MitSoft

Kvalifikuotos laiko žymų paslaugos

Laiko žymų paslaugų veiklos nuostatai

QTSS/PS

Unikalus objekto identifikatorius (OID): **1.3.6.1.4.1.57890.1.3.1**

Versija 1.00

Galioja nuo 2024-10-01

UAB „MIT-SOFT“, Kalvarijų st. 276-100, LT-08316 Vilnius, Tel. +370 233 3922, Fax +370 5 213 6191, www.mitsoft.lt, info@mitsoft.lt, Įmonės kodas 120792080, PVM mokėtojo kodas LT207920811

Patvirtinimai

Versijų istorija

Versija	Galioja nuo	Aprašas
1.00	2024-10-01	Pirma oficiali dokumento versija

Dokumento patvirtinimas

	Vardas pavardė	Data	Parašas
Patikrino	Adomas Birštunas	2024-08-19	
Patvirtino	Antanas Mitašiūnas	2024-08-20	

Turinys

1. ĮVADAS

Uždaroji akcinė bendrovė "MIT-SOFT" (toliau – MitSoft) buvo įkurta 1991 m. rugpjūčio 1 d. ir nuo 1996 m. dirba elektroninių dokumentų, turinčių tokią pat teisinę galią kaip ir ranka pasirašyti dokumentai, sukūrimo ir tikrinimo programinės įrangos kūrimo ir paslaugų teikimo srityje. Informacija apie MitSoft yra pateikiama interneto svetainėje http://www.mitsoft.lt/.

MitSoft veiklos nuostatus suskirstė į tris dalis:

- Kvalifikuotų patikimumo užtikrinimo paslaugų veiklos nuostatai (QTS PS) aprašo visoms kvalifikuotoms paslaugoms bendras praktikas;
- Ilgalaikės apsaugos paslaugų veiklos nuostatai (QLPS PS) ir Laiko žymų paslaugų veiklos nuostatai (QTSS PS) aprašo praktikas specifines kiekvienai kvalifikuotai paslaugai.

1.1. Apžvalga

Standartas ETSI EN 319 421 "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-stamps" specifikuoja kvalifikuotų laiko žymų taisykles: Geriausių praktikų laiko žymų taisyklės (BTSP) Laiko žymų tarnyboms (TSA), sudarančioms viešųjų raktų sertifikatais paremtas laiko žymas 1 sekundės ar didesniu tikslumu, laiko žymų paslaugų taisyklės (OID: 0.4.0.2023.1.1). Taisyklėse 0.4.0.2023.1.1 apibrėžti reikalavimai nėra orientuoti nei į konkrečius technologinius sprendimus, nei į laiko žymų tarnybos (TSA) – patikimų paslaugų teikėjo, teikiančio laiko žymų sudarymo paslaugas, panaudojant vieną ar daugiau laiko žymas sudarančių įrenginių - organizacinę struktūrą. Taisyklių 0.4.0.2023.1.1 įgyvendinimo techniniai sprendimai, procedūros, darbuotojų tvarkos yra aprašyti šiuose MitSoft kvalifikuotų laiko žymų paslaugų veiklos nuostatuose (toliau – QTSS PS).

Veiklos nuostatai QTSS PS yra paremti šiais teisės aktais ir norminiais dokumentais:

a) Europos Parlamento ir Tarybos Reglamentu (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB [eIDAS];

b) standartu ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers";

c) standartu ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing qualified time-stamps".

Teikiant laiko žymų paslaugas, TSP atlieka elektroninės formos laiko duomenų generavimo funkciją, kurie susieja kitus elektroninius duomenis su konkrečiu laiku, nustatant įrodymus, kad tie kiti elektroniniai duomenys egzistavo tuo konkrečiu laiku.

Pastaba dėl sutrumpinimų apibrėžimų. Laiko žymos reiškia kvalifikuotas elektronines laiko žymas, kaip tai apibrėžta ES Reglamente Nr. 910/2014 [eIDAS]. Kvalifikuotų laiko žymų paslaugų taisyklės reiškia Geriausių praktikų laiko žymų taisykles (BTSP) su OID 0.4.0.2023.1.1.

MitSoft TSA laiko žymų teikimo sąlygos tenkina standarto ETSI EN 319 421 reikalavimus atskleidimo pareiškimui.

1.2. Identifikacija

QTSS PS unikalus identifikatorius (OID) yra 1.3.6.1.4.1.57890.1.3.1; jo laukų reikšmės yra pateiktos Lentelėje 1.

Lentelė 1. QTSS PS unikalaus identifikatoriaus laukų reikšmės

Pavadinimas	Reikšmė
ISO	1
ISO pripažįstama organizacija	3
JAV Gynybos Departamentas	6
Internetas	1
Privati įmonė	4
IANA įregistruota privati įmonė	1
Uždaroji akcinė bendrovė "MIT-SOFT"	57890
Padalinys: Kvalifikuotos patikimumo užtikrinimo paslaugos	1
Dokumento tipas: Kvalifikuotų laiko žymų paslaugų veiklos nuostatai	3
Dokumento versija	1

PSPS aktuali versija yra prieinama MitSoft TSA interneto svetainėje.

1.3. Laiko žymų paslaugų naudotojai ir taikymo sritys

Kvalifikuotos laiko žymų paslaugos pateikia priemones, garantuojančias duomenų egzistavimo įrodymą, kuris patvirtina, kad tie duomenys egzistavo konkrečiu laiko momentu ir nebuvo pakeist. MitSoft TSA kvalifikuotų laiko žymų paslaugų naudotojais gali būti juridiniai ar fiziniai asmenys, kuriems reikalingos TSA paslaugos.

Nei BTSP, nei QTSS PS neuždeda jokių ribojimų kvalifikuotų laiko žymų paslaugų naudojimui. Jos gali būti naudojamos, kai pasirašantis asmuo ar pasirašymo paslaugų teikėjas nori užfiksuoti laiką ir apsaugoti duomenis nuo nepastebimo pakeitimo.

TSA teikia paslaugas viešai, tačiau jos taip pat gali būti naudojamos uždarose naudotojų grupėse.

1.4. Atitiktis. Jos patvirtinimas ir patikrinimas

TSA patvirtina, kad MitSoft laiko žymų paslaugos yra ES kvalifikuotos laiko žymų paslaugos ir atitinka BTSP.

TSA veiklos atitiktis BTSP ir QTSS PS yra tikrinama, kaip nustatyta QTSS PS, ne rečiau kaip kas dveji metai.

1.5. Kontaktinė informacija

QTSS PS valdo uždaroji akcinė bendrovė "MIT-SOFT", kurios kontaktiniai duomenys yra pateikti Lentelėje 2.

Lentelė 2. MitSoft TSA kontaktiniai duomenys

TSA:	Uždaroji akcinė bendrovė "MIT-SOFT"
Adresas:	Kalvarijų g. 276-100, LT-08316 Vilnius
Tel:	+370 5 233 3922
URL:	https://www.mitsoft.lt/
El. paštas:	info@mitsoft.lt

2. Nuorodos

[eIDAS]	–	Europos Parlamento ir Tarybos Reglamentu (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB.
[EN 319 401]	–	ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
[EN 319 421]	–	ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-stamps.
[EN 319 422]	–	ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
[ISO 15408]	-	ISO/IEC 15408 (parts 1 to 3): Information security, cybersecurity and privacy protection -- Evaluation criteria for IT security.
[ISO 27001]	–	ISO/IEC 27001:2022: "Information security, cybersecurity and privacy protection – Information security management systems - Requirements".
[ISO 27002]	–	ISO/IEC 27002:2022: "Information security, cybersecurity and privacy protection – Information security controls".
[ISO 27005]	–	ISO/IEC 27005:2022: "Information security, cybersecurity and privacy protection – Guidance on managing security risks".
[RFC 3161]	–	RFC 3161: Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP).
[RFC 5816]	–	RFC 5816: ESSCertIDv2 Update for RFC 3161.
[TS 119 312]	–	ETSI TS 119 312 "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites" standard.
[QTS PS]	-	MitSoft „Kvalifikuotų patikimumo užtikrinimo paslaugų veiklos nuostatai", Versija 1.00.
[QTSS CPS]	-	MitSoft „TSA Sertifikatų taisyklės ir veiklos nuostatai".

3. Terminų apibrėžimas ir sutrumpinimai

Abonentas: juridinis ar fizinis asmuo, turintis sutartinius abonento įsipareigojimus su laiko žymų paslaugų teikėju.

Aparatinis saugumo modulis (HSM), arba kriptografinis saugumo modulis: aparatūrinė ir programinė įranga, naudojama kriptografinės raktų poros – privataus ir viešojo raktų - generavimui, tų privačių raktų saugojimui ir/ar elektroninių parašų kūrimui.

Egzistavimo įrodymas: įrodymai, kurie įrodo, kad skaitmeninis objektas egzistavo tam tikru laiko momentu.

ES kvalifikuotas TSA: kvalifikuotas patikimų paslaugų teikėjas, sudarantis kvalifikuotas elektronines laiko žymas, kaip tai nustatyta Reglamente (ES) Nr. 910/2014 [eIDAS].

Katalogas (repozitorius): vieta internete, kurioje laiko žymų paslaugų informacija yra prieinama naudotojams.

Kompromitavimas: praradimas, vagystė, modifikavimas, neteisėtas naudojimas, ar bet koks kitoks konfidencialių duomenų saugumo pažeidimas.

Koordinuotas universalus laikas (UTC): sekundinė laiko skalė kaip apibrėžta Rekomendacijose ITU-R TF.460-6 [1].

Laiko žyma: elektroninės formos duomenys, kuriais kiti elektroninės formos duomenys susiejami su tam tikru laiku ir taip sukuriamas įrodymas, kad pastarieji egzistavo tuo metu(= elektroninė laiko žyma [eIDAS]).

Laiko žymos žetonas: specifikacijoje IETF RFC 3161 apibrėžtas duomenų objektas, išreiškiantis laiko žymą.

Laiko žymų naudotojai: laiko žymų gavėjai, įskaitant abonentus, kurie jomis pasitiki.

Laiko žymų sudarymas: elektroninių laiko žymų generavimas.

Laiko žymų sudarymo įrenginys (TSU): aparatūrinės ir programinės įrangos rinkinys, valdomas kaip vienetas ir vienu momentu turintis vieną aktyvų laiko žymų pasirašymo raktą.

Laiko žymų sudarymo paslaugos: patikimos laiko žymų sudarymo paslaugos.

Laiko žymų taisyklės: užvardinta taisyklių aibė, kuri nurodo laiko žymos taikomumą konkrečiai bendruomenei ir/ar taikomųjų programų klasei su vienodais saugumo reikalavimais.

Laiko žymų tarnyba (TSA): TSP teikiantis laiko žymų sudarymo paslaugas panaudojant vieną ar daugiau laiko žymų sudarymo įrenginių.

Pasikliaujanti šalis: laiko žymos gavėjas, kuris pasitiki ta laiko žyma.

Pasirašantis asmuo: esybė, kuri yra skaitmeninio parašo sudarytoja.

Patikimas sąrašas: sąrašas, kuris pateikia informaciją apie patikimų paslaugų teikėjo teikiamų patikimų paslaugų statusą ir jų statuso istoriją dėl atitikties taikomiems reikalavimams ir taikomos teisėtvarkos atitinkamoms nuostatoms.

Patikimų paslaugų teikėjas (TSP): esybė, teikianti vieną ar daugiau patikimų paslaugų.

TSA atskleidimo pareiškimas: aibė teiginių apie TSA taisykles ir praktikas, kurios išskirtinai reikalauja abonentų ir pasikliaujančių šalių dėmesio atkreipimo, pavyzdžiui, privalomų reikalavimų įgyvendinimo.

TSA sistema: IT produktų ir komponentų organizuota kompozicija laiko žymų sudarymo paslaugų teikimui palaikyti.

TSA veiklos nuostatai /laiko žymų paslaugų veiklos nuostatai: veiklos nuostatai, kuriuos TSA taiko sudarant laiko žymas.

Pastaba: Tai yra specifinis patikimumo užtikrinimo paslaugų veikos nuostatų tipas, kaip tai yra apibrėžta standarte ETSI EN 319 401 [4].

UTC(k): „k" laboratorijos realizuota ir palaikoma pagal sutarimą su UTC laiko skalė, su tikslu pasiekti ±100 ns.

BIPM – Tarptautinis svorių ir matų biuras (*Bureau International des Poids et Mesures*)

BTSP – Geriausios praktikos laiko žymų taisyklės (*Best practice Time-Stamp Policy*)

ESI – Elektroniniai parašai ir infrastruktūra (*Electronic Signature and Infrastructure*)

ETSI – Europos telekomunikacijų standartų institutas (*European Telecommunications Standards Institute*)

OID – Objekto identifikatorius (*Object IDentifier*)

OVR – Bendrinis reikalavimas (*General Requirement*)

PS - Veiklos nuostatai (*Practice Statement*)

QLPS – Kvalifikuotos ilgalaikės apsaugos paslaugos (*Qualified Long-term Preservation Service*)

QTS - Kvalifikuotos patikimumo užtikrinimo paslaugos (*Qualified Trust Services*)

QTSP – Kvalifikuotų patikimumo užtikrinimo paslaugų teikėjas (*Qualified Trust Service Provider*)

QTSS – Kvalifikuotos laiko žymų paslaugos (*Qualified Time-Stamping Service*)

RRT – Ryšių Reguliavimo Tarnyba

TSA – Laiko žymų tarnyba (*Time-Stamping Authority*)

TSP – Patikimumo užtikrinimo paslaugų teikėjas (*Trust Service Provider*)

TSU – Laiko žymų sudarymo įrenginys (*Time-Stamping Unit*)

UTC – Pasaulinis koordinuotasis laikas (*pranc. universel temps coordonné*)

4. MitSoft TSA: Bendrosios nuostatos

Kvalifikuotų laiko žymų paslaugų apibrėžimas pagal ETSI EN 319 421 susideda iš dviejų tipų reikalavimų: taisyklių bendrųjų reikalavimų, vienodų visoms patikimumo užtikrinimo paslaugų teikėjų kvalifikuotų paslaugų klasėms, apibrėžtų standartu ETSI EN 319 401 ir į paslaugą orientuotų reikalavimų, skirtų apibrėžti kvalifikuotų laiko žymų paslaugų specifinius reikalavimus pagal standartą ETSI EN 319 421 ir kvalifikuotų laiko žymų profilį pagal standartą ETSI EN 319 422.

Laiko žymų paslaugų teikimo funkcijų klasifikavimui yra išskirtos šios paslaugų komponentės:

1) Laiko žymų teikimas: laiko žymų generavimo paslaugų komponentė.
2) Laiko žymų valdymas: laiko žymų paslaugų veikimo stebėsenos ir valdymo komponentė, užtikrinanti paslaugų teikimą kaip TSA specifikuota. Ši paslaugų komponentė yra atsakinga už laiko žymų paslaugų teikimo sistemos įdiegimą ir išdiegimą.

Šis paslaugų komponenčių padalinimas neuždeda apribojimų laiko žymų paslaugų teikimo įgyvendinimui.

5. Įvadas į laiko žymų teikimo taisykles

Teisinius reikalavimus patikimų paslaugų teikėjams (TSP), visuomenei teikiantiems paslaugas, tame tarpe laiko žymų paslaugų teikėjams, pateikia EU eIDAS Reglamentas. Reglamentas taip pat pateikia labiau specifinius reikalavimus specifinei TSP kategorijai – kvalifikuotiems TSP ir dar labiau specifinius tiems kvalifikuotiems TSP, kurie sudaro kvalifikuotas laiko žymas. Šios laiko žymų taisyklės BTSP tenkina Reglamento reikalavimus, keliamus kvalifikuotiems TSP, sudarantiems kvalifikuotas elektronines laiko žymas.

Elektroninio parašo galiojimo patikrinimui būtina įrodyti, kad parašo sudarymo metu pasirašančio asmens elektroninio parašo sertifikatas buvo galiojantis. Tam yra būtina gauti patikimų paslaugų teikėjo patikimą laiką. Toks patikimas laikas gali būti pateiktas kaip laiko žyma. Laiko žymos taip pat gali būti naudojamos taikymuose, kuriuose yra reikalingas įrodymas, kad duomenys egzistavo iki konkretaus laiko.

Susidomėjimas laiko žymomis išaugo verslo sektoriuje ir tapo viena iš svarbiausių skaitmeninių parašų komponenčių, pasiekiamų per specifikacijos IETF RFC 3161 laiko žymų protokolą su standarte ETSI EN 319 422 apibrėžtu profiliu. Ilgo galiojimo skaitmeninių parašų patikimam validavimui bei kitiems laiko žymų taikymams yra priimti būtini saugumo ir kokybės minimalūs reikalavimai.

Laiko žymų taisyklės apibrėžia užvardintą taisyklių aibę, kurios nurodo laiko žymų taikomumą konkrečiai bendruomenei ir/ar taikymų su vienodais saugumo reikalavimais klasei.

6. TAISYKLĖS IR PRAKTIKOS

6.1. Rizikos vertinimas

Žiūrėti [QTS PS] dokumento 5 skyrelį.

6.2. Laiko žymų paslaugų veiklos nuostatai

Žiūrėti [QTS PS] dokumento 6.1 skyrelį.

Papildomai, kvalifikuotų laiko žymų paslaugų teikimui:

a) Šiuose Laiko žymų paslaugų veiklos nuostatuose (QTSS PS) yra pateikiamos BTSP taisyklėse nurodytų reikalavimų įgyvendinimo praktikos ir procedūros.

b) QTSS PS identifikuoja visų TSA paslaugas palaikančių išorinių organizacijų įsipareigojimus, įskaitant taikomas taisykles ir praktikas.

BTSP yra vienintelės MitSoft TSA palaikomos kvalifikuotų patikimų paslaugų taisyklės:

a) Santraukos algoritmai, naudojami reprezentuoti laiko žyma apsaugotus duomenis, ir laiko tikslumas laiko žymose pagal UTC yra specifikuoti šių QTSS PS skyriuje 7.7.1. Laiko žymų teikimas.

b) Abonentų įsipareigojimai yra specifikuoti QTSS PS skyriuje 6.5.3. Abonentų įsipareigojimai.

c) Pasikliaujančių šalių įsipareigojimai yra specifikuoti QTSS PS skyriuje 6.6. Pasikliaujančių šalių įsipareigojimai.

d) Laiko žymų sudarymo paslaugos yra kvalifikuotos laiko žymų paslaugos pagal (ES) Reglamentą Nr. 910/2014 [eIDAS]. TSA veikia Lietuvos Respublikoje ir tenkina ES ir Lietuvos teisės ir norminius aktus.

MitSoft TSA atskleidimo pareiškimas yra specifikuotas MitSoft kvalifikuotų laiko žymų paslaugų teikimo sąlygose.

6.3. Paslaugų teikimo sąlygos

Žiūrėti [QTS PS] dokumento 6.2 skyrelį.

Papildomai, kvalifikuotų laiko žymų paslaugų teikimo sąlygos specifikuoja:

a) Taikomas BTSP taisykles.

b) Informaciją, kaip patikrinti laiko žymas, ir bet kokius galimus susijusius laiko žymų galiojimo apribojimus.

c) Ar kvalifikuotos laiko žymų paslaugos buvo įvertintos atitikčiai BTSP ir, jeigu taip, pagal kokią atitikties įvertinimo schemą.

6.4. Informacijos saugumo taisyklės

Žiūrėti [QTS PS] dokumento 6.3 skyrelį.

6.5. TSA įsipareigojimai

6.5.1. Bendrosios nuostatos

TSA užtikrina, kad visi TSA taikomi reikalavimai yra įgyvendinti kaip taikytina BTSP. TSA užtikrina įgyvendinimą:

a) šiuose veiklos nuostatuose apibrėžtas procedūras, įskaitant paslaugų laiko žymų generavimą ir valdymą;
b) bet kokių papildomų įsipareigojimų, nurodytų Paslaugų teikimo sąlygose ar įtrauktų pagal nuorodą, laikymąsi;
c) atšauktų sertifikatų sąrašai (CRL) TSU sertifikatams yra atnaujinami ir ši informacija yra prieinama nuolat (detaliau žiūrėti [QTSS CPS], skyrius 4.10. Paslaugos sertifikatų būsenai nustatyti);
d) teikiamos laiko žymos deklaruojamos esančiomis kvalifikuotomis elektroninėmis laiko žymomis ir turi atitinkamą plėtinį (detaliau, žiūrėti skyrių 7.7.1. Laiko žymų teikimas).

6.5.2. TSA įsipareigojimai abonentams

Žiūrėti [QTS PS] dokumento 6.1.1.1 skyrelį.

6.5.3. Abonentų įsipareigojimai

Pasitikėdamas kvalifikuota laiko žyma, abonentas turi patikrinti, kad laiko žyma buvo sukurta korektiškai (detaliau, žiūrėti skyrių 6.6. Informacija pasikliaujančioms šalims).

6.5.4. Intelektualios nuosavybės teisės

Žiūrėti [QTS PS] dokumento 6.1.1.5 skyrelį.

6.5.5. Atsakomybė

Žiūrėti [QTS PS] dokumento 6.1.1.2 skyrelį.

6.5.6. Teisinės nuostatos ir interpretavimas

Žiūrėti [QTS PS] dokumento 6.1.1.3 skyrelį.

6.6. Informacija pasikliaujančioms šalims

Pasikliaujančioji šalis, pasitikėdama kvalifikuota laiko žyma, turi patikrinti, kad kvalifikuota laiko žyma buvo korektiškai pasirašyta ir kad privatus raktas, panaudotas laiko žymos pasirašymui, nebuvo kompromituotas (atskleistas trečiosioms šalims ar dėl kitokių priežasčių nenaudotinas) iki patikrinimo laiko.

Laiko žyma yra tikrinama TSU sertifikato galiojimo laikotarpyje, todėl privataus rakto galiojimas gali būti patikrintas įsitikinant, kad TSU sertifikatas nebuvo atšauktas. Laiko žymų patikrinimo nurodymai yra specifikuoti Kvalifikuotų laiko žymų paslaugų teikimo sąlygose.

Be to, pasikliaujančioji šalis turi sutikti su laiko žymų naudojimo ribojimais, apibrėžtais BTSP ir imtis visų kitų atsargumo priemonių.

7. TSA VALDYMAS IR VEIKIMAS

7.1. Įvadas

TSA gali nustatyti kvalifikuotų laiko žymų paslaugų kainas. TSA laikosi sekančiuose punktuose nurodytų praktikų.

7.2. Vidinė organizacija

Žiūrėti [QTS PS] dokumento 7.1 skyrelį.

7.3. Personalo saugumas

Žiūrėti [QTS PS] dokumento 7.2 skyrelį.

a) Patikimos rolės yra apibrėžtos MitSoft QTSP informacijos saugumo taisyklėse. Papildomai nurodyta rolė, apimanti šias atsakomybės:
   - HSM saugumo pareigūnas: įgaliotas sukurti ir sunaikinti kriptografinius raktus ir sertifikatus, vykdyti HSM priežiūrą (įdiegti, atnaujinti ir konfigūruoti HSM). Atsakingas už dvigubos kontrolės išskirstytų prieigos raktų sugeneravimą ir išsaugojimą.

7.4. Turto valdymas

Žiūrėti [QTS PS] dokumento 7.3 skyrelį.

7.5. Prieigos valdymas

Žiūrėti [QTS PS] dokumento 7.4 skyrelį.

7.6. Kriptografinis valdymas

7.6.1. Bendrosios nuostatos

TSA užtikrina kriptografinių raktų ir kriptografinių įrenginių saugumą per visą jų gyvavimo ciklą, kaip detalizuota sekančiuose skyreliuose.

7.6.2. TSU raktų generavimas

TSA generuoja savo kriptografinius raktus valdomoje aplinkoje. Konkrečiai:

a) TSU privačių raktų generavimas yra vykdomas fiziškai saugioje aplinkoje darbuotojų patikimose rolėse, taikant bent dvigubą kontrolę (žiūrėti [EN 319 421] punktą 7.6.2.). Darbuotojai, įgalioti atlikti šią funkciją, yra riboti tik tais, kurie yra būtini šiai funkcijai atlikti pagal TSA praktikas.

b) TSU raktų poros generavimas (TSU sertifikatams ir TSA šakniniams sertifikatams) yra vykdomas kriptografiniame modulyje, kuris užtikrina EAL4+ ar didesnį lygį pagal ISO/IEC 15408 [ISO 15408].

c) TSU rakto generavimo algoritmas, sugeneruoto privataus rakto ilgis ir laiko žymų parašo algoritmo rakto ilgis yra pripažinti tinkamais naudoti TSA teikiamoms laiko žymoms. Konkretūs parašo algoritmai ir raktų ilgiai, naudojami laiko žymų teikimui, yra apibrėžti TSU sertifikatų profiliuose (žiūrėti [QTSS CPS], skyrelis 7.1.2. TSU sertifikato profilis).

d) TSU privatus raktas yra sugeneruojamas kriptografinio modulio viduje ir niekada neeksportuojamas iš jo ir niekada neimportuojamas į jį.

e) TSU turi tik vieną aktyvų pasirašymo raktą bet kuriuo laiko momentu.

7.6.3. TSU privataus rakto apsauga

TSA užtikrina, kad TSU privatus raktas išlieka konfidencialus ir palaiko jo integralumą. Konkrečiai:

a) TSU privatus raktas yra laikomas ir naudojamas kriptografiniame modulyje, kuris užtikrina EAL4+ ar didesnį lygį pagal ISO/IEC 15408 [ISO 15408].

b) TSU privatūs raktai yra kuriami kriptografiniame modulyje ir niekada jo nepalieka. TSU privačių raktų generavimą vykdo tik patikimų rolių darbuotojai, esant bent dvigubai kontrolei, fiziškai saugioje aplinkoje patalpose, apsaugotose nuo nekontroliuojamos prieigos (žiūrėti [EN 319 421] punktą 7.6.3.). Darbuotojai, įgalioti atlikti šią funkciją, yra riboti tik tais, kurie yra būtini šiai funkcijai atlikti pagal TSA praktikas.

c) TSU privačių raktų kopijos nėra daromos.

7.6.4. TSU viešojo rakto sertifikatas

TSA užtikrina TSU parašo patikrinimo (viešųjų) raktų integralumą ir autentiškumą, o bet kurie susiję parametrai yra prižiūrimi, juos pateikiant pasikliaujančioms šalims. Konkrečiai:

a) TSU parašų patikrinimo (viešieji) raktai yra pateikiami pasikliaujančioms šalims viešųjų raktų sertifikatuose.

b) TSU parašų patikrinimo (viešojo) rakto sertifikatas yra pačios TSA sudarytas pagal MitSoft TSA sertifikatų taisykles su OID 1.3.6.1.4.1.57890.1.2.1 ir apibrėžtas [QTSS CPS].

c) TSU negali teikti laiko žymų tol, kol atitinkamas parašo patikrinimo (viešojo rakto) sertifikatas nebus į jas talpinamas.

TSU sertifikato profilis yra apibrėžtas MitSoft TSA sertifikatų taisyklėse ir veiklos nuostatuose (žiūrėti [QTSS CPS] (skyrelis 7.1.2. TSU sertifikato profilis) ir užtikrina atitiktį reikalavimams, apibrėžtiems ETSI EN 319 422 [EN 319 422].

7.6.5. TSU kriptografinių raktų keitimas

Siekiant patenkinti kriptografinio saugumo reikalavimus ir sumažinti algoritmo nusilpimo ar raktų kompromitavimo poveikį, TSU raktų keitimas yra vykdomas kas dveji metai, naudojant algoritmą, kuris yra pripažįstamas būti tinkamu bent 5 metų laikotarpiui.

Atsižvelgiant į sertifikavimo ir sertifikato įtraukimo į Patikimą sąrašą procedūras, privačių raktų galiojimas yra apribotas 3 metais. Sertifikatas turi plėtinį, nurodantį atitinkamo privataus rakto naudojimo laikotarpį.

Tam, kad leisti pakankamą laiko žymų galiojimo laikotarpį, TSU sertifikato galiojimo laikotarpis nustatytas 7,5 metams. Jeigu pasirodys, kad panaudoti algoritmai tampa nebetinkami šiam laikotarpiui, įtakojami sertifikatai yra atšaukiami.

Privačių raktų naudojimo ir sertifikatų galiojimo tikslūs laikotarpiai yra apibrėžti TSU sertifikatų profilyje (žiūrėti [QTSS CPS], skyrelis 7.1.2. TSU sertifikato profilis).

7.6.6. Pasirašymo kriptografinės įrangos gyvavimo ciklo valdymas

TSA užtikrina kriptografinės įrangos saugumą per visą jos gyvavimo ciklą. Konkrečiai, TSA užtikrina, kad:

a) Laiko žymų pasirašymo kriptografinė įranga nėra pažeista transportuojant ir sandėliuojant. Prieš diegimą aparatinė įranga saugumo pareigūno buvo patikrinta pagal informacijos saugumo taisykles ir rezultatai yra dokumentuoti aparatinės įrangos žurnale.

b) TSU privačių raktų generavimas ir aktyvavimas yra atliktas darbuotojų

patikimose pareigose, taikant bent dvigubą kontrolę, fiziškai saugioje aplinkoje. Šie įvykiai yra dokumentuoti aparatinio įrenginio žurnale. Raktų atsarginės kopijos nėra daromos.

c) TSU privatūs pasirašymo raktai, išsaugoti kriptografiniame modulyje, kuris daugiau nebenaudojamas gamyboje, yra sunaikinami, panaudojant saugią nunulinimo (*angl. zeroization*) procedūrą, aprašytą įrenginio dokumentacijoje, taip, kad praktiškai nebūtų įmanoma jų atstatyti.

7.6.7. TSU raktų gyvavimo ciklo pabaiga

TSU raktų galiojimo laikotarpis yra apibrėžtas TSU sertifikato profilyje (žiūrėti [QTSS CPS], skyrelis 7.1.2. TSU sertifikato profilis). Rakto galiojimo pabaigos data yra nustatyta rakto generavimo metu ir įtraukta į TSU viešojo rakto sertifikatą.

TSA užtikrina, kad TSU privatūs pasirašymo raktai nėra naudojami po jų galiojimo laikotarpio pabaigos. Konkrečiai:

a) Nauja raktų pora yra sugeneruojama kas dveji metai, vieni metai prieš jų galiojimo pabaigos datą pagal atitinkamas procedūras (žiūrėti skyrelį 7.6.2. TSU rakto generavimas). Atitinkamas viešojo rakto sertifikatas yra sugeneruojamas ir jo įtraukimo į Lietuvos patikimą sąrašą procedūros yra inicijuojamos (žiūrėti [QTSS CPS], skyrelis 4.7. Sertifikato rakto pakeitimas). Nedelsiant, kai naujas sertifikatas yra įtrauktas į Patikimą sąrašą, naujas pasirašymo raktas yra aktyvuojamas, automatiškai deaktyvuojant senąjį raktą kadangi TSU vienu metu gali turėti tik vieną aktyvų pasirašymo raktą.

b) Deaktyvuotas pasirašymo raktas yra sunaikinamas pagal atitinkamas procedūras taip, kad jis negalėtų būti atstatytas.

7.7. Laiko žymų sudarymas

7.7.1. Laiko žymų teikimas

MitSoft kvalifikuotos laiko žymų paslaugos teikia kvalifikuotas elektronines laiko žymas tik pagal (ES) Reglamentą Nr. 910/2014 [eIDAS].

TSA užtikrina, kad laiko žymos yra teikiamos saugiai ir talpina korektišką datą ir laiką. Konkrečiai:

a) TSU laiko žymose naudojamos laiko vertės trasuojamos su bent viena UTC(k) laboratorijos platinamų realaus laiko reikšmių verte.

b) Į laiko žymą įtraukta laiko vertė nuo UTC nesiskiria daugiau negu tikslumas apibrėžtas TSA bei nurodytas pačioje laiko žymoje.

c) Jeigu yra nustatoma, kad laiko žymų paslaugų teikėjo laikrodis nukrypo (žiūrėti skyrelį 7.7.2 Laikrodžio sinchronizavimas su UTC) daugiau negu deklaruotas tikslumas, tai laiko žymos nėra teikiamos.

d) Laiko žymos yra pasirašomos panaudojant tik šiai paskirčiai sugeneruotą raktą.

e) Laiko žymų generavimo sistema atmeta bet kokį mėginimą teikti laiko žymą, jei pasirašymo privataus rakto galiojimas pasibaigė.

Teikiamos laiko žymos atitinka laiko žymos profilį, apibrėžtą ETSI EN 319 422 [EN 319 422]. Sugeneruotos laiko žymos struktūra atitinka RFC 3161 [RFC 3161] ir atnaujinimus, apibrėžtus RFC 5816 [RFC 5816].

TSA priimama laiko žymos užklausos struktūra yra pateikta Lentelėje 3; TSA teikiamos laiko žymos struktūra yra pateikta Lentelėje 4.

Lentelė 3. Laiko žymos užklausos struktūra

Laukas	Privaloma	Aprašas	Reikšmė
version	Taip	Aprašo laiko žymos užklausos versiją	1
messageImprint	Taip	Apima laiko žyma saugomų duomenų santrauką	Santraukos algoritmo OID ir laiko žyma apsaugomų duomenų santraukos reikšmė; Palaikomi algoritmai: • SHA-256 (OID: 2.16.840.1.101.3.4.2.1)[1] • SHA-384 (OID: 2.16.840.1.101.3.4.2.2) • SHA-512 (OID: 2.16.840.1.101.3.4.2.3) • SHA3-256 (OID: 2.16.840.1.101.3.4.2.8) • SHA3-384 (OID: 2.16.840.1.101.3.4.2.9) • SHA3-512 (OID: 2.16.840.1.101.3.4.2.10)
reqPolicy	Ne	Nurodo TSA taisykles, pagal kurias teikiamos laiko žymos	Jei specifikuota, turi būti 0.4.0.2023.1.1[2]
nonce	Ne	Leidžia klientui patikrinti atsakymų eiliškumą, kai lokalus laikrodis nėra prieinamas	Jei specifikuota, ta pati reikšmė bus įdėta į laiko žymą
certReq	Ne	Nurodo, ar sertifikatas turi būti įdėtas į laiko žymą	Jei yra ir nustatyta Taip, tai atitinkamas TSU sertifikatas bus įtrauktas į laiko žymą
extensions	Ne	Papildoma užklausos informacija	Jeigu yra, turi būti pažymėtas kaip nekritinis

Lentelė 4. Laiko žymos struktūra

Laukas	Privaloma	Aprašas	Reikšmė
version	Taip	Aprašo laiko žymos struktūros versiją	1
policy	Taip	Nurodo TSA taisykles, pagal kurias buvo sudarytas atsakymas	OID: 0.4.0.2023.1.1[3]
messageImprint	Taip	Apima duomenų, kuriuos saugo laiko žyma, santrauką	Lygi laiko žymos užklausos atitinkamo lauko reikšmei (TimeStampReq)
serialNumber	Taip	TSA kiekvienai laiko žymai priskirtas sveikas skaičius	Sveikas skaičius (iki 160 bitų ilgio), unikalus kiekvienai TSU teikiamai laiko žymai
genTime	Taip	Laikas, kuriuo metu TSA sukūrė laiko žymą	UTC laikas, nurodantis laiką, kada buvo sukurta laiko žyma. Gali įtraukti sekundės dalis

[1] Nuorodos į algoritmų aprašus yra pateiktos ETSI TS 119 312 [TS 119 312].
[2] Geriausios praktikos taisyklės laiko žymoms, apibrėžtos ETSI EN 319 421 [EN 319 421].
[3] Geriausios praktikos taisyklės laiko žymoms, apibrėžtos ETSI EN 319 421 [EN 319 421].

accuracy	Ne	Pateikia galimą teikiamų laiko žymų laiko nuokrypį nuo UTC laiko	0.5 s (500 ms)
ordering	Ne	Laiko žymų eiliškumas	Nepateikiamas
nonce	Ne	Leidžia klientui patikrinti atsakymų eiliškumą, kai lokalus laikrodis nėra prieinamas	Lygi laiko žymos užklausos atitinkamo lauko reikšmei (TimeStampReq), jeigu įtrauktas
tsa	Ne	Pateikia užuominą identifikuojant TSA pavadinimą	Atitinka subjekto DN lauko reikšmei, panaudotai laiko žymos parašo patvirtinimo sertifikate. Pavyzdžiui, "CN=MitSoft QTSA TSU-1, O=MitSoft, organizationIdentifier=NTRLT-120792080, C=LT"
extensions	Ne	Papildoma informacija prie atsakymo	Požymis, kad ši laiko žyma yra teikiama kaip kvalifikuota elektroninė laiko žyma pagal (ES) Reglamentą (EU) Nr. 910/2014: qcStatements=esi4-qtstStatement-1

7.7.2. Laikrodžio sinchronizavimas su UTC

TSA užtikrina, kad TSU laikrodžiai yra sinchronizuoti su UTC laiku deklaruotu tikslumu. Konkrečiai:

a) TSU laikrodžiai yra sinchronizuoti su UTC naudojant laiko palyginimą su UTC(k) laboratorijų platinamu laiku, publikuojamu, Bureau International des Poids et Mesures (BIPM) leidžiamame, "Circular T" ir patikslinimuose. Laikrodžių laikas yra trasuojamas su UTC per palyginimų grandinę, kurios neapibrėžtumas yra deklaruoto tikslumo ribose.

b) TSU laikrodžiai yra apsaugoti nuo grėsmių, įskaitant neturinčių teisėtos prieigos darbuotojų klastojimo, radijo ir elektros impulsų staigių šuolių, kurie gali nepastebimai paveikti laikrodį, išvedant jį iš kalibravimo ribų.

c) TSA naudojamos sistemos yra pajėgios aptikti, ar laikas, kuris būtų nurodomas laiko žymose, pasislenka ar išeina iš sinchronizavimo su UTC ribų.

d) Jei yra nustatyta, kad laikas, kuris būtų nurodomas laiko žymose, pasislenka ar išeina iš sinchronizavimo su UTC ribų, tai laiko žymų teikimas yra stabdomas.

e) TSU laikrodžiai palaiko sinchronizaciją kai susiformuoja keliamoji sekundė, kaip apie tai praneša atitinkama įstaiga. Laiko pakeitimas, atsižvelgiant į keliamąją sekundę, vykdomas paskutinę minutę tos dienos, kada suplanuota atlikti keliamąją sekundę. Sistemos registruoja šio pakeitimo tikslų laiką. Jeigu keliamoji sekundė yra įterpiama, apsisaugojimui nuo galimų dviprasmiškumų ir problemų, kai sistemos negali susitvarkyti su 61 sekunde per minutę, laiko žymos nėra teikiamos keliamąją sekundę ir sekundę prieš ją.

7.8. Fizinis ir aplinkos saugumas

Žiūrėti [QTS PS] dokumento 7.6 skyrelį.

Kvalifikuotoms laiko žymų paslaugoms yra taikomos saugumo priemonės:

- Kelių asmenų dalyvavimo prieigos kontrolė yra taikoma užtikrinti kriptografinių modulių, esančių fizinio ir aplinkos saugumo požiūriu saugiose patalpose, saugumą.

7.9. Veikimo saugumas

Žiūrėti [QTS PS] dokumento 7.7 skyrelį.

7.10. Tinklo saugumas

Žiūrėti [QTS PS] dokumento 7.8 skyrelį.

Papildomai:

a) TSU sistemos yra laikomos kritinėmis QTSP sistemomis ir, kaip tokios, yra palaikomos ir apsaugotos saugumo zonoje. Tinklo prieiga prie laiko žymų paslaugų, teikiamų TSU sistemomis yra galima tik per saugumo įrenginius ir dedikuotus atvirkštinius tarpinius serverius (*angl. reverse proxy servers*).

b) Tam, kad užtikrinti išorinės prieigos aukštą prieinamumo prie laiko žymų paslaugų lygį, reikalingos turimos perteklinės išorinio tinklo jungtys.

7.11. Incidentų valdymas

Žiūrėti [QTS PS] dokumento 7.9 skyrelį.

7.12. Įrodymų surinkimas

Žiūrėti [QTS PS] dokumento 7.10 skyrelį.

Papildomai:

a) Visi TSU raktų ir TSU sertifikatų gyvavimo ciklo įvykiai yra dokumentuojami ir išsaugomi.

b) TSU laikrodžio sinchronizavimo su UTC visi įvykiai yra dokumentuojami ir išsaugomi. Įrašai apima informaciją susijusią su planiniu laiko žymų laikrodžio pakartotiniu kalibravimu ar sinchronizavimu, o taip pat informaciją apie visus įvykius, susijusius su sinchronizavimo praradimo aptikimu.

c) Kvalifikuotų laiko žymų paslaugų įrašai yra saugomi per laikotarpį, tinkamą pateikti būtinus teisinius įrodymus, ir sutinkamai su paskelbtomis TSA paslaugų teikimo sąlygomis.

7.13. Veiklos tęstinumo valdymas

Žiūrėti [QTS PS] dokumento 7.11 skyrelį.

Papildomai, TSA veiklos tęstinumo planas apima TSU privačių pasirašymo raktų kompromitaciją ar įtariamą kompromitaciją arba TSU laikrodžio kalibravimo praradimą.

7.14. TSA užbaigimas ir užbaigimo planas

Žiūrėti [QTS PS] dokumento 7.12 skyrelį.

Papildomai:

a) TSU privatūs raktai yra sunaikinami tokiu būdu, kad privatūs raktai negali būti atstatyti.
b) TSA atšaukia TSU sertifikatus.

7.15. Atitiktis

Žiūrėti [QTS PS] dokumento 7.13 skyrelį.

8. PAPILDOMI REIKALAVIMAI KVALIFIKUOTOMS ELEKTRONINĖMS LAIKO ŽYMOMS PAGAL (ES) REGLAMENTĄ Nr. 910/2014

8.1. TSU viešojo rakto sertifikatas

MitSoft TSA yra institucija išduodanti sertifikatus, kuriuos naudoja MitSoft kvalifikuotos laiko žymų paslaugos, ir šių sertifikatų išdavimas yra sudėtinė laiko žymų sudarymo paslaugų dalis. Šis dokumentas apima reikalavimus laiko žymų paslaugų teikėjams, teikiantiems laiko žymas pagal ETSI EN 319 421 [EN 319 421]. MitSoft TSA sertifikatų taisyklių ir veiklos nuostatų dokumentas (žiūrėti [QTSS CPS]) apima reikalavimus, susijusius su sertifikatų (įskaitant TSU sertifikatų) išleidimu ir valdymu. MitSoft TSA sertifikatų taisyklės (žiūrėti [QTSS CPS]) užtikrina aukštą saugumo lygį, įskaitant kvalifikuoto parašo kūrimo įtaiso naudojimą kriptografinių raktų saugojimui.

8.2. TSU teikiantys nekvalifikuotas ir kvalifikuotas elektronines laiko žymas pagal (ES) Reglamentą Nr. 910/2014

MitSoft TSA teikia tik kvalifikuotas laiko žymas pagal (ES) Reglamentą Nr. 910/2014.

MitSoft TSA teikia laiko žymas naudojant du skirtingus TSU įrenginius, išleidžiančius kvalifikuotas elektronines laiko žymas, siekiant užtikrinti aukštą paslaugos prieinamumą.

MitSoft TSA teikia kvalifikuotas laiko žymas ir neteikia nekvalifikuotų laiko žymų.