SSC GDL CA
LAIKO ŽYMOS TAISYKLES - VEIKLOS NUOSTATAI

Versija 1.8

2014

Pakeitimu istorija

Versija	Data	Komentaras
1.4	2013.04.15	Naujas leidinys
1.5	2013.06.25	Atnaujinta redakcija
1.6	2013.06.27	Atnaujintas pagal ER
1.7	2014.02.17	Atnaujintas pagal ER rekomendacijas, OID patikslinimas
1.8	2014.04.22	Patikslintas 7.4.11 p.

TURINYS

1 Įžanga

Daugelių atvejuose šiuolaikiniuose aplikacijose el. parašo kūrimo laikas atlieka ypatinga vaidmenį. Laiko žyma yra duomuo, kuri pasirašo patikimas Laiko žymos paslaugų teikėjas (*angl. Time Stamping Authority* - TSA).

Šis dokumentas – TSP-S - papildo SSC GDL CA teikiamų paslaugų *Taisykles* ir *Nuostatus* laiko žymos paslaugos aspektais. TSP-S gali būti naudojamas vertinant SSC GDL CA laiko žymos paslaugas. Pagrindinių sertifikavimo paslaugų sąlygos pateiktos SSC GDL CA dokumentuose CP ir CPS.

TSP-S yra SSC GDL CA išleistų dokumentų CP ir CPS praplėtimas laiko žymos paslaugų atžvilgių.

2 Naudotojai ir tinkamumas

TSP-S taisykles ir nuostatai nėra orientuoti į konkretu aplikacija arba naudojimo scenarijui, dokumentas taip pat siekia pademonstruoti reikalavimu keliamu ilgai saugomu el. parašu laiko žymos reikalavimu laikimosi.

3 Apibrėžimai ir sutrumpinimai

TSP-S naudojamu terminologija ir apibrėžimai atitinka:

[CWA14167-1] , [ETSI101042] , [ETSI101456] ir [ETSI102023].

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 (angl. Universal Time, Coordinated) laiko šaltinių.

4.2 Laiko žymos tarnyba (TSA)

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

Laiko žymos *žymes* generuojami atsakant į paslaugos Užsakovu užklausas. TSA kalibruoja savo laikrodi su patikimu laiko šaltinių[1] ir formuoja patikimas žymes. Sugeneruota žyme gali buti bet kada patikrinta trečiuoju šalių.

Technine tarnyba, generuojančia laiko žymes vadinasi Laiko žymos dalinys (angl. *Time Stamp Unit* - TSU). TSA gali valdyti keletą TSU, kiekviena iš kurių generuoja žymes ir pasirašo savo TSA sertifikatu. TSU sukurtos žymes sudėty įeina *timestamp_data – duomuo* kuri turi pasirašyti TSA ir el. parašas *timestamp_signature, kuris yr*a generuojamas TSA sertifikato pagalba.

TSA gali deleguoti savo funkcijas tretiesiems asmenims. Tačiau ir tokių atvejų už paslaugos atitikimą šio dokumento reikalavimams atsako TSA.

1 Pvz. nacionalinė metrologijos laboratorija

4.3 Užsakovai

Užsakovas yra asmuo, gaunantis laiko žymos žymes pagal sutarti, kurios sąlygos remiasi šiu 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 techninėms, organizacinėms ir procedūrinėms reikalavimams.

4.3.2 Paskirtis

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

4.3.3 Detalizavimo lygis

Ši TSA laiko žymos paslaugas teikia sutarčių, kuriuose detalizuojamos visos sąlygos, pagrindo. *Užsakovai* ir *Pasitikintys šalis* turi susipažinti su šių dokumentų ir su standartinių paslaugu teikimo sutarties šablonu (angl. *Standard Service Contract Template* - SSCT).

5 Laiko žymos taisykles

5.1 Apžvalga

Šis dokumentas koncentruojasi standartu 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/TSP

5.2 Identifikavimas

SSC GDL TSA išleisto šio TSP-S dokumento OID yra:

IANA Privačių įmonių registre: 1.3.6.1.4.1.22501.0.6.1.8

Lietuvos OID registre: 2.16.440.1.4.30003763.0.6.1.8

Bazinių laiko žymos Taisyklių OID kodas pagal [ETSI102023] yra: 0.4.0.02023.1.1

SSC GDL TSA OID yra nurodomas kiekvienoje SSC sugeneruotame žyme. Šis dokumentas prieinamas tiek Užsakovams taip pat ir *Pasitikintiems šalims*. Žyme su šio dokumento OID *Adobe Approved Trust List* (AATL)[2] programoje programoje laikoma patikima.

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

5.3 Naudotojai ir Tinkamumas

Žymes generuojamos SSC GDL TSA susieja *Užsakovo* pateiktos duomenys su laiku, generuojamu atitinkamu TSU. Taisykles, numatytos šiame dokumente, ne kaip ne riboja laiko

2 Užbaigus šiu metu vykdoma procedūra.

žymos paslaugos naudotoju ratą ir jos tinkamumą.

5.4 Atitikimas

OID nurodytas sugeneruotame žyme užtikrina jos atitikimą šio dokumento reikalavimus.

SSC GDL TSA palaiko audito mechanizmą, kai atitikimą reikalavimams reguliariai ir po kiekvieno esminio veiklos pakeitimo tikrina nepriklausomi auditoriai.

6 Įsipareigojimai it atsakomybe

6.1 TSA įsipareigojimai

6.1.1 Bendri įsipareigojimai

SSC GDL TSA yra atsakinga už šio dokumento 7 skyriuje nurodytu reikalavimu įgyvendinimo. Įgyvendinimo detales aprašomos pateikiamos SSC GDL TSA sutarties šablone - SSCT. SSC GDL TSA užtikrina bendra atsakomybe net ir jeigu tam tikros funkcijos yra deleguotos tretiesiems šalims.

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

6.1.2 TSA įsipareigojimai Užsakovams

Išsamiai SSC GDL TSA įsipareigojimai yra pateikti dokumente SSCT, kuris bendru atveju apima:

- atitikimą TSP-S ir kitiems taikomoms *Taisyklėms* ir procedūroms;
- UTC laiko šaltinio patikimumą ir tikslumą (1 sek.);
- atitikimą taikomoms teises aktams ir visiems susijusiems *Taisyklėms* ir procedūroms.

6.2 Užsakovu įsipareigojimai

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

Užsakovo įsipareigojimai nurodyti SSCT yra prieinami visiems *Užsakovams* ir *Pasitikintiems šalims*. Įsipareigojimai taip pat pateikiami dokumente SSC GDL CA PDS.

6.3 Pasitikinčių šalių įsipareigojimai

SSC GDL TSA laiko žymos paslaugos sąlygos prieinamos dokumentuose SSC GDL CA PDS ir SSCT su kuriais Pasitikintis šalis turi susipažinti prieš pasitikint TSA sugeneruotoms žymoms.

Pasirašymo sertifikato galiojimas gali būti patikrintas naudojantis CRL ir OCSP paslaugu nuorodais įrašytais į pasirašymo sertifikatą. Patikrinimai po TSU sertifikato galiojimo turi būti vykdomos pagal dokumento [ETSI102023] priedo 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 CA CP/CPS;

c) atsižvelgti į kitas perspėjimus kituose dokumentuose.

6.4 Atsakomybė

SSC GDL TSA atsakomybe išsamiai aprašyta dokumentuose SSC GDL CA PDS ir SSCT.

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 TSP-S, SSC GDL CP, SSC GDL CPS pažeidimo.

Sertifikavimo tarnybos, kurios išduotas sertifikatas naudojamas generuojant TSU parašus, atsakomybe nurodyta dokumentuose SSC GDL CP ir 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, CPS ir kiti vidiniai dokumentai nurodo kaip TSA užtikrina techninius, organizacinius ir procedūrinius TSP-S reikalavimus.

Atitinkamai su SSC GDL CP/CPS apie numatomus šio dokumento pakeitimus yra viešai skelbiamas.

Papildamos saugos priemones, įskaitant rizikos įvertinimą, galima rasti SSC GDL CP/CPS ir susijusiuose vidinėse dokumentuose.

7.1.2 TSA viešai skelbtina informacija

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

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

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

- TSA kontaktine informacija nurodyta SSC GDL CP/CPS;
- Laiko žymas pagal šias TSP-S turi OID, nurodytas šio dokumento 5.2 p.;
- TSA naudojamu kriptografiniai algoritmai ir raktu ilgiai atitinka ETSI TS 101.861:
  - Santraukos algoritmai: SHA-1, SHA-256, SHA-384, SHA-512;
  - Parašo algoritmai: 2048 bit *sha256WithRSAEncryption.*
- TSA pasirašymo sertifikato galiojimo laikas yra nemažiau 3 m.
- Jeigu TSA naudojami kriptografiniai algoritmai ir/ar raktu ilgiai pripažinami nesaugiu SSC

GDL CA apie tai informuoja Užsakovus ir Pasitikinčios šalys;

- Laiko žymos tikslumas yra 1 sek. ir laikas yra sinchronizuojamas su dviem UTC laiko šaltiniais;
- Archyvavimo sistema, aprašyta CP/CPS apima ir TSA paslaugos;
- SSC GDL TSA paslauga yra komercine paslauga;

SSC GDL TSA užtikrina, kad patikimumas reikalingas laiko žymos paslaugos teikimui, remiasi:

a) rizikos vertinimu;

b) visu nuostatu, proceduru, įskaitant ir SSC GDL TSA skirto SSCT atskleidimu ir prieinamumu;

c) visu deleguotu funkciju tinkamu atskleidimu;

d) aukšto lygio vadovas, tvirtinantis TSP-S užtikrina atitinkamą visu reikalavimų igyvendinimą;

e) TSP-S numato susipažinimo su TSP-S ir pastabu surinkimo procesą ir iš anksto nustatytas personalo pareigas.

Atnaujinta TSP-S 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 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 sertifikavimo tarnyba pagal patvirtintas saugumo taisykles (CP/CPS) kurios užtikrina visų atliekamų operacijų patikimumą.

7.2.4 Re-keying TSU's Key

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

7.2.5 TSU rakto gyvavimo ciklo pabaiga

SSC GDL 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 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:

- laiko žyma pažymėtos datos santrumpą;
- unikalų serijos numerį;
- TSP IOD;

---

3 Šiu metu NIST (JAV) ir PTB (VFR).

4 UTC laiko skales patikslinimas numato laiko po laiko pridedama ar atimama sekunde, kuri vadinama *keliamąją sekundę*. Du kart per metus Birželio 30 ir Gruodžio 31 d. paskutine minute gali būti atliktas laiko patikslinimas, kad užtikrinti laiko skirtumas tarp UTC ir UT1 neviršija 0.9 sekundes. Istoriškai laiko patikslinimas įprastai buvo atliekamas pridedant sekunde prie UTC laiko, sudarant galimybe Žemei susilyginti su patikslintu laiku. Todėl, laiko patikslinimo datos paskutine minute turės 61 sekundes. Įprastai laiko patikslinimo datas skelbiamos keletą mėn. iš anksto: http://hpiers.obspm.fr/iers/bul/bulc/bulletinc.dat.

- 1 sekundės tikslumu pateikta UTC laiko reikšmę atitinkančią UTC šaltinius;
- elektroninį parašą sugeneruota naudojant unikalų pasirašymo raktą;
- SSC GDL TSA identifikatorių ir TSU.

7.4 TSA valdymas ir eksploatavimas

7.4.1 Saugumo valdymas

SSC saugumo valdymo nuostatos pateikiamos SSC GDL sertifikavimo tarnybos CP/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 CP/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 CP/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 ETSI TS 102.023:

a) Laiko žymos teikimui bei valdymui:

- fizinė prieiga prie įrenginių susijusių su laiko žymėjimo paslaugomis leidžiama tik įgaliotiems darbuotojams;
- vykdoma kontrolė kad būtu išvengta nuostolių, pažeidimų, grėsmės turtui ar verslo veiklos nutraukimo;
- 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:

- Paslaugos eksploatuojamos aplinkoje fiziškai apsaugančioje jas nuo sukompromitavimo dėl neteisėtos prieigos prie sistemos ar duomenų;
- Fizinė apsauga vykdoma sukuriant aiškiai apibrėžtą saugumo perimetrą aplink laiko žymėjimo valdymo mechanizmą. Visos su kitomis organizacijomis bendros patalpos yra už šio perimetro ribų;
- 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;
- Vykdoma kontrole siekiant apsaugoti nuo įrangos, informacijos, duomenų laikmenų ir programinės įrangos susijusios su laiko žymėjimo paslaugomis išgabenimo be leidimo;
- Visos duomenų saugojimo laikmenos saugiai tvarkomos laikantis informacijos klasifikavimo schemos reikalavimų, nebenaudojamos laikmenos su jautriais duomenimis saugiai sunaikinamos. Sunaikinimo įrodymai surenkami ir archyvuojami.
- Duomenų apdorojimo ir saugojimo pajegumai stebimi siekianrt užtikrinti atitinkamu jų poreikius.

7.4.5 Veiklos valdymas

SSC GDL TSA veikia remiantis ETSI TS 102.023. TSA veiklos valdymo kontrolė įtraukta į bendrą SSC GDL sertifikavimo tarnybos valdymo kontrolę. Papildoma informacija susijusi su valdymu pateikta SSC GDL sertifikavimo tarnybos CP/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 sertifikavimo tarnybos sistemos prieigos valdymo nuostatus. Papildoma informacija pateikiama SSC GDL sertifikavimo tarnybos CP/CPS dokumentuose.

7.4.7 Patikimų sistemų diegimas ir priežiųra

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 CP/CPS dokumentuose.
SSC GDL TSA paslauga TÜV Informationstechnik GmbH (VFR) 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 CP/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 CP/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 CP/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. The SSC GDL TSA tvarko įrašus įskaitant tikslaus laiko:

- Laiko žymų prašymai bei sukurtos laiko žymos;
- Įvykiai susyja su TSA administravimu (įskaitant sertifikatų valdymo, raktų valdymo);
- Įvykiai susyja su laikrodžio sinchronizacijos (sekminga ar nesekminga sinchronizacija);
- 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 ETSI TS 102.023 standartus.

Svarbūs SSC GDL sertifikavimo tarnybos dokumentai prieinami saugykloje.

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

8 NUORODOS

8.1 Normatyvinės nuorodos

Žemiau pateiktų dokumentų reikalavimai, jeigu yra taikytini, laikytini šio dokumento sudėtine dalimi. Jeigu nurodomas dokumentas atnaujinamas, nuoroda šiame dokumente nurodo ankstesnę versiją.

[CWA14167-1] CEN CWA 14167-1, Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.

[ETSI101042] ETSI TS 101 042, Policy requirements for certification authorities issuing public key certificates (Normalized level only).

[ETSI101456] ETSI TS 101 456 Policy, Requirements for Certification Authorities Issuing Qualified Certificates.

[ETSI102023] ETSI TS 102 023 Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities

[CENSSCD] CWA 14169 Secure Signature Creation Devices EAL4+.

[ALGO] ETSI SR 002 176 - Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures.

8.2 Informacinės nuorodos

[LT-PDP-LAW] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas, Nr. X-1444, 2008.02.01 su pakeitimais.

[LT-ES-LAW] Lietuvos Respublikos Elektroninio parašo įstatymas, Nr. VIII-1822, 2000.07.11 su pakeitimais.

[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.

[ISO/IEC 10118-1] ISO/IEC 10118-1, Information technology -- Security techniques -- Hash- functions -- Part 1: General.

[ETSI TS 101 862] Qualified Certificate Profile, DTS/SEC-004003

[RFC3039] RFC3039, Internet X.509 Public Key Infrastructure Qualified Certificates Profile, Santesson, et al.

[CC] Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408, ISO/IEC.

[ETSI101861] ETSI TS 101.861, Time-stamping Profile.

[ETSI101733] ETSI TS 101.733, CMS Advanced Electronic Signatures

[SSC_CP] SSC GDL CA Sertifikato taisyklės.

[SSC_CPS] SSC GDL CA Sertifikavimo veiklos nuostatai.

[RFC3126] RFC 3126, Electronic Signature Formats for Long Term Electronic Signatures.

[RFC3161] RFC 3161, Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP).