiklos nuostatai ir laiko žymų teikimo sąlygos ....7
3.1.1 Laiko žymų tarnybos veiklos nuostatai ....7
3.1.2 Laiko žymų teikimo sąlygos ....7
3.2 Raktų valdymo ciklas ....8
3.2.1 TSA raktų generavimas ....8
3.2.2 Privačiųjų TSU raktų apsauga ....8
3.2.3 TSU viešojo rakto skelbimas ....9
3.2.4 TSU kriptografinių raktų keitimas ....9
3.2.5 TSU kriptografinių raktų poros gyvavimo ciklo pabaiga ....9
3.2.6 Kriptografinio modulio gyvavimo ciklo valdymas ....9
3.3 Laiko žymų teikimas ....10
3.3.1 Laiko žyma ....10
3.3.2 Laikrodžių sinchronizavimas su UTC ....11
3.4 TSA darbas ir jo vadyba ....11
3.4.1 Saugumo vadyba ....11
3.4.2 Išteklių klasifikavimas ir vadyba ....12
3.4.3 Paslaugų saugumas personalo atžvilgiu ....12
3.4.4 Fizinis ir aplinkos saugumas ....13
3.4.5 Darbo tvarkymas ....14
3.4.6 Prieigos prie sistemos tvarkymas ....15
3.4.7 Patikimųjų sistemų įdiegimas ir priežiūra ....15
3.4.8 TSA paslaugų sukompromitavimas ....15
3.4.9 TSA veiklos nutraukimas ....16
3.4.10 Teisinių reikalavimų vykdymas ....16
3.4.11 Informacijos apie TSA darbą kaupimas ....17
3.5 Organizaciniai dalykai ....17
4 TEKSTE VARTOJAMOS SĄVOKOS IR SANTRUMPOS ....18
5 NUORODOS ....19

BalTstamp laiko žymų teikimo veiklos nuostatų istorija:

| Versija | Data | Aprašas |
|---|---|---|
| Versija 0.1 | 2011-04-11 | Pirmoji projekto versija |
| Versija 1.0 | 2011-04-20 | Pirma versija |
| Versija 1.1 | 2013-02-01 | Pakoreguota pirma versija |

BalTstamp laiko žymų teikimo veiklos nuostatų tvirtinimas:

| Dokumento rengimas | Vardas, pavardė | Data | Parašas |
|---|---|---|---|
| Dokumentą parengė | Emilis Urba | 2013-01-28 | |
| Dokumentą patikrino | Rimantas Miškinis | 2013-01-31 | |
| Dokumentą patvirtino | Vincentas Vitkauskas | 2013-02-01 | |

# 1 ĮVADAS

Uždaroji akcinė bendrovė „BalTstamp“ (toliau – BalTstamp) įsteigta 2011 m. sausio 31 d. tiksline paskirtimi teikti kvalifikuotų laiko žymų paslaugas juridiniams ir fiziniams asmenims siekiant užtikrinti kvalifikuotų elektroninių parašų galiojimą per visą elektroninių dokumentų, kuriuose panaudoti kvalifikuoti elektroniniai parašai, gyvavimo ciklą. Informacija apie BalTstamp teikiama interneto svetainėje adresu http://www.baltstamp.lt

## 1.1 Apžvalga

BalTstamp laiko žymų taisyklės (angl. TSP – *time stamp policy*) nustato BalTstamp laiko žymų tarnybos (toliau – TSA, pagal anglišką atitikmenį *time stamp authority*) darbo tvarką ir reikalavimus (taip pat ir saugumo reikalavimus), kurių laikomasi formuojant ne blogesnio kaip dviejų dešimtųjų sekundės tikslumo laiko žymas, patvirtintas viešojo rakto sertifikatais.

TSP išdėstyti reikalavimai nesusieti su konkrečiais technologiniais sprendimais ar TSA organizacine struktūra. TSP reikalavimų įgyvendinimo techniniai sprendimai, procedūros ir personalo politika aprašyta šiuose BalTstamp laiko žymų teikimo veiklos nuostatuose (toliau – TSPS, pagal anglišką atitikmenį *time stamping practice statement*).

TSPS remiasi šiais teisės ir norminiais dokumentais:

a) Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2011 m. balandžio 19 d. įsakymu Nr.1V-407 „Laiko žymos formavimo paslaugų teikimo tvarka“ (Žin., 2011, Nr.48-2349);

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

c) standartu LST ETSI TS 101 861 „Laiko žymėjimo profilis“.

TSA, teikdama laiko žymų paslaugas, vykdo laiko žymos sudarymo ir valdymo funkcijas.

*Pastaba dėl sąvokų*. Čia ir toliau tekste minima TSA reiškia BalTstamp TSA; TSP reiškia BalTstamp TSP; TSPS reiškia BalTstamp TSPS ir t.t. Tai yra, viskas, apie ką kalbama, taikytina BalTstamp TSA ir tik jai.

## 1.2 Identifikavimas

Šių TSPS unikalus identifikatorius (OID) yra **1.3.6.1.4.1.38424.1.4.1**; jo laukų reikšmės nurodytos *lentelėje* ***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 |
| Uždaroji akcinė bendrovė „BalTstamp“ | 38424 |
| Padalinys BalTstamp | 1 |

| | |
|---|---|
| Dokumento tipas (laiko žymų teikimo veiklos nuostatai) | 4 |
| Dokumento versija | 1 |

Galiojanti TSPS versija skelbiama interneto svetainėje http://www.baltstamp.lt/

### 1.3 Laiko žymų naudotojai ir taikymo sritys

TSA sudaryta laiko žyma galima paženklinti saugų elektroninį parašą, sukurtą saugia parašo formavimo įranga ir patvirtintą galiojančiu kvalifikuotu sertifikatu, o kartu ir pasirašytus duomenis. Prireikus tai leistų įrodyti, kad elektroninis parašas buvo sukurtas iki žymoje nurodyto laiko. Tačiau laiko žyma galima paženklinti ir nepasirašytus duomenis. Tokia laiko žyma patvirtina, kad duomenys buvo paženklinti laiko žymoje nurodytu laiku, bet nepatvirtina duomenų autorystės. TSA teikiamų laiko žymų naudotojai gali būti fiziniai ir juridiniai asmenys, kuriems reikalingos TSA teikiamos laiko žymos.

TSP bei TSPS nenustato jokių laiko žymų naudojimo apribojimų. Laiko žymas galima naudoti pasirašant ir vykdant elektroninius sandorius, pateikiant prašymus bei pasiūlymus, archyvuojant elektroninius dokumentus ir t.t.

TSA gali teikti viešąsias paslaugas, tačiau taip pat gali aptarnauti ir uždarąsias naudotojų grupes.

### 1.4 Atitiktis. Jos patvirtinimas ir tikrinimas

TSA, įrašydama sukurtose laiko žymose TSP unikalų identifikatorių pažymi, kad laiko žyma atitinka TSP ir TSPS. Taip TSA prisiima visus TSP nustatytus įsipareigojimus ir pagal šiuos TSPS vykdo visus TSP reikalavimus veiklai.

Kaip TSA veikla atitinka TSP ir TSPS, tikrinama TSA nustatyta vidaus tvarka.

### 1.5 Kontaktinė informacija

Šiuos TSPS tvarko uždaroji akcinė bendrovė „BalTstamp“. UAB BalTstamp kontaktiniai duomenys pateikti *lentelėje **Nr. 2:***

*Lentelė Nr. 2. TSA kontaktinė informacija*

| | |
|---|---|
| **TSA:** | Uždaroji akcinė bendrovė „BalTstamp“ |
| **Adresas:** | Dariaus ir Girėno g. 40, LT-02189 Vilnius |
| **Tel.:** | +370-5-216 72 11 |
| **Faksas:** | +370-5-216 72 12 |
| **URL:** | http://www.baltstamp.lt |
| **El. paštas:** | info@baltstamp.lt |

## 2 ĮSIPAREIGOJIMAI IR ATSAKOMYBĖ

### 2.1 TSA įsipareigojimai

#### 2.1.1 Bendroji dalis

TSA užtikrina TSP reikalavimų tinkamą įgyvendinimą. TSA užtikrina, kad būtų laikomasi:

a) procedūrų, nurodytų šiuose TSPS, įskaitant ir Fizinių ir technologijos mokslų centro (FTMC) Metrologijos skyriaus Laiko ir dažnio etalono laboratorijos (LDEL) teikiamas laiko žymų komponenčių formavimo ir generuojamų laiko žymų metrologinės sieties su

Pasaulio suderintojo laiko skale UTC paslaugas pagal šių nuostatų reikalavimus;

b) visų papildomų įsipareigojimų, tiesiogiai ar nuorodomis nurodytų laiko žymoje, laikymąsi.

### 2.1.2 TSA įsipareigojimai abonentams

TSA vykdo savo įsipareigojimus, nurodytus savo paskelbtose laiko žymų teikimo sąlygose, įskaitant paslaugų prieinamumą ir tikslumą.

## 2.2 Laiko žymų abonentų įsipareigojimai

Abonentas, gavęs laiko žymą, turėtų patikrinti, ar ji pasirašyta teisingai ir ar laiko žymos pasirašymo privatus raktas galioja ir nebuvo sukompromituotas.

Jei laiko žyma tikrinama, kol galioja TSU sertifikatas, pasirašymo rakto galiojimą galima patikrinti, įsitikinus, kad TSU sertifikatas nėra atšauktas. Tačiau jei tikrinimo metu atitinkamo sertifikato galiojimas jau yra pasibaigęs, laiko žymos patikrinti dažnai nebebūna galima, nes CA neįsipareigoja skelbti duomenų apie nebegaliojančio sertifikato atšaukimą, įskaitant atšaukimą dėl rakto sukompromitavimo. Vis dėlto laiko žymą galima patikrinti ir pasibaigus TSU sertifikato galiojimui, jei tikrinimo metu galima sužinoti, ar:

a) iki laiko žymos tikrinimo laiko nebuvo sukompromituotas TSU privatusis raktas;

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

c) parašo algoritmas ir parašo rakto ilgis, kuriais naudojantis buvo pasirašyti laiko žymos duomenys, tikrinimo metu tebėra technologiškai patikimi ir nepasiekiami kriptografinėms atakoms.

*Pastaba dėl sąvokų*: privatųjį raktą TSA naudoja tik laiko žymoms pasirašyti ir niekam daugiau; laiko žymos pasirašomos laiko žymų įrenginyje (toliau – TSU, pagal anglišką atitikmenį *time-stamping unit*). Todėl čia ir kitur vartojamos iš [ETSI 1] perimtos sąvokos *privatusis raktas*, *pasirašymo (parašo) raktas*, *TSU pasirašymo raktas*, *TSU privatusis pasirašymo raktas* yra tapačios.

## 2.3 Laiko žymomis pasitikinčių asmenų įsipareigojimai

Laiko žymomis pasitikintis asmuo, pasikliaudamas laiko žyma, privalo patikrinti, ar paslaugų teikėjas laiko žymą pasirašė teisingai ir ar privatusis raktas, kuriuo buvo pasirašyta, iki tikrinimo laiko nebuvo sukompromituotas (atskleistas tretiesiems asmenims ar dėl kitų priežasčių tapęs netinkamu naudoti).

Be to, laiko žymomis pasitikintys asmenys privalo laikytis TSP nurodytų laiko žymos naudojimo apribojimų (jei jų būtų) ir bet kurių kitų atsargumo priemonių.

## 2.4 Atsakomybė

TSA atsakomybė ir įsipareigojimai išdėstyti sudarytose paslaugų teikimo sutartyse.

## 2.5 Teisinės nuostatos ir interpretavimas

### 2.5.1 Pagrindiniai teisės aktai

Laiko žymų formavimą, teikimą, reikalavimus teikėjams bei atsakomybę reglamentuoja:

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

b) Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2011 m. balandžio 19 d. įsakymas Nr. 1V-407 „Laiko žymos formavimo paslaugų teikimo tvarka“ (Žin., 2011, Nr. 48-2349).

### 2.5.2 Ginčų sprendimo tvarka

Visi ginčai tarp TSA ir abonentų sprendžiami geranoriškomis derybomis. Ginčo neišsprendus, kreipiamasi į Lietuvos Respublikos teisėsaugos institucijas.

## 2.6 Mokesčiai

TSA gali nustatyti laiko žymų paslaugų kainas.

## 2.7 Intelektinės nuosavybės teisės

Cituojant bet kokią TSA dokumentaciją, reikia pateikti nuorodą į jos šaltinį.

# 3 TSA VEIKLA

## 3.1 Veiklos nuostatai ir laiko žymų teikimo sąlygos

### 3.1.1 Laiko žymų tarnybos veiklos nuostatai

TSA užtikrina, kad jos patikimumas būtų pakankamas laiko žymų paslaugoms teikti. Būtent:

a) TSA yra atlikusi rizikos įvertinimą, siekdama įvertinti verslo išteklius bei jiems kylančias grėsmes, kad būtų galima numatyti reikiamas saugumo priemones ir darbines procedūras;

b) šiuose veiklos nuostatuose yra aprašytos praktikos ir procedūros, naudojamos TSP nustatytiems reikalavimams įvykdyti;

c) juose taip pat nustatyti visų išorės organizacijų, palaikančių TSA paslaugas, įsipareigojimai, įskaitant taikytinas taisykles ir nuostatus;

d) TSA veiklos nuostatai ir kita reikiama dokumentacija yra prieinama laiko žymų abonentams ir pasitikintiems asmenims, kas leistų įvertinti, kaip ši dokumentacija atitinka TSP;

e) visiems savo abonentams ir galimiems pasitikintiems asmenims TSA pateikia naudojimosi laiko žymų paslaugomis sąlygas, kaip nurodyta [ETSI 1] 7.1.2 str.;

f) TSA turi aukšto lygio vadovybę, turinčią įgaliojimus TSA veiklos nuostatams patvirtinti;

g) vyresnioji TSA vadovybė užtikrina, kad šie veiklos nuostatai būtų tinkamai vykdomi;

h) TSA yra nustačiusi šių savo veiklos nuostatų peržiūros tvarką, taip pat ir atsakomybę už jų priežiūrą;

i) TSA praneša apie numatomus veiklos nuostatų pakeitimus, o juos patvirtinusi atnaujintus nuostatus nedelsdama padaro prieinamus abonentams ir pasitikintiems asmenims.

### 3.1.2 Laiko žymų teikimo sąlygos

TSA visiems savo abonentams, o taip pat potencialiems laiko žymomis pasitikintiems asmenims skelbia laiko žymų teikimo sąlygas.

Laiko žymų teikimo sąlygose TSA teikia tokius duomenis:

a) kontaktinę TSA informaciją;

b) taikomas TSP;

c) bent vieną santraukos *(hash)* sudarymo algoritmą, kurį galima pritaikyti duomenų, kuriems teikiama laiko žyma, santraukai sudaryti;

d) parašo, naudojamo laiko žymai pasirašyti, tikėtiną gyvavimo trukmę (ji gali priklausyti nuo privačiojo rakto ilgio, santraukos bei pasirašymo algoritmų);

e) laiko žymose nurodomo laiko tikslumą UTC atžvilgiu;

f) laiko žymos paslaugų naudojimo apribojimus, jei tokių būtų;

g) abonentų įsipareigojimus, kaip aprašyta [ETSI 1] 6.2 skyriuje;

h) laiko žymomis pasitikinčiųjų asmenų įsipareigojimus, kaip aprašyta [ETSI 1] 6.3 skyriuje;

i) informaciją, kaip patikrinti laiko žymą, kad laiko žymomis pasitikintieji asmenys galėtų jomis pasitikėti pagrįstai (žiūr. [ETSI 1] 6.3 skyrių), ir laiko žymų galiojimo trukmės apribojimus (jei tokių būtų);

j) kiek laiko saugomi sukaupti įrašai apie įvykius;

k) nuorodą į taikomą šalies teisę, įskaitant teiginį, kad laikomasi Lietuvos Respublikos teisės aktų reikalavimų laiko žymų atžvilgiu;

l) atsakomybės apribojimus;

m) ginčų ir nesutarimų sprendimo tvarką;

n) įvertinimą, kaip TSA veikla atitinka TSP.

Šie duomenys teikiami naudotojui suprantama kalba interneto svetainėje http://www.baltstamp.lt/. Atsiradus pasikeitimų, svetainės turinys atnaujinamas nedelsiant.

## 3.2 Raktų valdymo ciklas

### 3.2.1 TSA raktų generavimas

Savo kriptografinius raktus TSA generuoja esant kontroliuojamoms sąlygoms. Būtent:

a) TSU pasirašymo raktą kriptografiniame modulyje fiziškai saugioje aplinkoje (patalpoje, apsaugotoje nuo neįgaliotų asmenų prieigos) generuoja darbuotojai, einantys pasitikėjimo pareigas, esant bent dvigubai kontrolei (žiūr. [ETSI 1] 7.4.3 str.). Šią funkciją vykdyti įgaliojami tik tie asmenys, kuriems tai priklauso daryti pagal pareiginius nurodymus.

b) kriptografinis modulis, kuriame generuojamas TSU pasirašymo raktas, tenkina trečiojo lygio saugumo reikalavimus pagal standartą [FIPS 1];

c) TSU raktų generavimo algoritmas, gaunamo pasirašymo rakto ilgis bei pasirašymo algoritmas, naudojamas laiko žymoms pasirašyti, yra pripažinti tinkamais laiko žymoms, kokias teikia TSA, t.y. rakto ilgis – 2048 bitai, pasirašymo algoritmas – RSA.

### 3.2.2 Privačiųjų TSU raktų apsauga

TSA užtikrina savo TSU privačiųjų raktų apsaugą ir slaptumą. Būtent:

a) TSU privatieji pasirašymo raktai yra generuojami, laikomi ir naudojami kriptografiniame modulyje, kuris tenkina trečiojo lygio saugumo reikalavimus pagal standartą [FIPS 1];

b) TSU privačiojo rakto atsarginės kopijas fiziškai saugioje aplinkoje (patalpoje, apsaugotoje nuo neįgaliotų asmenų prieigos) kopijuoja, saugo ir atkuria tik pasitikėjimo

pareigas einantys darbuotojai, esant bent dvigubai kontrolei (žiūr. [ETSI 1] 7.4.4 str.). Šią funkciją vykdyti įgaliojami tik tie asmenys, kuriems priklauso tai daryti pagal pareiginius nurodymus;

c) kiekvienos TSU privačiojo rakto kopijos konfidencialumas yra kriptografiškai apsaugotas prieš jai patenkant į kriptografinio įrenginio išorę saugojimui.

### 3.2.3 TSU viešojo rakto skelbimas

TSA užtikrina, kad TSU parašo tikrinimo (viešieji) raktai ir visi susiję parametrai išliktų autentiški ir nepakitę, juos perduodant pasitikintiems asmenims.

Būtent:

a) TSU parašo tikrinimo (viešasis) raktas pasitikintiems asmenims skelbiamas viešojo rakto sertifikate;

b) TSU naudoja parašo tikrinimo (viešojo) rakto sertifikatą, išduotą sertifikavimo tarnybos, užtikrinančios ne žemesnį saugumo lygį nei aprašytas šiais nuostatais įgyvendinamose TSP.

### 3.2.4 TSU kriptografinių raktų keitimas

TSU sertifikato galiojimo trukmė nustatoma ne ilgesnė nei tas laikas, per kurį pasirinktas algoritmas ir rakto ilgis gali būti laikomi tinkamu naudoti:

- RSA 2048 bitų raktams – iki 2025 metų pabaigos.

TSU raktų poros galiojimo laikotarpis yra prilyginamas TSU sertifikato galiojimo laikotarpiui. TSU sertifikato keitimas, išlaikant tą pačią raktų porą, netaikomas.

### 3.2.5 TSU kriptografinių raktų poros gyvavimo ciklo pabaiga

TSA užtikrina, kad TSU privatieji pasirašymo raktai nebūtų naudojami pasibaigus jų gyvavimo laikotarpiui. Būtent:

a) TSA turi procedūras, pagal kurias privatus raktas, pasibaigus jo galiojimui, pakeičiamas nauju, t.y. darbuotojai, kurių pareiginėse instrukcijose tai numatyta, seka ir užtikrina, kad raktai, kurie pagal žurnalo, sertifikato arba jo atšaukimo duomenis tapo nebegaliojantys, nebebūtų naudojami. Atėjus galiojimo laiko pabaigai, šie darbuotojai negrįžtamai ištrina privatųjį raktą iš kriptografinio modulio, o taip pat visas kopijas iš žurnale nurodytų laikmenų. Tai atlikę, dar kartą įsitikina, kad privačiojo rakto nebegalima atkurti netgi specialiomis ištrintų bylų atkūrimo programomis. Laikmenas, iš kurių negalima saugiai ištrinti duomenų, sunaikina fiziškai. Tuomet generuoja ir įdiegia naują raktų porą kaip jau aprašyta skyrelyje 3.2.1 TSA raktų generavimas;

b) TSU privatieji pasirašymo raktai bei jų dalys su visomis kopijomis sunaikinami, kad privačiųjų raktų nebebūtų galima atkurti;

c) laiko žymų generavimo sistema atmeta bet kokius mėginimus suteikti laiko žymą, jei pagal sistemos konfigūraciją privatusis pasirašymo raktas nebegalioja.

### 3.2.6 Kriptografinio modulio gyvavimo ciklo valdymas

TSA užtikrina kriptografinės įrangos saugumą viso jos gyvavimo ciklo metu.

Būtent, TSA užtikrina, kad:

a) laiko žymas pasirašanti kriptografinė įranga nebūtų sugadinta ar kitaip paveikta pristatymo (transportavimo) metu;

b) laiko žymas pasirašanti kriptografinė įranga nebūtų sugadinta ar kitaip paveikta saugojimo metu;

c) TSU pasirašymo raktų įdiegimas, aktyvavimas ir kopijavimas kriptografinėje įrangoje būtų atliekamas tik darbuotojų, kuriems patikėtos pasitikėjimo pareigos, esant mažiausiai dvigubai kontrolei, fiziškai saugioje aplinkoje;

d) laiko žymas pasirašanti kriptografinė įranga tinkamai funkcionuotų;

e) TSU kriptografiniame modulyje saugomi TSU privatūs pasirašymo raktai būtų ištrinti, pasibaigus modulio naudojimo laikui;

f) kriptografinio modulio gyvavimo ciklo yra registruojami ir reguliariai peržiūrimi šie įvykiai:

- kriptografinio modulio aktyvavimas;
- konfigūracijos keitimas;
- įjungimas ir išjungimas;
- raktų generavimas;
- raktų naikinimas.

## 3.3 Laiko žymų teikimas

### 3.3.1 Laiko žyma

TSA užtikrina, kad laiko žymos būtų teikiamos saugiai ir kad jose būtų nurodyta teisinga data bei paros laiko vertė. Būtent:

a) laiko žymoje yra nurodytas TSP identifikatorius;

b) kiekviena laiko žyma turi savo unikalų identifikatorių;

c) TSU naudojamas laikas yra susietas su laiku UTC(LT);

d) laiko žymoje nurodyta laiko vertė gali skirtis nuo UTC ne daugiau nei nurodyta šiose TSP;

e) užfiksavus, kad TSU laikrodis nukrypo nuo paskelbto tikslumo (žiūr. [ETSI 1] 7.3.2 str. c), laiko žymos neteikiamos;

f) laiko žymoje yra ja tvirtinamų duomenų santrauka *(hash)*, kaip ji pateikta užsakovo;

g) laiko žyma yra pasirašyta raktu, sukurtu tik šiam tikslui ir nenaudojamu niekam kitam;

h) laiko žymoje yra:

- šalies, kurioje įkurta TSA, t.y., Lietuvos, identifikatorius;
- TSA identifikatorius;
- įrenginio, išdavusio laiko žymą, identifikatorius.

Laiko žymos sandara atitinka [ETSI 2] reikalavimus.

BalTstamp TSA laiko žymos sandara, laukų pavadinimai ir jų reikšmės pateikiami *lentelėje* ***Nr.3:***

*Lentelė Nr. 3. TSA laiko žymos sandara*

| Pavadinimas | Reikšmė |
|---|---|
| version | 1 |
| policy | 1.3.6.1.4.1.38424.1.3.1 |
| messageImprint | Sutampa su atitinkamo užklausos (TimeStampReq) lauko reikšme |
| serialNumber | Sveikasis skaičius (iki 160 bitų ilgio), unikalus kiekvienai TSA laiko žymai |
| genTime | UTC laikas, nurodantis, kada sukurta laiko žyma |
| accuracy | 200 ms |

| | |
|---|---|
| nonce | Sutampa su atitinkamo užklausos (TimeStampReq) lauko reikšme, jei toks laukas buvo įtrauktas |
| Tsa | Atitinka sertifikato, kuriuo pasirašyta laiko žyma, subject lauko reikšmę:<br><br>CN = BalTstamp QTSA TSU1<br>O = BalTstamp UAB<br>C = LT<br>SERIALNUMBER = 210<br><br>arba<br><br>C = LT<br>L = Vilnius<br>O = BalTstamp UAB<br>CN = BalTstamp QTSA TSU2 |

### 3.3.2 Laikrodžių sinchronizavimas su UTC

TSA užtikrina, kad jos laikrodis būtų sinchronizuojamas su UTC deklaruojamu tikslumu. Būtent:

TSU laikrodžiai nuolat sinchronizuojami su Valstybiniu laiko ir dažnio etalonu, atkuriančiu visuotinio koordinuotojo laiko Lietuvos skalę UTC(LT), kurios sietis su UTC užtikrinama nuolatinių palyginimų būdu; sieties charakteristikos skelbiamos Tarptautinio svorių ir matų biuro (pr. *Bureau International des Poids et Mesures*, BIPM) leidinyje „Circular T“. Todėl TSU laikrodžiai negali nukrypti daugiau nei per dvi dešimtąsias sekundės;

TSU laikrodžiai yra apsaugoti nuo pavojų, galinčių sukelti nepastebimus šuolius, galinčius pažeisti laikrodžių kalibravimą. Tai neįgaliotų darbuotojų įsikišimas, radijo ar elektros trikdžiai ir pan.

TSA užtikrina, kad atitinkamai tarnybai paskelbus apie keliamąją sekundę (*leap second*), nesutriktų laikrodžių sinchronizavimas, o keliamoji sekundė būtų įvedama atitinkamos dienos paskutiniąją minutę. Įrašuose nurodomas tikslus šių pokyčių laikas.

## 3.4 TSA darbas ir jo vadyba

### 3.4.1 Saugumo vadyba

TSA užtikrina, kad taikomos adekvačios ir atitinkančios pripažintai geriausiai praktikai administravimo ir valdymo procedūros.

TSA prisiima atsakomybę už visus TSP apibrėžtus laiko žymų paslaugų teikimo aspektus, įskaitant ir tas funkcijas, kurias atlieka trečiosios šalys. TSA naudojasi Fizinių ir technologijos mokslų centro Metrologijos skyriaus Laiko ir dažnio etalono laboratorijos paslaugomis generuoti laiko žymų komponentes, reikalingas teikiamoms laiko žymoms formuoti ir užtikrinti generuojamų laiko žymų metrologinę sietį su Pasaulio suderintojo laiko skale UTC pagal šių nuostatų reikalavimus. TSA prisiima atsakomybę už visų laiko žymų teikime dalyvaujančių šalių taikomų praktikų skelbimą.

Už informacinio saugumo gairių bei taisyklių nustatymą, infrastruktūros nuolatinį palaikymą, saugumo priemonių ir darbinių procedūrų TSA įrangai, patalpoms, sistemoms ir informacijos ištekliams, reikalingiems laiko žymoms teikti, dokumentavimą, tvarkymą ir vykdymą, o taip pat informacinių ir kitų išteklių apsaugą yra atsakingas Priežiūros

komitetas, sudarytas iš BalTstamp ir FTMC vadovybės. TSA užtikrina informacinio saugumo gairių bei taisyklių pateikimą visiems susijusiems darbuotojams, kurių darbui tai reikalinga.

Saugumo priemonės ir darbinės procedūros TSA įrangai, patalpoms, sistemoms ir informacijos ištekliams, reikalingiems laiko žymoms teikti, yra dokumentuojamos, tvarkomos ir vykdomos.

Informacinio saugumo infrastruktūra, reikalinga saugumui užtikrinti, yra išlaikoma nuolat. Bet kokie pokyčiai, turintys reikšmės saugumui, tvirtinami TSA vadovybės.

### 3.4.2 Išteklių klasifikavimas ir vadyba

TSA užtikrina, kad jos informaciniai ir kiti ištekliai būtų tinkamai saugomi. Būtent, TSA inventorizuoja visus išteklius ir klasifikuoja jų apsaugos reikalavimus pagal rizikos analizę.

### 3.4.3 Paslaugų saugumas personalo atžvilgiu

TSA vykdo tokią personalo ir samdymo praktiką, kuri didintų pasitikėjimą TSA darbu. Būtent (bendroji dalis):

a) TSA samdo darbuotojus, turinčius eksperto lygio žinias, patirtį ir kvalifikaciją, reikalingą teikiant TSA siūlomas paslaugas ir atliekant tarnybines pareigas;

b) darbuotojų pareigos ir vaidmuo užtikrinant saugumą, kaip nurodyta TSA saugumo taisyklėse, yra nustatyti pareiginėse instrukcijose. Pasitikėjimo pareigos, nuo kurių priklauso TSA veiklos saugumas, yra aiškiai nurodytos;

c) TSA darbuotojai (ir nuolatiniai, ir laikini) turi pareigines instrukcijas, parengtas pareigų ir mažiausių privilegijų atskyrimo požiūriu. Instrukcijos nustato pareigybių kritiškumą, pagrįstą pareigomis ir prieigos lygiais, patikimumo ir kvalifikacijos patikrinimu bei mokymu. Pareiginės instrukcijos apima sugebėjimų ir patirties reikalavimus;

d) darbuotojai vykdo administracines ir vadybines procedūras ir procesus, kurie atitinka TSA informacinio saugumo vadybos procedūras.

Laiko žymų teikimo vadovybei taikytini papildomi reikalavimai:

e) TSA samdo vadovaujančius darbuotojus, kurie:

- išmano laiko žymų technologiją;
- išmano elektroninių parašų technologiją;
- išmano TSU laikrodžių sinchronizavimą pagal UTC;
- išmano saugumo procedūras, skirtas darbuotojams, atsakingiems už saugumą;
- turi patirtį informacinio saugumo bei rizikos įvertinimo srityse;

f) TSA darbuotojai, einantys pasitikėjimo pareigas, neturi interesų konfliktų, kurie galėtų pakenkti TSA veiklos nešališkumui;

g) pasitikėjimo pareigos apima tokias pareigybes:

- saugumo pareigūnus, atsakingus už saugumo nuostatų vykdymą ir administravimą;
- sistemos administratorius, įgaliotus įdiegti, konfigūruoti ir prižiūrėti TSA patikimąsias sistemas, skirtas laiko žymų tvarkymui;
- sistemos operatorius, atsakingus už kasdienį darbą su TSA patikimosiomis sistemomis ir įgaliotus daryti sistemos atsargines kopijas ir atlikti atkūrimą;
- auditorius, įgaliotus peržiūrėti TSA patikimųjų sistemų archyvus ir audito įrašus (audit logs);

h) TSA darbuotojus į pasitikėjimo pareigas formaliai skiria vadovybė, atsakinga už saugumą;

i) TSA neskiria į pasitikėjimo pareigas ar vadovybę asmenų, apie kuriuos yra žinoma, kad jie yra padarę rimtų nusikaltimų ar kitų teisės pažeidimų, dėl kurių šie asmenys gali būti netinkami tokiam darbui. Darbuotojams neleidžiama eiti pasitikėjimo pareigų, kol nebus atliktas reikalingas patikrinimas.

Už tinkamų darbuotojų, atitinkančių TSP 3.4.3 keliamus reikalavimus, samdymą, žinių ir patikimumo patikrinimą, pareigų (įskaitant pasitikėjimo pareigybes) nustatymą ir aprašymą pareiginėse instrukcijose atsakinga TSA vadovybė. Darbuotojams užtikrinama prieiga prie visų darbui reikalingų dokumentų.

Visi šie asmenys gali atlikti tik jų pareigose numatytus veiksmus.

### 3.4.4 Fizinis ir aplinkos saugumas

TSA užtikrina, kad galimybė patekti į kritiškai svarbias vietas būtų kontroliuojama, o fizinis pavojus ištekliams būtų kuo mažesnis. Būtent:

a) laikomasi tokių reikalavimų laiko žymų teikimui ir vadybai:

- patalpos ir įranga, susijusios su laiko žymų paslaugomis, fiziškai prieinamos tik atitinkamai įgaliotiems asmenims;
- yra įdiegtos priemonės, skirtos išvengti išteklių praradimui bei sugadinimui, informacijos nutekėjimui ir vagystei, o taip pat darbo nutrūkimui;
- yra įdiegtos priemonės, skirtos išvengti informacijos bei jos apdorojimo įrangos sukompromitavimui bei vagystei;

b) TSA kontroliuoja prieigą prie kriptografinio modulio, kad būtų patenkinti kriptografinių modulių saugumo reikalavimai, nustatyti [ETSI 1] 7.2.1 ir 7.2.2 str.;

c) laikosi papildomų reikalavimų laiko žymų teikimo valdymui:

- laiko žymų teikimo valdymo įranga dirba aplinkoje, kuri fiziškai apsaugo įrangą nuo sukompromitavimo dėl neįgaliotos prieigos prie duomenų ar sistemų;
- fizinį saugumą užtikrina aiškiai nustatytas saugumo perimetras apie laiko žymų teikimo valdymo įrangą. Saugumo perimetro viduje nėra patalpų, kuriomis yra dalomasi su kokiomis nors kitomis organizacijomis;
- yra įdiegtos fizinio ir aplinkos saugumo priemonės, apsaugančios pačius sistemos resursus, patalpas, kuriose jie laikomi, ir pagalbinę įrangą. TSA fizinio ir aplinkos saugumo taisyklės, skirtos sistemoms, susijusioms su laiko žymų teikimo valdymu, aptaria prieigos fizinę kontrolę, apsaugą nuo gamtos nelaimių, priešgaisrinę saugą, pagalbinių priemonių (pvz., įtampos ir telekomunikacijų) sutrikimus, pastato sugriuvimą, vandentiekio avarijas, apsaugą nuo vagystės bei įsibrovimo, o taip pat sistemos atkūrimą po nelaimės;
- yra įdiegtos priemonės, skirtos su laiko žymomis susijusios įrangos (taip pat ir programinės), informacijos bei laikmenų apsaugai nuo neįgalioto išnešimo.

TSA laiko žymų generavimo įranga veikia LDEL, kurios darbuotojai įgalioti prižiūrėti TSA įrangą ir dirbti su ja, patalpose, prižiūrimose pagal LDEL kokybės vadybos sistemos reikalavimus. LDEL ribos kartu nustato saugumo perimetrą, į kurio vidų neįgalioti asmenys patekti negali. FTMC pastatas, kuriame įsikūrusi LDEL, FTMC nustatyta tvarka saugomas budėtojų bei apsaugos tarnybos. Taip išvengiama išteklių (įskaitant laikmenas) neįgalioto išnešimo bei sugadinimo.

LDEL patalpose veikia moderni oro kondicionavimo sistema, palaikanti reikiamą oro

temperatūrą ir valanti orą nuo dulkių. Nutrūkus elektros energijos tiekimui iš tinklo, atsarginiai energijos šaltiniai (UPS) ir dyzelinis elektros generatorius užtikrina normalų sistemos darbą 4 valandas.

Informacijos bei jos apdorojimo įrangos sukompromitavimui bei vagystei išvengti taikomos tokios priemonės: TSA sistemos įrenginiuose ribojamas interneto ryšys – jis leidžiamas tik tiek, kiek to reikalauja laiko žymų teikimas. Įdiegtos ugniasienės ir apsaugos nuo įsilaužimo priemonės.

### 3.4.5 Darbo tvarkymas

TSA užtikrina, kad jos sistemos dalys būtų saugios ir kad su jomis būtų dirbama teisingai bei su kuo mažesne sutrikimų rizika.

Būtent (bendroji dalis):

a) TSA sistemos dalių visuma ir informacija yra apsaugota nuo virusų, piktybinių ir nenumatytų programų;

b) yra taikomos pranešimo apie incidentus bei atsako į juos procedūros, kad nuostoliai dėl saugumo incidentų ir sutrikimų būtų kuo mažesni;

c) su laikmenomis, naudojamomis patikimosiose TSA sistemose, elgiamasi saugiai, kad jos būtų apsaugotos nuo pakenkimo, vagystės, neįgaliotos prieigos ir pasenimo;

d) yra nustatytos ir vykdomos procedūros visoms pasitikėjimo ir administracinėms pareigybėms, nuo kurių priklauso laiko žymos paslaugų teikimas.

**Laikmenų tvarkymas ir saugumas**

e) Su visomis laikmenomis elgiamasi saugiai, pagal informacijos klasifikavimo schemos reikalavimus (žiūr. [ETSI 1] 7.4.2 str.). Nebereikalingos laikmenos su svarbiais duomenimis saugiai sunaikinamos.

**Sistemos planavimas**

f) Stebimi ir prognozuojami pajėgumo poreikiai, kad būtų užtikrinta reikiama duomenų apdorojimo sparta ir saugojimo talpa.

**Pranešimas apie incidentus bei atsakas į juos**

g) TSA veikia operatyviai ir koordinuotai, kad įvykus incidentui būtų greitai reaguojama ir kad galima žala dėl saugumo spragų būtų kuo mažesnė. Apie visus incidentus pranešama kaip galima greičiau.

Laiko žymų valdymo įrangai taikomos papildomos priemonės:

**Darbinės procedūros ir atsakomybė**

h) saugumo užtikrinimas yra atskirtas nuo kitų darbų. Saugumo užtikrinimo pareigos apima:

- darbines procedūras ir pareigas;
- saugiųjų sistemų planavimą ir priėmimą eksploatacijon;
- apsaugą nuo piktybinių programų;
- patalpų ir tvarkos priežiūrą;
- kompiuterių tinklo tvarkymą;
- aktyvų audito žurnalų stebėjimą, įvykių analizę ir reagavimą į juos;
- darbą su laikmenomis ir jų apsaugą;
- apsikeitimą duomenimis ir programine įranga.

Šiuos darbus tvarko pasitikėjimo pareigas einantys darbuotojai, tačiau atlikti gali ir prižiūrimi techniniai darbuotojai, kaip tai aprašyta atitinkamose saugumo taisyklėse ir

pareiginiuose dokumentuose.

### 3.4.6 Prieigos prie sistemos tvarkymas

TSA užtikrina, kad prieigą prie jos sistemos turėtų tik atitinkamai įgalioti asmenys. Būtent (bendroji dalis):

a) TSA vidiniam tinklui apsaugoti nuo neįgaliotos prieigos, įskaitant abonentus ir trečiąsias šalis, yra įdiegta ugniasienė, sukonfigūruota taip, kad uždraustų visus protokolus ir kreipinius, nereikalingus TSA darbui;

b) TSA efektyviai administruoja sistemos vartotojų prieigą, reikalingą operatorių, administratorių bei auditorių darbui. Taip užtikrinamas sistemos saugumas, įskaitant vartotojų paskyrų tvarkymą ir auditavimą, o taip pat savalaikį prieigos sąlygų pakeitimą arba prieigos nutraukimą;

c) prieiga prie informacijos ir taikomųjų sistemos funkcijų yra apribota pagal prieigos kontrolės politiką, o TSA sistema turi pakankamai kompiuterinio saugumo priemonių, kad būtų atskirtos TSPS numatytos pasitikėjimo pareigos, įskaitant saugumo administratoriaus ir darbinių funkcijų atskyrimą. Sistemos vidinių programų naudojimas yra apribotas ir griežtai kontroliuojamas;

d) TSA darbuotojai, prieš jiems panaudojant kritines sistemos funkcijas, tinkamai identifikuojami, o jų tapatumas patvirtinamas;

e) TSA darbuotojai yra atskaitingi už savo veiklą. Tam naudojami įvykių registrai (*event logs*) (žiūr. [ETSI 1] 7.4.10 str.).

Laiko žymų valdymo įrangai taikomos papildomos priemonės:

f) vietinio tinklo įrenginiai (pvz., maršrutizatoriai (*routers*)) laikomi fiziškai saugioje aplinkoje, o jų konfigūracija periodiškai audituojama, tikrinant, ar atitinka TSA nustatytus reikalavimus;

g) yra įdiegta nuolatinio stebėjimo ir įspėjimo įranga, kad TSA galėtų užfiksuoti, registruoti ir laiku reaguoti, jei būtų bet kokių neįgaliotų ir/ar netaisyklingų bandymų prieiti prie jos resursų.

### 3.4.7 Patikimųjų sistemų įdiegimas ir priežiūra

TSA naudoja patikimąsias sistemas ir produktus, apsaugotus nuo modifikavimo galimybės.

*Pastaba*: rizikos analizė nustato (žiūr. [ETSI 1] 7.1.1 str.), kokioms kritinėms funkcijoms reikia patikimųjų sistemų ir kokių reikia užtikrinimo lygių.

Būtent:

a) siekiant užtikrinti IT sistemų saugumą, bet kokio sistemų kūrimo projekto, vykdomo pačios TSA arba TSA vardu, kūrimo ir reikalavimų nustatymo etape atliekama saugumo reikalavimų analizė;

b) išleidžiant, modifikuojant ir taisant bet kokias darbines programas, taikomos pakeitimų tvarkymo procedūros.

### 3.4.8 TSA paslaugų sukompromitavimas

TSA užtikrina, kad įvykių, galinčių paveikti TSA paslaugų saugumą, įskaitant TSU privačiųjų pasirašymo raktų sukompromitavimą bei užfiksuotą sieties su UTC(LT) praradimą, atveju abonentams ir pasitikintiems asmenims būtų atskleista atitinkama informacija. Būtent:

a) TSA atkūrimo po incidentų planas aptaria tikrą ar įtariamą TSU privačiųjų

pasirašymo raktų sukompromitavimą bei TSU laikrodžio sieties praradimą, kuris galėjo atsiliepti išduotoms laiko žymoms;

b) tikro ar įtariamo sukompromitavimo arba sieties praradimo atveju abonentams ir pasitikintiems asmenims atskleidžiamas šio įvykio aprašymas;

c) tikro ar įtariamo TSU veiklos (pvz., raktų) sukompromitavimo arba sieties praradimo atveju TSU nutraukia laiko žymų išdavimą iki padėtis bus ištaisyta;

d) rimto TSA veiklos sukompromitavimo arba TSU sieties praradimo atveju, jei tik įmanoma, abonentams ir pasitikintiems asmenims atskleidžiama informacija, leidžianti nustatyti, kurioms būtent laiko žymoms šis įvykis galėjo atsiliepti, jei tai nepažeidžia TSA vartotojų privatumo arba TSA paslaugų saugumo.

### 3.4.9 TSA veiklos nutraukimas

TSA stengiasi, kad jos veiklos sustabdymo atveju galimi paslaugos teikimo pertraukimai, kuriuos patirtų abonentai ir pasitikintys asmenys, būtų kuo trumpesni, ir užtikrina duomenų, reikalingų laiko žymoms patikrinti, tolesnį teikimą. Būtent:

a) prieš nutraukdama laiko žymų paslaugos teikimą, TSA atlieka bent šias procedūras:

- abonentams ir pasitikintiems asmenims padaro prieinamą informaciją apie veiklos nutraukimą;
- panaikina visų subrangovų įgaliojimus veikti TSA vardu vykdant bet kokias funkcijas, susijusias su laiko žymų teikimu;
- patikimai šaliai perduoda įpareigojimus prižiūrėti įvykių registrą ir audito archyvus (žiūr. [ETSI 1] 7.4.10 str.), reikalingus protingą laikotarpį įrodyti TSA veiklos teisingumą;
- vykdo pati arba perduoda patikimai šaliai savo įsipareigojimus protingą laikotarpį pasitikintiems asmenims padaryti prieinamą savo viešąjį raktą arba jo sertifikatą;
- sunaikina TSU privatųjį raktą ir visas jo atsargines kopijas taip, kad jų nebebūtų galima atkurti;

b) TSA yra numačiusi, kaip padengti išlaidas, reikalingas šiems minimaliems reikalavimams įvykdyti, jei TSA bankrutuotų ar dėl kitų priežasčių nebegalėtų padengti šių išlaidų pati;

c) TSA šiuose savo veiklos nuostatuose yra numačiusi paslaugų teikimo sustabdymo nuostatas, apimančias:

- pranešimą visiems susijusiems asmenims;
- TSA įsipareigojimų perdavimą kitoms šalims;

d) TSA imasi priemonių, kad TSU sertifikatai būtų atšaukti.

### 3.4.10 Teisinių reikalavimų vykdymas

TSA užtikrina teisinių reikalavimų vykdymą, būtent:

a) TSA užtikrina Europos duomenų apsaugos direktyvos, kaip ji yra perkelta į Lietuvos teisės aktus, reikalavimų vykdymą;

b) TSA imtasi reikiamų techninių ir organizacinių priemonių tam, kad būtų užkirstas kelias neįgaliotam ar neteisėtam asmens duomenų apdorojimui, o taip pat netyčiniam asmens duomenų praradimui, sunaikinimui bei sugadinimui;

c) TSA saugo iš naudotojų gautą informaciją nuo atskleidimo, nebent tam būtų

duotas jų sutikimas ar teismo sankcija.

### 3.4.11 Informacijos apie TSA darbą kaupimas

TSA užtikrina, kad 10 metų laikotarpį būtų užrašoma ir saugoma visa reikiama informacija apie TSA darbą, kad būtų galima pateikti įrodymus, jei to prireiktų dėl atliekamų teisinių veiksmų. Būtent:

**Bendroji dalis**

a) TSA yra nustačiusi, kokius įvykius ir duomenis reikia fiksuoti;

b) TSA užtikrina dabar pildomų ir archyvuotų įrašų, susijusių su laiko žymų paslaugomis, saugumą ir slaptumą;

c) TSA pilnai ir konfidencialiai archyvuoja įrašus, susijusius su laiko žymų paslaugomis, kaip numatyta paskelbtuose TSA veiklos nuostatuose;

d) jei dėl teisinių dalykų reikia įrodyti TSA darbo teisingumą, TSA pateikia įrašus, susijusius su laiko žymų paslaugomis;

e) TSA užrašo raktų tvarkymo, laikrodžių sinchronizavimo bei su aplinkos sąlygomis susijusių svarbių įvykių tikslų laiką;

f) įrašai, susiję su laiko žymų paslaugomis, saugomi ir pasibaigus TSU pasirašymo raktų galiojimui, kiek tai reikalinga teisinių įrodymų požiūriu ir kaip pasakyta laiko žymų teikimo sąlygose (žiūr. [ETSI 1] 7.1.2 str.);

g) įrašai daromi taip, kad nebūtų galima lengvai jų ištrinti ar sunaikinti (jei jie nėra patikimai perrašyti į ilgalaikio saugojimo laikmenas) per laikotarpį, kurį jie yra saugotini;

h) visa apie abonentus sukaupta informacija saugoma konfidencialiai, išskyrus tuos atvejus, kai yra gautas abonento sutikimas platesniam jos paskelbimui;

**TSU raktų tvarkymas**

i) yra kaupiami įrašai apie visus įvykius, susijusius su TSU raktų gyvavimo ciklu;

j) yra kaupiami įrašai apie visus įvykius, susijusius su TSU sertifikatų gyvavimo ciklu;

**Laikrodžių sinchronizavimas**

k) yra kaupiami įrašai apie visus įvykius, susijusius su TSU laikrodžio sinchronizavimu su UTC;

l) yra kaupiami įrašai apie visus įvykius, susijusius su aptiktu sinchronizavimo praradimu.

## 3.5 Organizaciniai dalykai

TSA užtikrina, kad jos organizacija būtų patikima. Būtent, kad:

a) TSA taisyklės ir procedūros nebūtų diskriminuojančios;

b) TSA paslaugos būtų prieinamos visiems prašantiesiems, kurių veikla sutinka su paskelbta TSA veiklos sritimi ir kurie sutinka laikytis TSA nustatytų įpareigojimų;

c) TSA būtų juridinis asmuo pagal Lietuvos Respublikos įstatymus;

d) TSA turėtų kokybės ir informacinio saugumo vadybos sistemą, tinkamą teikiamoms laiko žymų paslaugoms;

e) TSA turėtų reikiamus pagrindus ir galimybes savo įsipareigojimams, kylantiems iš jos darbo ir veiklos, įvykdyti;

f) turėtų finansinį stabilumą ir išteklius, reikalingus veiklai (įskaitant jos nutraukimą) pagal šias TSP;

g) turėtų reikiamą darbuotojų, turinčių atitinkantį laiko žymų teikimo darbo pobūdį bei

apimtį išsilavinimą, pasirengimą, technines žinias bei patirtį, skaičių;

h) turėtų taisykles ir procedūrą, skirtą spręsti skundams ir ginčams, gautiems dėl laiko žymos paslaugų teikimo ar kitų susijusių dalykų;

i) TSA turėtų tinkamai dokumentuotas sutartis bei sutartinius ryšius su paslaugų teikime dalyvaujančiomis trečiomis šalimis.

# 4 TEKSTE VARTOJAMOS SĄVOKOS IR SANTRUMPOS

**Abonentas** (angl. *subscriber*) – asmuo, kuriam yra reikalingos TSA paslaugos, kuris sutinka su laiko žymų paslaugų teikimo sąlygomis ir naudojasi teikiamomis paslaugomis.

**Aparatinis saugumo modulis (kriptografinis modulis)** (angl. *hardware security module – HSM*) – aparatinė ir programinė įranga, kuri naudojama šifravimo raktų poroms – privatiesiems ir viešiesiems raktams – generuoti, privatiesiems raktams saugoti ir laiko žymų pasirašymui.

**Kompromitacija** – kriptografinio modulio privataus rakto atskleidimas, pavogimas, modifikavimas, neteisėtas panaudojimas arba kitoks jo saugumo pažeidimas.

**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 žymų taisyklės** (angl. *TSP – time stamp policy*) – laiko žymų sudarymo, tvarkymo ir tikrinimo taisyklės, nustatančios laiko žymų paslaugų teikėjo ir naudotojų teises ir pareigas.

**Laiko žymų tarnyba** (angl. *TSA – time stamp authority*) – sertifikavimo paslaugų teikėjas, teikiantis laiko žymų paslaugas.

**Laiko žymų teikimo veiklos nuostatai** (*time stamping practice statement*) – laiko žymų tarnybos patvirtintos laiko žymų tasyklių įgyvendinimo praktikos.

**Saugykla** (angl. *repository*) – internetu prieinama laiko žymų tarnybos informacija, skelbiama laiko žymų naudotojams.

**BIPM** – Tarptautinis svorių ir matų biuras (pr. *Bureau International des Poids et Mesures*).

**CA** – sertifikatų tarnyba (angl. *certificate authority*).

**ETSI** – European Telecommunications Standards Institute.

**FTMC** – Fizinių ir technologinių mokslų centras.

**LDEL** – Laiko ir dažnio etalono laboratorija.

**OID** – objekto identifikatorius (angl. *object identifier*).

**RRT** – Lietuvos Respublikos ryšių reguliavimo tarnyba.

**TSA** – laiko žymų tarnyba *(*angl. *time stamp authority*).

**TSP** – laiko žymų taisyklės (angl. *time stamp policy*).

**TSPS** – laiko žymų teikimo veiklos nuostatai (angl. *time stamping practice statement*).

**TSU** – laiko žymų įrenginys (angl. *time stamping unit*).

**UTC** – pasaulinis koordinuotasis laikas (pr. *universel temps coordonné*).

# 5 NUORODOS

[ELP] – Lietuvos Respublikos elektroninio parašo įstatymas (Žin., 2000, Nr. 61-1827; Žin., 2002, Nr. 64-2572).

[ETSI 1] – standartas LST ETSI TS 102 023 LST ETSI TS 102 023 „Strateginiai reikalavimai, keliami laiko žymėjimo paslaugų teikėjams“.

[ETSI 2] – standartas LST ETSI TS 101 861 „Laiko žymėjimo profilis“.

[FIPS 1] – standartas FIPS PUB 140-2 „Security Requirements for Cryptographic Modules“.