MitSoft

Kvalifikuotos laiko žymų paslaugos

Sertifikatų taisyklės ir veiklos nuostatai

QTSS-CPS-LT

Unikalus objekto identifikatorius (OID): **1.3.6.1.4.1.57890.1.2.1**

Versija 1.00

Galioja nuo 2024-09-01

UAB „MIT-SOFT“, Kalvarijų g. 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	2024-09-01	Pirma oficiali dokumento versija

Dokumento patvirtinimas

	Vardas pavardė	Data	Parašas
Patikrino	Adomas Birštunas	2024-09-01	
Patvirtino	Antanas Mitašiūnas	2024-09-01	

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/.

1.1. Apžvalga

MitSoft laiko žymų paslaugų teikimo tarnyba (TSA) yra įmonė išleidžianti kvalifikuotas elektronines laiko žymas ir taip pat sertifikatus, naudojamus teikiant MitSoft kvalifikuotų laiko žymų paslaugas (QTSS). MitSoft TSA sertifikatų taisyklės apibrėžia MitSoft sudaromų sertifikatų pagrindinius reikalavimus. MitSoft TSA Sertifikavimo veiklos nuostatai apibrėžia praktikas, naudojamas įgyvendinant šias MitSoft TSA sertifikatų taisykles. MitSoft TSA Sertifikatų taisyklės ir MitSoft TSA Sertifikavimo veiklos nuostatai yra pateikti kaip vienas MitSoft TSA Sertifikatų taisyklių ir veiklos nuostatų (CPS) dokumentas. Kadangi MitSoft TSA išleidžia sertifikatus tik QTSS reikmėms, šis CPS dokumentas pateikia nuorodas į tam tikras [QTSS PS] dokumento dalis, siekiant išvengti reikalavimų kartojimo. CPS dokumentas yra paruoštas atsižvelgiant į standarto ETSI EN 319 411-1 [EN 319 411-1] reikalavimus, ir pritaikant QTSS poreikiams.

Pastaba dėl sutrumpinimų apibrėžimų. Laiko žymos reiškia kvalifikuotas elektronines laiko žymas, kaip tai apibrėžta ES Reglamente Nr. 910/2014 [eIDAS]. Sertifikatų taisyklės reiškia MitSoft TSA sertifikatų taisykles. Sertifikavimo veiklos nuostatai reiškia MitSoft TSA sertifikavimo veiklos nuostatus. MitSoft TSA ar MitSoft QTSA reiškia MitSoft laiko žymų tarnybą.

1.2. Identifikavimas

MitSoft TSA sertifikatų taisyklių unikalus identifikatorius (OID) yra 1.3.6.1.4.1.57890.1.2.1; jo laukų reikšmės yra pateiktos Lentelėje 1.

Lentelė 1. CP 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: MitSoft TSA sertifikatų taisyklės	2
Dokumento versija	1

1.3. Viešųjų raktų infrastruktūros dalyviai

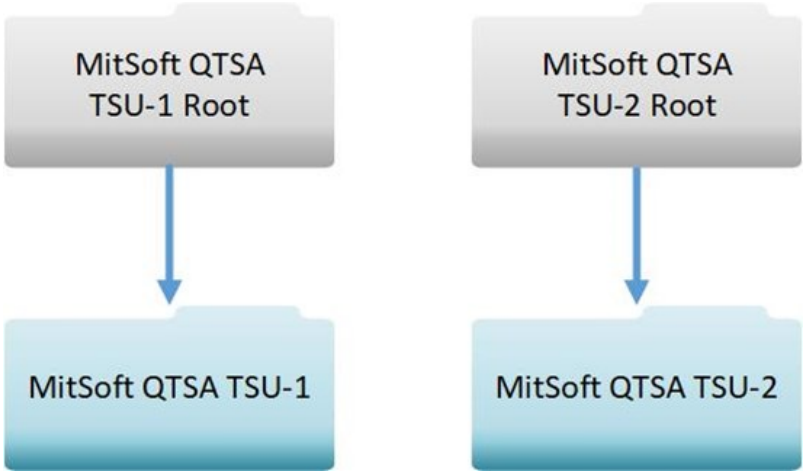
MitSoft TSA sertifikavimo tarnyba yra naudojama tik kaip sertifikatų QTSS reikmėms leidėjas. Kitiems taikymams ši sertifikavimo tarnyba netaikoma. Dėl to nėra registravimo tarnybos.

TSA išleidžia sertifikatus tik MitSoft kvalifikuotų laiko žymų paslaugų reikmėms ir todėl ji neturi savo abonentų.

1.3.1. Sertifikavimo tarnyba

Yra naudojamos dvi identiškos struktūros sertifikatų hierarchijos. Kiekvienos hierarchijos raktai ir sertifikatai talpinami skirtinguose dedikuotuose HSM įrenginiuose. Hierarchijos viršūnėje yra šakninis save pasirašantis sertifikatas, kuris yra naudojamas TSU sertifikatų ir sertifikatų atšaukimo sąrašo pasirašymui.

Šiame paveikslėlyje yra pateikta TSA sertifikatų hierarchija:



MitSoft TSA generuoja ir saugo save pasirašančių šakninių sertifikatų ir TSU sertifikatų raktus HSM įrenginyje, kuris yra eIDAS sertifikuotas kaip kvalifikuotas parašo kūrimo įrenginys ir kvalifikuotas spaudo kūrimo įrenginys (QSCD). HSM įrenginiai yra saugūs kriptografiniai įrenginiai, kurie pasižymi EAL4+ ar aukštesniu atitikties užtikrinimo lygiu pagal ISO/IEC 15408 [ISO 15408].

1.3.2. Registravimo tarnyba

Netaikoma.

1.3.3. Abonentai

Netaikoma.

1.3.4. Pasikliaujančios šalys

Numatyta, kad TSA sertifikatus naudos MitSoft QTSS pasikliaujančios šalys kvalifikuotų laiko žymų patikrinimui.

1.3.5. Kiti dalyviai

Netaikoma.

1.4. Sertifikatų naudojimas

Save pasirašantys sertifikavimo tarnybos šakniniai sertifikatai ir jų privatūs raktai yra naudojami tik MitSoft kvalifikuotų laiko žymų paslaugų TSU sertifikatų išleidimui ir

atitinkamų CRL pasirašymui. Bet koks kitoks save pasirašančių šakninių sertifikatų privačių raktų panaudojimas yra draudžiamas.

Išleisti TSU sertifikatai ir jų privatūs raktai yra naudojami tik MitSoft kvalifikuotose laiko žymų paslaugose tik kvalifikuotų elektroninių laiko žymų pasirašymui. Bet koks kitas TSU sertifikatų privačių raktų panaudojimas yra draudžiamas.

1.5. Taisyklių administravimas

MitSoft TSA sertifikatų taisyklės yra administruojamos Uždarosios akcinės bendrovės "MIT-SOFT", kurios kontaktiniai duomenys yra pateikti Lentelėje 2.

MitSoft TSA sertifikatų taisyklės ir veiklos nuostatai yra patvirtinti Uždarosios akcinės bendrovės "MIT-SOFT" direktoriaus.

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

1.6. Nuorodos

[eIDAS] – 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, 2014 m. liepos 23 d.

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

[EN 319 411-1] - ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[EN 319 412-1] - ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.

[EN 319 412-3] - ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.

[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 5280] - RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

[RFC 5480] - RFC 5480: Elliptic Curve Cryptography Subject Public Key Information.

[TS 119 312] – ETSI TS 119 312 "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites" standard.

[QTSS PS] - MitSoft „Kvalifikuotų laiko žymų paslaugų veiklos nuostatai", Versija 1.00.

1.7. Apibrėžimai 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.

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 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 paslauga: patikima laiko žymų sudarymo paslauga.

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

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.

Sertifikatų taisyklės: užvardinta taisyklių aibė, kuri nurodo sertifikato taikomumą konkrečiai bendruomenei ar taikymų klasei su vienodais saugumo reikalavimais.

Sertifikavimo veiklos nuostatai: praktikos, kurias sertifikavimo tarnyba (CA) naudoja, valdant, išleidžiant, atšaukiant, atnaujinant sertifikatus ar keičiant jų raktus.

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

Pastaba: Tai yra specifinis patikimų paslaugų veiklos nuostatų tipas, kaip tai yra apibrėžtas standarte ETSI EN 319 401 [4].

CA – Sertifikavimo tarnyba (*Certification Authority*)

CP - Sertifikatų taisyklės (*Certificate Policy*)

CRL - Atšauktų sertifikatų sąrašas (*Certificate Revocation List*)

CPS - MitSoft TSA sertifikatų taisyklės ir veiklos nuostatai (*MitSoft TSA Certificate Policy and Practice Statement*)

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

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

OID – Objekto identifikatorius (*Object IDentifier*)

PS - Veiklos nuostatai (*Practice Statement*)

QTSP – Kvalifikuotas patikimų 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*)

2. PUBLIKAVIMAS IR KATALOGO ATSAKOMYBĖS

Visi sertifikatai ir atšauktų sertifikatų sąrašai (CRL) yra prieinami MitSoft kataloge. MitSoft katalogas yra viešai prieinamas abonentams ir pasikliaujančioms šalims.

TSU sertifikatai yra viešinami kataloge po jų įtraukimo į Lietuvos patikimą sąrašą.

CRL taip pat yra viešai prieinami MitSoft kataloge.

Reguliaraus CRL sąrašo skelbimo dažnumas yra atliekamas ne rečiau kaip kas 24 val. Nereguliarus CRL sąrašas gali būti išleistas ir paskelbtas betarpiškai po sertifikato atšaukimo.

3. IDENTIFIKAVIMAS IR AUTENTIFIKAVIMAS

CA išleidžia sertifikatus tik pačiai MitSoft TSA ir neišleidžia sertifikatų kitiems subjektams. Taigi, nėra reikalavimų galutinių naudotojų, besikreipiančių į CA dėl sertifikato gavimo, tapatybės ar kitų atributų identifikavimui ir autentifikavimui.

Vidinės MitSoft TSA procedūros yra taikomos raktų generavimui ir TSU sertifikatų QTSS išleidimui. TSU sertifikatai gali būti atšaukti tik pačios MitSoft TSA, panaudojant vidines procedūras.

4. OPERACINIAI REIKALAVIMAI SERTIFIKATŲ GYVAVIMO CIKLUI

Sertifikatai yra išleisti MitSoft kvalifikuotoms laiko žymų paslaugoms, panaudojant vidines procedūras, kurios įgyvendina reikalavimus TSU sertifikatų generavimui, apibrėžtus ETSI EN 319 421 [EN 319 421].

4.1. Sertifikatų prašymai

Netaikoma.

4.2. Sertifikatų prašymų apdorojimas

Netaikoma.

4.3. Sertifikatų išleidimas

TSU sertifikatai yra išleidžiami tik MitSoft kvalifikuotoms laiko žymų paslaugoms. Kiti abonentai negali pateikti prašymų sertifikatams.

Save pasirašančių šakninių CA sertifikatų ir TSU sertifikatų raktų generavimas bei sertifikatų išleidimas yra vykdomas darbuotojų patikimose rolėse ir pagal bent dvigubą kontrolę užtikrinančias vidines procedūras.

4.4. Sertifikatų priėmimas

Netaikoma.

4.5. Raktų poros ir sertifikato naudojimas

Šakninių CA sertifikatų privatūs raktai gali būti naudojami tik TSU sertifikatų ir atitinkamų CRL sąrašų pasirašymui. Bet koks kitas šakninių CA sertifikatų privačių raktų naudojimas yra draudžiamas.

TSU sertifikatų privatūs raktai gali būti naudojami tik MitSoft kvalifikuotų laiko žymų paslaugų išleidžiamų laiko žymų pasirašymui. Bet koks kitas TSU sertifikatų privačių raktų naudojimas yra draudžiamas.

Privatūs raktai negali būti naudojami už privačių raktų naudojimo laikotarpio ribų.

Pasikliaujančios šalys turėtų naudoti TSU sertifikatus ir viešuosius raktus tik laiko žymų patikrinimui ir TSU identifikavimui.

4.6. Sertifikato atnaujinimas

Sertifikato atnaujinimas (naujo sertifikato išleidimas, nekeičiant viešojo rakto; angl. *Certificate renewal*) nėra vykdomas. Vietoje to yra taikomas sertifikato raktų pakeitimas (naujo sertifikato su nauju viešuoju raktu išleidimas; angl. *certificate re-key*).

4.7. Sertifikato raktų pakeitimas

Save pasirašančių šakninių CA sertifikatų ir TSU sertifikatų raktų pakeitimą (angl. *certificate re-key*) atlieka MitSoft TSA darbuotojai, panaudodami vidines procedūras, tenkinančias TSU raktų generavimo reikalavimus, apibrėžtus ETSI EN 319 421 [EN 319 421]. MitSoft TSA užtikrina, kad raktų poros generavimas ir sertifikatų išleidimas yra atliekamas patikimose rolėse esančių asmenų, esant bent dvigubai kontrolei.

Kriptografiniai algoritmai, raktų ilgiai ir kiti sertifikatų laukai yra aprašyti sertifikatų profiliuose (žiūrėti skyrelį 7.1. Sertifikatų profiliai).

4.7.1. Sertifikatų raktų pakeitimo aplinkybės

QTSS turi naudoti galiojančius TSU sertifikatus su privačiais raktais, kurių galiojimo laikotarpis nėra pasibaigęs, taigi, MitSoft TSA užtikrina reguliarų ir savalaikį TSU sertifikatų raktų pakeitimą. Papildomai, be reguliarių TSU sertifikatų raktų pakeitimų, TSU sertifikatų raktai yra keičiami, jei:

- duomenys TSU sertifikate neatitinka TSA teisinio statuso;
- kriptografiniai algoritmai, naudojami laiko žymų kūrimui, dėl MitSoft TSA verslo sprendimų, yra keičiami;
- TSU sertifikatų profilis buvo pakeistas dėl neatitikimo atnaujintų standartų, teisės aktų ar MitSoft QTSP verslo sprendimų reikalavimams;
- esant sertifikatų atšaukimui.

Šakninio CA sertifikato raktų pakeitimas yra atliekamas tik dėl atitinkamų raktų galiojimo pabaigos ar praradimo.

4.7.2. Kas gali prašyti naujų viešųjų raktų sertifikavimo

Sertifikatų raktų keitimas yra atliekamas tik MitSoft TSA prašymu.

4.7.3. Sertifikatų raktų pakeitimo užklausos vykdymas

Netaikoma.

4.7.4. Pranešimas abonentui apie naujo sertifikato išleidimą

Netaikoma.

4.7.5. Sertifikato su atnaujintais raktais priėmimas

Netaikoma.

4.7.6. Sertifikatų su atnaujintais raktais skelbimas CA

Naujai išteisti sertifikatai yra skelbiami MitSoft kataloge.

4.7.7. Pranešimas susijusioms šalims apie naujo sertifikato išleidimą

MitSoft TSA informuoja Lietuvos Respublikos Ryšių reguliavimo tarnybą, vykdančią kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų Nacionalinės priežiūros įstaigos funkcijas, apie TSU naujo sertifikato išleidimą MitSoft QTSS. MitSoft TSA prašo RRT inicijuoti naujo TSU sertifikato įtraukimo į Lietuvos patikimą sąrašą procedūrą.

4.8. Sertifikato keitimas

Sertifikato keitimas (naujo sertifikato su atnaujintais atributais išleidimas, nekeičiant viešojo rakto; angl. *certificate modification*) nėra atliekamas. Vietoje to yra taikomas sertifikato raktų pakeitimas (naujo sertifikato su nauju viešuoju raktu išleidimas; angl. *certificate re-key*).

4.9. Sertifikato atšaukimas ir sustabdymas

TSU sertifikato atšaukimas gali būti iššauktas tokiais netikėtais įvykiais, kaip TSU privataus rakto praradimas, ar teisėsaugos įstaigų pareigūnų oficialus kreipimasis. Bet

kuriuo atveju, aplinkybių tyrimą atliekamas ir atšaukimo procedūrą inicijuojama tik MitSoft vadovybės sprendimu.

Atšaukimą atlieka TSA darbuotojai, naudojant vidines procedūras.

Informacija apie atšauktą sertifikatą yra skelbia MitSoft svetainėje.

MitSoft kvalifikuotų laiko žymų paslaugų abonentai taip pat yra informuojami pagal abonentų kontaktinius duomenis, pateiktus TSA.

Papildomai, TSA informuoja Lietuvos Respublikos Ryšių reguliavimo tarnybą, vykdančią kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų Nacionalinės priežiūros įstaigos funkcijas apie TSU sertifikato atšaukimą. RRT gali naudoti savas, kitų pasikliaujančių šalių informavimo apie TSU sertifikato atšaukimą, procedūras.

TSU sertifikato pristabdymas nėra taikoms.

4.10. Paslaugos sertifikatų būsenai nustatyti

MitSoft TSA teikia CRL kaip sertifikato statuso paslaugą. Reguliarių CRL sąrašų publikavimo dažnumas yra ne retesnis kaip 24 val.

CRL yra publikuojami MitSoft kataloge ir yra viešai prieinami MitSoft TSA abonentams ir trečiosioms šalims.

Išleistų CRL laukai yra aprašyti CRL profilyje (žiūrėti skyrelį 7.2. CRL profiliai).

Sertifikatų galiojimo patikros protokolas (OCSP - *Online Certificate Status Protocol*) nėra palaikomas.

4.11. Prenumeratos pabaiga

Netaikoma.

4.12. Raktų saugojimas ir atstatymas

Šakninių CA sertifikatų ir TSU sertifikatų privačių raktų atsarginės kopijos nėra daromos. Šakninių CA sertifikatų ir TSU sertifikatų privačių raktų atstatymo procedūros nėra taikomos. Privataus rakto praradimo atveju:

- Nauja raktų pora ir nauji sertifikatai yra generuojami.
- Kol naujas TSU sertifikatas išleidžiamas ir RRT įtraukiamas į Patikimą sąrašą, kitas TSU bus naudotojams liko žymų paslaugų teikimui.

5. ĮRANGA, VALDYMAS IR VEIKIMO SAUGUMO PRIEMONĖS

MitSoft TSA naudoja tą pačią fizinio ir aplinkos saugumo įrangą, procedūrines ir personalo saugumo priemones, kokios taikomos kvalifikuotų laiko žymų paslaugų veikime ir valdyme.

5.1. Fizinio saugumo priemonės

Žiūrėti [QTSS PS] dokumento 7.8 skyrelį.

5.2. Procedūrinės saugumo priemonės

Žiūrėti [QTSS PS] dokumento 7.3 skyrelį.

5.3. Personalo saugumo priemonės

Žiūrėti [QTSS PS] dokumento 7.3 skyrelį.

5.4. Audito išsaugojimo procedūros

Žiūrėti [QTSS PS] dokumento 7.12 skyrelį.

Papildomai:

a) Įrašai, liečiantys visus įvykius, susijusius su CA sertifikatų ir jų raktų gyvavimo ciklu, yra išsaugomi.

b) Įrašai, liečiantys sertifikatų atšaukimo užklausas ir atliktų veiksmų ataskaitas, yra padaryti.

5.5. Įrašų archyvavimas

Žiūrėti [QTSS PS] dokumento 7.12 skyrelį.

5.6. Atnaujinto rakto perdavimas

Netaikoma.

5.7. Kompromitavimas ir atkūrimas nelaimės atveju

Žiūrėti [QTSS PS] dokumento 7.9 ir 7.13 skyrelius.

5.8. Sertifikavimo ar registravimo tarnybų užbaigimas

Žiūrėti [QTSS PS] dokumento 7.14 skyrelį.

Papildomai:

a) Šakninių CA sertifikatų privatūs raktai yra sunaikinami tokiu būdu, kad privatūs raktai nebegali būti atstatyti.

6. TECHNINĖS SAUGUMO PRIEMONĖS

6.1. Raktų poros generavimas ir diegimas

Raktų poros ir sertifikato generavimas yra atliekamas tiktai darbuotojų patikimose rolėse, esant bent dvigubai kontrolei, pagal MitSoft TSA vidines procedūras.

Privatūs raktai yra generuojami kriptografiniame modulyje, niekada nėra eksportuojami iš jo ir niekada nėra importuojami į jį.

CA ir TSU pasirašymo raktų ilgiai ir CA bei TSU pasirašymo raktų kriptografiniai algoritmai yra parenkami pagal standarto ETSI TS 119 312 [TS 119 312] rekomendacijas.

Panaudoti kriptografiniai algoritmai, raktų dydžiai, panaudojimo paskirtys, galiojimo laikotarpiai ir kiti sukurtų sertifikatų laukai bei išplėtimai yra aprašyti sertifikatų profiliuose (žiūrėti skyrelį 7.1. Sertifikatų profiliai).

6.2. Privačių raktų apsauga ir kriptografinio modulio inžinerinės apsaugos priemonės

Privatūs pasirašymo raktai yra laikomi ir naudojami kriptografiniame modulyje, kuris užtikrina EAL+ ir aukštesnį atitikties užtikrinimo lygį pagal standartą ISO/IEC 15408 [ISO 15408].

Tie patys apsaugos reikalavimai yra taikomi šakninio CA sertifikato privatiems raktams kaip ir TSU sertifikatų privatiems raktams, apibrėžtiems [QTSS PS] 7.6.3 skyrelyje.

6.3. Kiti raktų poros valdymo aspektai

Privataus rakto naudojimo laikotarpis yra taikomas TSU sertifikatų raktams. Privataus rakto naudojimo laikotarpio detalizavimas yra apibrėžtas sertifikato profilyje (žiūrėti skyrelį 7.1. Sertifikato profilis).

6.4. Aktyvavimo duomenys

Netaikoma.

6.5. Kompiuterio saugumo priemonės

Žiūrėti [QTSS PS] dokumento 7.5 skyrelį.

6.6. Techninės gyvavimo ciklo kontrolės priemonės

Žiūrėti [QTSS PS] dokumento 7.9 skyrelį.

7. SERTIFIKATŲ, CRL, IR OCSP PROFILIAI

7.1. Sertifikatų profiliai

7.1.1. Šakninio CA sertifikato profilis

Save pasirašantis šakninis CA sertifikatas yra naudojamas MitSoft TSA sertifikatų išleidimui. Šakninio CA sertifikato profilis apibrėžia X.509 3-ios versijos sertifikato struktūrą ir jis atitinka RFC 5280 [RFC 5280] ir ETSI EN 319 412-3 [EN 319 412-3].

7.1.1.1 Sertifikato laukai

Sertifikato laukai sertifikato profilyje yra pateikti Lentelėje 1.

Lentelė 1. Sertifikato laukai šakninio CA sertifikato profilyje.

Laukas	Privalomas	Aprašas	Galimos reikšmės
Versija (*Version*)	Taip	Aprašo užkoduoto sertifikato versiją	X.509 3-ios versijos sertifikatas (sveikoji reikšmė yra 2)
Serijinis numeris *(Serial Number*)	Taip	Tai yra teigiamas sveikas, priskirtas kiekvienam TSA sertifikatui	<Atsitiktinai sugeneruotas unikalus sertifikato numeris>
Leidėjo DN (*Issuer DN*)	Taip	Identifikuoja esybę, kuri pasirašė ir išleido sertifikatą	<Issuer distinguished name>[1]. DN turi šiuos atributus: • C (countryName), • O (organizationName), • 2.5.4.97 (organizationIdentifier), • CN (commonName). Pavyzdžiui, "CN=MitSoft QTSA TSU-1 Root, O=MitSoft, organizationIdentifier= NTRLT-120792080, C=LT"
Subjekto DN (*Subject DN*)	Taip	Identifikuoja esybę, susijusią su viešuoju raktu, išsaugotu subjekto viešojo rakto lauke	<Subject distinguished name>1. DN turi šiuos atributus: • C (countryName), • O (organizationName), • 2.5.4.97 (organizationIdentifier), • CN (commonName). Pavyzdžiui, "CN=MitSoft QTSA TSU-1 Root, O=MitSoft, organizationIdentifier= NTRLT-120792080, C=LT"
Sertifikato galiojimo laikotarpio pradžia (*Not Before*)	Taip	Sertifikato galiojimo laikotarpio pradžia. Sertifikato galiojimo laikotarpis yra laiko intervalas, kurio metu TSA garantuoja, kad ji palaikys informaciją apie sertifikato statusą.	<Data su laiku, užkoduotu pagal UTCTime>

[1] DN turi būti suderinamas su ETSI EN 319 412-3 [EN 319 412-3].

Sertifikato galiojimo laikotarpio pabaiga (*Not After*)	Taip	Sertifikato galiojimo laikotarpio pabaiga. Sertifikato galiojimo laikotarpis yra laiko intervalas, kurio metu TSA garantuoja, kad ji palaikys informaciją apie sertifikato statusą.	< Data su laiku, užkoduotu pagal UTCTime>
Parašo algoritmas (*Signature Algorithm*)	Taip	Nurodo algoritmo identifikatorių, kurį TSA panaudojo sertifikato pasirašymui.	ecdsa-with-SHA512[2] (OID: 1.2.840.10045.4.3.4)
Subjekto viešasis raktas (*Subject Public Key*)	Taip	Yra naudojamas nurodyti viešąjį raktą ir algoritmą, su kuriuo naudojamas raktas, identifikavimui.	ECC viešasis raktas[2] (OID: 1.2.840.10045.2.1) su P-521 elipsine kreive (*elliptic curve*)[3] (OID: 1.3.132.0.35)
Parašo reikšmė (*Signature Value*)	Taip	Nurodo skaitmeninį parašą, apskaičiuotą su ASN.1 DER kuduote tbsCertificate laukui	

7.1.1.2 Sertifikato plėtiniai

Sertifikato plėtiniai sertifikato profilyje yra pateikti Lentelėje 2.

Lentelė 2. Sertifikato plėtiniai šakniniame CA sertifikate.

Plėtinys	Privalomas	Kritinis	Aprašas	Galimos reikšmės
Subjekto rakto identifikatorius (*Subject Key Identifier*) (2.5.29.14)	Taip	Ne	Pateikia sertifikato, turinčio konkretų viešąjį raktą, identifikavimo priemones	<subjekto viešojo rakto SHA-1 santrauka>
Baziniai ribojimai (*Basic Constraints*) (2.5.29.19)	Taip	Taip	Identifikuoja ar sertifikato subjektas yra CA ir maksimalų leistino sertifikavimo kelio, apimančio sertifikatą, gylį	cA: TRUE; pathLenConstraint: 0
Rakto naudojimas (*Key Usage*) (2.5.29.15)	Taip	Taip	Apibrėžia sertifikate esančio rakto paskirtį	keyCertSign (5), cRLSign (6)

[2] Nuorodos į algoritmo aprašus yra pateiktos ETSI TS 119 312 [TS 119 312].
[3] Elipsinės kreivės yra apibrėžtos RFC 5480 [RFC 5480].

7.1.2. TSU sertifikato profilis

Šis profilis apibrėžia MitSoft TSA kvalifikuotų laiko žymų pasirašymo sertifikato vidinę struktūrą. TSU sertifikatas yra naudojamas tik kvalifikuotų laiko žymų pasirašymui. TSU sertifikato profilis apibrėžia X.509 3-ios versijos sertifikato struktūrą ir jis yra suderinamas su RFC 5280 [RFC 5280] ir ETSI EN 319 412-3 [EN 319 412-3].

TSU sertifikato profilis atitinka reikalavimus, apibrėžtus ETSI EN 319 422 [EN 319 422].

7.1.2.1 Sertifikato laukai

Sertifikato laukai TSU sertifikato profilyje yra pateikti Lentelėje 3.

Lentelė 3. Sertifikato laukai TSU sertifikato profilyje.

Laukas	Privalomas	Aprašas	Galimos reikšmės
Versija (*Version*)	Taip	Aprašo užkoduoto sertifikato versiją	X.509 3-ios versijos sertifikatas (sveikoji reikšmė yra 2)
Serijinis numeris (*Serial Number*)	Taip	Tai yra teigiamas sveikas, priskirtas kiekvienam TSA sertifikatui	<Atsitiktinai sugeneruotas unikalus sertifikato numeris>
Leidėjo DN (*Issuer DN*)	Taip	Identifikuoja esybę, kuri pasirašė ir išleido sertifikatą	<Issuer distinguished name>[4]. DN turi šiuos atributus: • C (countryName), • O (organizationName), • 2.5.4.97 (organizationIdentifier), • CN (commonName). Pavyzdžiui, "CN=MitSoft QTSA TSU-1 Root, O=MitSoft, organizationIdentifier= NTRLT-120792080, C=LT"
Subjekto DN (*Subject DN*)	Taip	Identifikuoja esybę, susijusią su viešuoju raktu, išsaugotu subjekto viešojo rakto lauke	<Subject distinguished name>[4]. DN turi šiuos atributus: • C (countryName), • O (organizationName), • 2.5.4.97 (organizationIdentifier), • CN (commonName). Pavyzdžiui, "CN=MitSoft QTSA TSU-1 Root, O=MitSoft, organizationIdentifier= NTRLT-120792080, C=LT"
Sertifikato galiojimo laikotarpio pradžia (*Not Before*)	Taip	Sertifikato galiojimo laikotarpio pradžia. Sertifikato galiojimo laikotarpis yra laiko intervalas, kurio metu TSA garantuoja, kad ji palaikys informaciją apie sertifikato statusą.	<Data su laiku, užkoduotu pagal UTCTime>

[4] DN turi būti suderinamas su ETSI EN 319 412-3 [EN 319 412-3].

Sertifikato galiojimo laikotarpio pabaiga (*Not After*)	Taip	Sertifikato galiojimo laikotarpio pabaiga. Sertifikato galiojimo laikotarpis yra laiko intervalas, kurio metu TSA garantuoja, kad ji palaikys informaciją apie sertifikato statusą.	< Data su laiku, užkoduotu pagal UTCTime>. Not After = Not Before + 2740 dienos
Parašo algoritmas (*Signature Algorithm*)	Taip	Nurodo algoritmo identifikatorių, kurį TSA panaudojo sertifikato pasirašymui.	ecdsa-with-SHA512[5] (OID: 1.2.840.10045.4.3.4)
Subjekto viešasis raktas (*Subject Public Key*)	Taip	Yra naudojamas nurodyti viešąjį raktą ir algoritmą, su kuriuo naudojamas raktas, identifikavimui.	ECC viešasis raktas (OID: 1.2.840.10045.2.1) su P-384 elipsine kreive (*elliptic curve*)[6] (OID: 1.3.132.0.34)
Parašo reikšmė (*Signature Value*)	Taip	Nurodo skaitmeninį parašą, apskaičiuotą su ASN.1 DER koduote tbsCertificate laukui	

7.1.2.2 Sertifikato plėtiniai

Sertifikato plėtiniai TSU sertifikato profiliui yra pateikti Lentelėje 4.

Lentelė 4. Sertifikatų plėtiniai TSU sertifikato profilyje.

Plėtinys	Privalomas	Kritinis	Aprašas	Galimos reikšmės
Tarnybos rakto identifikatorius (Authority Key Identifier) (2.5.29.35)	Ne	Ne	Pateikia viešojo rakto, atitinkančio privačiam raktui, naudojamam pasirašyti sertifikatą, identifikavimo priemones	<leidėjo viešojo rakto SHA-1 santrauka>
Subjekto rakto identifikatorius (*Subject Key Identifier*) (2.5.29.14)	Taip	Ne	Pateikia sertifikato, turinčio konkretų viešąjį raktą, identifikavimo priemones	<subjekto viešojo rakto SHA-1 santrauka>
Baziniai ribojimai (*Basic Constraints*) (2.5.29.19)	Ne	Taip	Identifikuoja, ar sertifikato subjektas yra CA ir maksimalų leistino sertifikavimo kelio, apimančio sertifikatą, gylį.	cA: FALSE; pathLenConstraint: None
Rakto naudojimas (*Key Usage*) (2.5.29.15)	Taip	Taip	Apibrėžia sertifikate esančio rakto paskirtį	digitalSignature (0)

[5] Nuorodos į algoritmo aprašus yra pateiktos ETSI TS 119 312 [TS 119 312].
[6] Elipsinės kreivės yra apibrėžtos RFC 5480 [RFC 5480].

Išplėstinis raktų naudojimas (*Extended Key Usage*) (2.5.29.37)	Taip	Taip	Nurodo vieną ar daugiau paskirčių, kurioms sertifikato viešas raktas gali būti naudojamas papildomai ar vietoje pagrindinių paskirčių, nurodytų rakto naudojimo išplėtime	id-kp-timeStamping (1.3.6.1.5.5.7.3.8)
Sertifikatų taisyklės (*Certificate Policies*) (2.5.29.32)	Taip	Ne	Turi seką iš vienos ar daugiau taisyklių, kurių kiekviena susideda iš objekto identifikatoriaus (OID) ir papildomų kvalifikatorių	Certificate policyIdentifier: 1.3.6.1.4.1.57890.1.2.1, CPS kvalifikatorius (id-qt-cps): <URL, kuris rodo į šį CPS dokumentą>
CRL teikimo vietos (*CRL Distribution Points*) (2.5.29.31)	Taip	Ne	Identifikuoja, kaip yra gaunama CRL informacija	DistributionPointName: <URL, kuris rodo į CRL, įtraukiantį sertifikatus pagal visas atšaukimo priežastis>
Prieiga prie tarnybos informacijos (*Authority Information Access*) (1.3.6.1.5.5.7.1.1)	Taip	Ne	Nurodo, kaip pasiekti sertifikato, kuriame yra šis plėtinys, leidėjo informaciją ir paslaugas	accessMethod: caIssuers (1.3.6.1.5.5.7.48.2), accessLocation: <URL, kuris rodo į leidėjo sertifikatą>
Privataus rakto naudojimo laikotarpis (*Private Key Usage Period*) (2.5.29.16)	Taip	Ne	Naudojamas riboti TSU pasirašymo rakto galiojimo laikotarpį	notBefore: <TSU pasirašymo rakto naudojimo pradžia>; notAfter: <TSU pasirašymo rakto naudojimo pabaiga>. notAfter = notBefore + 3 metai

7.2. CRL profiliai

7.2.1. TSU sertifikatų CRL profiliai

MitSoft TSU sertifikatų CRL sąrašai yra išleidžiami pagal RFC 5280 [RFC 5280].

7.2.1.1 CRL laukai

TSU sertifikatų CRL profilio CRL laukai yra pateikti Lentelėje 5.

Lentelė 5. TSU sertifikatų CRL profilio laukai.

Laukas	Privalomas	Aprašas	Galimos reikšmės
Versija (*Version*)	Taip	Aprašo užkoduoto CRL versiją	2 versiojos CRL (sveikoji reikšmė yra 1)
Parašo algoritmas (*Signature Algorithm*)	Taip	Nurodo algoritmo, kurį panaudojo CRL leidėjas CertificateList pasirašymui, identifikatorių	ecdsa-with-SHA512[7] (OID: 1.2.840.10045.4.3.4)
Leidėjo vardas (*Issuer Name*)	Taip	Identifikuoja esybę, kuri pasirašė ir išleido CRL	<Issuer distinguished name>[8]. DN turi šiuos atributus: • C (countryName), • O (organizationName), • 2.5.4.97 (organizationIdentifier), • CN (commonName). Pavyzdžiui, "CN=MitSoft QTSA TSU-1 Root, O=MitSoft, organizationIdentifier= NTRLT-120792080, C=LT"
Šio atnaujinimo data (*This Update*)	Taip	Nurodo šio CRL išleidimo datą	< Data su laiku, užkoduotu pagal UTCTime >
Sekančio atnaujinimo data (*Next Update*)	Taip	Nurodo datą, iki kurios bus išleistas sekantis CRL	< Data su laiku, užkoduotu pagal UTCTime>
Parašo reikšmė (*Signature Value*)	Taip	Nurodo skaitmeninį parašą, apskaičiuotą su ASN.1 DER koduote tbsCertList laukui	
Atšaukti sertifikatai (*Revoked Certificates*)	Ne	Atšauktų sertifikatų ir jų serijinių numerių sąrašas, jeigu yra atšauktų sertifikatų	<Atšauktų sertifikatų sąrašas> Kiekvienam atšauktam sertifikatui turėtų būti pateikti šie duomenys: • Sertifikato serijinis numeris, • Atšaukimo data, • Atšaukimo priežasties kodas pagal RFC 5280

[7] Nuorodos į algoritmo aprašus yra pateiktos ETSI TS 119 312 [TS 119 312].
[8] DN turėtų atitikti ETSI EN 319 412-3 [EN 319 412-3].

7.2.1.2 CRL plėtiniai

TSU sertifikatų CRL profilio CRL plėtiniai yra pateikti Lentelėje 6.

Lentelė 6. TSU sertifikatų CRL profilio CRL plėtiniai

Plėtinys	Privalomas	Kritinis	Aprašas	Galimos reikšmės
Tarnybos rakto identifikatorius (*Authority Key Identifier*) (2.5.29.35)	Taip	Ne	Pateikia viešojo rakto, atitinkančio privačiam raktui, kuriuo pasirašytas CRL, identifikavimo priemones	<CRL leidėjo sertifikato subjekto rakto identifikatorius>
CRL numeris (*CRL Number*) (2.5.29.20)	Taip	Ne	Turi CRL leidėjo duotai CRL apimčiai monotoniškai didėjančios sekos numerį	<CRL eilinis numeris>
Išleistų CRL platinimo vieta (*CRL Distribution Points*) (2.5.29.28)	Taip	Taip	Identifikuoja CRL platinimo vietą ir konkretaus CRL taikymo sritį, nurodo ar CRL apima atšaukimo informaciją tik apie galutinius naudotojų sertifikatus, tik apie TSA sertifikatus, tik apie atributinius sertifikatus, ar tik apie sertifikatus atšauktus pagal priežastis iš ribotos priežasčių kodų aibės	distributionPoint: <URL, kuris rodo į CRL, padengiantį dėl visų priežasčių atšautus sertifikatus>; onlyContainsUserCerts: False; onlyContainsCACerts: False; indirectCRL: False; onlyContainsAttributeCerts: False; onlySomeReasons: not-used
Pasibaigusio galiojimo sertifikatai CRL'e (*ExpiredCertsOnCRL*) (2.5.29.60)	Taip	Ne	Nurodo, kad CRL, turintis šį plėtinį, turės pasibaigusio galiojimo sertifikato atšaukimo statuso informaciją	<CRL leidėjo sertifikato galiojimo pradžia>

7.3. OCSP profiliai

Netaikoma.