BALTSTAMP LAIKO ŽYMŲ TEIKIMO SĄLYGOS V5.4

Galioja nuo 2023-11-06

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 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB ir standartų ETSI EN 319 421 (anksčiau skelbto kaip ETSI TS 102 023 ir perimto kaip LST ETSI TS 102 023 „Strateginiai reikalavimai, keliami laiko žymėjimo paslaugų teikėjams") bei ETSI EN 319 422 (anksčiau skelbto kaip ETSI TS 101 861 ir perimto kaip 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:	Sabina Sinicienė, uždarosios akcinės bendrovės „BalTstamp" direktorė
Adresas:	Dariaus ir Girėno g. 40, LT-02189 Vilnius
Tel.:	+370-673-23045
URL:	http://www.baltstamp.lt/
El. paštas:	info@baltstamp.lt

Dėl laiko žymos suformavimo 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 Geriausių praktikų laiko žymų taisyklių (BTSP – angl. *best practices time-stamp policy*, OID: 0.4.0.2023.1.1), apibrėžtų standarte ETSI EN 319 421.

Laiko žyma leidžia įrodyti, kad elektroninis parašas buvo sukurtas iki žymoje nurodyto laiko. Laiko žyma taip pat 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: SHA256, SHA384, SHA512.

5. TSU raktų generavimo algoritmas, gautų pasirašymo raktų ilgis bei pasirašymo algoritmas; raktų bei viešojo rakto sertifikatų galiojimo laikotarpis. Dviejuose savo laiko žymų įrenginiuose (angl. time stamping units, TSUs) TSA naudoja 2048 bitų ilgio RSA raktus; pasirašymo algoritmas – RSA. Raktas, naudojamas laiko žymų įrenginyje TSU-1, galioja iki 2025-11-11, o raktas, naudojamas laiko žymų įrenginyje TSU-2 – iki 2025-10-29. Viešojo rakto sertifikatų, naudojamų laiko žymų įrenginiuose formuojant laiko žymas, galiojimo laikotarpiai yra tokie pat kaip ir raktų.

6. Laiko žymų tikslumas. Laiko žymoje nurodoma laiko vertė laiko žymos sudarymo momentą ženklina ***vienos sekundės ar didesniu, iki dviejų dešimtųjų sekundės, tikslumu***, kurį užtikrina TSA įrenginių nuolatinė sietis 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) Laiko ir dažnio etalono laboratorijoje, dalyvaujančioje Pasaulio suderintojo laiko generavime, kaip to reikalauja standartas ETSI EN 319 421. Sieties charakteristikos skelbiamos Tarptautinio svorių ir matų biuro (BIPM – pr. *Bureau International des Poids et Mesures*) leidinyje „Circular T".

7. Paslaugos pasiekiamumas. TSA neprisiima kitokių įsipareigojimų dėl paslaugos pasiekiamumo nei nurodyta sutartyse su abonentais.

8. 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.

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

10. 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).

11. 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.

12. Įvykių įrašai. Su laiko žymomis susiję įrašai, kurių duomenis prireikus galima panaudoti teisiniam laiko žymų korektiškumo įrodymui, saugomi visą sertifikato, kuriuo jos pasirašytos, galiojimo trukmę, ir ne trumpiau nei 2 metus po jo galiojimo pabaigos. Kiti TSA sistemos operacijų ir veiklos registravimo žurnalai (angl. *event logs*) saugomi ne trumpiau nei 2 metus.

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

- 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;
- 2018 m. balandžio 26 d. Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymas;
- 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";
- 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";
- standartas ETSI EN 319 421, anksčiau skelbtas kaip ETSI TS 102 023 ir perimtas kaip LST ETSI TS 102 023 „Strateginiai reikalavimai, keliami laiko žymėjimo paslaugų teikėjams";
- standartas ETSI EN 319 422, anksčiau skelbtas kaip ETSI TS 101 861 ir perimtas kaip LST ETSI TS 101 861 „Laiko žymėjimo profilis".

14. 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.

15. Atsakomybė, garantija ir jos apribojimai. TSA atsako už neteisėtus savo veiksmus ir dėl tyčia ar dėl neatsargumo fiziniam ar juridiniam asmeniui padarytą žalą dėl pareigų pagal Reglamentą (ES) Nr. 910/2014 nevykdymo, kaip tai numatyta šio reglamento 13 straipsnio 1 dalyje. TSA padarytą žalą abonentams atlygina Lietuvos Respublikos įstatymų nustatyta tvarka ir neprisiima jokių papildomų įsipareigojimų, išskyrus tuos, kurie išdėstyti sudarytose paslaugų teikimo sutartyse.

16. Taikytini susitarimai ir veiklos nuostatai. TSA teikia laiko žymų paslaugas pagal Geriausių praktikų laiko žymų taisykles (OID: 0.4.0.2023.1.1), laikydamasi savo veiklos nuostatų (OID: 1.3.6.1.4.1.38424.1.4.4), šių sąlygų bei sudarytų sutarčių su abonentais.

17. Auditas. TSA veiklos atitiktis laiko žymų taisyklėms ir laiko žymų teikimo veiklos nuostatams yra tikrinama nustatyta vidaus tvarka. Atitiktis Reglamento (ES) Nr. 910/2014 reikalavimams patvirtinama bent kas 24 mėnesius, akredituotai atitikties vertinimo įstaigai atliekant auditą.