SSC GDL TSPPS
LAIKO ŽYMOS TAISYKLĖS - VEIKLOS NUOSTATAI

Versija 2.1

2017

Peržiūrių Istorija

Versija	Data	Peržiūros Detalės
1.4	2013.04.15	Peržiūros detalės
1.5	2013.06.25	Nauja publikacija
1.6	2013.06.27	ER peržiūra
1.7	2014.02.17	ER rekomendacijos, OID versijos sinchronizacija
2.0	2016.06.01	eIDAS peržiūra
2.1	2017.04.29	CAB Etapas I ER peržiūra

TURINYS

1 Įžanga

Daugelyje šiuolaikinėse aplikacijose laikas kada sugeneruoti informacija arba duomenys atlieka kritinį vaidmenį. Laiko žyma yra duomuo, kuri pasirašo patikimas Laiko žymos paslaugų teikėjas (*angl. Time Stamping Authority* - TSA).

Šis dokumentas papildo SSC GDL TSP teikiamų paslaugų *Taisykles* ir *Nuostatus* laiko žymos paslaugos aspektais pagal eIDAS 42 straipsnio reikalavimus.

Dokumentas gali būti naudojamas vertinant SSC GDL TSP laiko žymos paslaugas.

Kitų patikimumo užtikrinimo paslaugų nuostatas galima rasti SSC_GDL_CP and SSC_GDL_CPS dokumentuose.

Šis dokumentas yra SSC GDL CA išleistų dokumentų SSC_GDL_CP ir CPS praplėtimas laiko žymos paslaugų atžvilgiu.

2 Naudotojai ir tinkamumas

Ši politika neapsiriboja jokia konkrečia aplikacija arba naudojimo scenarijumi, taip pat siekiama atitikti eIDAS 3 straipsnio 33 ir 34 punktuose nustatytus apibrėžimus.

3 Apibrėžimai ir sutrumpinimai

Šio dokumento tikslais taikomos ETSI TR 119 001 ir ETSIEN319421 pateiktos sąvokos ir apibrėžimai.

4 Bendra koncepcija

4.1 Laiko žymos paslaugos

Tradiciškai laiko žymos paslauga pristatoma dviem komponentais: paslaugos teikimo ir valdymo. Paslaugos teikimo komponente generuoja laiko žymos objektus, vadinamus žyme (angl. Token), o valdymo komponente stebi ir valdo laiko žymos veiklą. Valdymo komponente yra atsakinga už laiko žymos programines ir technines įrangos instaliavimą ir laiko sinchronizavimą su patikimu UTC laiko šaltiniu.

4.2 Laiko žymos tarnyba (TSA)

Viena iš plačiai primažinamų el. parašo sukūrimo laiko gavimo metodų yra patikimos TSA naudojimas *Užsakovais* ir *Pasitikinčiomis šalimis*.

Laiko žymos tokenai generuojami atsakant į paslaugos Užsakovų užklausas. TSA kalibruoja savo laikrodį su nacionaliniu metrologijos institutais ir observatorijomis, kurios prisdeda prie UT, išsiųsdamos jų laikrodžio duomenis Bureau International des Poids et Mesures (BIPM) ir pateikia prašytojui patikimus laiko žymos tokenus. Trečioji šalis gali bet katada patvirtinti tokeną.

Technine tarnyba, generuojančia laiko žymą vadinasi Laiko žymos dalinys (angl. *Time Stamp Unit* - TSU). TSA gali valdyti vieną ar daugiau TSU, kiekvieną iš kurių generuoja laiko žymas su unikaiu TSA pasirašymo sertifikatu.

TSU sukurtas Laiko žymos tokenas sudaro timestamp_data, pagal kurį reikia generuoti TSA skaitmeninį parašą ir timestamp_signature skaitmeninis parašas, kuris yra generuojamas naudojant TSA pasirašymo sertifikatą.

TSA gali deleguoti savo funkcijas tretiesiems asmenims. Tačiau bet kuriuo atveju už paslaugos atitikimą šio dokumento reikalavimams atsako TSA.

4.3 Užsakovai

Užsakovas yra asmuo, gaunantis laiko žymos kriptografinę laikmeną pagal sutartį, kurios sąlygos remiasi šiuo dokumento nuostatais.

4.3.1 Laiko žymos taisykles ir TSA veiklos nuostatai

Laiko žymos taisykles (angl. *Time Stamp Policy* - TSP) yra aukštesnio lygio dokumentas, taikomas visiems TSU, kurios valdo TSA. Laiko žymos veiklos nuostatai (angl. *Time Stamp Practice statement* - TSPS) aprašo kaip konkretus TSA užtikrina atitikimą techniniams, organizaciniams ir procedūriniams reikalavimams.

4.3.2 Paskirtis

Šis dokumentas – TSPS, yra konsoliduota TSP ir TSPS versija.

4.3.3 Detalizavimo lygis

Ši TSA laiko žymos paslaugas teikia sutarčių, kuriuose detalizuojamos visos sąlygos, pagrindu. Bendroji užsakovo sutartis (angl. Generic Subscriber agrement) ir Pasitikinčios šalies sutartis (angliškai Relying party agreement) yra pagrindiniai informacijos šaltiniai Klientui, tačiau jis turi susipažinti tiek su šiuo dokumentu tiek su Laiko žymos paslaugų teikimo sutartimi.

5 Laiko žymos taisykles

5.1 Apžvalga

Šis dokumentas koncentruojasi į eIDAS 42 straipsnio ir ETSIEN319421 reikalavimus. tu ETSI TS 102 023, ETSI TS 101 861 ir RFC 3161 reikalavimais. Pagal šius standartus žyme yra duomenų objektas identifikuojamas, taikomu OID kodu, ir kuris gali būti gautas HTTP protokolu.

Pagal šio dokumento reikalavimu išduoto žymes tikslumas yra 1 sek.

Einamoji šio dokumento versija gali būti pasiekta čia: http://gdl.repository.ssc.lt/

5.2 Identifikavimas

SSC GDL TSP išduoda kvalifikuotas elektronines laiko žyma pagal šio TSPPS dokumento OID:

IANA Privačių įmonių registre: 1.3.6.1.4.1.22501.0.6.2.1

Lietuvos OID registre: 2.16.440.1.4.30003763.0.6.2.1[1]

TSP taip pat išduoda elektroninės laiko žymas pagal BTSP OID kaip nurodyta ETSIEN319421: 0.4.0.02023.1.1.

BTSP OID arba SSC GDL TSA OID yra nurodomas kiekvienoje SSC sugeneruotoje laiko žymoje. Šis dokumentas prieinamas tiek *Užsakovams* taip pat ir *Pasitikinčioms šalims*. Žyme su šio OID Adobe gaminamoje progaminėje įrangoje programoje laikoma-patikima.

Šio dokumento OID identifikatorius taip pat gali būti skelbiamas dokumente SSC GDL TSP PDS (angl. *PKI Disclosure Statement*), kuris yra prieinamas tiek *Užsakovams* taip pat ir *Pasitikinčioms šalims*.

[1] Turi būti patvirtintos nacionalinės valdžios institucijos.

5.3 Naudotojai ir Tinkamumas

Žymes generuojamos SSC GDL TSA susieja *Užsakovo* pateiktus duomenis su laiku, generuojamu atitinkamu TSU. Taisykles, numatytos šiame dokumente, ne kaip ne riboja Užsakovo pateiktų duomenų semantikos, naudotojų rato, elektroninių laiko žymų taikymo.

5.4 Atitikimas

Siekiant užtikrinti atitikimą šioms taisyklėms ir veiklos nuostatoms tik OIDai nurodyti šiame dokumente gali būti nurodomi SSC GDL TSA išduodamose laiko žymose. SSC GDL TSA palaiko audito mechanizmą, kai atitikimą reikalavimams reguliariai ir po kiekvieno esminio veiklos susijusios su šia paslauga pakeitimu tikrina nepriklausomi auditoriai.

6 Įsipareigojimai it atsakomybė

6.1 TSA įsipareigojimai

6.1.1 Bendri įsipareigojimai

SSC GDL TSA yra atsakinga už šio dokumento 7 skyriuje nurodytų reikalavimų įgyvendinimą. Įgyvendinimo detalės pateikiamos SSC GDL TSA sutarties šablone. SSC GDL TSA užtikrina bendrą atsakomybę net jeigu tam tikros funkcijos yra deleguotos trečiosioms šalims.

Šiuo metu SSC GDL TSA teikia savo paslaugas be trečiuju šalių dalyvavimo.

6.1.2 TSA įsipareigojimai Užsakovams

Išsamiai SSC GDL TSA įsipareigojimai yra pateikti dokumentuose GSA, RPA ir paslaugų teikimo sutartyje, kurie bendru atveju apima:

(a) atitikimą TSPPS ir kitiems taikomoms *Taisyklėms* ir procedūroms;

(b) UTC laiko šaltinio patikimumą ir tikslumą (1 sek.);

(c) atitikimą taikomoms teises aktams ir visiems susijusiems *Taisyklėms* ir procedūroms.

6.2 Užsakovu įsipareigojimai

SSC GDL TSA sugeneruota ir pasirašyta žyma turi būti patikrinta dėl el parašo tikslumo ir pasirašymo sertifikato galiojimo. Patikrinimai turi būti atliekamos atitinkamų standartu nurodytu būdu.

Užsakovo įsipareigojimai nurodyti SSC GDL TSP GSA, RPA and TSC yra prieinami visiems *Užsakovams* ir *Pasitikintiems šalims* SSC TSP repozitoriume adresu: gdl.repository.ssc.lt. Įsipareigojimai taip pat pateikiami dokumente SSC GDL TSP PDS.

6.3 Pasitikinčių šalių įsipareigojimai

SSC GDL TSA laiko žymos paslaugos sąlygos prieinamos dokumentuose SSC GDL TSP PDS (PKI Disclosure Statement) ir RPA (Relying party agreement) su kuriais Pasitikintis šalis turi susipažinti prieš pasitikint TSA sugeneruotoms žymoms.
Pasirašymo sertifikato galiojimas gali būti patikrintas naudojantis CRL ir OCSP paslaugomis nuorodos į kurias įrašytos į pasirašymo sertifikatą. Patikrinimai po TSU sertifikato galiojimo turi būti vykdomos pagal dokumento ETSIEN319421 priedą D.

Priimant sprendimą ar pasitikėti žymei *Pasitikintys šalys* turi:

a) patikrinti žymes el. parašą ir įsitikinti, kad naudojamas privatus raktas nėra kompromituotas;

b) atsižvelgti į bet kokius galimus laiko žymos naudojimo apribojimus, nurodytus dokumentuose SSC_GDL_CP/SSC_GDL_CPS;

c) atsižvelgti į kitas perspėjimus kituose dokumentuose.

6.4 Atsakomybė

SSC GDL TSA atsakomybe išsamiai aprašyta dokumente TSC.

SSC GDL TSA nesuteikia jokios išreikštos ar tariamos garantijos dėl paslaugos pasiekiamumo arba tikslumo ir jokiomis aplinkybėmis ir jokiais atvejais nebus laikoma atsakinga už pelno, apivartos, reputacijos, kontraktų, programines įrangos ar duomenų praradimą, už bet kokios

kompiuterinės ar kitos įrangos naudojimą, kas gali nuvykti dėl SSC GDL TSPPS, SSC_GDL_CP, SSC_GDL_CPS pažeidimo.

Sertifikavimo tarnybos, kurios išduotas sertifikatas naudojamas generuojant TSU parašus, atsakomybe nurodyta dokumentuose SSC_GDL_CP or SSC_GDL_CPS.

Nacionaline teise gali nustatyti papildomus atsakomybes apribojimus. Kai šios išimtys nėra taikomos, SSC GDL TSA atsisako bet koki ar visu garantijų ir atsakomybes ribojimo.

7 Reikalavimai veiklai

7.1 Nuostatai ir Viešai skelbtina informacija

7.1.1 TSA veiklos nuostatai

Šioje TSP-S dalyje pateikiamos TSA veiklos bendri taisykles. Dokumentai SSC_GDL_CP, SSC_GDL_CPS and the TSP's kiti vidiniai dokumentai nurodo kaip TSA užtikrina techninius, organizacinius ir procedūrinius TSPPS reikalavimus.

Atitinkamai su SSC_GDL_CP/SSC_GDL_CPS. apie numatomus šio dokumento pakeitimus yra viešai skelbiamas.

Papildamos saugos priemones, įskaitant rizikos įvertinimą, galima rasti SSC_GDL_CP/SSC_GDL_CPS. ir susijusiuose vidinėse dokumentuose.

7.1.2 TSA viešai skelbtina informacija

SSC GDL TSP paslaugų teikimo sąlygos, įskaitant elektroninės laiko žymos paslaugos reikalavimus, ginčių sprendimas pagal nacionaline teise yra pateikiami *Talpykloje*:

http://gdl.repository.ssc.lt/

Detalus paslaugų teikimo sąlygos yra pateiktos dokumente TSC, kuris yra prieinamas visiems potencialioms *Užsakovams*. Žemiau pateikti bendra informacija apie SSC GDL TSA paslauga:

(a) TSA kontaktinė informacija gali būti rasta SSC_GDL_CPS dokumente;

(b) Pagal šį TSP išduotos laiko žymos turi OID nurodyta skyriuje 5.2 ;

(c) Kriptografinis algoritmas, rakto ilgis naudojamas TSA atitinka ETSI TS 119 312:

i. Patvirtinatas santraukos (hash) algoritmas: SHA-256, SHA-384, SHA-512;

ii. Patvirtintas parašo algoritmas: 2048 bit sha256WithRSAEncryption.

(d) TSA pasirašymo sertifikato galiojimo laikas NETURI BŪTI mažesnis kaip trys metai;

(e) Jeigu kriptografinis algoritmas ir/ar rakto ilgis naudoajas TSA tampa nesaugiu, SSC GDL TSP privalo apie tai informuoti Užsakovus ir Pasitikinčias šalis;

(f) Laiko žymos tikslumas 1 sec pagrįstas UTC(k);

(g) SSC GDL TSP Įrašų archyvavimo paslauga, nurodyta SSC_GDL_CPS padengia ir TSA paslaugas;

(h) SSC GDL TSA tai komercinė paslauga.

SSC GDL TSA užtikrina patikimumą, reikalingą suteikiant elektroninį žymą, remiantis šiais įsipareigojimais:

(a) rizikos vertinimas įskaitant verslo resursus ir gresmes šiems resursams;

(b) visų taisyklių, prodecūrų atskleidimas ir prienamumas, įskaitant SSC GDL TSA specifinį TSC;

(c) visi santykiai susiję su SSC GDL TSA teikiamomis paslaugomis buvo tinkamai atskleisti.

(d) aukšto lygio valdymo organas patvirtintas TSPPS užtikrina tinkamą visų politikos reikalavimų ir praktikos įgyvendinimą.

(e) TSPPS įdiegė peržiūros procesą ir iš anksto apibrėžė personalo atsakomybę;

Atnaujinta TSPPS versija prieinama iš karto po jos patvirtinimo.

7.2 Rakto valdymo ciklas

7.2.1 TSA rakto generavimas

TSA rakto generavimo funkcija yra palaikomas SSC GDL TSP Root CA sertifikavimo tarnybos komponentas. Personalas įgaliotas atlikti šia funkciją dirba SSC. Raktai generuojami naudojantis *FIPS 140-2 Level 3 HSM* ir tuomet sinchronizuojami su TSU HSM turinčiu tą patį sertifikavimo saugumo lygmenį.

7.2.2 TSU privataus rakto apsauga

FIPS 140-2 Level 3 sertifikuoto HSMs naudojimas kartu su patikimu personalu ir saugumo procedūromis užtikrina TSU privataus rakto apsaugą. Operacijos su TSU privačiu raktu atliekamos tik patikimam personalui dalyvaujant, naudojant bent dvigubą kontrolę fiziškai saugioje aplinkoje. Atsarginės TSU privataus rakto kopijos saugomos dubliuotame HSM siekiant užtikrinti aukšta konfidencialumo lygį.

7.2.3 TSU viešojo rakto platinimas

TSU parašo patvirtinimo raktus valdo SSC GDL TSP sertifikavimo tarnyba pagal patvirtintas saugumo taisykles SSC_GDL_CPS kurios užtikrina visų atliekamų operacijų patikimumą.

7.2.4 Re-keying TSU's Key

SSC GDL TSP sertifikavimo tarnyba valdo TSU pasirašymo sertifikatus ir užtikrina visų susijusių operacijų patikimumą pasiremiant SSC_GDL_CPS sertifikavimo tarnybos saugumo politika.

7.2.5 TSU rakto gyvavimo ciklo pabaiga

SSC GDL TSP sertifikavimo tarnyba pakeičia TSU pasirašymo sertifikatus prieš baigiantis jų galiojimui. Pasibaigus privataus rakto galiojimui TSU atmeta bet kokius bandymus pasirašyti laiko žymas. Pasibaigę privatūs raktai sunaikinami.

7.2.6 Kriptografilių modulių naudojimas pasirašant laiko žymas gyvavimo ciklas

SSC GDL TSP sertifikavimo tarnyba ivygdo procesus bei procedūras užtikrinančias kad HSM skirtas jų paslaugoms saugojimo ar pervežimo metu nebūtu sugadintas. Priėmimas, testavimas, įdiegimas ir aktyvavimas atliekamas M iš N įgaliotų patikimų asmenų fiziškai saugioje aplinkoje. Nutraukus naudojimą privatūs raktai sunaikinami remiantis gamintojo nurodymais.

7.3 Laiko žymų uždėjimas

7.3.1 Laiko žymos spaudas

Laiko žymos spaudas generuojamas SSC GDL TSA talpina iš anksto nustatyta unikalų politikos OID, laiko vertes sekundės tikslumu kurios pateiktos bent vienoje iš UTC laboratorijos[3] platinamų realaus laiko reikšmių. Jeigu TSU laikrodis nukrypsta nuo standartinės paklaidos reikšmės TSA servisas nutraukia spaudų pasirašymą.

Laiko žymos spaudai pasirašomi naudojant sertifikatą skirta tik šiam servisui ir apima pasirašytų duomenų santrauką.

7.3.2 Laikrodžio sinchronizacija su UTC

TSA užtikrina 1 sekundės tikslumą UTC sinchronizuotame laike su kalibruotame pagal daugelį nepriklausomų ir patikimų laiko šaltinių[4].

TSU laikrodis apsaugotas naudojant HSM ir mažiausiai du kartus per parą su kalibruojamas pagal standartinį UTC laiko šaltinį. TSU laikrodžiai gali stebėti laiko nuokrypį ir pareikalauti papildomo per kalibravimo. Jei TSU laikrodis nukrypsta nuo nustatyto tikslumo ir per kalibracija nepavyksta tai užfiksuojama ir TSA nutraukia laiko žymų pasirašimą kol nebus atstatytas teisingas laikas. Rankinė TSU laikrodžio administracija reikalauja M iš N patikimų asmenų dalyvavimo. SSC TSU laiko visų UTC kalibravimų audito žurnalus.

Laiko žymos spaudai pasirašyti SSC GDL TSA įtraukia:

(a) laiko žyma pažymėtos datos santrumpą;

(b) unikalų serijos numerį;

(c) TSU OID;

3 Šiuo metu NIST (JAV) ir PTB (VFR).

4 UTC laiko skalės patikslinimas numato laiko po laiko pridedamą ar atimamą sekundę, kuri vadinama *keliamoji sekundė*. Du kart per metus Birželio 30 ir Gruodžio 31 d. paskutine minute gali būti atliktas laiko patikslinimas, kad užtikrinti, jog laiko skirtumas tarp UTC ir UT1 neviršija 0.9 sekundžių. Istoriškai laiko patikslinimas įprastai buvo atliekamas pridedant sekundę prie UTC laiko, sudarant galimybei Žemei susilyginti su patikslintu laiku. Todėl, laiko patikslinimo datos paskutinė minutė turės 61 sekundžių. Įprastai laiko patikslinimo datos skelbiamos keletą mėn. iš anksto: http://hpiers.obspm.fr/iers/bul/bulc/bulletinc.dat.

(d) 1 sekundės tikslumu pateikta UTC laiko reikšmę atitinkančią UTC šaltinius;

(e) elektroninį parašą sugeneruota naudojant unikalų pasirašymo raktą;

(f) SSC GDL TSA identifikatorių ir TSU.

7.4 TSA valdymas ir eksploatavimas

7.4.1 Saugumo valdymas

SSC saugumo valdymo nuostatos pateikiamos CP/CPS sertifikavimo tarnybos SSC_GDL_CPS dokumentuose padedančiuose išlaikyti patikimas saugumo nuostatas laikantis geriausios praktikos ir atitinkamų standartų užtikrinančių tinkamą kriptografinės įrangos funkcionavimą.

7.4.2 Turto klasifikavimas ir valdymas

Siekiant užtikrinti kad informacija ir kitas turtas gautu atitinkamą apsaugą SSC prižiūri bei inventorizuoja visą savo turtą. Turtas suklasifikuojamas pagal atitinkamas saugumo klases bei jam paskiriama atitinkama apsauga. Papildoma informacija pateikiama SSC GDL sertifikavimo tarnybos SSC_GDL_CPS dokumentuose.

7.4.3 Personalo saugumas

Siekiant padidinti PKI operacijų patikimumą SSC personalo lygmenyje palaiko atitinkamus standartus bei saugumą. Papildoma informacija pateikiama SSC GDL sertifikavimo tarnybos SSC_GDL_CPS dokumentuose.

Konkrečios kontrolės priemonės pritaikytos laiko žymų valdymui užtikrina kad personalas turi atitinkamas žinias susijusias su laiko žymų ir el. parašo technologijomis bei žinias apie TSU, UTC kalibravimo procesus. SSC GDL TSA personalas supažindintas su saugumo procedūromis ir atsakomybe. Saugumo politikos įgyvendinimas grindžiamas patirtimi susijusia su informacijos saugumu bei rizikos vertinimu.

7.4.4 Fizinis ir aplinkos saugumas

SSC GDL TSA dirba aukšto saugumo duomenų centre besilaikant nuostatų pateiktų ETSIEN319421:

a) Laiko žymos teikimui bei valdymui:
   i. fizinė prieiga prie įrenginių susijusių su laiko žymėjimo paslaugomis leidžiama tik įgaliotiems darbuotojams;
   ii. vykdoma kontrolė kad būtu išvengta nuostolių, pažeidimų, grėsmės turtui ar verslo veiklos nutraukimo;
   iii. vykdoma kontrolė siekiant išvengti informacijos ar jos saugojimo įrenginių vagystes ar sukompromitavimo.
b) Prieigos kontrolė taikoma kriptografiniams moduliams laikantis atitinkamų saugumo reikalavimų;

Papildomos kontrolės priemonės taikomos TSA valdymui:

(a) Paslaugos eksploatuojamos aplinkoje fiziškai apsaugančioje jas nuo sukompromitavimo dėl neteisėtos prieigos prie sistemos ar duomenų;
(b) Fizinė apsauga vykdoma sukuriant aiškiai apibrėžtą saugumo perimetrą aplink laiko žymėjimo valdymo mechanizmą. Visos su kitomis organizacijomis bendros patalpos yra už šio perimetro ribų;
(c) Fizinė ir aplinkos saugumo kontrolė įgyvendinama siekiant apsaugoti patalpas talpinančias sistemos resursus, pačius resursus bei jų veiklai palaikyti reikalingas patalpas. SSC informacijos saugumo politika (kuri apima sistemas susijusias su laiko žymėjimo valdymu) aprašo fizinės prieigos kontrolę, priešgaisrinės saugos veiksmus, palaikančiųjų mazgų (energijos tiekimo, telekomunikacijų) gedimus, apsauga prieš vagystes, įsilaužimus bei veiksmus nelaimės padarinių šalinimui;
(d) Vykdoma kontrole siekiant apsaugoti nuo įrangos, informacijos, duomenų laikmenų ir programinės įrangos susijusios su laiko žymėjimo paslaugomis išgabenimo be leidimo;
(e) Visos duomenų saugojimo laikmenos saugiai tvarkomos laikantis informacijos klasifikavimo schemos reikalavimų, nebenaudojamos laikmenos su jautriais duomenimis saugiai sunaikinamos. Sunaikinimo įrodymai surenkami ir archyvuojami.
(f) Duomenų apdorojimo ir saugojimo pajegumai stebimi siekianrt užtikrinti atitinkamu jų poreikius.

7.4.5 Veiklos valdymas

SSC GDL TSA veikia remiantis ETSIEN319421. TSA veiklos valdymo kontrolė įtraukta į bendrą SSC GDL TSP sertifikavimo tarnybos valdymo kontrolę. Papildoma informacija susijusi su valdymu pateikta SSC GDL sertifikavimo tarnybos SSC_GDL_CPS dokumentuose.

7.4.6 Sistemos prieigos valdymas

SSC TSA įrenginiams, sistemoms bei informacijai taiko atitinkamas fizinės ir loginės prieigos kontrolės priemones. SSC GDL TSA sistemos prieigos valdymo nuostatai įtraukti į SSC GDL TSP sertifikavimo tarnybos sistemos prieigos valdymo nuostatus. Papildoma informacija pateikiama SSC GDL sertifikavimo tarnybos SSC_GDL_CPS dokumentuose.

7.4.7 Patikimų sistemų diegimas ir priežiūra

SSC GDL TSA naudoja patikimas sistemas apsaugotas nuo modifikavimo. SSC GDL TSA sistemų diegimo ir priežiūros nuostatai įtraukti į bendrus SSC sertifikavimo tarnybos sistemų diegimo ir priežiūros nuostatus. Papildoma informacija pateikiama SSC GDL sertifikavimo tarnybos SSC_GDL_CPS dokumentuose.
SSC GDL TSA paslauga įgaliotos atitikties vertinimo įstaigos įvertinta kaip atitinkanti nustatytus laiko žymos politikos standartus.

7.4.8 TSA paslaugos sukompromitavimas

TSU privataus rakto sukompromitavimo atveju, TSA laikosi procedūrų išdėstytų SSC GDL sertifikavimo tarnybos SSC_GDL_CPS dokumentuose. Tai apima atitinkamo sertifikato atšaukimą bei jo įtraukimą į CRL. TSU nepasirašo laiko žymų jei jos privatus raktas nėra galiojantis.

TSU nepasirašo laiko žymų jei jos laikrodis yra už nustatytų tikslumo ribų remiantis UTC laiku. Pasirašymas atkuriamas kai imamasi veiksmų siekiant atstatyti laiko kalibraciją. Kaip aprašoma 7.4.11 šio dokumento poskyryje, SSC GDL TSA taip pat saugo audito žurnalus.

7.4.9 TSA veiklos nutraukimas

Atveju kuomet SSC GDL TSA nutraukia savo veiklą, SSC turi imtis procedūrų nustatytų

SSC GDL sertifikavimo tarnybos SSC_GDL_CPS dokumentuose labiau detalizuotų SSC vidaus darbo nutraukimo procedūrų. Minimaliai tai apima naudotojų informavimą, TSU sertifikatų atšaukimą, įvykių bei audito archyvų perdavimą atitinkamai šaliai, taip pat prieigą prie privačių raktų.

7.4.10 Teisinių reikalavimų laikymasis

SSC GDL TSA atitinka taikytinus nacionalinius [LT-PDP-LAW] ir tarptautinius teisinius reikalavimus, taip pat Europos duomenų apsaugos direktyvos reikalavimus. Turi būti imtasi tinkamų techninių bei organizacinių priemonių prieš nesankcionuotą ar neteisėtą asmens duomenų tvarkymą bei prieš atsitiktinį asmeninių duomenų praradimą, sunaikinimą ar pažeidimą.

Informacija kurią naudotojai pateikia TSA turi būti visiškai apsaugota nuo atskleidimo nebent tam buvo duotas jų leidimas arba tai vykdoma teismo sprendimu ar kitais teisiniais reikalavimais.

7.4.11 Laiko žymėjimo paslaugos operacijų informacijos įrašymas

SSC GDL TSA pasiremdama SSC verslo praktika 11 metų saugo įrašus bei visą su TSA veikla susijusią informaciją. Įrašai pažymimi laiko žyma siekiant apsaugoti duomenų vientisumą ir perkeliami į apsaugotą serverį saugojimui bei tolimesniam archyvavimui. Įrašai laikomi konfidencialiais remiantis SSC GDL sertifikavimo tarnybos SSC_GDL_CPS dokumentais. Jokie naudotojų asmeniniai duomenys neperduodami tarp jurisdikcijų.

Įrašai susyja su laiko žymos formavimo operacijomis yra pateikiami naudotojo prašymu arba jei to reikalauja teismo nutartis ar kitas teises aktas. SSC GDL TSA tvarko įrašus įskaitant tikslaus laiko:

(a) Laiko žymų prašymai bei sukurtos laiko žymos;

(b) Įvykiai susiję su TSA administravimu (įskaitant sertifikatų valdymo, raktų valdymo ir laikrodžio sinchronizacijos);

(c) Įvykiai susyja su TSU raktų ir sertifikatų gyvavimo ciklu.

7.5 Organizacinė

SSC organizacinė struktūra, veiklos kryptys, procedūros ir kontrolės priemonės taikomos SSC GDL TSA. SSC organizacines procedūros atitinka standartus iš šio dokumento 8 skyriaus bei ETSIEN319421. standartus.

Svarbūs SSC GDL TSP sertifikavimo tarnybos dokumentai prieinami saugykloje.

Kiti vidaus procedūrų dokumentai gali būti pateikiami tik griežtai kontroliuojamomis sąlygomis.

8 NUORODOS

8.1 Normatyvinės nuorodos

Žemiau pateikti dokumentai yra reikalavimai, kurie taikytini šioms TSPPS nuostatos. Atnaujintoje TSPPS versijoje taikoma referencinio dokumento versija, kuri yra ankstesnė nei atnaujinimo data.

[eIDAS] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[ETSI TR 119 001] Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations

[ETSI EN 319 401] Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[ETSIEN319411-1] Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[ETSIEN319411-2] Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

[ETSIEN319412-2] Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.

[ETSIEN319412-3] Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.

[ETSIEN319421] Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

[ETSIEN319412-4] Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organisations.

[CABF-NCSSR] Network and Certificate System Security Requirements, CA/Browser Forum.

[CABF-BR] CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates.

[CABF-EV] CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates.

[ETSIEN319403] Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

[SSC_GDL_CP] SSC GDL TSP Certificate Policy

[SSC_GDL_CPS] SSC GDL TSP Certificate Practice Statement

8.2 Informacinės nuorodos

[LT-PDP-LAW]	The Law on Persona data protection of Lithuanian Republic No. I-1444, 1st February 2008.
[ETSI TR 119 300]	Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for Cryptographic Suites.
[ETSI TS 119 312]	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
[RFC3647]	RFC3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices.
[RFC2119]	RFC 2119, Key words for use in RFCs to Indicate Requirement Levels. March 1997.
[RFC6960]	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.
[RFC5280]	RFC 5280, Internet X.509 Public Key Infrastructure: Certificate and CRL Profile.
[Dir1999/93/EC]	Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
[ETSIEN319422]	Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
[RFC3126]	RFC 3126, Electronic Signature Formats for Long Term Electronic Signatures.
[RFC3161]	RFC 3161, Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP).
[TSPDS]	SSC GDL Trust Services PKI Disclosure Statement.