BALTSTAMP
LAIKO ŽYMŲ TEIKIMO VEIKLOS NUOSTATAI

Unikalus objekto ID (OID): **1.3.6.1.4.1.38424.1.4.4**
Versija: 4.0

Galioja nuo 2020-10-30

2020

TURINYS

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	Pirmoji versija
Versija 1.1	2013-02-01	Pakoreguota pirmoji versija
Versija 1.2	2014-07-23	Pakoreguota pirmoji versija
Versija 1.3	2016-07-01	Pakoreguota pirmoji versija
Versija 2.0	2016-12-01	Antroji projekto versija
Versija 2.1	2017-03-31	Pakoreguota antroji versija
Versija 3.0	2019-08-01	Trečioji versija
Versija 4.0	2020-10-30	Ketvirtoji versija

BalTstamp laiko žymų teikimo veiklos nuostatų tvirtinimas:

Dokumento rengimas	Vardas, pavardė	Data	Parašas
Dokumentą parengė	Emilis Urba	2020-09-30	
Dokumentą patikrino	Rimantas Miškinis	2020-10-15	
Dokumentą patvirtino	Vincentas Vitkauskas	2020-10-30	

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 https://www.baltstamp.lt/

1.1 Apžvalga

Standartas ETSI EN 319 421 apibrėžia Geriausių praktikų laiko žymų taisykles (toliau – BTSP, pagal anglišką atitikmenį *best practices time-stamp policy*) laiko žymų tarnyboms (toliau – TSA, pagal anglišką atitikmenį *time-stamping authority*), kurių laikomasi formuojant ne blogesnio nei 1 sekundės tikslumo laiko žymas, patvirtintas viešojo rakto sertifikatais. BTSP išdėstyti reikalavimai nesusieti su konkrečiais technologiniais sprendimais ar TSA organizacine struktūra. BTSP 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) 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentu (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB [eIDAS];

b) standartu ETSI EN 319 421, anksčiau skelbtu kaip ETSI TS 102 023 ir perimtu kaip LST ETSI TS 102 023 „Strateginiai reikalavimai, keliami laiko žymėjimo paslaugų teikėjams" [EN 319 421];

c) standartu ETSI EN 319 422, anksčiau skelbtu kaip ETSI TS 101 861 ir perimtu kaip LST ETSI TS 101 861 „Laiko žymėjimo profilis" [EN 319 422].

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 BTSP; 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 **1.3.6.1.4.1.38424.1.4.4**; 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	4

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

1.3 Laiko žymų naudotojai ir taikymo sritys

TSA sudaryta laiko žyma galima paženklinti pažangų elektroninį parašą, sukurtą kvalifikuotu elektroninio parašo kūrimo įtaisu 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 sudaryti iki laiko žymoje nurodyto laiko. TSA teikiamų laiko žymų naudotojai gali būti fiziniai ir juridiniai asmenys, kuriems reikalingos TSA teikiamos laiko žymos.

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

Kaip TSA veikla atitinka BTSP ir TSPS, tikrinama TSA nustatyta vidaus tvarka, bent kas du metus.

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:	https://www.baltstamp.lt/
El. paštas:	info@baltstamp.lt

2 TAISYKLĖS IR VEIKLA

2.1 Rizikų vertinimas

TSA atlieka rizikų vertinimą siekiant nustatyti, išanalizuoti ir įvertinti veiklos ištekliams kylančias grėsmes, atsižvelgiant į veiklos ir technines problemas. Remiantis rizikų vertinimo rezultatais parenkamos tinkamos rizikų mažinimo priemonės, kurios užtikrina, kad saugumo lygis atitiktų rizikos laipsnį.

TSA nustato reikiamus saugumo reikalavimus ir darbines procedūras, būtinas pasirinktoms rizikų mažinimo priemonėms įgyvendinti, kaip aprašyta informacijos saugumo taisyklėse ir šiuose veiklos nuostatuose.

Rizikų vertinimas ir sprendimas laikyti liekamąsias rizikas priimtinomis tvirtinamas BalTstamp TSA vadovo.

2.2 Laiko žymų tarnybos veiklos nuostatai

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

a) šiuose veiklos nuostatuose yra aprašytos praktikos ir procedūros, naudojamos TSP nustatytiems reikalavimams įvykdyti;
b) juose taip pat nustatyti visų išorės organizacijų, palaikančių TSA paslaugas, įsipareigojimai, įskaitant taikytinas taisykles ir nuostatus;
c) TSA veiklos nuostatai ir kita dokumentacija, reikalinga atitikties TSP įvertinimui, yra prieinama laiko žymų abonentams ir pasitikintiems asmenims BalTstamp TSA svetainėje, arba pateikiama pareikalavus;
d) BalTstamp TSA vadovas yra atsakingas už TSA veiklą bendrai, ir turi įgaliojimus veiklos nuostatams patvirtinti;
e) BalTstamp TSA vadovas užtikrina, kad šie veiklos nuostatai būtų tinkamai vykdomi, supažindindamas su jais darbuotojus pagal užimamas pareigas;
f) veiklos nuostatų peržiūros tvarka nustatyta skyrelyje 2.12 Veiklos nuostatų keitimo procedūros;
g) TSA praneša apie numatomus veiklos nuostatų pakeitimus, o juos patvirtinusi, kaip numatyta (d) punkte viršuje, atnaujintus nuostatus nedelsdama padaro prieinamus, kaip reikalaujama (c) punkte viršuje;
h) priemonės, numatytos veiklos nutraukimo atveju, išdėstytos skyrelyje 3.14 TSA veiklos nutraukimas.

BTSP yra vienintelės TSA įgyvendinamos laiko žymų taisyklės:

a) santraukų skaičiavimo algoritmai, kurie gali būti naudojami duomenims, kuriems dedama laiko žyma, atvaizduoti, nurodyti skyrelyje 3.7.1 Laiko žymų teikimas;
b) laiko žymose nurodomo laiko tikslumas UTC atžvilgiu nurodytas skyrelyje 3.7.1 Laiko žymų teikimas;
c) TSA 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.;

d) abonentų įsipareigojimai nurodyti skyrelyje 2.6 Laiko žymų abonentų įsipareigojimai;
e) pasitikinčiųjų asmenų įsipareigojimai nurodyti skyrelyje 2.7 Laiko žymomis pasitikinčių asmenų įsipareigojimai;
f) informacija, kaip patikrinti laiko žymas, pateikta skyrelyje 2.7 Laiko žymomis pasitikinčių asmenų įsipareigojimai;
g) teikiamos laiko žymos yra kvalifikuotos elektroninės laiko žymos, kaip apibrėžta Reglamente (ES) Nr. 910/2014 [eIDAS].

2.3 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) taikomas TSP;
b) tikėtiną viešojo rakto sertifikatų gyvavimo trukmę;
c) abonentų įsipareigojimus, jei tokių būtų;
d) informaciją, kaip patikrinti laiko žymas, ir laiko žymų galiojimo trukmės apribojimus, jei tokių būtų;
e) kiek laiko saugomi sukaupti įrašai apie įvykius;
f) atsakomybės apribojimus;
g) teikiamų paslaugų naudojimo apribojimus, įskaitant nuostolių, kilusių dėl tokių apribojimų nepaisymo, atlyginimo apribojimus;
h) nuorodą į taikomą šalies teisę;
i) ginčų ir nesutarimų sprendimo tvarką;
j) informaciją apie tai, ar buvo įvertinta paslaugų atitiktis TSP, ir, jei buvo, tai kokiu būdu;
k) kontaktinę TSA informaciją;
l) įsipareigojimus dėl paslaugos pasiekiamumo.

Šios sąlygos skelbiamos naudotojui suprantama kalba interneto svetainėje https://www.baltstamp.lt/, ir gali būti papildytos TSA ir abonentų sudarytose sutartyse.

2.4 Informacijos saugumo taisyklės

TSA turi informacijos saugumo taisykles, patvirtintas BalTstamp TSA vadovo, kurios nustato organizacijos taikomus informacijos saugumo valdymo būdus.

TSA užtikrina, kad būtų taikomos adekvačios ir atitinkančios pripažintą geriausią praktiką 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 BalTstamp TSA vadovas. 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 BalTstamp TSA vadovo.

2.5 Laiko žymų tarnybos įsipareigojimai

2.5.1 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;
c) TSU sertifikatų galiojimą užtikrina CA įsipareigojimas atnaujinti savo atšauktų sertifikatų sąrašą (angl. Certificate Revocation List, CRL) ne rečiau kaip kartą per septynias dienas. Tai nurodyta CA sertifikatų politikoje;
d) siekiant užtikrinti paslaugos teikimą ir jo patikimumą, pažaidos tyrimai (vulnerability scans) atliekami ne rečiau nei kartą per metus, o įsilaužimo bandymai (penetration tests) atliekami ne rečiau nei kartą per penkerius metus.

2.5.2 TSA įsipareigojimai abonentams

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

2.6 Laiko žymų abonentų įsipareigojimai

Abonentas, pasikliaudamas laiko žyma, privalo patikrinti, ar ji pasirašyta teisingai ir ar laiko žymos pasirašymo privatus raktas galioja ir nebuvo sukompromituotas (išsamiau žr. skyrelį 2.7 Laiko žymomis pasitikinčių asmenų įsipareigojimai).

2.7 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).

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 [EN 319 421] perimtos sąvokos *privatusis raktas*, *pasirašymo (parašo) raktas*, *TSU pasirašymo raktas*, *TSU privatusis pasirašymo raktas* yra tapačios.

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

2.8 Atsakomybė

TSA atsakomybė ir įsipareigojimai išdėstyti sudarytose paslaugų teikimo sutartyse.

2.9 Teisinės nuostatos ir interpretavimas

2.9.1 Pagrindiniai teisės aktai

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

a) 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB;
b) 2018 m. balandžio 26 d. Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymas;
c) 2018 m. birželio 21 d. Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus įsakymu Nr. 1V-588 patvirtintas „Kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų ir kvalifikuotų patikimumo užtikrinimo paslaugų statuso suteikimo ir jų įrašymo į nacionalinį patikimą sąrašą bei kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų veiklos ataskaitų teikimo tvarkos aprašas";
d) 2019 m. birželio 4 d. Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus įsakymu Nr. 1V-594 patvirtintas „Pranešimų apie patikimumo užtikrinimo paslaugų saugumo ir (ar) vientisumo pažeidimus teikimo tvarkos aprašas".

2.9.2 Ginčų sprendimo tvarka

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

2.10 Mokesčiai

TSA gali nustatyti laiko žymų paslaugų kainas.

2.11 Intelektinės nuosavybės teisės

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

2.12 Veiklos nuostatų keitimo procedūros

Veiklos nuostatai gali būti keičiami pastebėjus jose klaidų, iškilus reikalui jas atnaujinti arba gavus susijusių šalių pasiūlymus.

Veiklos nuostatų pakeitimai skirstomi į dvi kategorijas:

a) esminiai pakeitimai, apie kuriuos turi būti pranešama naudotojams ir kuriuos atlikus turi būti keičiamas veiklos nuostatų OID;

b) neesminiai pakeitimai, apie kuriuos TSA neprivalo pranešti kitoms šalims ir kuriuos atlikus veiklos nuostatų OID nekeičiamas.

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

Kitokie pakeitimai (taipogi visi pakeitimai, dėl kurių keičiasi laiko žymos paslaugų saugumo lygis) yra esminiai.

Veiklos nuostatai yra prižiūrimi, keičiami ir tvirtinami pagal tokią procedūrą:

a) už saugumą atsakingi TSA darbuotojai kartą per metus, skaičiuojant nuo paskutinės veiklos nuostatų redakcijos, juos peržiūri ir įsitikina jų tinkamumu. Jei nustatoma, kad veiklos nuostatus reikia keisti, darbuotojai inicijuoja keitimą;

b) pakeitimus taip pat gali inicijuoti kiti TSA darbuotojai arba laiko žymų naudotojai. Sprendimą, ar reikia rengti veiklos nuostatų pakeitimus, priima BalTstamp TSA vadovas ir paveda tai atlikti darbuotojams, kurių veiklos sritį numatomas pakeitimas atitinka;

c) darbuotojai, kuriems tai pavesta, rengia naują veiklos nuostatų redakciją;

d) sprendimą dėl naujos veiklos nuostatų redakcijos patvirtinimo priima BalTstamp TSA vadovas; esminių pakeitimų atveju pakeičiamas veiklos nuostatų redakcijos versijos pirmasis skaitmuo bei atitinkamai OID versijos elementas (paskutinysis skaitmuo). Atlikus neesminį pakeitimą, pakeičiami veiklos nuostatų redakcijos versijos antrasis ir tolimesni skaitmenys;

e) patvirtinta nauja veiklos nuostatų redakcija paskelbiama BalTstamp TSA svetainėje;

f) apie pakeistus veiklos nuostatus ne vėliau kaip per 3 darbo dienas informuojama priežiūros įstaiga.

3 TSA VALDYMAS IR VEIKIMAS

3.1 Įvadas

TSA laikosi visų praktikų, nurodytų tolimesniuose punktuose.

Laiko žymos pateikiamos atsakant į užklausas TSA nuožiūra, atsižvelgiant į susitarimus su abonentu.

3.2 Organizaciniai dalykai

3.2.1 Organizacijos patikimumas

TSA užtikrina, kad jos organizacija būtų patikima. Būtent:

a) TSA yra juridinis asmuo pagal Lietuvos Respublikos įstatymus, įregistruota Juridinių asmenų registre kaip UAB BalTstamp; įmonės kodas: 302608545;

b) TSA turi kokybės ir informacinio saugumo vadybos sistemą, tinkamą teikiamoms laiko žymų paslaugoms;

c) yra įdarbintas reikiamas darbuotojų, turinčių atitinkantį laiko žymų teikimo darbo pobūdį bei apimtį išsilavinimą, pasirengimą, technines žinias bei patirtį, skaičius;

d) TSA taisyklės ir veiklos nuostatai yra pagrįsti tarptautiniais standartais ir yra nediskriminuojantys;

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

f) TSA turi reikiamus susitarimus ir išteklius savo įsipareigojimams, kylantiems iš jos darbo ir veiklos, įvykdyti;

g) TSA turi finansinį stabilumą ir išteklius, reikalingus veiklai (įskaitant jos nutraukimą) pagal TSP;

h) taisyklės ir procedūros, skirtos spręsti skundams ir ginčams, gautiems dėl laiko žymos paslaugų teikimo ar kitų susijusių dalykų, yra nurodytos kaip apibrėžta skyrelyje 2.3 Laiko žymų teikimo sąlygos;

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

3.2.2 Pareigų atskyrimas

Siekiant sumažinti neteisėto ar netyčinio TSA išteklių modifikavimo ar piktnaudžiavimo jais galimybes, konfliktuojančios pareigos ir atsakomybių sritys yra atskirtos kaip apibrėžta TSA informacijos saugumo taisyklėse (žr. skyrelį 2.4 Informacijos saugumo taisyklės).

3.3 Saugumas personalo atžvilgiu

TSA vykdo tokią personalo ir samdymo praktiką, kuri didintų pasitikėjimą TSA darbu. Būtent:

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

b) darbuotojams, pažeidusiems TSA taisykles ar procedūras, taikomos drausminės nuobaudos;

c) darbuotojų pareigos ir vaidmuo užtikrinant saugumą, kaip nurodyta TSA informacijos saugumo taisyklėse, yra nustatyti pareiginėse instrukcijose. Pasitikėjimo pareigos,

nuo kurių priklauso TSA veiklos saugumas, yra aiškiai nurodytos;

d) 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;

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

f) 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;

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

h) 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*);

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

j) 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 šiuos reikalavimus, samdymą, žinių ir patikimumo patikrinimą, pareigų (įskaitant pasitikėjimo pareigybes) nustatymą ir aprašymą pareiginėse instrukcijose atsakingas BalTstamp TSA vadovas. Darbuotojams užtikrinama prieiga prie visų darbui reikalingų dokumentų.

Visi darbuotojai gali atlikti tik jų pareigose numatytus veiksmus.

3.4 Išteklių tvarkymas

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

Su visomis laikmenomis elgiamasi saugiai, pagal informacijos klasifikavimo schemos reikalavimus. Nebereikalingos laikmenos su svarbiais duomenimis saugiai sunaikinamos.

3.5 Prieigos kontrolė

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

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 veiksmingai 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 taisykles, 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*) (žr. skyrelį 3.12 Įrodymų kaupimas).

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.

3.6 Kriptografinės priemonės

3.6.1 Bendroji dalis

TSA užtikrina kriptografinių raktų ir modulių saugumą per visą jų gyvavimo ciklą, kaip aprašyta tolimesniuose šio skyriaus skyreliuose.

3.6.2 TSU 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 (žr. [EN 319 421] 7.3 str.). Šią funkciją vykdyti įgaliojami tik tie asmenys, kuriems tai priklauso daryti pagal pareiginius nurodymus;

b) kriptografinis modulis, kuriame generuojamas TSU pasirašymo raktas, atitinka trečiojo lygio saugumo reikalavimus pagal standartą [FIPS 140];

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;

d) TSU raktai nėra importuojami į kelis veikiančius kriptografinius modulius;
e) vienu metu aktyvus yra tik vienas TSU pasirašymo raktas.

3.6.3 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 atitinka trečiojo lygio saugumo reikalavimus pagal standartą [FIPS 140];
b) TSU privačiojo rakto atsargines kopijas fiziškai saugioje aplinkoje (patalpoje, apsaugotoje nuo neįgaliotų asmenų prieigos) kopijuoja, saugo ir atkuria tik pasitikėjimo pareigas einantys darbuotojai, esant bent dvigubai kontrolei (žr. [EN 319 421] 7.8 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.

3.6.4 TSU viešojo rakto sertifikatas

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, arba pačios TSA.
c) TSU atmeta bet kokius mėginimus suteikti laiko žymą tol, kol į jį nėra įkeltas atitinkamas viešojo rakto sertifikatas.

3.6.5 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 2029 metų pabaigos.

TSU sertifikato keitimas, išlaikant tą pačią raktų porą, neatliekamas.

3.6.6 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 buvusi sugadinta ar kitaip paveikta pristatymo (transportavimo) ir saugojimo metu. Prieš įdiegiant, įranga yra patikrinama saugumo pareigūnų, kaip tai numatyta informacijos saugumo taisyklėse, o patikrinimo rezultatai dokumentuojami kriptografinio modulio žurnale;
b) TSU pasirašymo raktų generavimas ir aktyvavimas kriptografinėje įrangoje būtų atliekamas tik darbuotojų, kuriems patikėtos pasitikėjimo pareigos, esant mažiausiai dvigubai kontrolei, fiziškai saugioje aplinkoje, šiuos įvykius dokumentuojant kriptografinio modulio žurnale. Raktų dublikatai nėra daromi;
c) TSU kriptografiniame modulyje saugomi privatūs TSU raktai, pasibaigus modulio naudojimo laikui, būtų ištrinti naudojant saugią nulinimo procedūrą, aprašytą

modulio dokumentacijoje, tokiu būdu, kad jų praktiškai nebebūtų įmanoma atkurti.

3.6.7 TSU kriptografinių raktų gyvavimo ciklo pabaiga

TSU raktų poros galiojimo laikotarpis yra prilyginamas atitinkamo TSU sertifikato galiojimo laikotarpiui. TSA užtikrina, kad TSU privatieji 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 3.6.2 TSU raktų generavimas;
b) TSU privatieji pasirašymo raktai bei jų dalys su visomis kopijomis sunaikinami, kad privačiųjų raktų nebebūtų galima atkurti.

3.7 Laiko žymų sudarymas

3.7.1 Laiko žymų teikimas

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

a) TSU naudojamas laikas yra susietas su laiku UTC(LT);
b) laiko žymoje nurodyta laiko vertė gali skirtis nuo UTC ne daugiau nei nurodyta TSP ir pačioje laiko žymoje;
c) užfiksavus, kad TSU laikrodis nukrypo nuo paskelbto tikslumo (žr. skyrelį 3.7.2 Laikrodžių sinchronizavimas su UTC), laiko žymos neteikiamos;
d) laiko žyma yra pasirašyta raktu, sukurtu tik šiam tikslui;
e) laiko žymų generavimo sistema atmeta bet kokius mėginimus suteikti laiko žymą, jei privatusis pasirašymo raktas nebegalioja.

Teikiamos laiko žymos atitinka [EN 319 422] reikalavimus. BalTstamp TSA priimamos laiko žymų užklausos sandara pateikta *lentelėje* ***Nr.3***; BalTstamp TSA sudaromos laiko žymos sandara pateikta *lentelėje* ***Nr.4***.

Lentelė Nr. 3. Laiko žymų užklausos sandara

Laukas	Reikšmė
version	1
messageImprint	Duomenų, kuriems dedama laiko žyma, santraukos algoritmo identifikatorius (OID) ir santraukos reikšmė; gali būti naudojami šie algoritmai: - SHA-1 (OID: 1.3.14.3.2.26), tačiau jį naudoti nerekomenduotina - SHA-256 (OID: 2.16.840.1.101.3.4.2.1) - SHA-384 (OID: 2.16.840.1.101.3.4.2.2) - SHA-512 (OID: 2.16.840.1.101.3.4.2.3)
reqPolicy	Jei nurodoma, turi būti 0.4.0.2023.1.1

nonce	Jei nurodoma, ta pati reikšmė bus įtraukta į laiko žymą
certReq	Jei įtraukta ir lygi *true*, atitinkamo TSU sertifikatas bus įtrauktas į laiko žymą
extensions	Negali būti nurodyta

Lentelė Nr. 4. Laiko žymos sandara

Laukas	Reikšmė
version	1
policy	0.4.0.2023.1.1
messageImprint	Sutampa su atitinkamo užklausos (*TimeStampReq*) lauko reikšme
serialNumber	Sveikasis skaičius (iki 160 bitų ilgio), unikalus kiekvienai TSU laiko žymai
genTime	UTC laikas, nurodantis, kada sukurta laiko žyma
accuracy	1 s ar geriau (iki 200 ms), atsižvelgiant į tai, kaip numatyta sutartyje
nonce	Sutampa su atitinkamo užklausos (*TimeStampReq*) lauko reikšme, jei toks laukas buvo įtrauktas
tsa	Atitinka sertifikato, kuriuo pasirašyta laiko žyma, lauko *Subject* reikšmę: C = LT L = Vilnius organizationIdentifier = NTRLT-302608545 O = BalTstamp UAB CN = BalTstamp QTSA TSU1 arba C = LT L = Vilnius O = BalTstamp UAB CN = BalTstamp QTSA TSU2
extensions	Gali turėti *qcStatements* plėtinį su *esi4-qtstStatement-1* požymiu

3.7.2 Laikrodžių sinchronizavimas su UTC

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

a) 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;

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

c) TSA naudojamos sistemos geba aptikti, kad laikas, kuris būtų nurodytas laiko žymoje, neleistinai nukrypsta, arba prarandama sinchronizacija su UTC;

d) aptikus, kad laikas, kuris būtų nurodytas laiko žymoje, neleistinai nukrypsta, arba prarandama sinchronizacija su UTC, laiko žymų teikimas sustabdomas;

e) TSA užtikrina, kad atitinkamai tarnybai paskelbus apie keliamąją sekundę (*leap second*), nesutriktų laikrodžių sinchronizavimas, o keliamoji sekundė būtų įvedama atitinkamos dienos paskutiniąją minutę. Sistemos užfiksuoja tikslų šių pokyčių laiką. Jei keliamoji sekundė yra įterpiama, siekiant išvengti dviprasmiškumo ir problemų

sistemose, negalinčiose tinkamai dirbti su 61 sekunde minutėje, laiko žymos neteikiamos per keliamąją sekundę ir sekundę iki jos.

3.8 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 [EN 319 421] 7.6.2 ir 7.6.3 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.

3.9 Veikimo saugumas

Kritinėms funkcijoms, kaip nustatyta rizikos vertinime, TSA naudoja patikimąsias sistemas ir produktus, apsaugotus nuo modifikavimo galimybės. TSA užtikrina, kad jos sistemų dalys būtų saugios ir kad su jomis būtų dirbama teisingai bei su kuo mažesne sutrikimų rizika.

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;
c) TSA sistemos dalių visuma ir informacija yra apsaugota nuo virusų, piktybinių ir nenumatytų programų;
d) su laikmenomis, naudojamomis patikimosiose TSA sistemose, elgiamasi saugiai, kad jos būtų apsaugotos nuo pakenkimo, vagystės, neįgaliotos prieigos ir pasenimo;
e) siekiant apsaugoti laikmenas nuo pasenimo ir nusidėvėjimo per įrašų saugojimo laikotarpį, taikomos laikmenų tvarkymo procedūros;
f) yra nustatytos ir vykdomos procedūros visoms pasitikėjimo ir administracinėms pareigybėms, nuo kurių priklauso laiko žymos paslaugų teikimas;
g) Stebimi ir prognozuojami pajėgumo poreikiai, kad būtų užtikrinta reikiama duomenų apdorojimo sparta ir saugojimo talpa.

3.10 Tinklo saugumas

TSA eksploatuoja ir saugo TSU sistemas saugioje zonoje, į kurią gali patekti tik pasitikėjimo pareigas einantys darbuotojai. TSU sistemų konfigūracija yra sugriežtinta taip, kad būtų naudojamos tik veikimui reikalingos paskyros, programos, servisai, protokolai ir prievadai. Šios praktikos įgyvendinimui TSA informacijos saugumo taisyklėse numatytos pasitikėjimo pareigos su atitinkamomis atsakomybėmis.

3.11 Incidentų valdymas

TSA nuolat stebi sistemų veiklą prieigos prie sistemų ir jų naudojimosi atžvilgiu.

Neįprasta sistemų veikla, kuri reiškia galimus saugumo pažeidimus, įskaitant galimus įsilaužimus, yra aptinkama ir apie ją pranešama pasiunčiant pavojaus signalą.

TSA veikia operatyviai ir koordinuotai, kad įvykus incidentui būtų greitai reaguojama ir kad galima žala dėl saugumo spragų būtų kuo mažesnė. Apie incidentus pranešama kaip numatyta incidentų valdymo procedūrose.

Pranešimo apie incidentus bei atsako į juos procedūros yra taikomos taip, kad nuostoliai dėl saugumo incidentų ir sutrikimų būtų kuo mažesni.

3.12 Įrodymų kaupimas

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

Bendroji dalis

a) TSA savo informacijos saugumo taisyklėse 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 (žr. [EN 319 421] 6.3 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.

3.13 Veiklos tęstinumo valdymas

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.

3.14 TSA veiklos nutraukimas

TSA siekia, 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) TSA turi aktualų veiklos nutraukimo planą;
b) prieš nutraukdama laiko žymų paslaugos teikimą, TSA atlieka bent šias procedūras:
   - abonentams, pasitikintiems asmenims ir priežiūros įstaigai pateikia informaciją apie veiklos nutraukimą ne vėliau kaip prieš 3 mėnesius iki veiklos nutraukimo dienos, pasinaudojant turimais kontaktiniais duomenimis;
   - 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 (žr. [EN 319 421] 7.14 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;
c) TSA yra numačiusi, kaip padengti išlaidas, reikalingas šiems minimaliems reikalavimams įvykdyti, jei TSA bankrutuotų ar dėl kitų priežasčių nebegalėtų padengti šių išlaidų pati;
d) TSA šiuose savo veiklos nuostatuose yra numačiusi paslaugų teikimo sustabdymo nuostatas, apimančias:
   - pranešimą visiems susijusiems asmenims;
   - TSA įsipareigojimų perdavimą kitoms šalims;
e) TSA imasi priemonių, kad TSU sertifikatai būtų atšaukti.

3.15 Teisinių reikalavimų vykdymas

TSA užtikrina teisinių reikalavimų vykdymą, būtent:

a) atitiktis Reglamento (ES) Nr. 910/2014 [eIDAS] reikalavimams patvirtinama bent kas 24 mėnesius, akredituotai atitikties vertinimo įstaigai atliekant auditą;
b) TSA nekelia jokių specialių reikalavimų paslaugų naudojimui, kurie ribotų galimybes jomis naudotis neįgaliems asmenims;
c) TSA užtikrina Europos duomenų apsaugos direktyvos 95/46/EB, kaip ji yra perkelta į Lietuvos teisės aktus, reikalavimų vykdymą:
   - laiko žymų paslaugų teikimo tikslais TSA reikalauja pateiki laiko žymų užklausą, kaip apibrėžta [EN 319 422], kartu su autentifikavimo duomenimis, jei tokių reikia pasirinktam autentifikavimo būdui;
   - TSA apdoroja šiuos duomenis kartu su komunikacinio lygmens atributais, kaip to reikia laiko žymos išdavimui ir taikomų standartų reikalavimų įgyvendinimui, įskaitant stebėjimą saugumo, apskaitos ir pajėgumų planavimo tikslais;
   - jokie kiti duomenys, įskaitant asmens duomenis, nėra kaupiami ar apdorojami teikiant paslaugas;

- TSA imasi reikiamų techninių ir organizacinių priemonių tam, kad būtų užkirstas kelias neįgaliotam ar neteisėtam gautų duomenų apdorojimui, atskleidimui, netyčiniam praradimui, sunaikinimui bei sugadinimui.

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 – saugotinų duomenų pametimas, pavogimas, modifikavimas, neteisėtas panaudojimas arba kitoks 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-stamping 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*) – vieta internete, kurioje skelbiama laiko žymų tarnybos informacija naudotojams.

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

BTSP – geriausių praktikų laiko žymų taisyklės (angl. *best practices time-stamp policy*).

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-stamping 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

[eIDAS] – 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB.

[EN 319 401] – Standartas ETSI EN 319 401: „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[EN 319 421] – Standartas ETSI EN 319 421: „Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

[EN 319 422] – Standartas ETSI EN 319 421: „Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

[FIPS 140] – Standartas FIPS PUB 140-2 „Security Requirements for Cryptographic Modules" (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf).