BALTSTAMP
LAIKO ŽYMŲ TAISYKLĖS

Unikalus objekto ID (OID): **1.3.6.1.4.1.38424.1.3.1**
Versija: 1.1

Galioja nuo 2014-07-25

2014

TURINYS

BalTstamp laiko žymų taisyklių istorija:

Versija	Data	Aprašas
Versija 0.1	2011-04-11	Pirmoji projekto versija
Versija 1.0	2011-04-15	Pirma versija
Versija 1.1	2014-07-23	Pirma versija su redakciniais pakeitimais

BalTstamp laiko žymų taisyklių tvirtinimas:

Dokumento rengimas	Vardas, pavardė	Data	Parašas
Dokumentą parengė	Emilis Urba	2014-07-01	
Dokumentą patikrino	Rimantas Miškinis	2014-07-21	
Dokumentą patvirtino	Vincentas Vitkauskas	2014-07-23	

1 ĮVADAS

Uždaroji akcinė bendrovė „BalTstamp" (toliau BalTstamp) įsteigta 2011 m. sausio 31 d. tiksline paskirtimi teikti kvalifikuotų laiko žymų paslaugas juridiniams ir fiziniams asmenis 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 (toliau – TSP, pagal anglišką atitikmenį *time stamp policy*) nustato BalTstamp laiko žymų tarnybos (toliau – TSA, pagal anglišką atitikmenį *time-stamping 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. Siekiant pagrįsti laiko žymų naudotojų pasitikėjimą TSA teikiamomis laiko žymomis, TSP skelbiamos viešai.

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

TSP 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 žymos paslaugas, vykdo laiko žymos sudarymo ir valdymo funkcijas.

1.2 Identifikavimas

Šių TSP unikalus identifikatorius (OID) yra **1.3.6.1.4.1.38424.1.3.1**; jo laukų reikšmės nurodytos *lentelėje* ***Nr. 1:***

Lentelė Nr. 1. TSP unikalaus identifikatoriaus laukų reikšmės

Pavadinimas	**Reikšmė**
ISO	1
ISO pripažinta organizacija	3
JAV Gynybos departamentas	6
Internetas	1
Privati įmonė	4
IANA registruota privati įmonė	1
Uždaroji akcinė bendrovė „BalTstamp"	38424
Padalinys BalTstamp	1
Dokumento tipas (laiko žymų taisyklės)	3
Dokumento versija	1

Galiojanti TSP 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 sudaryti iki laiko žymoje nurodyto laiko. TSA teikiamų laiko žymų naudotojai gali būti fiziniai ir juridiniai asmenys, kuriems reikalingos TSA teikiamos laiko žymos.

TSP 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 identifikatorių, apibrėžtą 1.2 skyriuje, pažymi, kad laiko žyma atitinka šias TSP. Taip TSA prisiima visus TSP nustatytus įsipareigojimus ir vykdo visus joje aprašytus reikalavimus veiklai.

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

1.5 Kontaktinė informacija

Šias TSP tvarko Uždaroji akcinė bendrovė „BalTstamp", kurios 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 turi užtikrinti pasirinktų patikimų TSP reikalavimų tinkamą įgyvendinimą. TSA turi užtikrinti, kad būtų laikomasi:

a) procedūrų, nurodytų šiose TSP, net jei TSA paslaugų funkcionalumą perimtų subrangovai;

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

Visas laiko žymų paslaugas TSA turi teikti laikydamasi savo TSPS.

2.1.2 TSA įsipareigojimai abonentams

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

2.2 Laiko žymų abonentų įsipareigojimai

Abonentas, gavęs laiko žymą, turi patikrinti, ar ji pasirašyta teisingai ir ar privatusis raktas, kuriuo buvo pasirašyta, nėra sukompromituotas (atskleistas tretiesiems asmenims ar dėl kitų priežasčių netinkamas naudoti).

Abonentas privalo laikytis laiko žymos naudojimo apribojimų (jei jų būtų) ir atsargumo priemonių, nurodytų šiose TSP, o taip pat sutartyse, sudarytose su paslaugų teikėju. Be to, abonentas turi vykdyti įpareigojimus, išdėstytus TSA laiko žymų teikimo sąlygose.

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).

Pastaba: 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.

Be to, laiko žymomis pasitikintys asmenys privalo laikytis laiko žymos naudojimo apribojimų ir atsargumo priemonių, nurodytų šiose taisyklėse, o taip pat sutartyse, sudarytose su paslaugų teikėju.

2.4 Atsakomybė

TSA atsako už neteisėtus veiksmus ir padarytą žalą abonentams atlygina Lietuvos Respublikos įstatymų nustatyta tvarka ir neprisiima jokių papildomų įsipareigojimų, išskyrus tuos, kurie 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 „Dėl Laiko žymos formavimo paslaugų teikimo tvarkos aprašo patvirtinimo" (Žin., 2011, Nr. 48-2349).

2.5.2 Ginčų sprendimo tvarka

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

2.6 Mokesčiai

TSA gali nustatyti laiko žymos paslaugų kainas.

2.7 Intelektinės nuosavybės teisės

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

3 REIKALAVIMAI TSA VEIKLAI

3.1 Veiklos nuostatai ir laiko žymų teikimo sąlygos

3.1.1 Laiko žymų tarnybos veiklos nuostatai

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

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

b) TSA turi turėti savo veiklos nuostatus, kuriuose aprašytos praktikos ir procedūros, naudojamos šiose TSP nustatytiems reikalavimams įvykdyti;

c) TSA veiklos nuostatai turi nustatyti visų išorės organizacijų, palaikančių TSA paslaugas, įsipareigojimus, įskaitant taikytinas politikas ir praktikas;

d) TSA veiklos nuostatai ir kita dokumentacija turi būti prieinami abonentams ir pasitikintiems asmenims, kas leistų įvertinti, kaip ši dokumentacija atitinka TSP;

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

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

g) vyresnioji TSA vadovybė turi užtikrinti, kad veiklos nuostatai būtų tinkamai vykdomi;

h) TSA turi nustatyti savo nuostatų peržiūros tvarką, taip pat ir atsakomybę už jų priežiūrą;

i) TSA turi pranešti apie numatomus veiklos nuostatų pakeitimus, o juos patvirtinusi pagal (f), atnaujintus TSPS turi nedelsdama padaryti prieinamus pagal (d) abonentams ir pasitikintiems asmenims.

3.1.2 Laiko žymų teikimo sąlygos

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

Laiko žymų teikimo sąlygose TSA turi pateikti 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 įstatymų reikalavimų laiko žymų atžvilgiu;

l) atsakomybės apribojimus;

m) ginčų ir nesutarimų sprendimo tvarką;

n) ar buvo įvertinta, kaip TSA atitinka savo nuostatus, ir, jei taip, kokia nepriklausoma įstaiga tai atliko.

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

3.2 Raktų tvarkymo ciklas

3.2.1 TSA raktų generavimas

Savo kriptografinius raktus TSA turi generuoti esant kontroliuojamoms sąlygoms. Būtent:

a) TSU pasirašymo raktą kriptografiniame modulyje fiziškai saugioje aplinkoje (patalpoje, apsaugotoje nuo neįgaliotų asmenų prieigos) turi generuoti 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 TSPS.

b) kriptografinis modulis, kuriame generuojamas TSU pasirašymo raktas, turi atitikti trečiojo lygio saugumo reikalavimus pagal standartą [FIPS 1] arba reikalavimus, kuriuos nustato [CWA 1], arba jis turi būti patikimoji sistema, užtikrinanti EAL 4 saugumo kriterijus pagal [ISO/IEC 1] ar ekvivalenčius;

c) TSU rakto generavimo algoritmas, gaunamo pasirašymo rakto ilgis bei pasirašymo algoritmas, naudojamas laiko žymoms pasirašyti, turi būti kurios nors nacionalinės priežiūros įstaigos pripažinti tinkamais laiko žymoms, kokias teikia TSA, arba atitikti egzistuojančią praktiką, laiko žymų tarnybų taikomą laiko žymų sudarymui.

3.2.2 Privačiųjų TSU raktų apsauga

TSA turi užtikrinti savo TSU privačiųjų raktų apsaugą ir slaptumą. Būtent:

a) TSU privatieji pasirašymo raktai turi būti laikomi ir naudojami kriptografiniame modulyje, kuris atitinka trečiojo lygio saugumo reikalavimus pagal standartą [FIPS 1] arba reikalavimus, kuriuos nustato [CWA 1], arba jis yra patikimoji sistema, užtikrinanti EAL 4 saugumo kriterijus pagal [ISO/IEC 1] ar ekvivalenčius;

b) jei daromos TSU privačiųjų raktų atsarginės kopijos, raktus fiziškai saugioje aplinkoje (patalpoje, apsaugotoje nuo neįgaliotų asmenų prieigos) turi kopijuoti, saugoti ir atkurti 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 TSPS;

c) atsarginės privačiųjų raktų kopijos turi būti laikomos kriptografiškai apsaugotose laikmenose, kitose patalpose nei kriptografinis modulis. Patalpos saugumo lygis atitinka TSA veiklos nuostatuose nurodytas sąlygas. TSU sertifikato gyvavimo bei atitinkamų parašo formavimo duomenų (privačiojo rakto) galiojimo trukmė turi būti nustatoma atsižvelgiant į naudojamus duomenų santraukos apskaičiavimo ir parašo kūrimo algoritmus bei laiko žymoms tvirtinti naudojamo elektroninio parašo rakto ilgį.

3.2.3 TSU viešojo rakto skelbimas

TSA turi užtikrinti, 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 turi būti skelbiamas viešojo rakto sertifikate;

b) TSU turi naudoti parašo tikrinimo (viešojo) rakto sertifikatą, išduotą sertifikavimo tarnybos, užtikrinančios tokį pat arba aukštesnį saugumo lygį nei aprašytas šiose TSP.

3.2.4 TSU kriptografinių raktų keitimas

TSU sertifikato galiojimo trukmė turi būti nustatoma ne ilgesnė nei tas laikas, per kurį pasirinktas algoritmas ir rakto ilgis gali būti laikomas tinkamu naudoti. TSU sertifikato galiojimo trukmė nustatoma ne ilgesnė už TSU raktų poros galiojimo laikotarpį. TSU sertifikato keitimas išlaikant tą pačią raktų porą netaikomas.

3.2.5 TSU kriptografinių raktų poros gyvavimo ciklo pabaiga

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

a) TSA turi turėti darbines arba technines procedūras, pagal kurias senas raktas, pasibaigus jo galiojimui, pakeičiamas nauju;

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

c) laiko žymų generavimo sistema turi atmesti bet kokius mėginimus sudaryti laiko žymą, jei privatusis

pasirašymo raktas nebegalioja.

3.2.6 Kriptografinio modulio, naudojamo laiko žymoms pasirašyti, gyvavimo ciklo tvarkymas

TSA turi užtikrinti kriptografinės įrangos saugumą viso jos gyvavimo ciklo metu.

Būtent, TSA turi užtikrinti, 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 dubliavimas 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.

3.3 Laiko žymų teikimas

3.3.1 Laiko žyma

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

a) laiko žymoje turi būti nurodytas TSP identifikatorius;

b) kiekviena laiko žyma turi turėti savo unikalų identifikatorių;

c) TSU naudojamas laikas turi būti 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 turi būti neteikiamos;

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

g) laiko žyma turi būti pasirašyta raktu, sukurtu išimtinai tam tikslui;

h) laiko žymoje turi būti:

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

Laiko žymos sandara turi atitikti [ETSI 2] reikalavimus.

3.3.2 Laikrodžių sinchronizavimas su UTC

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

- TSU laikrodžiai turi būti 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 turi būti apsaugoti nuo pavojų, galinčių sukelti nepastebimus šuolius, galinčius pažeisti laikrodžių kalibravimą. Tokias grėsmes gali sukelti neįgaliotų darbuotojų įsikišimas, radijo ar elektros trikdžiai ir pan.;
- TSA turi užtikrinti, 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 turi užtikrinti, kad būtų taikomos adekvačios ir atitinkančios pripažintą geriausią praktiką administracinės ir vadybinės procedūros. Būtent:

Bendroji dalis

a) TSA turi prisiimti atsakomybę už laiko žymos paslaugų teikimą visais atžvilgiais pagal šias TSP, nesvarbu, ar kurios nors funkcijos būtų patikėtos subrangovams, ar ne. TSA aiškiai apibrėžia trečiųjų šalių atsakomybę, be to, sudaro reikiamus susitarimus tam, kad subrangovai privalėtų imtis visų TSA reikalaujamų priemonių. TSA imasi atsakomybės už tai, kad visų dalyvaujančių šalių veiklos nuostatai būtų paskelbti;

b) TSA turi nustatyti informacinio saugumo gaires per atitinkamą aukšto lygio forumą, atsakingą už informacinio saugumo taisyklių nustatymą. TSA turi užtikrinti šių taisyklių paskelbimą ir perdavimą visiems darbuotojams, kurių darbui tai reikalinga;

c) informacinio saugumo infrastruktūra, reikalinga saugumui užtikrinti, turi būti išlaikoma nuolat. Bet kokie pokyčiai, turintys reikšmės saugumui, turi būti tvirtinami TSA vadovybės.

d) saugumo priemonės ir darbinės procedūros TSA įrangai, patalpoms, sistemoms ir informacijos ištekliams, reikalingiems laiko žymoms teikti, turi būti dokumentuojamos, tvarkomos ir vykdomos;

e) TSA turi užtikrinti, kad informacinis saugumas būtų išlaikomas ir tada, kai atsakomybė už TSA funkcijas yra perduota kitai įstaigai.

3.4.2 Išteklių klasifikavimas ir vadyba

TSA turi užtikrinti, kad jos informaciniai ir kiti ištekliai būtų tinkamai saugomi. Būtent, TSA turi inventorizuoti visus išteklius ir klasifikuoti jų apsaugos reikalavimus pagal rizikos analizę.

3.4.3 Paslaugų saugumas personalo atžvilgiu

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

a) TSA turi samdyti 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, turi būti nustatyti pareiginėse instrukcijose. Pasitikėjimo pareigos, nuo kurių priklauso TSA veiklos saugumas, turi būti aiškiai aprašytos;

c) TSA darbuotojai (ir nuolatiniai, ir laikini) turi turėti pareigines instrukcijas, parengtas pareigų ir mažiausių privilegijų atskyrimo požiūriu. Instrukcijos turi nustatyti pareigybių kritiškumą, pagrįstą pareigomis ir prieigos lygiais, patikimumo ir kvalifikacijos patikrinimu bei mokymu. Kur taikytina, bendrosios ir specifinės TSA pareigybės aprašytos skirtingai. Pareiginės instrukcijos apima sugebėjimų ir patirties reikalavimus;

d) darbuotojai turi vykdyti administracines ir vadybines procedūras ir procesus, kurie atitinka TSA informacinio saugumo vadybos procedūras;

Laiko žymų teikimo vadovybei taikytini papildomi reikalavimai:

e) TSA turi samdyti 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 turėti 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 atsarginės kopijas ir atlikti atkūrimą;
- auditorius, įgaliotus peržiūrėti TSA patikimųjų sistemų archyvus ir audito įrašus (audit logs);

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

i) TSA negali skirti 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 negali būti leidžiama eiti pasitikėjimo pareigų, kol nebus atliktas reikalingas patikrinimas.

3.4.4 Fizinis ir aplinkos saugumas

TSA turi užtikrinti, kad galimybė patekti į kritiškai svarbias vietas būtų kontroliuojama, o fizinis pavojus ištekliams būtų kuo mažesnis. Būtent (bendroji dalis):

a) turi būti laikomasi tokių reikalavimų laiko žymų teikimui ir vadybai:
- patalpos ir įranga, susijusios su laiko žymų paslaugomis, turi būti fiziškai prieinamos tik atitinkamai įgaliotiems asmenims;
- turi būti įdiegtos priemonės, skirtos išvengti išteklių praradimui bei sugadinimui, informacijos nutekėjimui ir vagystei, o taip pat darbo nutrūkimui;
- turi būti įdiegtos priemonės, skirtos išvengti informacijos bei jos apdorojimo įrangos sukompromitavimui bei vagystei;

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

c) turi laikytis papildomų reikalavimų laiko žymų teikimo valdymui:
- laiko žymų teikimo valdymo įranga turi dirbti aplinkoje, kuri fiziškai apsaugotų įrangą nuo sukompromitavimo dėl neįgaliotos prieigos prie duomenų ar sistemų;
- fizinį saugumą turi užtikrinti aiškiai nustatytas saugumo perimetras apie laiko žymų teikimo valdymo įrangą. Saugumo perimetro viduje negali būti patalpų, kurios kartu priklausytų kokioms nors kitoms organizacijoms;
- turi būti 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;
- turi būti įdiegtos priemonės, skirtos su laiko žymomis susijusios įrangos (taip pat ir programinės), informacijos bei laikmenų apsaugai nuo neįgalioto išnešimo.

3.4.5 Darbo tvarkymas

TSA turi užtikrinti, 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 turi būti apsaugota nuo virusų, piktybinių ir nenumatytų programų;

b) turi būti 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, turi būti elgiamasi saugiai, kad jos būtų apsaugotos nuo pakenkimo, vagystės, neįgaliotos prieigos ir pasenimo;

d) turi būti nustatytos ir vykdomos procedūros visoms pasitikėjimo ir administracinėms pareigybėms, nuo kurių priklauso laiko žymos paslaugų teikimas;

Laikmenų tvarkymas ir saugumas

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

Sistemos planavimas

f) turi būti stebimi ir prognozuojami pajėgumo poreikiai, kad būtų užtikrinta reikiama duomenų apdorojimo sparta ir saugojimo talpa;

Pranešimas apie incidentus bei atsakas į juos

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

Laiko žymų valdymui turi būti taikomos papildomos priemonės:

Darbinės procedūros ir atsakomybė

h) saugumo užtikrinimas turi būti 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;
- audito žurnalų aktyvų stebėjimą, įvykių analizę ir reagavimą į juos;
- darbą su laikmenomis ir jų apsaugą;
- apsikeitimą duomenimis ir programine įranga.

Šiuos darbus turi tvarkyti 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 turi užtikrinti, 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, turi būti įdiegta ugniasienė, sukonfigūruota taip, kad uždraustų visus protokolus ir kreipinius, nereikalingus TSA darbui;

b) TSA turi efektyviai administruoti 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 turi būti apribota pagal prieigos kontrolės politiką, o TSA sistema turi turėti pakankamai kompiuterinio saugumo priemonių, kad būtų atskirtos TSPS numatytos pasitikėjimo pareigos, įskaitant saugumo administratoriaus ir darbinių funkcijų atskyrimą. Sistemos vidinių programų naudojimas turi būti apribotas ir griežtai kontroliuojamas;

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

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

Laiko žymų valdymui turi būti taikomos papildomos priemonės:

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

g) turi būti 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 turi naudoti 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 jos vardu, saugumo reikalavimų analizė turi būti atliekama nuo pat reikalavimų specifikavimo ir projektavimo etapų;

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

3.4.8 TSA paslaugų sukompromitavimas

TSA turi užtikrinti, 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 turi aptarti tikrą ar įtariamą TSU privačiųjų pasirašymo raktų sukompromitavimą bei TSU laikrodžio sieties praradimą, kuris galėjo įtakoti išduotoms laiko žymoms;

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

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

d) rimto TSA veiklos sukompromitavimo arba TSU kalibravimo praradimo atveju, jei tik įmanoma, abonentams ir pasitikintiems asmenims turi būti atskleista informacija, leidžianti nustatyti, kurias būtent laiko žymas šis įvykis galėjo įtakoti, jei tai nepažeidžia TSA vartotojų privatumo arba TSA paslaugų saugumo.

3.4.9 TSA veiklos nutraukimas

TSA turi stengtis, kad jos veiklos sustabdymo atveju galimi paslaugos teikimo pertraukimai, kuriuos patirtų abonentai ir pasitikintys asmenys, būtų kuo trumpesni, ir turi užtikrinti informacijos, reikalingos laiko žymoms patikrinti, tolesnį teikimą. Būtent:

a) prieš nutraukdama laiko žymų paslaugos teikimą, TSA turi atlikti bent jau šias procedūras:

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

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

c) TSA savo veiklos nuostatuose turi būti numačiusi paslaugų teikimo sustabdymo nuostatas, apimančias:

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

d) TSA turi imtis priemonių, kad TSU sertifikatai būtų atšaukti.

3.4.10 Teisinių reikalavimų vykdymas

TSA turi užtikrinti teisinių reikalavimų vykdymą, būtent:

a) TSA turi užtikrinti Europos duomenų apsaugos direktyvos, kaip ji yra perkelta į Lietuvos įstatymus, o taip pat [ADA] reikalavimų vykdymą;

b) TSA turi imtis 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 turi saugoti iš naudotojų gautą informaciją nuo atskleidimo, nebent tam būtų duotas jų sutikimas ar teismo sankcija.

3.4.11 Informacijos apie TSA darbą kaupimas

TSA turi užtikrinti, kad nustatytą 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 turi būti nustačiusi, kokius įvykius ir duomenis reikia fiksuoti;

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

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

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

e) TSA turi užrašyti svarbių aplinkos įvykių, raktų tvarkymo, laikrodžių sinchronizavimo tikslų laiką;

f) įrašai, susiję su laiko žymų paslaugomis, turi būti 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 turi būti daromi taip, kad nebūtų galima lengvai jų ištrinti ar sunaikinti (jei jie nėra patikimai perrašyti į ilgalaikio saugojimo laikmenas) laikotarpį, kurį jie turi būti saugomi;

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

TSU raktų tvarkymas

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

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

Laikrodžių sinchronizavimas

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

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

3.5 Organizaciniai dalykai

TSA turi užtikrinti, 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 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 politiką ir procedūrą, skirtą spręsti skundams ir ginčams, gautiems dėl laiko žymos paslaugų teikimo ar kitų susijusių dalykų;

i) jei paslaugos teikiamos naudojantis subrangovais ar kitomis trečiosiomis šalimis, TSA turėtų tinkamai dokumentuotas sutartis bei sutartinius ryšius.

3.6 TSP keitimo procedūros

TSP gali būti keičiamos pastebėjus jose klaidų, 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 kuriuos atlikus turi būti keičiamas TSP OID;

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

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

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

esminiai.

TSP yra prižiūrimos, keičiamos ir tvirtinamos pagal tokią procedūrą:

a) už saugumą atsakingi TSA darbuotojai kartą per metus, skaičiuojant nuo paskutinės TSP redakcijos, peržiūri ir įsitikina TSP tinkamumu. Jei nustato, kad TSP reikia keisti, inicijuoja TSP keitimą;

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

c) darbuotojai, kuriems tai pavesta, rengia naują TSP redakciją;

d) jei pakeitimas esminis, parengtos naujos TSP redakcijos projektas 30 kalendorinių dienų skelbiamas saugykloje internete ir laukiama susijusių šalių pastabų. Atsižvelgus į gautas pastabas (jei jų būtų), nauja TSP redakcija teikiama tvirtinti. Neesminių pastabų atveju nauja redakcija teikiama tvirtinti iš karto, tik ją parengus;

e) sprendimą teikti tvirtinti naują TSP redakciją priima TSA vadovybė; esminių pakeitimų atveju pakeičiamas TSP redakcijos versijos pirmasis skaitmuo bei atitinkamai OID versijos elementas (paskutinysis skaitmuo). Atlikus neesminį pakeitimą, pakeičiami TSP redakcijos versijos antrasis ir tolimesni skaitmenys;

f) naują TSP redakciją tvirtina BalTstamp direktorius;

g) patvirtinta nauja TSP redakcija paskelbiama saugykloje.

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 saugumo modulis) (angl. *hardware security module – HSM*) – aparatinė ir programinė įranga, kuri naudojama šifravimo raktų poroms – privatiesiems ir viešiesiems raktams – generuoti, privatiesiems raktams saugoti ir/arba elektroniniams parašams kurti.

Elektroninis parašas (parašas) – duomenys, kurie įterpiami, prijungiami ar logiškai susiejami su kitais duomenimis jų autentiškumui patvirtinti ir pasirašančiajam asmeniui identifikuoti.

Kompromitacija – saugotinų duomenų pametimas, pavogimas, modifikavimas, neteisėtas panaudojimas arba kitoks saugumo pažeidimas.

Kriptografinis modulis – žiūr. aparatinis saugumo modulis.

Kvalifikuotas sertifikatas – sertifikatas, kurį sudarė Lietuvos Respublikos Vyriausybės ar jos įgaliotos institucijos nustatytus reikalavimus atitinkantis sertifikavimo paslaugų teikėjas.

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 paslaugų teikėjo, o taip pat laiko žymos naudotojų teises ir pareigas. Laiko žymų taisyklės nustato ir įgyvendina paslaugų teikėjas, o laiko žymų naudotojas renkasi tokį paslaugų teikėją, kurio taisyklės ir kitos sąlygos jam priimtinos.

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

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

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

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

Saugykla (angl. *repository*) – vieta internete, kurioje skelbiama laiko žymų tarnybos informacija naudotojams.

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

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

BIPM – Tarptautinis svorių ir matų biuras (pr. *Bureau International des Poids et Mesures*).
CA – sertifikatų tarnyba (angl. *certificate authority*).
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 tarnybos 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

[ADA] – LR asmens duomenų teisinės apsaugos įstatymas;

[ELP] – LR elektroninio parašo įstatymas ir jo 4, 8, 14, 16 straipsnių pakeitimo ir papildymo įstatymas;

[ETSI 1] – standartas 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“;

[CWA 1] – Common Workshop Agreement 14167-2;

[ISO/IEC 1] – standartas ISO/IEC 15408 „Information technology – Security techniques – Evaluation criteria for IT security“. Part 1 – Introduction and general model; Part 2 – Security functional components; Part 3 – Security assurance components.