BALTSTAMP LAIKO ŽYMŲ TEIKIMO SĄLYGOS

1. Paskirtis. Uždarosios akcinės bendrovės „BalTstamp" laiko žymų tarnyba BalTstamp (toliau tekste TSA – angl. *time-stamping authority*) skelbia laiko žymų abonentams ir pasitikinčioms šalims laiko žymų teikimo ir naudojimo bendrąsias sąlygas. Laiko žymų tarnybos BalTstamp teikiamos laiko žymų formavimo paslaugos atitinka Lietuvos Respublikos ryšių reguliavimo tarnybos (RRT) direktoriaus 2011 m. balandžio 19 d. įsakymo Nr. 1V-407 „Laiko žymos formavimo paslaugų teikimo tvarka" (Žin., 2011, Nr. 48-2349) ir standartų LST ETSI TS 102 023 „Strateginiai reikalavimai, keliami laiko žymėjimo paslaugų teikėjams" bei LST ETSI TS 101 861 „Laiko žymėjimo profilis" reikalavimus. Šias sąlygas gali papildyti TSA ir abonentų sudarytos sutartys.

2. Kontaktų duomenys. Visais su laiko žymų teikimu susijusiais klausimais galima kreiptis nurodytu adresu:

Asmuo:	Vincentas Vitkauskas, uždarosios akcinės bendrovės „BalTstamp" direktorius
Adresas:	Dariaus ir Girėno g. 40, LT-02189 Vilnius
Tel.:	+370-682-58844
Faksas:	+370-5-2167212
URL:	http://www.baltstamp.lt/
El. paštas:	info@baltstamp.lt

Laiko žymos suformavimui galima kreiptis standartiniu protokolu RFC 3161 adresu: http://tsa.baltstamp.lt, tačiau neregistruotiems naudotojams taikomas kreipinių skaičiaus apribojimas: ne daugiau kaip 100 kreipinių per kalendorinį mėnesį, mėnesio pradžią ir pabaigą skaičiuojant UTC laiku. Registruotų naudotojų kreipiniai aptarnaujami:

a) saugiu (https) protokolu ir identifikuojami vardu bei slaptažodžiu pagal HTTP „basic" schemą;

b) atviru (http) protokolu ir identifikuojami pagal IP adresą.

Kreipinių srautui taikomi apribojimai: ne daugiau kaip 5 kreipiniai per sekundę ir ne daugiau kaip 1000 kreipinių per valandą, nebent sutartyje su abonentu numatyta kitaip.

Naudotojų registravimui galima kreiptis čia nurodytais kontaktų duomenimis.

3. Laiko žymų taisyklės. Visos laiko žymos sudaromos laikantis galiojančių BalTstamp laiko žymų taisyklių (OID:1.3.6.1.4.1.38424.1.3.1).

Pagal šias taisykles sudarytų laiko žymų pagrindinė paskirtis yra sukaupti kvalifikuoto elektroninio parašo galiojimo įrodymus per visą pasirašyto elektroninio dokumento galiojimo laikotarpį, t.y. kad kvalifikuotas elektroninis parašas yra patvirtintas galiojančiu kvalifikuotu sertifikatu, kaip to reikalauja Lietuvos Respublikos elektroninio parašo įstatymas (Žin., 2000, Nr. 61-1827; Žin., 2002, Nr. 64-2572). Laiko žyma leidžia įrodyti, kad elektroninis parašas buvo sukurtas iki žymoje nurodyto laiko. Taip pat, 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.

4. Duomenų santrauka. Duomenų, kuriems reikalinga laiko žyma, santraukai (angl. *hash*) sudaryti gali būti naudojami šie algoritmai: SHA1, SHA256, SHA384, SHA512.

5. Sertifikatų galiojimas. TSA turi du sertifikatus, kuriais laiko žymų įrenginiuose (TSU – angl. time stamping unit) patvirtinamos sudarytos laiko žymos. Vienas sertifikatas galioja 5 metus; galiojimas baigiasi 2016-06-13. Kitas sertifikatas galioja 10 metų; galiojimas baigiasi 2022-05-15.

6. Laiko žymų tikslumas. Laiko žymoje nurodoma laiko vertė laiko žymos sudarymo momentą ženklina ***dviejų dešimtųjų sekundės tikslumu***, remiantis TSA įrenginių pastovia sietimi su Valstybiniu

laiko ir dažnio etalonu, atkuriančiu visuotinio koordinuotojo laiko Lietuvos skalę UTC(LT), kurios sietis su UTC užtikrinama nuolatinių palyginimų būdu Fizinių ir technologijos mokslų centro (FTMC) Metrologijos skyriaus Laiko ir dažnio etalono laboratorijoje, dalyvaujančioje Pasaulio suderintojo laiko generavime, kaip to reikalauja RRT direktoriaus 2011 m. balandžio 19 d. įsakymas Nr. 1V-407 ir standartas LST ETSI TS 102 023. Sieties charakteristikos skelbiamos Tarptautinio svorių ir matų biuro (BIPM – pr. *Bureau International des Poids et Mesures*) leidinyje „Circular T".

7. Naudojimo apribojimai. 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.

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

9. 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).

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

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

b) laiko žymai formuoti panaudoti duomenų santraukos (angl. *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.

Informacija, reikalinga laiko žymoms tikrinti, teikiama nenutrūkstamai.

11. Įvykių įrašai. TSA sistemos operacijų ir veiklos registravimo žurnalai (angl. *event logs*), kurių duomenis prireikus galima panaudoti teisiniam įrodymui, saugomi 10 metų, ir ne trumpiau nei 1 metai po atitinkamo pasirašymo rakto galiojimo pabaigos.

12. Taikoma teisė. TSA veikia Lietuvos Respublikoje ir vykdo jos įstatymus ir teisės norminius aktus. Pagrindiniai teisės ir norminiai aktai yra šie:

- Lietuvos Respublikos elektroninio parašo įstatymas (Žin., 2000, Nr. 61-1827; Žin., 2002, Nr. 64-2572);
- Lietuvos Respublikos ryšių reguliavimo tarnybos (RRT) direktoriaus 2011 m. balandžio 19 d. įsakymo Nr. 1V-407 „Laiko žymos formavimo paslaugų teikimo tvarka" (Žin., 2011, Nr. 48-2349);
- LST ETSI TS 102 023 „Strateginiai reikalavimai, keliami laiko žymėjimo paslaugų teikėjams";
- LST ETSI TS 101 861 „Laiko žymėjimo profilis".

13. Skundų ir ginčų sprendimas. Visi skundai ir ginčai tarp TSA ir laiko žymų paslaugų naudotojų sprendžiami geranoriškomis derybomis. Ginčo neišsprendus, kreipiamasi į Lietuvos teisėsaugos įstaigas.

14. Atsakomybė, garantija ir jos apribojimai. TSA atsako už neteisėtus savo veiksmus ir padarytą žalą abonentams atlygina Lietuvos Respublikos įstatymų nustatyta tvarka ir neprisiima jokių papildomų įsipareigojimų, išskyrus tuos, kurie išdėstyti sudarytose paslaugų teikimo sutartyse.

15. Taikytini susitarimai ir veiklos nuostatai. TSA teikia laiko žymų paslaugas pagal BalTstamp laiko žymų taisykles (OID:1.3.6.1.4.1.38424.1.3.1), laikydamasi savo veiklos nuostatų (OID:1.3.6.1.4.1.38424.1.4.1), šių sąlygų bei sudarytų sutarčių su abonentais.

16. Auditas. TSA veiklos atitikimas laiko žymų taisyklėms ir laiko žymų teikimo veiklos nuostatams yra tikrinamas nustatyta vidaus tvarka.