mitsoft

Kvalifikuotos ilgalaikės apsaugos paslaugos

Apsaugos paslaugų veiklos nuostatai

QLPS/PS-LT

Unikalus objekto ID (OID): **1.3.6.1.4.1.57890.1.4.1**

Versija 1.30

Galioja nuo 2026-09-01

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

Patvirtinimai

Versijų istorija

Versija	Galioja nuo	Aprašas
1.00		Pirma oficiali dokumento versija auditui
1.10		Patikslinta pagal pastabas
1.11		Ištaisytos smulkios formulavimo klaidos, lyginant EN ir LT variantus
1.12	2023-05-15	Leidžiami CMS parašai PDF dokumente; išaiškinimas dėl skaitmeninių parašų, kurie nėra galiojantys, ilgalaikės apsaugos
1.20	2024-10-01	Visoms kvalifikuotoms patikimumo užtikrinimo paslaugoms bendros praktikos perkeltos į atskirą dokumentą
1.30	2026-09-01	Atnaujintas pagal naujus reikalavimus

Dokumento patvirtinimas

	Vardas Pavardė	Data	Parašas
Peržiūrėjo	Arūnas Stočkus	2026-07-20	
Patvirtino	Antanas Mitašiūnas	2026-07-20	

Turinys

1. ĮVADAS 5
1.1. Apžvalga 5
1.2. Identifikacija 6
1.3. Apsaugos paslaugų naudotojai ir taikymo sritis 6
1.4. Atitiktis. Validavimas ir patikrinimas 6
1.5. Kontaktiniai duomenys 7
2. Nuorodos 8
3. Sąvokų ir santrumpų apibrėžimas 9
4. MitSoft PSP: Bendrosios sąvokos 12
4.1. Apsaugos paslaugų funkciniai tikslai 12
4.2. Apsaugos saugyklų modeliai 12
4.2.1. Apsaugos paslauga su saugykla (WST) 13
4.2.1.1 Architektūra 13
4.2.1.2 MitSoft apsaugos paslaugų darbų seka 13
4.2.2. Apsaugos paslauga be saugyklos (WOS) 15
4.2.2.1 Architektūra 15
4.2.2.2 MitSoft apsaugos paslaugų darbų seka 16
5. Rizikos vertinimas 18
6. TAISYKLĖS IR PRAKTIKOS 19
6.1. Apsaugos paslaugų veiklos nuostatai 19
6.1.1. PSP įsipareigojimai 20
6.2. Paslaugų teikimo sąlygos 21
6.3. Informacijos saugumo taisyklės 21
6.4. Apsaugos profilis 21
6.5. Apsaugos įrodymų taisyklės 21
6.6. Parašo validavimo taisyklės 22
6.7. Abonentinė sutartis 22
7. PSP VALDYMAS IR VEIKIMAS 23
7.1. Vidinė organizacija 23
7.2. Žmogiškieji ištekliai 23
7.3. Turto valdymas 23
7.4. Prieigos kontrolė 23
7.5. Kriptografinis valdymas 23
7.6. Fizinis ir aplinkos saugumas 23
7.7. Veiklos saugumas 23
7.8. Tinklo saugumas 23
7.9. Incidentų valdymas 23

7.10. Įrodymų surinkimas 24
7.11. Veiklos tęstinumo valdymas 24
7.12. PSP veiklos užbaigimas ir užbaigimo planai 24
7.13. Atitiktis 24
7.14. Kriptografijos stebėsena 24
7.15. Apsaugos įrodymų papildymas 26
7.16. Eksporto-importo paketas 26
7.17. Tiekimo grandinė 27
8. Veiklos ir pranešimų protokolai 28
8.1. Apsaugos protokolas 28
8.2. Pranešimų protokolas 29
9. Apsaugos procesas 30
9.1. Apsaugos duomenų ir įrodymų saugojimas 30
9.2. Apsaugos įrodymai 30
9.3. Skaitmeninių parašų apsauga 30
A priedas (norminis). Kvalifikuota apsaugos paslauga kvalifikuotiems elektroniniams parašams (QES), kaip apibrėžta Reglamento (ES) Nr. 910/2014 34 straipsnyje 32

1. ĮVADAS

Uždaroji akcinė bendrovė "MIT-SOFT" (toliau –MitSoft) įsteigta 1991 m. rugpjūčio 1 d. ir nuo 1996 m. dirba elektroninių dokumentų, turinčių tokią pat teisinę galią kaip ranka pasirašyti dokumentai popieriuje, sudarymo 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 TS 119 511 "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers providing long-term preservation of digital signatures or general data using digital signature techniques" specifikuoja kvalifikuotų elektroninių parašų ir elektroninių spaudų galiojimo statuso apsaugos kvalifikuotų paslaugų taisykles: (OID: 0.4.0.19511.1.2). Šiose taisyklėse specifikuoti reikalavimai nėra orientuoti nei į konkrečius technologinius sprendimus, nei į apsaugos paslaugų teikėjo (*angl. Preservation Service Provider - PSP*) organizacinę struktūrą. Taisyklių 0.4.0.19511.1.2 reikalavimų įgyvendinimo techniniai sprendimai, procedūros ir darbuotojų tvarkos yra aprašyti šiuose MitSoft Kvalifikuotų ilgalaikės apsaugos paslaugų veiklos nuostatuose (toliau – sutrumpintai QLPS PS: *angl. Qualified Long-term Preservation Service Practice Statement*).

Veiklos nuostatai remiasi 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) 2025 m. rugsėjo 29 d. Komisijos įgyvendinimo reglamentu (ES) 2025/1946, kuriuo dėl kvalifikuotų elektroninių parašų ir kvalifikuotų elektroninių spaudų kvalifikuotų ilgalaikio išsaugojimo paslaugų nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 taikymo taisyklės;

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

d) Standartu ETSI TS 119 511: "Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers providing long-term preservation of digital signatures or general data using digital signature techniques";

e) Standartu ETSI TS 119 512: "Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services";

f) Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymu, 2018 m. balandžio 26 d. Nr. XIII-1120;

g) Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2026 m. birželio 23 d. nutarimu Nr. TN-276 „Dėl Kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo statuso suteikimo ir kai kurių veiklos reikalavimų vykdymo tvarkos aprašo patvirtinimo".

Teikiant ilgalaikės apsaugos paslaugas, MitSoft PSP vykdo apsaugos objektų stebėseną ir papildymą *(angl. augmentation)*.

Pastaba dėl sutrumpinimų apibrėžimų. Kvalifikuotų apsaugos paslaugų taisyklės (*angl. Qualified Preservation Service Policy - QPSP*) reiškia taisykles 0.4.0.19511.1.2. Čia apsaugos paslaugos (*angl. Preservation Service - PS*) reiškia MitSoft kvalifikuotas ilgalaikės apsaugos paslaugas, PSP reiškia MitSoft PSP; QLPS PS reiškia MitSoft QLPS PS, ir taip toliau, t.y. viskas, kas yra sakoma, taikoma tik MitSoft PSP.

1.2. Identifikacija

QLPS PS unikalus identifikatorius (OID) yra 1.3.6.1.4.1.57890.1.4.1; Identifikatoriaus laukų reikšmės yra pateiktos 1 lentelėje.

1 lentelė. QLPS PS OID 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 ilgalaikės apsaugos paslaugų veiklos nuostatai	4
Dokumento versija	1

QLPS PS aktuali versija yra prieinama MitSoft PSP interneto svetainėje.

1.3. Apsaugos paslaugų naudotojai ir taikymo sritis

Kvalifikuotos ilgalaikės apsaugos paslaugos įgalina pratęsti elektroninių parašų ir spaudų galiojimo statusą per ilgą laikotarpį, nepaisant kriptografinių technologijų, tokių kaip: kriptografiniai algoritmai, raktų ilgiai ar santraukų funkcijos senėjimo, raktų kompromitavimo ar nesant galimybės patikrinti viešųjų raktų sertifikatų galiojimo statusą. MitSoft PSP ilgalaikės apsaugos paslaugų naudotojais gali būti juridiniai ir fiziniai asmenys, kuriems reikalingos PSP teikiamos ilgalaikės apsaugos paslaugos.

Nei QPSP, nei QLPS PS neuždeda jokių ribojimų šių Kvalifikuotų ilgalaikės apsaugos paslaugų naudojimui. Apsaugos paslaugos gali būti naudojamos, kai dokumentų savininkas nenori pats rūpintis elektroninių parašų ir spaudų galiojimo statusu ir deleguoja tai PSP.

PSP teikia viešas paslaugas, tačiau paslaugos gali būti naudojamos ir uždarose naudotojų grupėse.

1.4. Atitiktis. Validavimas ir patikrinimas

PSP patvirtina, kad MitSoft apsaugos paslaugos yra ES eIDAS kvalifikuotos elektroninių parašų ir elektroninių spaudų apsaugos paslaugos ir pagal apibrėžtus apsaugos profilius atitinka reikalavimus šiems QPSP saugyklų modeliams: su saugykla WST *(angl. With STorage – WST)* ir be saugyklos WOS *(angl. WithOut Storage - WOS)*,

bei skaitmeninių parašų apsaugos tikslui PDS *(angl. Preservation Digital Signatures – PDS)* ir QPSP veikloms.

MitSoft PSP veiklos atitiktis QPSP ir QLPS PS reikalavimams yra tikrinama ne rečiau kaip kas du metai.

1.5. Kontaktiniai duomenys

Veiklos nuostatus prižiūri uždaroji akcinė bendrovė "MIT-SOFT", kurios kontaktiniai duomenys yra pateikti 2 lentelėje.

2 lentelė. MitSoft PSP kontaktiniai duomenys

PSP:	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.

[CIR2025/1946] – Commission implementing Regulation (EU) 2025/1946 of 29 September 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards qualified preservation services.

[ENISA] – Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA.

[EN 319 102-1] – ETSI EN 319 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.

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

[EN 319 422] – ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.

[ISO 27002] – ISO/IEC 27002:2013: "Information technology – Security techniques – Code of practice for information security management".

[ISO 27005] – ISO/IEC 27005:2011: "Information technology – Security techniques – Information security risk management".

[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 Trust Infrastructures (ESI); Cryptographic Suites" standard.

[TS 119 511] – ETSI TS 119 511: "Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers providing long-term preservation of digital signatures or general data using digital signature techniques".

[TS 119 512] – ETSI TS 119 512: "Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services".

[QTS PS] - MitSoft „Kvalifikuotų patikimumo užtikrinimo paslaugų veiklos nuostatai".

3. Sąvokų ir santrumpų apibrėžimas

Abonentas: juridinis ar fizinis asmuo, turintis sutartinius abonento įsipareigojimus su apsaugos patikimų paslaugų teikėju.

Apsaugos interfeisas: programinės įrangos komponentė, apsaugos paslaugos pusėje įgyvendinanti apsaugos protokolą.

Apsaugos įrodymas: apsaugos paslaugos sudarytas įrodymas, kuris gali būti panaudotas pademonstruoti, kad vienas ar daugiau apsaugos tikslų duotam apsaugos objektui yra pasiekti.

Apsaugos įrodymų taisyklės: taisyklių aibė, kuri specifikuoja reikalavimus ir vidinius procesus, skirtus generuoti ar nurodyti kaip validuoti apsaugos įrodymus.

Apsaugos klientas: programinės įrangos komponentė ar dalis, kurį sąveikauja su apsaugos paslauga apsaugos protokolu.

Apsaugos laikotarpis: apsaugos paslaugai su saugykla – laikotarpis, per kurį apsaugos paslauga apsaugo pateiktus apsaugos objektus ir susijusius įrodymus.

Apsaugos manifestas: apsaugos objekto konteineryje duomenų objektas, kuris nurodo apsaugos duomenų objektus ar papildomus duomenis ir metaduomenis apsaugos objekto konteineryje.

Apsaugos objektas: tipizuotas duomenų objektas, apsaugos paslaugos sistemai pateiktas, joje apdorotas ar iš jos paimtas.

Apsaugos objekto konteineris: konteineris, kuris apima duomenų objektų rinkinį ir galimai susijusius metaduomenis, pateikdamas informaciją apie duomenų objektus ir galimai apsaugos manifestą, specifikuojantį jų turinį ir sąryšius.

Apsaugos paslauga: paslauga, gebanti pratęsti skaitmeninių parašų galiojimo statusą ir/ar pateikti duomenų egzistavimo įrodymus per ilgą laikotarpį.

Apsaugos paslaugų taisyklės: patikimų paslaugų taisyklės apsaugos paslaugoms.

Apsaugos paslaugų teikėjas: patikimų paslaugų teikėjas, teikiantis apsaugos paslaugas.

Apsaugos paslaugų veiklos nuostatai: patikimų paslaugų veiklos nuostatai apsaugos paslaugoms.

Apsaugos profilis: unikaliai identifikuota įgyvendinimo detalių aibė, tinkanti apsaugos saugyklos modeliui ir vienam ar daugiau apsaugos tikslų, kurie specifikuoja, kaip apsaugos įrodymai yra generuojami ir validuojami.

Apsaugos protokolas: protokolas komunikuoti tarp apsaugos paslaugos ir apsaugos kliento.

Apsaugos saugyklos modelis: vienas iš šių apsaugos paslaugos įgyvendinimo būdų: su saugykla, su laikina saugykla, be saugyklos.

Apsaugos schema: bendrinė procedūrų ir taisyklių aibė, tinkanti apsaugos saugyklos modeliui ir vienam ar daugiau apsaugos tikslų, kurie apibūdina, kaip apsaugos įrodymai yra generuojami ir validuojami.

Apsaugos tikslas: vienas iš šių tikslų, pasiektas per apsaugos laikotarpį: skaitmeninių parašų galiojimo statuso pratęsimas per ilgą laikotarpį, duomenų egzistavimo įrodymų pateikimo pratęsimas per ilgą laikotarpį ar iš išorės pateiktų apsaugos įrodymų papildymas.

Archyvinė laiko žyma: ArchiveTimeStamp XAdES parašams, archive-time-stamp CAdES parašams, ar DocumentTimeStamp PAdES parašams.

Duomenų objektas: dvejetainiai / aštuntainiai duomenys, kuriuos programa apdoroja (pvz., transformuoja, skaičiuoja santrauką arba pasirašo) ir kurie gali būti susieti su papildoma informacija, pvz., identifikatoriumi, kodavimu, dydžiu ar tipu.

Egzistavimo įrodymas: įrodymas, kad objektas egzistavo specifiniu momentu (data/laikas).

Eksporto-importo paketas: iš apsaugos paslaugų gauti duomenys, apimantys pateikimo duomenų objektus (SubDO), apsaugos įrodymus ir su apsauga susijusius metaduomenis, kurie leidžia kitai apsaugos paslaugai importuoti šiuos duomenis tam, kad pratęstų šių duomenų apsaugos tikslo pasiekimą.

ES kvalifikuota apsaugos paslauga: apsaugos paslauga, kuri tenkina kvalifikuotų elektroninių parašų ir/ar kvalifikuotų elektroninių spaudų kvalifikuotų apsaugos paslaugų reikalavimus, nustatytus ES eIDAS Reglamente 910/2014 [eIDAS].

ES kvalifikuota laiko žymų tarnyba: kvalifikuotas laiko žymų paslaugų teikėjas, sudarantis kvalifikuotas elektronines laiko žymas, kaip tai nustatyta ES eIDAS Reglamente 910/2014 [eIDAS].

Ilgalaikė apsauga: skaitmeninių parašų galiojimo statuso pratęsimas per ilgą laikotarpį ir/ar duomenų egzistavimo įrodymų pateikimo pratęsimas per ilgą laikotarpį, nepaisant kriptografinių technologijų, tokių kaip kriptografiniai algoritmai, raktų ilgiai ar santraukų funkcijos, senėjimas, raktų kompromitavimas ar galimybės patikrinti viešųjų raktų sertifikatų galiojimo statusą praradimas.

Ilgalaikis: laikotarpis, kurio eigoje gali įvykti technologiniai pokyčiai.

Katalogas (repozitorius): vieta internete, kurioje ilgalaikės apsaugos paslaugos informacija yra prieinama naudotojams.

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]).

Metaduomenys: duomenys apie kitus duomenis.

Numatoma įrodymų trukmė: trukmė, kurią apsaugos paslauga tikisi, kad apsaugos įrodymai gali būti naudojami apsaugos tikslui pasiekti, apsaugos paslaugų su laikina saugykla ar be saugyklos atvejais.

Pasirašantis asmuo: esybė, kuri yra skaitmeninio parašo sudarytoja.

Pateikimo duomenų objektas (SubDO): kliento pateiktas originalus duomenų objektas.

Patikimas sąrašas: sąrašas, kuris pateikia informaciją apie patikimų paslaugų teikėjų patikimų paslaugų statusą ir statuso istoriją dėl atitikties taikomiems reikalavimams ir atitinkantis galiojančių teisės aktų nuostatas.

Pranešimų protokolas: protokolas, kurį naudoja apsaugos paslauga informuoti apsaugos klientą.

Sukompromitavimas: praradimas, vagystė, pakeitimas, neteisėtas naudojimas, ar kitoks konfidencialių duomenų saugumo pažeidimas.

Validavimo duomenys: duomenys, kurie yra naudojami skaitmeninių parašų validavimui.

ETSI – Europos Telekomunikacijų Standartų Institutas (*European Telecommunications Standardization Institute*)

OID – Objekto identifikatorius (*Object IDentifier*)

PS – Veiklos nuostatai (*Practice Statement*)

PSP – Apsaugos paslaugų teikėjas (*Preservation Service Provider*)

POC – Apsaugos objekto konteineris (*Preservation Object Container*)

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

QPSP – Kvalifikuotų apsaugos paslaugų taisyklės 0.4.0.19511.1.2 (*Qualified Preservation Service Policy*)

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*)

SubDO – Pateikimo duomenų objektas (*Submission Data Object*)

4. MitSoft PSP: Bendrosios sąvokos

4.1. Apsaugos paslaugų funkciniai tikslai

Kvalifikuotos ilgalaikės apsaugos paslaugos apibrėžimos standarte ETSI TS 119 511 numato tris apsaugos paslaugos funkcinius tikslus: skaitmeninių parašų apsauga (*angl. Preservation of Digital Signatures – PDS*), bendrųjų duomenų apsauga (*angl. Preservation of General Data - PGD*), pateiktų apsaugos įrodymų papildymas *(angl. AUGmentation of submitted preservation evidences - AUG)*. Bet kuri šių funkcinių tikslų kombinacija gali būti įgyvendinta konkrečioje apsaugos paslaugoje.

MitSoft PSP įgyvendina funkcinį tikslą PDS – skaitmeninių parašų apsaugą šių formatų (specifikacijų) elektroniniuose dokumentuose/konteineriuose: ADOC-V1.0, ADOC-V2.0, EGAS-V1.0, MDOC-V1.0, PDF-LT-V1.0, PDF-RC-V1.0, ASiC-E pagal ETSI TS 103174, ASiC-E pagal ETSI EN 319162-1, ASiC-S pagal ETSI TS 103174, ASiC-S pagal ETSI EN 319162-1, PDF su PAdES parašais pagal ETSI TS 103172, PDF su PAdES parašais pagal ETSI EN 319142-1, PDF su CMS parašais.

Apsaugos paslaugos ilgą laiką išsaugo kvalifikuotų elektroninių parašų ir kvalifikuotų elektroninių spaudų galiojimo statusą. Apsaugos paslaugos ilgą laiką išsaugo pažangių elektroninių parašų ir pažangių elektroninių spaudų, kurie nėra kvalifikuoti, galiojimo statusą tik tuo atveju, jei toks reikalavimas yra nurodytas Abonentinėje sutartyje. Toliau šiame dokumente tokie parašai yra vadinami elektroniniais parašais ar spaudais, ar tiesiog skaitmeniniais parašais.

Apsaugos paslaugos ilgą laiką išsaugo galiojančių elektroninių parašų ir galiojančių elektroninių spaudų galiojimo statusą. Apsaugos paslaugos ilgą laiką išsaugo elektroninių parašų ir elektroninių spaudų, kurie nėra galiojantys, galiojimo statusą tik tuo atveju, jei toks reikalavimas yra nurodytas Abonentinėje sutartyje ir tai leidžia parašo taisyklės.

4.2. Apsaugos saugyklų modeliai

Kvalifikuotos ilgalaikės apsaugos paslaugos apibrėžimos standarte ETSI TS 119 511 numato tris apsaugos saugyklos modelius: apsaugos paslauga su saugykla (*angl.* With STorage - WST), apsaugos paslauga su laikina saugykla (*angl. With Temporary Storage - WTS*) ir apsaugos paslauga be saugyklos (*angl.* WithOut Storage - WOS).

Apsaugos procesas apima abi puses: apsaugos klientą (naudotoją) ir apsaugos paslaugų teikėją. Pareigų pasiskirstymas tarp apsaugos kliento ir apsaugos paslaugų teikėjo priklauso nuo taikomo apsaugos paslaugų saugyklos modelio.

Apsaugos saugyklos modelis WST leidžia apsaugos paslaugų maksimalią apimtį, pateikiamą paslaugų teikėjo, ir minimalią – apsaugos kliento, ir priešingai, apsaugos saugyklos modelis WOS maksimaliai riboja apsaugos paslaugų teikėjo dalyvavimą bendrame apsaugos procese.

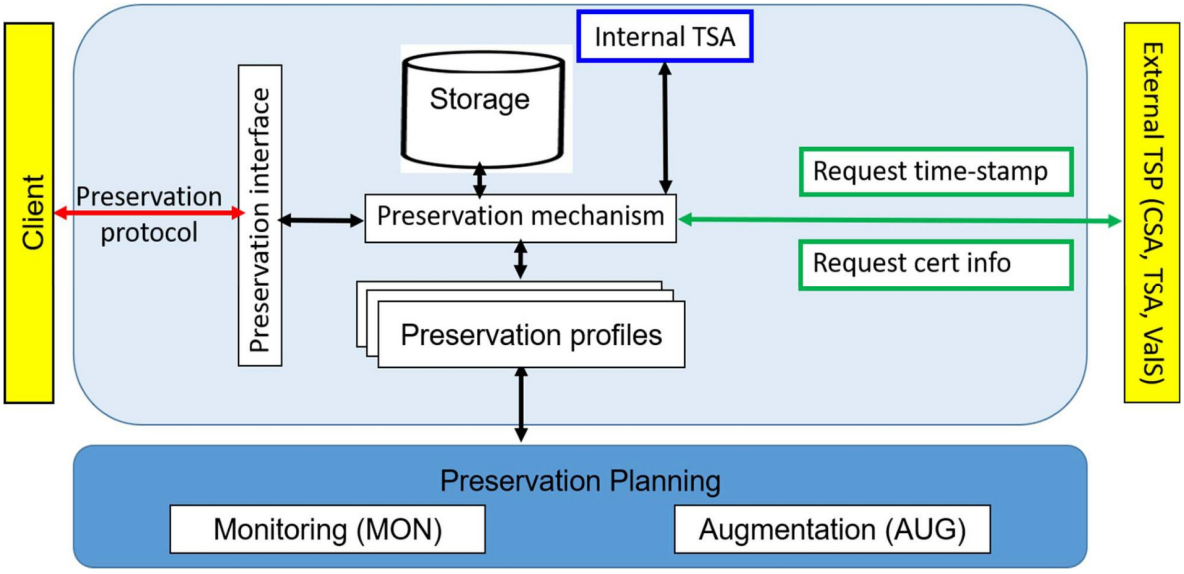
MitSoft PSP naudoja apsaugos saugyklos modelį WST tam, kad galėtų suteikti maksimalią apsaugos paslaugų apimtį apsaugos paslaugos teikėjo pastangomis. Naudojant apsaugos saugyklos modelį WST, apsaugos kliento veiksmai yra apriboti pateikimo duomenų objektų pateikimu ir, kai reikalinga, gavimu pateiktų duomenų objektų, apsaugos objektų, įskaitant apsaugos įrodymus. Šis variantas geriausiai tinka apsaugos paslaugų smulkiems abonentams.

Apsaugos paslaugų didieji abonentai gali turėti specifinių poreikių dėl apsaugos objektų didžiulės bendros apimties ar dėl bet kurios kitos priežasties. Todėl MitSoft PSP pateikia ir apsaugos be saugyklos WOS modelio paslaugas.

4.2.1. Apsaugos paslauga su saugykla (WST)

4.2.1.1 Architektūra

Apsaugos paslaugos su saugykla (WST) bendroji architektūra yra pateikta 1 paveikslėlyje [TS 119 511].

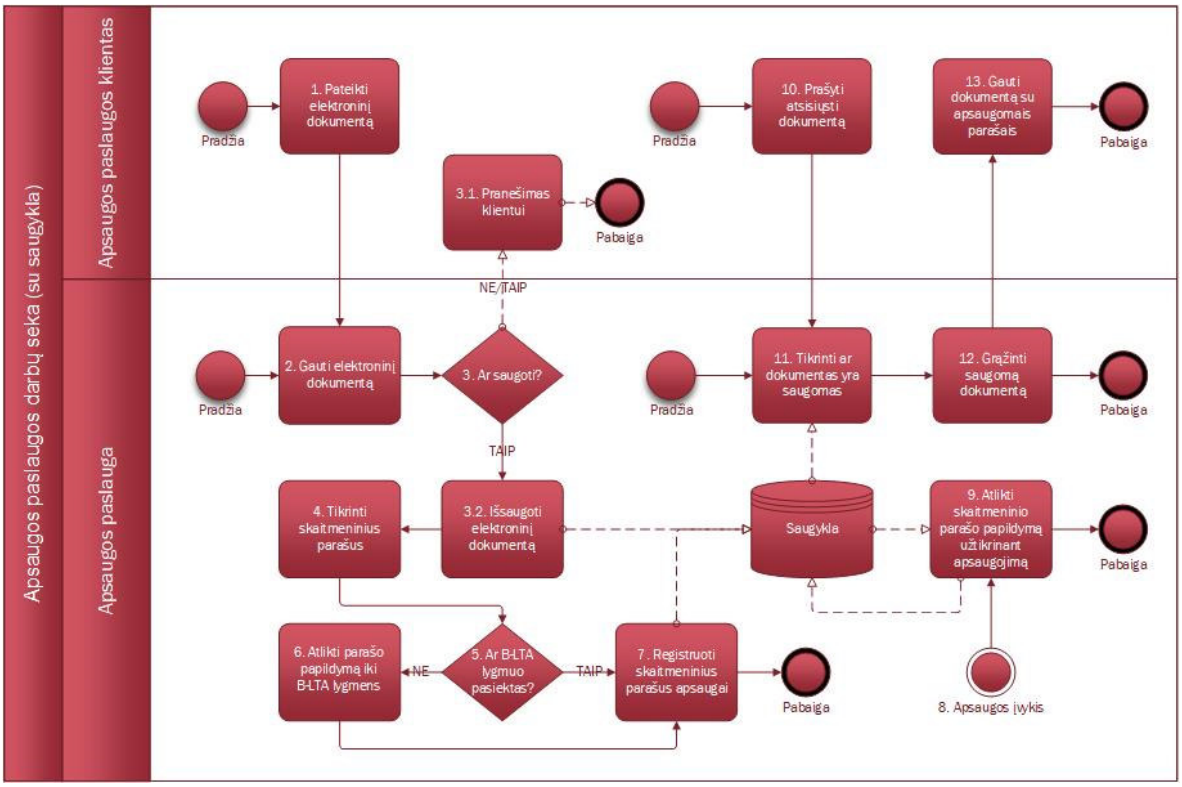


1 pav. Apsaugos paslaugos su saugykla (WST) bendroji architektūra

4.2.1.2 MitSoft apsaugos paslaugų darbų seka

MitSoft kvalifikuotos ilgalaikės apsaugos paslaugos su saugykla gauna elektroninius dokumentus ir/ar konteinerius iš paslaugos klientų. Gavus elektroninį dokumentą ir/ar konteinerį, apsaugos paslaugos atlieka validavimą. Pakartotinis validavimas atliekamas pagal išreikštinę kliento užklausą, o taip pat vykdant apsaugos paslaugų elektroninių dokumentų/konteinerių priežiūros procesą. Gautas elektroninis dokumentas/konteineris yra išsaugomas MitSoft apsaugos paslaugų saugykloje. Pagal apsaugos paslaugų priežiūros proceso prašymą apsaugos objektai yra laiku papildomi apsaugos įrodymais. Vėliau klientas gali paprašyti apsaugos paslaugų pateikti išsaugotą elektroninį dokumentą/konteinerį su įtrauktais apsaugos įrodymais.

Darbų su elektroniniu dokumentu/konteineriu seka MitSoft apsaugos paslaugoje su saugykla yra pateikta 2 paveikslėlyje.



2 pav. Darbų su elektroniniu dokumentu/konteineriu seka MitSoft apsaugos paslaugoje su saugykla (WST)

1. Apsaugos klientas pateikia elektroninį dokumentą/konteinerį apsaugos paslaugai.
2. Apsaugos paslauga gauna elektroninį dokumentą/konteinerį iš kliento.
3. Apsaugos paslauga tikrina, ar elektroninis dokumentas/konteineris yra priimtinas. Elektroninis dokumentas/konteineris turi tenkinti pagrindinius elektroninio dokumento/konteinerio formato reikalavimus ir turi turėti bent vieną elektroninį parašą arba elektroninį spaudą. Elektroninis dokumentas/konteineris neturi turėti virusų, kenkėjiško ir neleistino turinio.
   3.1. Apsaugos klientas gauna operacijos atsakymą (priimta ar ne) ir atmetimo atveju - apsaugos paslaugos atmetimo priežastį.
   3.2. Priėmimo atveju apsaugos paslauga išsaugo elektroninį dokumentą/konteinerį kartu su papildomais metaduomenimis.
4. Apsaugos paslauga validuoja elektroninį dokumentą/konteinerį ir jame esančius elektroninius parašus ir elektroninius spaudus.
5. Apsaugos paslauga tikrina, ar kiekvienas saugotinas elektroninis parašas ir elektroninis spaudas jau pasiekė B-LTA lygmenį (ar atitinkamą archyvinį parašo formatą parašams, kurie nėra baziniai parašai).
6. Apsaugos paslauga atlieka elektroninių parašų ir elektroninių spaudų papildymą. Po šio papildymo kiekvienas saugotinas elektroninis parašas/spaudas pasiekia B-LTA lygmenį (ar atitinkamą archyvinį parašo formatą parašams, kurie nėra baziniai parašai).
7. Apsaugos paslauga registruoja saugotinus elektroninius parašus ir elektroninius spaudus, esančius elektroniniame dokumente/konteineryje tolesnei apsaugai. Kiekvienam registruotam apsaugai skaitmeniniam parašui yra surenkami ir išsaugomi papildomi apsaugos metaduomenys. Apsaugai nebus registruojami elektroniniai parašai ir/ar elektroniniai spaudai, kuriuose yra klaidų neleidžiančių pasiekti B-LTA lygmens (ar atitinkamo archyvinio parašo formato parašams, kurie nėra baziniai parašai).

8. Priežiūros procesas atlieka elektroniniuose dokumentuose/konteineriuose saugomų elektroninių parašų/spaudų priežiūrą. Priežiūros procesas vykdo apsaugą, jeigu saugomas elektroninis parašas/spaudas turi būti papildytas tam, kad būtų užtikrinta jo apsauga dėl sertifikato galiojimo pabaigos artimiausiu metu ar kriptografinio algoritmo galimo pasenimo.
9. Apsaugos paslauga atlieka skaitmeninio parašo papildymą, pridėdama naują archyvinę laiko žymą tam, kad pratęstų jo galiojimo statuso išlaikymą. Apsaugos įrodymai yra įterpiami į skaitmeninius parašus, esančius elektroniniame dokumente/konteineryje. Atnaujintas elektroninis dokumentas/konteineris kartu su papildomais apsaugos metaduomenimis yra išsaugomas MitSoft apsaugos paslaugų saugykloje.
10. Tam tikru momentu apsaugos klientas gali nuspręsti paprašyti pateikti saugomą elektroninį dokumentą/konteinerį.
11. Apsaugos paslauga tikrina, ar prašomas elektroninis dokumentas/konteineris yra saugomas MitSoft apsaugos paslaugų saugykloje ir ar paslaugų naudotojas turi teisę prieigai prie prašomo elektroninio dokumento/konteinerio.
12. Apsaugos paslauga grąžina prašomą elektroninį dokumentą/konteinerį kartu su apsaugos įrodymais, įterptais į kliento skaitmeninius parašus, arba informuoja klientą, kad užklausa negali būti įvykdyta.
13. Apsaugos klientas gauna elektroninį dokumentą/konteinerį, turintį elektroninius parašus/spaudus su įterptais apsaugos įrodymais.

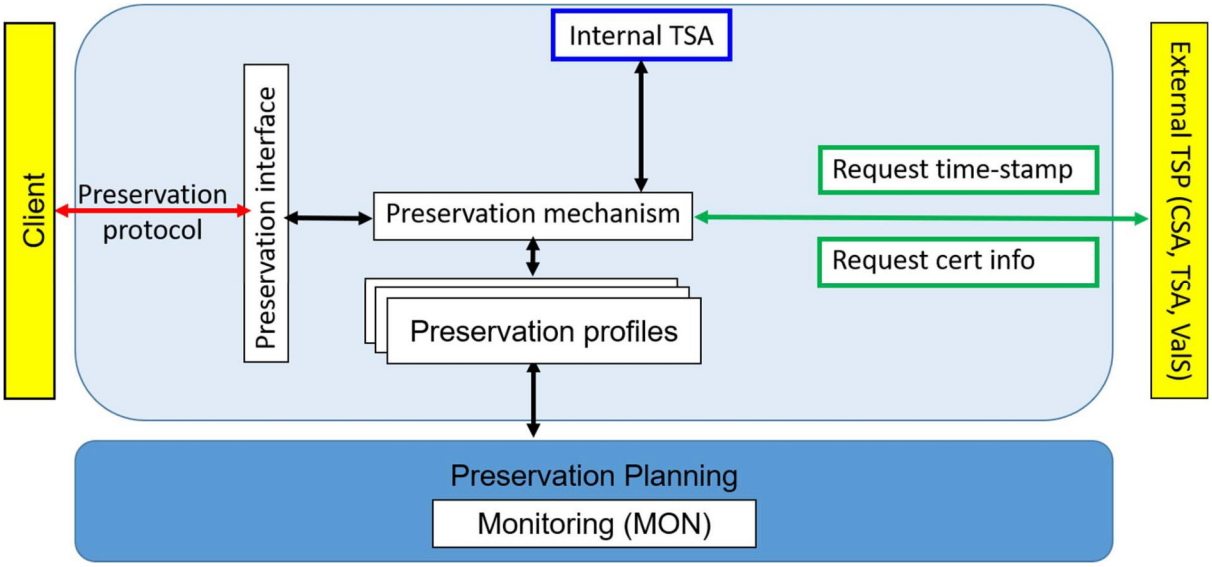
Validavimas yra atliekamas kiekvienam elektroniniame dokumente/konteineryje esančiam elektroniniam parašui ir elektroniniam spaudui.

Papildymas yra atliekamas saugotiname elektroniniame dokumente/konteineryje esančiam kiekvienam elektroniniam parašui ir elektroniniam spaudui, jeigu jis nebuvo pripažintas netinkamu apsaugai.

4.2.2. Apsaugos paslauga be saugyklos (WOS)

4.2.2.1 Architektūra

Apsaugos paslaugos be saugyklos (WOS) bendroji architektūra yra pateikta 3 paveikslėlyje [TS 119 511].

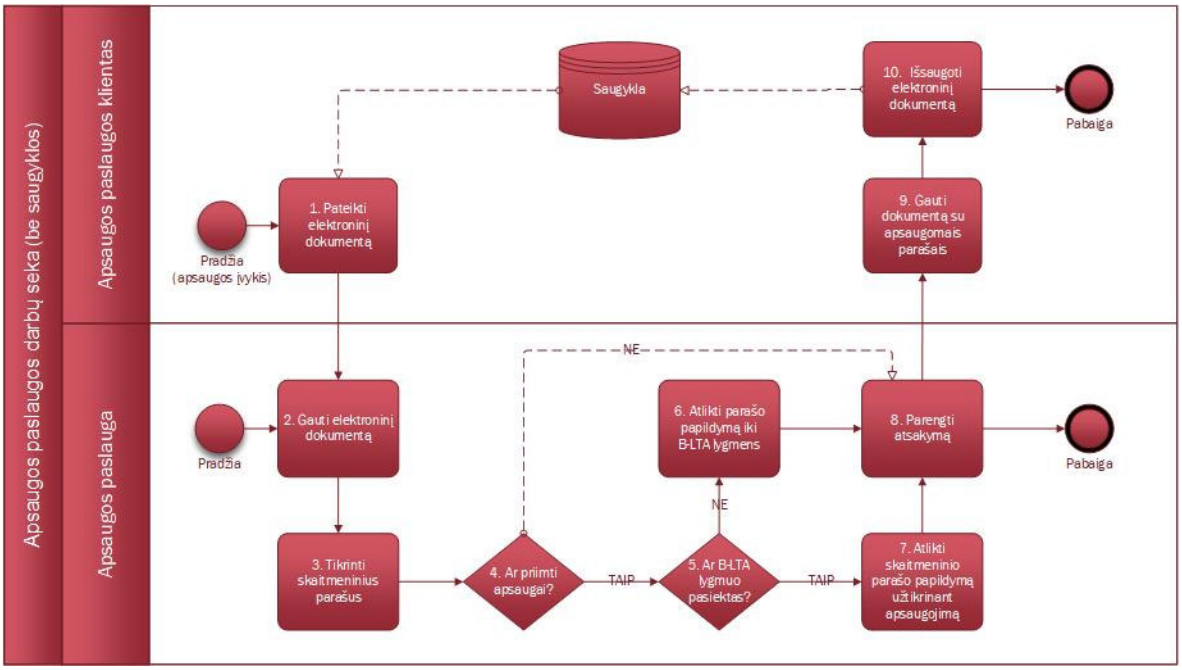


3 pav. Apsaugos paslaugos be saugyklos (WOS) bendroji architektūra

4.2.2.2 MitSoft apsaugos paslaugų darbų seka

MitSoft kvalifikuota ilgalaikės apsaugos paslauga be saugyklos gauna elektroninį dokumentą ar konteinerį iš apsaugos kliento. Gavusi elektroninį dokumentą ar konteinerį, apsaugos paslauga atlieka jo validavimą. Atlikus validavimą, yra vykdomas papildymas ir surinkti apsaugos įrodymai yra įtraukiami į elektroninius parašus/spaudus, esančius elektroniniame dokumente/konteineryje. Kaip apsaugos įrodymas, atnaujintas elektroninis dokumentas/konteineris kartu su apskaičiuota tikėtina įrodymų trukme yra grąžinamas apsaugos klientui. Nei elektroninis dokumentas/konteineris, nei elektroniniai parašai/spaudai nėra išsaugomi jokioje MitSoft apsaugos paslaugos saugykloje.

Darbų su elektroniniu dokumentu/konteineriu seka MitSoft apsaugos paslaugoje be saugyklos yra pateikta 4 paveikslėlyje.



4 pav. Darbų su elektroniniu dokumentu/konteineriu seka MitSoft apsaugos paslaugoje be saugyklos (WOS)

1. Apsaugos klientas pateikia elektroninį dokumentą/konteinerį apsaugos paslaugai, kai įvyksta apsaugos įvykis. Apsauga yra vykdoma, jeigu pateiktam naujam elektroniniam dokumentui/konteineriui apsauga turi būti inicijuota arba jeigu jau apsaugotas elektroninis dokumentas/konteineris turi būti pakartotinai papildytas, kadangi tikėtina įrodymų (esančių elektroninio dokumento/konteinerio skaitmeniniuose parašuose) trukmė baigiasi. Apsaugos įvykių valdymą atlieka apsaugos klientas, o ne apsaugos paslauga.
2. Apsaugos paslauga priima apsaugai elektroninį dokumentą/konteinerį, turintį bent vieną elektroninį parašą arba elektroninį spaudą.
3. Apsaugos paslauga validuoja elektroninį dokumentą/konteinerį ir jame esančius elektroninius parašus ir elektroninius spaudus.
4. Apsaugos paslauga tikrina, ar reikia apsaugoti elektroninį dokumentą/konteinerį ir elektroninius parašus bei elektroninius spaudus.
5. Apsaugos paslauga tikrina, ar kiekvienas saugotinas elektroninis parašas ir elektroninis spaudas jau pasiekė B-LTA lygmenį (ar atitinkamą archyvinį parašo formatą parašams, kurie nėra baziniai parašai).
6. Apsaugos paslauga atlieka elektroninių parašų ir elektroninių spaudų papildymą. Po šio papildymo kiekvienas saugotinas elektroninis parašas/spaudas pasiekia B-LTA

lygmenį (ar atitinkamą archyvinį parašo formatą parašams, kurie nėra baziniai parašai).

7. Apsaugos paslauga atlieka skaitmeninio parašo papildymą, pridėdama naują archyvinę laiko žymą tam, kad pratęstų jo galiojimo statuso išlaikymą. Apsaugos įrodymai yra įterpiami į skaitmeninius parašus, esančius elektroniniame dokumente/konteineryje. Skaitmeninio parašo papildymas, pridedant naujus apsaugos įrodymus, yra atliekamas tik tuo atveju, jeigu papildymo laikotarpis jau yra prasidėjęs, t.y. jei tikėtina, kad skaitmeninio parašo galiojimo pabaigos laikas yra artimoje ateityje.
8. Apsaugos paslauga paruošia atsakymą klientui. Apaugos paslauga apskaičiuoja naują tikėtiną įrodymo galiojimo trukmę ir papildymo laikotarpį. Sėkmės atveju, atsakymas susideda iš atnaujinto elektroninio dokumento/konteinerio su apsaugos įrodymais, įterptais į elektroninį dokumentą/konteinerį, duomenimis apie sekančio papildymo rekomenduojamą laiką ir apskaičiuotą tikėtiną įrodymo trukmę. Kitu atveju yra grąžinama atmetimo ar trikio priežastis.
9. Apsaugos klientas gauna atnaujintą elektroninį dokumentą/konteinerį iš apsaugos paslaugos. Jis taip pat gauna naują tikėtiną įrodymo trukmę ir sekančio papildymo rekomenduojamą laiką.
10. Apsaugos klientas išsaugo atnaujintą elektroninį dokumentą/konteinerį savoje saugykloje. Apsaugos klientas turi gautam elektroniniam dokumentui/konteineriui atnaujinti sekančio papildymo laiką (ir tikėtiną įrodymo trukmę) tam, kad galėtų laiku inicijuoti sekančio papildymo įvykį.

5. Rizikos vertinimas

Žiūrėti [QTS PS] dokumento 5 skyrelį.

6. TAISYKLĖS IR PRAKTIKOS

6.1. Apsaugos paslaugų veiklos nuostatai

Žiūrėti [QTS PS] dokumento 6.1 skyrelį.

Papildomai, teikiant kvalifikuotas ilgalaikės apsaugos paslaugas:

a) Praktikos ir procedūros, naudojamos įgyvendinti Kvalifikuotų apsaugos paslaugų taisyklėse (QPSP) ir šiuose Apsaugos paslaugų veiklos nuostatuose (QLPS PS) identifikuotus reikalavimus.

b) Pateikimo duomenų objektų (SubDO) ir susijusių apsaugos įrodymų prieinamumas yra pasiekiamas taip: apsaugos objekto konteineris (*angl. Preservation Object Container - POC*) yra pateiktas elektroninis dokumentas arba konteineris, kuris turi savyje elektroninius parašus ir/ar elektroninius spaudus (apsaugos objektus) su apsaugos paslaugos įterptais apsaugos įrodymais (laiko žymomis). POC yra sudaromas iš SubDO, tinkamu laiku papildant saugomus skaitmeninius parašus apsaugos įrodymais (laiko žymomis). Apsaugos profilyje apibrėžtos operacijos priima ir grąžina apsaugos objektą, kuris yra visas apsaugos objekto konteineris - elektroninis dokumentas ar konteineris (kartu su visais jame esančiais saugomais skaitmeniniais parašais), arba pateikimo duomenų objektas. Tokiu būdu, pateikimo duomenų objektai (SubDO) ir susiję apsaugos įrodymai yra talpinami tame pačiame konteineryje viso apsaugos laikotarpio metu. Žr. detaliau dokumento „Apsaugos profilis su saugykla" 4.8 skyrelį.

c) MitSoft QLPS PS identifikuoja visų išorinių organizacijų, palaikančių kvalifikuotas ilgalaikės apsaugos paslaugas, įsipareigojimus, įskaitant taikomas taisykles ir praktikas. Tokiomis išorinėmis organizacijomis yra kvalifikuotos laiko žymų tarnybos, sudarančios kvalifikuotas laiko žymas, ir kvalifikuoti sertifikavimo paslaugų teikėjai, sudarantys kvalifikuotus sertifikatus kvalifikuotiems elektroniniams parašams ar kvalifikuotiems elektroniniams spaudams bei šiems sertifikatams teikiantys OCSP ir CRL paslaugas pagal atitinkamai kvalifikuotų elektroninių laiko žymų paslaugų taisykles ir kvalifikuotų elektroninių parašų sertifikatų taisykles ir kvalifikuotų elektroninių spaudų sertifikatų taisykles. Šios išorinės OCSP ir CRL paslaugos taip pat yra naudojamos nustatyti nekvalifikuotų sertifikatų, kuriuos sudaro kvalifikuoti sertifikavimo paslaugų teikėjai, išleidžiantys nekvalifikuotus elektroninių parašų sertifikatus ar nekvalifikuotus elektroninių spaudų sertifikatus, statusui.

QPSP yra vienintelės MitSoft kvalifikuotų ilgalaikės apsaugos paslaugų palaikomos apsaugos paslaugų taisyklės:

a) Santraukos algoritmai, kurie gali būti panaudoti duomenims laiko žymoms sudaryti, yra specifikuoti 7.14 skyrelyje „Kriptografinė stebėsena".

b) Sutinkamai su QPSP, MitSoft PSP pateikia kvalifikuotas ilgalaikės elektroninių parašų ir elektroninių spaudų apsaugos paslaugas pagal saugyklų modelius: apsauga su saugykla (*angl. Preservation With Storage – WST*) ir apsauga be saugyklos (*angl. Preservation Without Storage – WOS*).

c) Sutinkamai su QPSP, MitSoft PSP pateikia kvalifikuotas ilgalaikes elektroninių parašų ir elektroninių spaudų apsaugos paslaugas pagal funkcinį tikslą: skaitmeninių parašų apsauga (*angl. Preservation Digital Signatures – PDS*).

d) Abonentų įsipareigojimai yra specifikuoti 6.1.1.3 skyrelyje „Abonento įsipareigojimai".

e) Pasikliaujančių šalių įsipareigojimai yra specifikuoti 6.1.1.4 skyrelyje „Pasikliaujančių šalių įsipareigojimai".

f) Informacija, kaip patikrinti apsaugos įrodymus, yra pateikta 6.5 skyrelyje „Apsaugos įrodymų taisyklės".
g) Kvalifikuotų elektroninių parašų ir spaudų ilgalaikės apsaugos paslaugos yra kvalifikuotos apsaugos paslaugos pagal ES Reglamentą Nr. 910/2014 [eIDAS].

6.1.1. PSP įsipareigojimai

6.1.1.1. Bendroji dalis

PSP užtikrina, kad visi PSP taikomi reikalavimai yra įgyvendinti orientuojantis į QPSP. PSP užtikrina įgyvendinimą to, ką nurodo:

a) Procedūros, apibrėžtos šiuose QLPS PS, įskaitant stebėsenos procedūras ir apsaugos įrodymų papildymą apsaugos objektuose;
b) Įsipareigojimai, nurodyti apsaugos profilyje ar įtraukti pagal profilyje esančias nuorodas.

6.1.1.2. PSP įsipareigojimai abonentams

Žiūrėti [QTS PS] dokumento 6.1.1.1 skyrelį.

6.1.1.3. Abonentų įsipareigojimai

Pasitikėdamas ilgalaikės apsaugos paslaugų įrodymais, abonentas turi patikrinti, ar apsaugos įrodymai buvo korektiškai sukurti ir validuoti (detaliau žr. 6.1.1.4 skyrelyje „Pasikliaujančių šalių įsipareigojimai").

6.1.1.4. Pasikliaujančių šalių įsipareigojimai

Pasikliaujančios šalys, pasitikėdamos apsaugos objektu, kuris apima apsaugos įrodymus, turi patikrinti, ar kvalifikuotos archyvinės laiko žymos buvo korektiškai pasirašytos ir ar privatus raktas, panaudotas pasirašyti archyvinę laiko žymą, nebuvo sukompromituotas (atskleistas trečioms šalims ar nenaudotinas dėl kitų priežasčių) iki tikrinimo momento.

Archyvinė laiko žyma yra tikrinama laiko žymų tarnybos sertifikato galiojimo laikotarpiu; pasirašymo rakto validumas gali būti patikrintas įsitikinant, kad laiko žymų tarnybos sertifikatas nebuvo atšauktas.

Be to, pasikliaujanti šalis turi laikytis ilgalaikės apsaugos paslaugų apribojimų, apibrėžtų QPSP taisyklėse ir imtis bet kokių kitų atsargumo priemonių.

6.1.1.5. Atsakomybė

Žiūrėti [QTS PS] dokumento 6.1.1.2 skyrelį.

6.1.1.6. Teisinės nuostatos ir interpretacijos

Žiūrėti [QTS PS] dokumento 6.1.1.3 skyrelį.

6.1.1.7. Mokesčiai

Žiūrėti [QTS PS] dokumento 6.1.1.4 skyrelį.

6.1.1.8. Intelektinės nuosavybės teisės

Žiūrėti [QTS PS] dokumento 6.1.1.5 skyrelį.

6.2. Paslaugų teikimo sąlygos

Žiūrėti [QTS PS] dokumento 6.2 skyrelį.

Papildomai, kvalifikuotų ilgalaikės apsaugos paslaugų teikimo sąlygos specifikuoja:

a) Taikomas QPSP.
b) Informaciją, kaip patikrinti apsaugos įrodymus ir bet kuriuos susijusius galiojimo laikotarpio apribojimus.
c) Ar kvalifikuotų ilgalaikės apsaugos paslaugų atitiktis QPSP buvo įvertinta ir, jeigu taip, tai pagal kokią atitikties įvertinimo schemą.
d) Kur rasti informaciją apie palaikomus apsaugos profilius.
e) Kaip galima pateikti prašymą eksporto-importo paketo gavimui.
f) Strategija, kurios QPSP laikysis, jei nebus galimybės surinkti ir patikrinti visų validavimo duomenų.

6.3. Informacijos saugumo taisyklės

Žiūrėti [QTS PS] dokumento 6.3 skyrelį.

6.4. Apsaugos profilis

MitSoft PSP palaiko šiuos apsaugos profilius:

- MitSoftQWST profilis – kvalifikuotų elektroninių parašų ir spaudų MitSoft apsaugos profilis su saugykla, kuris yra nurodytas unikaliu objekto identifikatoriumi (OID):
  - 1.3.6.1.4.1.57890.1.5.1
- MitSoftQWOS profilis – kvalifikuotų elektroninių parašų ir spaudų MitSoft apsaugos profilis be saugyklos, kuris yra nurodytas unikaliu objekto identifikatoriumi (OID):
  - 1.3.6.1.4.1.57890.1.5.2

Profilių aprašai yra prieinami MitSoft interneto svetainėje.

Pateikiami duomenų objektai yra elektroniniai dokumentai ar konteineriai, turintys elektroninius parašus ar elektroninius spaudus ir pasirašytus/patvirtintus duomenis. MitSoft PSP nepalaiko pateikiamų duomenų objektų, kurie turi tik pasirašytų duomenų santraukas. Apsaugos profiliai apibrėžia palaikomų duomenų objektų formatų aktualią aibę.

Saugotinų apsaugos objektų detalesnis apibūdinimas yra pateikiamas naudojamame apsaugos profilyje.

6.5. Apsaugos įrodymų taisyklės

MitSoft PSP palaiko šias apsaugos įrodymų taisykles:

- MitSoft kvalifikuotų ilgalaikės apsaugos paslaugų Apsaugos įrodymų taisyklės, kurios yra nurodytos unikaliu objekto identifikatoriumi (OID):
  - 1.3.6.1.4.1.57890.1.7.1.x

kur x rodo vėliausią taisyklių versiją. Abonentai gali rasti visas versijas MitSoft PSP repozitoriume.

6.6. Parašo validavimo taisyklės

MitSoft PSP palaiko šias parašo validavimo taisykles:

- MitSoft kvalifikuotų ilgalaikės apsaugos paslaugų Parašo taisyklės, kurios yra nurodytos unikaliu objekto identifikatoriumi (OID):
    - 1.3.6.1.4.1.57890.1.6.1.x

    kur x rodo vėliausią taisyklių versiją. Abonentai gali rasti visas versijas MitSoft PSP repozitoriume.

6.7. Abonentinė sutartis

MitSoft PSP teikia kvalifikuotas ilgalaikės apsaugos paslaugas abonentams, remiantis Abonentine sutartimi, kuri apima šiuos privalomus punktus:

- Paslaugų teikimo sąlygos, kurias Abonentas priima.
- Profiliai, kuriuos Abonentas naudos.
- Ar pažangūs elektroniniai parašai ir pažangūs elektroniniai spaudai (kurie nėra kvalifikuoti) irgi yra apsaugos objektai.
- Ar elektroniniai parašai ir elektroniniai spaudai, kurie nėra galiojantys (turintys kitą validavimo statusą nei PASSED), irgi yra apsaugos objektai (jei tik tai yra suderinta su parašo taisyklėmis).
- Pateikiamų apsaugos paslaugai elektroninių dokumentų/konteinerių formatai (specifikacijos).
- Papildymo laikotarpio trukmė.
- Atsargumo *(angl. caution)* laikotarpio trukmė.
- Abonento atstovas, įvardintas kaip MitSoft PSP ilgalaikės apsaugos paslaugų abonento administratorius.
- Kas abonento vardu turi prieigos teisę prie apsaugos objektų, įskaitant pateikiamus duomenų objektus ir apsaugos įrodymus.
- Kas abonento vardu turi teisę užprašyti apsaugos veiksmų sekų, susijusių su apsaugos objektais.
- Kas atsitinka su duomenimis pasibaigus apsaugos laikotarpiui.

7. PSP VALDYMAS IR VEIKIMAS

7.1. Vidinė organizacija

Žiūrėti [QTS PS] dokumento 7.1 skyrelį.

7.2. Žmogiškieji ištekliai

Žiūrėti [QTS PS] dokumento 7.2 skyrelį.

7.3. Turto valdymas

Žiūrėti [QTS PS] dokumento 7.3 skyrelį.

7.4. Prieigos kontrolė

Žiūrėti [QTS PS] dokumento 7.4 skyrelį.

7.5. Kriptografinis valdymas

MitSoft PSP kvalifikuotos ilgalaikės apsaugos paslaugos nenaudoja savų kriptografinių raktų nei kriptografinių įrenginių elektroninių parašų ir elektroninių spaudų apsaugai.

MitSoft PSP užtikrina, kad laiko žymos, naudojamos apsaugos procese, yra sudarytos ES kvalifikuotų laiko žymų paslaugų teikėjų, kurie laikosi patikimų paslaugų teikėjų, sudarančių kvalifikuotas laiko žymas, taisyklių ir saugumo reikalavimų, geriausių praktikų.

7.6. Fizinis ir aplinkos saugumas

Žiūrėti [QTS PS] dokumento 7.6 skyrelį.

7.7. Veiklos saugumas

Žiūrėti [QTS PS] dokumento 7.7 skyrelį.

7.8. Tinklo saugumas

Žiūrėti [QTS PS] dokumento 7.8 skyrelį.

Papildomai, kvalifikuotoms ilgalaikės apsaugos paslaugoms:

a) Apsaugos paslaugų sistemos architektūra yra suprojektuota ir įgyvendinta tokiu būdu, kad apsaugos kliento prieiga prie saugyklos, keičianti saugyklos turinį, yra atliekama tik pačios apsaugos paslaugų sistemos operacijomis.

b) Aukštas išorinės prieigos pasiekiamumo lygis prie apsaugos paslaugų nėra reikalaujamas.

7.9. Incidentų valdymas

Žiūrėti [QTS PS] dokumento 7.9 skyrelį.

7.10. Įrodymų surinkimas

Žiūrėti [QTS PS] dokumento 7.10 skyrelį.

Papildomai:

a) Įrašai apie kvalifikuotas ilgalaikės apsaugos paslaugas yra saugomi laiką, tinkamą pateikti būtinus teisinius įrodymus, kaip skelbiama PSP „Paslaugų teikimo sąlygose".

7.11. Veiklos tęstinumo valdymas

Žiūrėti [QTS PS] dokumento 7.11 skyrelį.

7.12. PSP veiklos užbaigimas ir užbaigimo planai

Žiūrėti [QTS PS] dokumento 7.12 skyrelį.

Papildomai, PSP užtikrina, kad tolerancijos laikotarpiu prižiūrint informaciją, reikalingą apsaugos objektams išsaugoti ir prieiti prie jų:

a) Užbaigimo planas nustato, kas įvyksta su saugomais apsaugos objektais užbaigus apsaugos paslaugų teikimą.

b) PSP nenaudoja pasirašymo kriptografijos, todėl neatlieka privalomų baigiamųjų veiksmų jos buvimo atveju.

c) PSP nepasirašo apsaugos įrodymų. Apsaugos įrodymai yra kvalifikuotos laiko žymų tarnybos pasirašytos laiko žymos.

7.13. Atitiktis

Žiūrėti [QTS PS] dokumento 7.13 skyrelį.

Papildomai:

- Siekdamas teikti ilgalaikės apsaugos paslaugas, PSP reikalauja pateikti apsaugos užklausą, kaip apibrėžta [TS 119 511], kartu su autentifikavimo duomenimis, jei tai tinka pasirinktam autentifikavimo būdui.

7.14. Kriptografijos stebėsena

MitSoft PSP kriptografijos stebėsena apima du kriptografinių algoritmų rinkinius, kuriuos naudoja apsaugos paslaugų sistema:

- Pateikimo duomenų objektuose jau naudojami kriptografiniai algoritmai.
- Kriptografiniai algoritmai, naudojami skaitmeninio parašo papildymui. Skaitmeninio parašo papildymas atliekamas: jei pateiktame apsaugos objekte nėra validavimo duomenų (ar jų dalies) ir jie papildomi iki B-LTA lygmens (arba atitinkamo parašo formato parašams, kurie nėra baziniai parašai), arba jei sertifikatas, naudojamas pasirašyti apsaugos įrodymus baigia galioti, arba kriptografiniai algoritmai, naudojami apsaugos įrodymuose, tampa mažiau saugūs.

Pateikimo duomenų objektuose naudojamų algoritmų kriptografijos stebėsena yra pagrįsta esama algoritmo patikimumo būsena ir naudojama tik skaitmeninio parašo validavimo metu (atliekama pateikus apsaugos objektą arba pagal užklausą).

Skaitmeninio parašo papildymui naudojamų algoritmų kriptografijos stebėsena yra pagrįsta numatoma algoritmo patikimumo būsena ir taikoma tik naujai kuriamiems apsaugos įrodymams (laiko žymoms).

MitSoft PSP kriptografijos stebėjimo įgyvendinimas yra pagrįstas kriptografinių algoritmų registru ir skaitmeninio parašo apsaugos metaduomenimis.

Kriptografinių algoritmų registre yra saugoma informacija apie palaikomus kriptografinius algoritmus ir jų patikimumo būseną. Išsaugomi duomenys apima:

- Algoritmo pavadinimą.
- Algoritmo identifikatorių (OID ir URI).
- Algoritmo tipą (santraukos funkcija, parašo algoritmas, kanonizavimo algoritmas).
- Raktų ilgį (tik parašų algoritmams).
- Algoritmo patikimumo būseną – ar jis patikimas šiuo metu ir gali būti naudojamas pateikimo duomenų objektuose, ar patikimas naudoti skaitmeninio parašo papildymo metu surinktiems apsaugos įrodymams.
- Numatomą algoritmo patikimumo laiką – laiką, iki kurio yra manoma, kad algoritmas dar bus patikimas. Numatomas algoritmo patikimumo laikas gali būti nustatytas ir gali būti perkeltas į priekį kriptografinių algoritmų registro peržiūros metu, jei atsiranda naujos informacijos apie algoritmo patikimumą.

Kriptografinių algoritmų registro peržiūrą ir atnaujinimus MitSoft PSP atlieka reguliariai ir atspindi rekomendacijas, pateiktas standarte ETSI TS 119 312 "Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites" [TS 119 312], bei užtikrinama atitiktis "Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA" [ENISA].

Numatomas kriptografinių algoritmų (jų parametrų ir raktų dydžių), naudojamų naujiems išsaugojimo įrodymams, atsparumo laikotarpis (pagal [TS 119 312] ir [ENISA]) papildymo metu yra 3 metai arba ilgiau.

Kriptografinių algoritmų registro peržiūrą ir atnaujinimą atlieka MitSoft PSP sistemos operatorius. Nustačius, kad įrodymų apsaugos taisyklėse apibrėžtas kriptografinis algoritmas tampa nepakankamai saugus naujiems apsaugos įrodymams kurti, išleidžiama nauja „Apsaugos įrodymų taisyklių" versija.

Skaitmeninio parašo išsaugojimo metaduomenys – tai duomenys apie skaitmeninio parašo apsaugos būseną, apsaugos įrodymuose naudojamus kriptografinius algoritmus, planuojamus papildymus ir apsaugos laikotarpį. Skaitmeninio parašo apsaugos metaduomenys renkami priimant pateikimo duomenų objektą, saugomi atskirai nuo apsaugos objektų apsaugos paslaugų saugykloje ir atnaujinami tolesnio papildymo metu. Skaitmeninio parašo apsaugos metaduomenys apima:

- Skaitmeninio parašo identifikatorių.
- Esamą skaitmeninio parašo lygmenį (B-B, B-T, B-LT, B-LTA, ar atitinkamas parašo formatas parašams, kurie nėra baziniai parašai).
- Indikatorių, ar skaitmeninio parašo apsauga turi būti vykdoma.
- Jei skaitmeninio parašo lygmuo yra B-LTA, santraukos algoritmą, naudojamą paskutinės archyvinės laiko žymos santraukos skaičiavimui, parašo algoritmą (su rakto ilgiu) ir santraukos algoritmą, kurį laiko žymų tarnyba naudoja pačiai laiko žymai pasirašyti.
- Sekančio planuojamo papildymo datą.
- Apsaugos laikotarpio pabaigos datą.

MitSoft PSP naudojamos sekančio papildymo datos įvertinimo taisyklės:

- Jei skaitmeninio parašo apsauga neatliekama, kita papildymo data nustatoma į NULL. Tai reiškia, kad šio skaitmeninio parašo papildymas nebus atliktas.
- Jei skaitmeninio parašo lygmuo yra B-B, tada kita papildymo data nustatoma į esamą datą. Tai reiškia, kad skaitmeninio parašo papildymas turi būti atliktas nedelsiant, kad būtų pasiektas bent B-T lygmuo.
- Jei skaitmeninio parašo lygmuo yra B-T arba B-LT, kita papildymo data nustatoma kaip parašo egzistavimo įrodymo laikas (parašo laiko žymos

generavimo laikas) + sertifikavimo įstaigos (pasirašančio asmens sertifikato sudarytojo) taikomas atidėjimo (*angl. grace*) laikotarpis. Jei atidėjimo laikotarpis nežinomas, naudojamas numatytasis 24 valandų atidėjimo laikotarpis. Tai reiškia, kad skaitmeninio parašo papildymas, kad būtų pasiektas B-LTA lygmuo, turi būti atliktas iš karto, kai tik atsiranda tinkami validavimo duomenys.

- Jei skaitmeninio parašo lygmuo yra B-LTA, tai kita papildymo data skaičiuojama pagal paskutinę archyvinę laiko žymą patvirtinančio sertifikato galiojimo datą ir numatomą naudojamų kriptografinių algoritmų patikimumo trukmę. Kadangi papildymo procesas užtrunka, o laiko žymomis, pasirašytomis naudojant tą patį laiko žymų tarnybos sertifikatą, gali būti apsaugota daug skaitmeninių parašų, kita papildymo data nustatoma per papildymo laikotarpį ir prieš atsargumo laikotarpį. Papildymo laikotarpis yra protingas laikotarpis, kuris prasideda likus kažkiek laiko iki numatomo skaitmeninio parašo galiojimo pabaigos ir tęsiasi iki numatomos skaitmeninio parašo galiojimo pabaigos datos. Siekiant sumažinti galimo išorinių paslaugų neprieinamumo riziką, kita papildymo data nustatoma prieš atsargumo laikotarpį. Apsaugos paslaugų naudojamas atsargumo laikotarpis nurodytas Abonentinėje sutartyje.
- Jei kriptografinio algoritmo registro peržiūra pripažįsta, kad kuris nors kriptografinis algoritmas taps mažiau saugus anksčiau, nei buvo tikėtasi, inicijuojamas nereguliarus papildymo įvykis. Tokiu atveju kita papildymo data atnaujinama pagal naują numatomą algoritmo patikimumo laiką. Šio įvykio paveikti skaitmeniniai parašai nustatomi naudojant skaitmeninio parašo apsaugos metaduomenis.

Skaitmeninio parašo papildymą sistema atlieka automatiškai. Sekančio papildymo data suaktyvina papildymo įvykį, kuris apsaugomą elektroninį dokumentą ar konteinerį (su skaitmeniniu parašu, kuris yra pildomas) įtraukia į papildymo eilę, kurią naudoja automatinis papildymo procesas.

7.15. Apsaugos įrodymų papildymas

Apsaugos tikslas PDS (ilgą laiką pratęsti skaitmeninių parašų galiojimo būseną) pasiekiamas savalaikiu elektroninių parašų ir elektroninių spaudų papildymu.

Naudojami apsaugos įrodymai yra laiko žymos, patvirtintos tiesiogiai patikimais kvalifikuotų laiko žymų tarnybų sertifikatais, kurie yra įtraukti į laiko žymas. Tai užtikrina, kad pačios laiko žymos papildymui nereikia papildomų validavimo duomenų.

Trūkstami validavimo duomenys surenkami iš karto, kai tik validavimo duomenys yra prieinami (iš karto pasibaigus atidėjimo laikotarpiui). Elektroniniai parašai ir elektroniniai spaudai, kuriems nėra tinkamų validavimo duomenų, nėra apsaugomi. Kvalifikuotų elektroninių parašų ir kvalifikuotų elektroninių spaudų sertifikatų sudarymo įstaigos (kaip kvalifikuoti patikimų paslaugų teikėjai, išduodantys kvalifikuotus sertifikatus) turi užtikrinti, kad kiekvienam tikrintinam sertifikatui būtų prieinami tinkami validavimo duomenys.

Papildymas yra atliekamas ne atskiriems apsaugos įrodymams, o visam skaitmeniniam parašui, įskaitant anksčiau pridėtus apsaugos įrodymus. Todėl apsaugos įrodymų papildymas yra pasiekiamas papildžius skaitmeninį parašą. Kriptografijos stebėsena ir reikalingas papildymo planavimas (išsamiau žr. 7.14 skyrių) užtikrina, kad PDS apsaugos tikslas bus pasiektas.

7.16. Eksporto-importo paketas

MitSoft PSP leidžia abonento atstovui, įvardintam MitSoft PSP ilgalaikės apsaugos paslaugos abonento administratoriumi, pateikti prašymą gauti eksporto-importo paketą (-us), kuriame yra apsaugomi duomenys, įrodymai ir visa informacija, reikalinga

įrodymams validuoti. Eksporto-importo paketo prašymas pateikiamas el. paštu, nurodant kriterijus, kuriais remiantis bus atrenkami apsaugos objektai, įtraukiami į eksporto-importo paketą.

Eksporto-importo paketas nėra šifruojamas ir pristatomas abonento paslaugos administratoriui, naudojant saugų duomenų perdavimo protokolą.

MitSoft PSP saugo visų išleistų eksporto-importo paketų įrašus, įskaitant:

1) įvykio datą;
2) kriterijus, kuriais remiantis buvo pasirinktas apsaugos objektų rinkinys, įtraukiamas į eksporto-importo paketą.

Eksporto-importo paketo struktūra yra apibrėžta atskirame dokumente „Eksporto-importo paketas“ *(angl. „Export-import package”)*.

Galiojanti eksporto-importo paketo apibrėžimo versija yra prieinama abonentams MitSoft PSP repozitoriume.

7.17. Tiekimo grandinė

Žiūrėti [QTS PS] dokumento 7.14 skyrelį.

8. Veiklos ir pranešimų protokolai

8.1. Apsaugos protokolas

Apsaugos protokolas įgyvendinamas naudojant apsaugos profilius ir jų palaikomas tinklinių paslaugų operacijas. Operacijos įgyvendinamos kaip REST tinklinės paslaugos. Yra taikomas tinklinių paslaugų kliento autentifikavimas ir ryšio šifravimas (*angl. Secure Sockets Layer - SSL*). Tik autentifikuoti klientai gali naudoti/iškviesti apsaugos profiliuose nurodytas operacijas

Apsaugos paslaugos yra teikiamos naudojant vieną iš galimų apsaugos profilių – MitSoftQWST ar MitSoftQWOS (žr. 6.4 skyrių). Abu apsaugos profiliai palaiko šią operaciją:

- `RetrieveInfo` (apibrėžta ETSI TS 119 512): leidžia gauti informaciją apie šiuo metu ir anksčiau palaikomus apsaugos profilius.

Apsaugos profilis MitSoftQWST palaiko šias operacijas:

- `Store` (apibrėžta apsaugos profilyje MitSoftQWST): leidžia perduoti elektroninį dokumentą/konteinerį, pasirašytą elektroniniu parašu(-ais)/spaudu(-ais), kartu su papildomais apsaugos paslaugų metaduomenimis tolesnei jo apsaugai ir saugojimui MitSoft apsaugos paslaugose; palaikomi pateikimo duomenų objektai ir jų formatai yra apibrėžti MitSoftQWST profilyje. Jei apsaugos objektas su pateiktu identifikatoriumi jau yra apsaugos paslaugų sistemoje, jis pakeičiamas pateiktu duomenų objektu.
- `Status` (apibrėžta apsaugos profilyje MitSoftQWST): leidžia gauti elektroninio dokumento/konteinerio ir jame esančių saugotinų elektroninių parašų/spaudų esamą būseną.
- `Download` (apibrėžta apsaugos profilyje MitSoftQWST): leidžia parsisiųsti elektroninį dokumentą/konteinerį kartu su jame esančiais elektroniniais parašais/spaudais bei apsaugos įrodymais.
- `Remove` (apibrėžta apsaugos profilyje MitSoftQWST): leidžia pašalinti šiuo metu apsaugomą elektroninį dokumentą/konteinerį kartu su jame esančiais elektroniniais parašais/spaudais ir apsaugos įrodymais; susiję metaduomenys taip pat pašalinami; elektroninio dokumento/konteinerio apsauga turi būti sustabdyta. Atitinkamo pateikimo duomenų objekto MitSoft PSP apsaugos paslaugų sistema nebesaugo.
- `PreservePO` (apibrėžta standarte ETSI TS 119 512): leidžia perduoti elektroninį dokumentą/konteinerį, pasirašytą elektroniniu parašu(-ais)/spaudu(-ais), apsaugos paslaugų sistemai tolesnei jo apsaugai ir saugojimui MitSoft PSP. Palaikomi pateikimo duomenų objektai ir jų formatai yra apibrėžti MitSoftQWST profilyje. Jei apsaugos objektas su pateiktu identifikatoriumi jau yra apsaugos paslaugų sistemoje, jis pakeičiamas pateiktu duomenų objektu.
- `RetrievePO` (apibrėžta standarte ETSI TS 119 512): leidžia gauti elektroninį dokumentą/konteinerį kartu su jame esančiais elektroniniais parašais/spaudais bei apsaugos įrodymais.
- `DeletePO` (apibrėžta standarte ETSI TS 119 512): leidžia ištrinti šiuo metu saugomą elektroninį dokumentą/konteinerį kartu su jame esančiais elektroniniais parašais/spaudais ir apsaugos įrodymais; susiję metaduomenys taip pat pašalinami; elektroninio dokumento/konteinerio apsauga turi būti sustabdyta. Atitinkamo pateikimo duomenų objekto MitSoft PSP apsaugos paslaugų sistema nebesaugo.
- `RetrieveTrace` (apibrėžta standarte ETSI TS 119 512): leidžia gauti elektroninio dokumento/konteinerio ir jame esančių elektroninių

parašų/spaudų audito seką. Audito sekoje pateikiama informacija apie apsaugos veiksmus, atliktus su apsaugos objektu.

- `Search` (apibrėžta standarte ETSI TS 119 512): leidžia ieškoti tarp klientui prieinamų apsaugos objektų.

Apsaugos profilis MitSoftQWOS palaiko šias operacijas:

- `Augment` (apibrėžta apsaugos profilyje MitSoftQWOS): leidžia atlikti pateikto elektroninio dokumento/konteinerio, pasirašyto elektroniniu parašu(-ais)/spaudu(-ais), apsaugos veiksmą; apsaugos veiksmas apima skaitmeninių parašų validavimą ir papildymą; grąžinamas pateiktas elektroninis dokumentas/konteineris su papildytu(-ais) elektroniniu parašu(-ais)/spaudu(-ais) ir juose esančiais apsaugos įrodymais; palaikomi pateikimo duomenų objektai ir jų formatai yra apibrėžti MitSoftQWOS profilyje. Taip pat grąžinama apskaičiuota numatoma įrodymų trukmė ir rekomenduojamas kito papildymo laikas.
- `Download` (apibrėžta apsaugos profilyje MitSoftQWOS): leidžia atsisiųsti elektroninį dokumentą/konteinerį, anksčiau papildytą Augment operacija. Ji naudojama tik efektyviam Augment operacijos rezultatui gauti.
- `PreservePO` (apibrėžta standarte ETSI TS 119 512): leidžia atlikti pateikto elektroninio dokumento/konteinerio, pasirašyto elektroniniu parašu(-ais)/spaudu(-ais), apsaugos veiksmą; apsaugos veiksmas apima skaitmeninių parašų validavimą ir papildymą; grąžinamas pateiktas elektroninis dokumentas/konteineris su papildytu(-ais) elektroniniu parašu(-ais)/spaudu(-ais) ir juose esančiais apsaugos įrodymais; pateikimo duomenų objektai ir jų formatai yra apibrėžti MitSoftQWOS profilyje. Taip pat grąžinama apskaičiuota numatoma įrodymų galiojimo trukmė ir rekomenduojamas kito papildymo laikas.

Išsami informacija apie palaikomas operacijas ir naudojamą apsaugos protokolą yra išsamiai aprašyta apsaugos profilių dokumentuose (nuorodas į dokumentus žr. 6.4 skyriuje).

8.2. Pranešimų protokolas

Netaikoma.

9. Apsaugos procesas

9.1. Apsaugos duomenų ir įrodymų saugojimas

MitSoft PSP saugo pateikimo duomenų objektus visą saugojimo laikotarpį arba iki išreikštinio prašymo juos pašalinti. Apsaugos paslaugoms teikiami apsaugos objektai PSP saugykloje nesaugomi, jei naudojamas apsaugos profilis be saugyklos (WOS). Visi apsaugos įrodymai yra įtraukiami į apsaugos objektus ir saugomi bei ištrinami kartu su apsaugos objektais ir pateikimo duomenų objektais.

Dauguma abonentų turi teisinius įsipareigojimus atlikti savo teisines procedūras prieš fizinį apsaugoto elektroninio dokumento ištrynimą, net ir pasibaigus apsaugos laikotarpiui. Todėl apsaugos objektai saugomi PSP saugykloje, kol juos pašalina abonentas. Abonentinės sutartys tarp PSP ir abonentų apibrėžia tikslią apsaugos objekto ir jo metaduomenų saugojimo tvarką, pasibaigus apsaugos laikotarpiui.

Pasibaigus apsaugos laikotarpiui, jokie apsaugos veiksmai (papildymai) nebebus atliekami.

9.2. Apsaugos įrodymai

Vieninteliai naudojami apsaugos įrodymai yra kvalifikuotos elektroninės laiko žymos, suderintos su toliau nurodytais standartais:

- RFC 3161 Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP) [RFC 3161].
- RFC 5816 ESSCertIDv2 Update for RFC 3161 [RFC 5816].
- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles [EN 319 422].

Naudojamos tik kvalifikuotos elektroninės laiko žymos, kurios atitinka šiuos reikalavimus:

- Tai yra kvalifikuota elektroninė laiko žyma pagal eIDAS reglamentą [eIDAS].
- Tai yra ES kvalifikuotos laiko žymų tarnybos išduota laiko žyma.
- Sertifikatas, naudojamas pasirašyti kvalifikuotą elektroninę laiko žymą, pateikiamas laiko žymoje.
- Sertifikatas, naudojamas pasirašyti kvalifikuotą elektroninę laiko žymą, yra įtrauktas į ES patikimą sąrašą.

Šie reikalavimai užtikrina, kad pačiai laiko žymai validuoti nereikia daugiau papildomų validavimo duomenų.

Kiekvienas apsaugos įrodymas (laiko žyma) yra išsaugomas elektroniniame paraše arba elektroniniame spaude, nes yra įtraukiamas į jį kaip atitinkamas laiko žymos atributas.

9.3. Skaitmeninių parašų apsauga

Skaitmeninių parašų apsauga yra pasiekiama laiku papildant skaitmeninį parašą. Tai atliekama 3 etapais:

- B-T lygmens apsaugos užtikrinimas. Jis atliekamas elektroninio dokumento/konteinerio pateikimo metu, jei skaitmeniniame paraše nėra galiojančios parašo laiko žymos. Gaunama nauja parašo laiko žyma ir įtraukiama į skaitmeninį parašą. Tai yra skaitmeninio parašo egzistavimo iki laiko žymoje nurodyto laiko įrodymas.
- B-LTA lygmens apsaugos užtikrinimas. Tai atliekama iš karto pasibaigus atidėjimo laikotarpiui (arba pateikimo metu, jei atidėjimo laikotarpis jau pasibaigęs), jei trūksta validavimo duomenų ar jų dalies arba visa apimanti

laiko žyma nepateikiama su skaitmeniniu parašu (B-LTA lygmuo nepasiektas). Trūkstami validavimo duomenys surenkami ir įtraukiami į skaitmeninį parašą. Tai užtikrina, kad visi reikalingi validavimo duomenys yra renkami tuo metu, kai jie vis dar yra prieinami ir vis dar tinkami validavimui. Gaunama ir į skaitmeninį parašą įtraukiama nauja archyvinė laiko žyma, apimanti visus skaitmeninio parašo duomenis, validavimo duomenis ir faktiškai pasirašytus duomenis. Tai suteikia validavimo duomenų, anksčiau pridėtų laiko žymų ir faktiškai pasirašytų duomenų egzistavimo įrodymą. Palaikomi saugojimo objektų formatai užtikrina, kad archyvinė laiko žyma tiesiogiai uždengia pasirašytus duomenis, net jei naudojami atskirtieji parašai.

- B-LTA lygmens apsaugos užtikrinimas. Jis atliekamas, kai priežiūros procesas iššaukia apsaugos įvykį (žr. 7.14 skyrelį). Nauja archyvinė laiko žyma gaunama ir įtraukiama į skaitmeninį parašą. Tai suteikia naują anksčiau pridėtų laiko žymų, validavimo duomenų, pasirašytų duomenų egzistavimo įrodymą ir apsaugą nuo sertifikato galiojimo pabaigos bei naudojamų kriptografinių algoritmų galimo pasenimo ateityje.

Skaitmeninio parašo papildymas (ir validavimas) grindžiamas standartu ETSI EN 319 102-1 Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation [EN 319 102-1] ir atliekamas pagal MitSoft PSP parašo validavimo taisykles.

Palaikomi apsaugos objektų formatai užtikrina, kad pasirašyti duomenys bus teikiami apsaugos paslaugų sistemai kartu su skaitmeniniu parašu. MitSoft PSP nepalaiko atskirtųjų parašų, kuriuose yra tik pasirašytų duomenų santraukos (be pačių pasirašytų duomenų).

A priedas (norminis). Kvalifikuota apsaugos paslauga kvalifikuotiems elektroniniams parašams (QES), kaip apibrėžta Reglamento (ES) Nr. 910/2014 34 straipsnyje

MitSoft PSP atitinka 2025 m. rugsėjo 29 d. Komisijos įgyvendinimo reglamento (ES) 2025/1946, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 taikymo taisyklės dėl kvalifikuotų apsaugos paslaugų, reikalavimus:

a) apsaugos paslauga saugo visą informaciją, reikalingą elektroninio parašo ar elektroninio spaudo kvalifikuotam statusui patikrinti, kuri kitu atveju nebūtų viešai prieinama iki saugojimo laikotarpio pabaigos;

b) apsaugos procesas ir taikomos parašo taisyklės (žr. 6.6 skyrių) užtikrina, kad bet kuriuo saugojimo laikotarpio metu saugoma informacija būtų tokia, jog, ją pateikus kaip įvesties duomenis procesui, nurodytam standarte ETSI TS 119 172-4, šio proceso rezultatas aiškiai parodytų, ar skaitmeninis parašas arba spaudas jo išsaugojimo metu buvo techniškai tinkamas įgyvendinti ES kvalifikuotą elektroninį parašą arba ES kvalifikuotą elektroninį spaudą.

c) Visos apsaugos įrodymuose naudojamos laiko žymos yra kvalifikuotos laiko žymos pagal Reglamentą (ES) Nr. 910/2014 (išsamesnė informacija 9.2 skyriuje).