

Kvalifikuotos ilgalaikės apsaugos paslaugos

Veiklos nuostatai

QLPS/PS-LT

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

Versija 1.12

Galioja nuo 2023-05-15

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

Dokumento patvirtinimas

	Vardas Pavardė	Data	Parašas
Peržiūrėjo	Saulius Ragaišis	2023-04-05	
Patvirtino	Antanas Mitašiūnas	2023-05-15	

Turinys

1. IVADAS.....	5
1.1. Apžvalga	5
1.2. Identifikacija	5
1.3. Apsaugos paslaugų naudotojai ir taikymo sritis.....	6
1.4. Atitiktis. Validavimas ir patikrinimas	6
1.5. Kontaktiniai duomenys	6
2. Nuorodos.....	7
3. Sąvokų ir santrumpų apibrėžimas	8
4. MitSoft PSP: Bendrosios sąvokos.....	11
4.1. Apsaugos paslaugų funkciniai tikslai	11
4.2. Apsaugos saugyklų modeliai.....	11
4.2.1. Apsaugos paslauga su saugykla (WST)	12
4.2.1.1 Architektūra.....	12
4.2.1.2 MitSoft apsaugos paslaugų darbų seka	12
4.2.2. Apsaugos paslauga be saugyklos (WOS).....	14
4.2.2.1 Architektūra.....	14
4.2.2.2 MitSoft apsaugos paslaugų darbų seka	15
5. Rizikos vertinimas	17
6. TAISYKLĖS IR PRAKTIKOS	18
6.1. Apsaugos paslaugų veiklos nuostatai	18
6.1.1. PSP įsipareigojimai	19
6.2. Paslaugų teikimo sąlygos.....	20
6.3. Informacijos saugumo taisyklės	21
6.4. Apsaugos profilis	21
6.5. Apsaugos įrodymų taisyklės.....	22
6.6. Parašo validavimo taisyklės	22
6.7. Abonentinė sutartis.....	22
7. PSP VALDYMAS IR VEIKIMAS	23
7.1. Vidinė organizacija	23
7.1.1. Organizacijos patikimumas	23
7.1.2. Pareigų atskyrimas	23
7.2. Žmogiškieji ištekliai.....	23
7.3. Turto valdymas.....	24
7.4. Prieigos kontrolė	24
7.5. Kriptografinis valdymas	25
7.6. Fizinis ir aplinkos saugumas	25
7.7. Veiklos saugumas	26

7.8. Tinklo saugumas	27
7.9. Incidentų valdymas.....	28
7.10. Įrodymų surinkimas	28
7.11. Veiklos tęstinumo valdymas	29
7.12. PSP veiklos užbaigimas ir užbaigimo planai	29
7.13. Atitiktis	30
7.14. Kriptografijos stebėseną.....	30
7.15. Apsaugos įrodymų papildymas	32
7.16. Eksporto-importo paketas	33
8. Veiklos ir pranešimų protokolai	34
8.1. Apsaugos protokolas.....	34
8.2. Pranešimų protokolas.....	35
9. Apsaugos procesas	36
9.1. Apsaugos duomenų ir įrodymų saugojimas.....	36
9.2. Apsaugos įrodymai.....	36
9.3. Skaitmeninių parašų apsauga.....	36

1. IVADAS

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/>.

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 PSPS: *angl. Preservation Service Practice Statement*).

Veiklos nuostatai remiasi šiais teisės aktais ir norminiais dokumentais:

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

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

Pastaba dėl sutrumpinimų apibrėžimų. Kvalifikuotos 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; PSPS reiškia MitSoft PSPS, ir taip toliau, t.y. viskas, kas yra sakoma, taikoma tik MitSoft PSP.

1.2. Identifikacija

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

1 lentelė. PSPS 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
MitSoft padalinys	1
Dokumento tipas (Veiklos nuostatai)	4
Dokumento versija	1

PSPS 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 PSPS 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 uždaroje 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 PSPS 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:	+370-5-2333922
Faksas:	+370-5-2136191
URL:	http://www.mitsoft.lt/
E-paštas:	info@mitsoft.lt

2. Nuorodos

- [eIDAS] – Europos Parlamento ir Tarybos Reglamentu (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB.
- [EN 319 102-1] – 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 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 Infrastructures (ESI); Cryptographic Suites" standard.
- [TS 119 511] – 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".
- [TS 119 512] – ETSI TS 119 512: "Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services".

3. Sąvokų ir santrumpų apibrėžimas

Abonentas: juridinis ar fizinis asmuo, turintis sutartinius abonto 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, kuri 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 kvalifikuotos 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, kurie susieja kitus elektroninius duomenis su tam tikru laiku, nustatant įrodymą, kad tie duomenys egzistavo nurodytu laiku (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 taikomiesiems 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*)
- QPSP** – Kvalifikuotų apsaugos paslaugų taisyklės 0.4.0.19511.1.2 (*Qualified Preservation Service Policy*)
- POC** – Apsaugos objekto konteineris (*Preservation Object Container*)
- PS** – Kvalifikuota ilgalaikės apsaugos paslauga (*Qualified long-term Preservation Service*)
- PSP** – Apsaugos paslaugų teikėjas (*Preservation Service Provider*)
- PSPS** – Kvalifikuotų ilgalaikės apsaugos paslaugų veiklos nuostatai (*Qualified long-term Preservation Service Practice Statement*)
- 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 apibrėžimas 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 funkcinį 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 apibrėžimas 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.

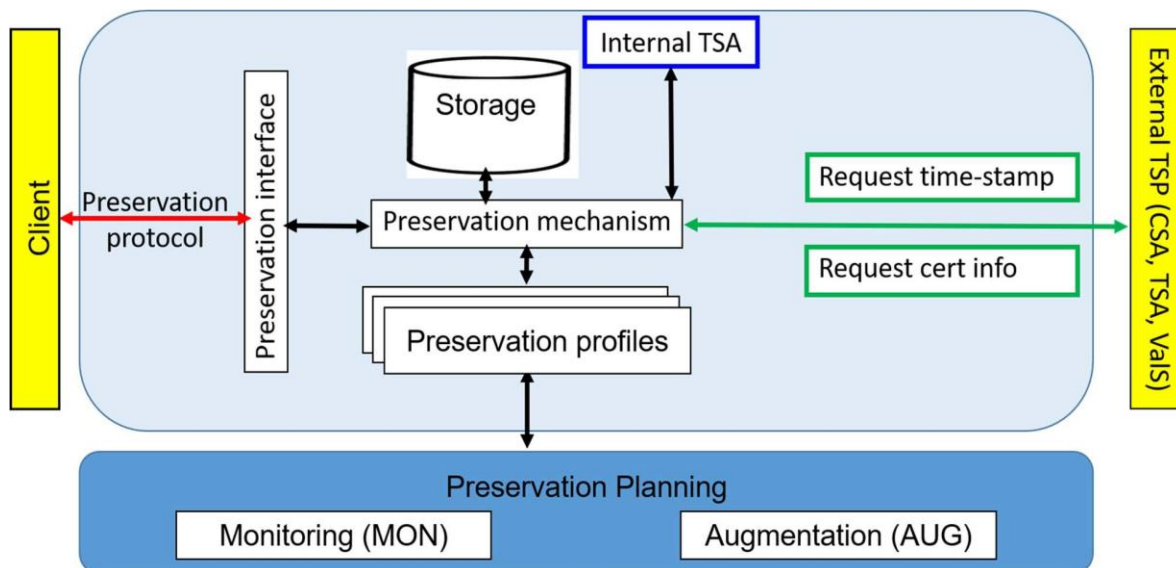
MitSoft PSP naudoja apsaugos saugyklos modelį WST tam, kad galėtų suteikti maksimalią apsaugos paslaugų apimtį apsaugos paslaugos teikėjo pastangomis. Naudojant apsaugos saugyklos modelį WST, apsaugos kliento veiksmai yra apriboti pateikimo duomenų objektų pateikimu ir, kai reikalinga, gavimu pateiktų 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].

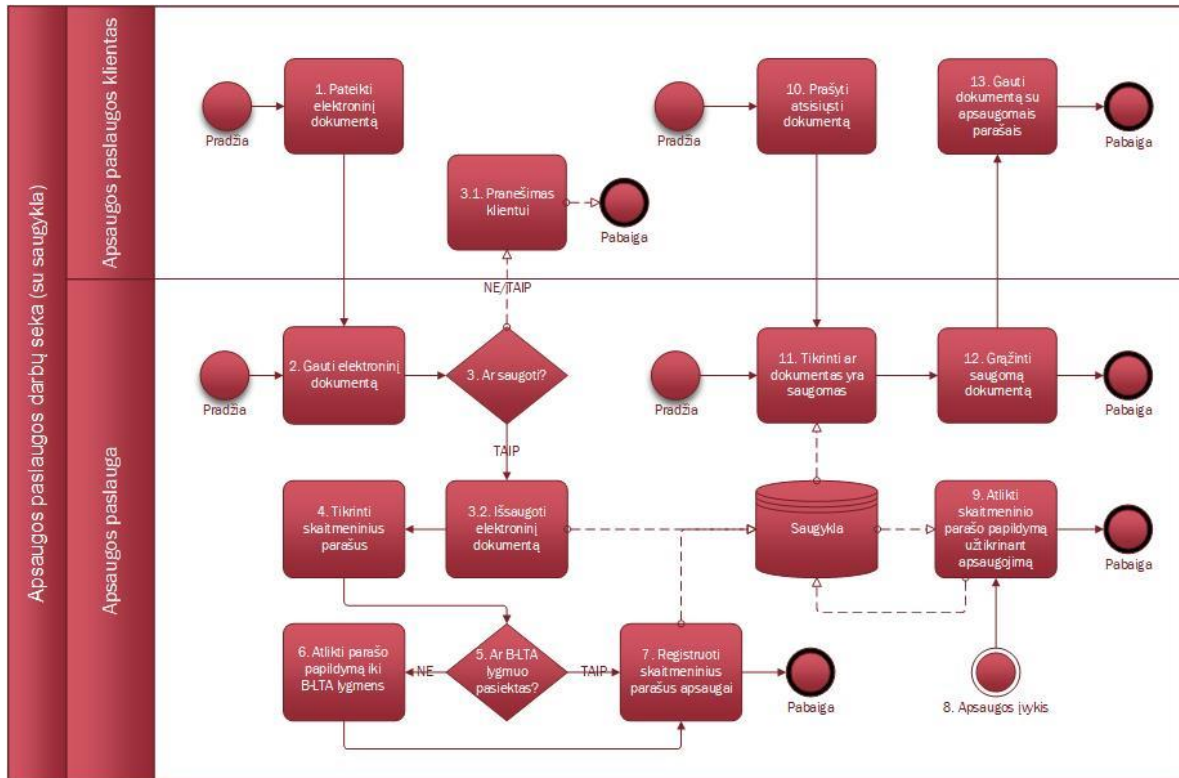


1 pav. Apsaugos paslaugos su saugykla (WST) bendroji architektūra

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 paslaugose su saugykla yra pateikta 2 paveikslėlyje.



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

1. Apsaugos klientas pateikia elektroninį dokumentą/konteinerį apsaugos paslaugoms.
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 paslaugų 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 elektrinius spaudus.
5. Apsaugos paslauga tikrina, ar kiekvienas saugotinas elektroninis parašas ir elektrinis spaudas jau pasiekė B-LTA lygmenį (ar atitinkamą archyvinį parašo formatą parašams, kurie nėra baziniai parašai).
6. Apsaugos paslauga atlieka elektroninių parašų ir elektrinių 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 elektrinius parašus ir elektrinius spaudus, esančius elektriniame dokumente/konteineryje tolesnei apsaugai. Kiekviename registruotame apsaugai skaitmeniniame paraše yra surenkami ir išsaugomi papildomi apsaugos metaduomenys. Apsaugai nebus registruojami elektriniai parašai ir/ar elektriniai 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 paslaugos 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.

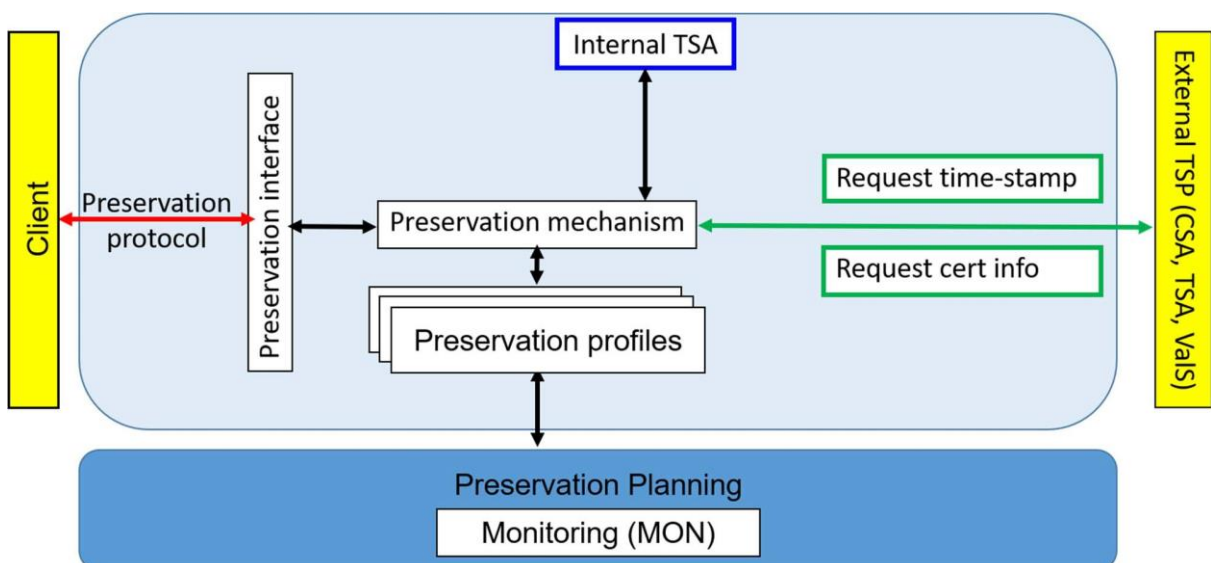
Validavimas yra atliekamas kiekvienam elektroniniame dokumente/konteineryje esančiam elektroniniam parašui ir elektroniniam spaudui.

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].

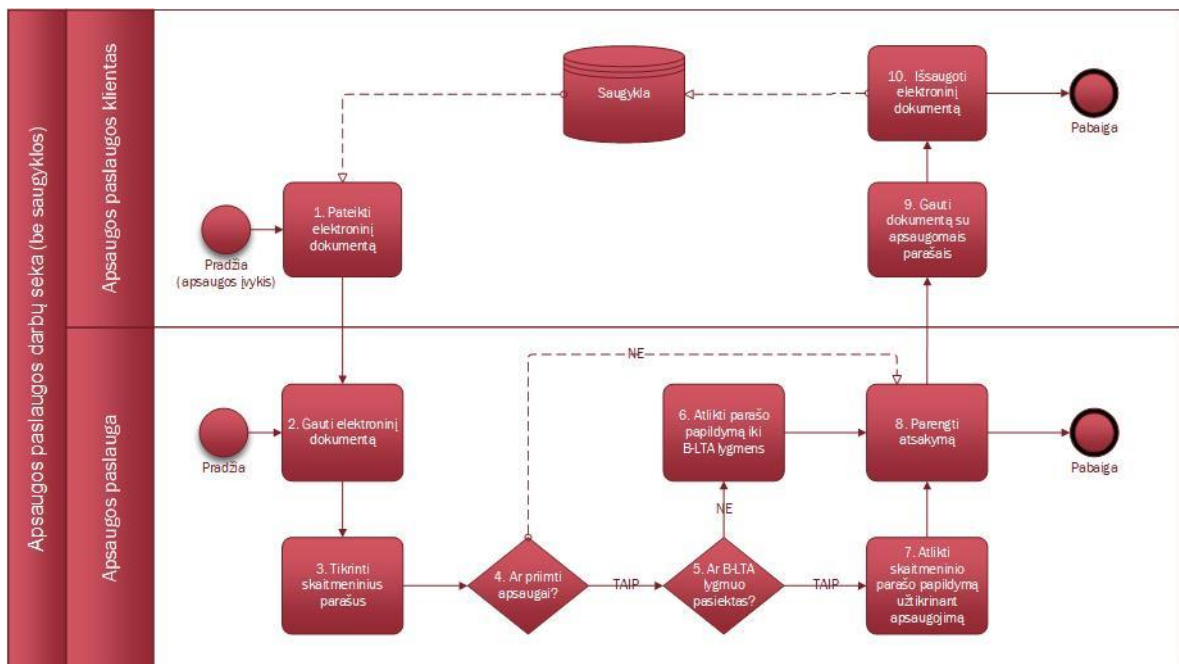


3 pav. Apsaugos paslaugos be saugyklos (WOS) bendroji architektūra

4.2.2.2 MitSoft apsaugos paslaugų darbų seka

MitSoft kvalifikuota ilgalaikės apsaugos paslaugos be saugyklos gauna elektroninį dokumentą ar konteinerį iš apsaugos kliento. Gavusi elektroninį dokumentą ar konteinerį, apsaugos paslaugos 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 gražinamas apsaugos klientui. Nei elektroninis dokumentas/konteineris, nei elektroniniai parašai /spaudai nėra išsaugomi jokiaje 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 paslaugose be saugyklos (WOS)

1. Apsaugos klientas pateikia elektroninį dokumentą/konteinerį apsaugos paslaugoms, 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 paslaugos.
2. Apsaugos paslaugos priima apsaugai elektroninį dokumentą/konteinerį, turintį bent vieną elektroninį parašą arba elektroninį spaudą.
3. Apsaugos paslaugos validuoja elektroninį dokumentą/konteinerį ir jame esančius elektroninius parašus ir elektroninius spaudus.
4. Apsaugos paslaugos tikrina, ar reikia apsaugoti elektroninį dokumentą/konteinerį ir elektroninius parašus bei elektroninius spaudus.
5. Apsaugos paslaugos 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 paslaugos 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 paslaugos 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, pridėdant 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 paslaugos paruošia atsakymą klientui. Apsaugos paslaugos 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 gražinama atmetimo ar triukio priežastis.
9. Apsaugos klientas gauna atnaujintą elektroninį dokumentą/konteinerį iš apsaugos paslaugų. 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

MitSoft PSP atlieka rizikos vertinimą tam, kad identifikuotų, analizuotų ir vertintų grėsmes veiklos turtui, atsižvelgdama į verslo ir techninius aspektus. Remiantis rizikos vertinimo rezultatais, pasirenkamos tinkamos rizikos mažinimo priemonės, kurios užtikrina, kad saugumo lygis atitiktų rizikos laipsnį.

PSP nustato visus saugumo reikalavimus ir veiklos procedūras, kurios yra būtinos įgyvendinant pasirinktas rizikos mažinimo priemones, kaip dokumentuota „Informacijos saugumo taisyklėse“ ir šiuose Apsaugos paslaugų veiklos nuostatuose PSPS.

Rizikos vertinimą patvirtina ir liekamąją riziką priima MitSoft direktorius.

PSP reguliariai (bent kartą metuose) peržiūri ir patikslina rizikos vertinimą.

6. TAISYKLĖS IR PRAKTIKOS

6.1. Apsaugos paslaugų veiklos nuostatai

MitSoft PSP užtikrina ir demonstruoja būtina patikimumą, teikiant kvalifikuotas ilgalaikės apsaugos paslaugas. Ypač:

- a) Praktikos ir procedūros, naudojamos įgyvendinti Kvalifikuotų apsaugos paslaugų taisyklėse QPSP ir šiuose Apsaugos paslaugų veiklos nuostatuose PPSPS 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 elektroninį dokumentą ar konteinerį, talpinantį elektroninius parašus ir/ar elektroninius spaudus (apsaugos objektus) su apsaugos paslaugos įterptais apsaugos įrodymais (laiko žymomis). POC yra sudarytas iš SubDO, tinkamu laiku papildant saugomus skaitmeninius parašus, apsaugos įrodymais (laiko žymomis). Apsaugos profilyje apibrėžtos operacijos priima ir gražina 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. daugiau dokumento „Apsaugos profilis su saugykla“ 4.8 skyrelį.
- c) MitSoft PPSPS identifikuoja visų išorinių organizacijų, palaikančių PSP 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.

Pagal paslaugų sutartį duomenų centras Rackray teikia MitSoft PSP kvalifikuotų ilgalaikės apsaugos paslaugų sistemai infrastruktūros paslaugas. Rackray yra ISO 27001 sertifikuotas ir TIER3 Facility sertifikuotas duomenų centras.

Duomenų centras Interneto vizija pagal sutartį teikia dedikuoto serverio paslaugas MitSoft PSP apsaugomų elektroninių dokumentų ir duomenų nutolintų atsarginių kopijų kaupimui pagal sutartyje numatytas sąlygas.
- d) PPSPS ir kita dokumentacija, reikalinga įvertinti paslaugos atitiktį QPSP, yra prieinama paslaugos abonentams ir pasikliaujančioms šalims MitSoft PSP svetainėje ir pateikiama pagal paklausimą.
- e) MitSoft direktorius yra atsakingas už PSP veiklą su galutine teise patvirtinti PPSPS.
- f) MitSoft direktorius užtikrina praktikų įgyvendinimą, pavesdamas tai tinkamam PSP personalui.
- g) MitSoft PSP turi Praktikų peržiūros procesą, apimant PPSPS priežiūrą.

- h) PSP tinkamai praneša apie ketinamus atlikti PSPS pakeitimus ir, juos patvirtinus pagal punktą e), pakeistą PSPS nedelsiant paskelbia, kaip tai reikalaujama pagal punktą d).
- i) Apsaugos paslaugų veiklos užbaigimo nuostatos yra pateiktos 7.12 skyrelyje „PSP veiklos užbaigimas ir užbaigimo planai“.

QPSP yra vienintelės MitSoft PSP palaikomos apsaugos paslaugų taisyklės:

- a) Santraukos algoritmai, kurie gali būti panaudoti duomenims su laiko žyma sudaryti, yra specifikuoti 7.14 skyrelyje „Kriptografinė stebėseną“.
- 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 ilgalaikės elektroninių parašų ir elektroninių spaudų apsaugos paslaugas pagal funkciją tikslą: skaitmeninių parašų apsauga (*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 PSPS, 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

PSP priima abonentų pretenzijas, kaip tai yra nurodyta skelbiamose Paslaugų teikimo sąlygose.

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

PSP atsakomybė ir įsipareigojimai yra apibrėžti paslaugų teikimo Abonentinėje sutartyje.

6.1.1.6. Teisinės nuostatos ir interpretacijos

6.1.1.6.1. Pagrindiniai teisiniai aktai

Ilgalaikės apsaugos įrodymų generavimas, jų teikimas, reikalavimai teikėjams ir atsakomybė yra reguliuojami teisės aktais:

- a) Europos Parlamento ir Tarybos Reglamente (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB.
- b) Lietuvos Respublikos Elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymas, 2018 m. balandžio 26 d. Nr. XIII-1120.
- c) Dėl Kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų ir kvalifikuotų patikimumo užtikrinimo paslaugų statuso suteikimo ir jų įrašymo į nacionalinį patikimą sąrašą bei kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų veiklos ataskaitų teikimo tvarkos aprašo patvirtinimo, Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2018 m. birželio 21 d. įsakymas Nr. 1V-588.
- d) Dėl Pranešimų apie patikimumo užtikrinimo paslaugų saugumo ir (ar) vientisumo pažeidimus teikimo tvarkos aprašo patvirtinimo (Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2019 m. birželio 4 d. įsakymas Nr. 1V-594).

6.1.1.6.2. Ginčų sprendimas

Bet kokie ginčai tarp PSP ir galutinių naudotojų yra sprendžiami geranoriškais derybomis. Tuo atveju, jei ginčo išspręsti nepavyksta, yra kreipiamasi į teisėsaugos įstaigas.

6.1.1.7. Mokesčiai

PSP gali nustatyti savo ilgalaikės apsaugos paslaugų kainas.

6.1.1.8. Intelektinės nuosavybės teisės

Cituojant bet kurį PSP dokumentą, yra reikalaujama pateikti nuorodą į šaltinį.

6.2. Paslaugų teikimo sąlygos

PSP skelbia visiems abonentams ir potencialioms pasikliaujančioms šalims kvalifikuotų ilgalaikės apsaugos paslaugų teikimo sąlygas.

Paslaugų teikimo sąlygos specifikuoja:

- a) Taikomas QPSP.
- b) Teikiamų paslaugų naudojimo bet kuriuos apribojimus, įskaitant žalos atlyginimo apribojimus, kylančius iš paslaugų naudojimo viršijant šiuos apribojimus.

- c) Abonentų įsipareigojimus.
- d) Informaciją, kaip patikrinti apsaugos įrodymus ir bet kuriuos susijusius galiojimo laikotarpio apribojimus.
- e) Laikotarpį, kurį yra saugomi PSP įvykių žurnalai.
- f) Atsakomybės apribojimus.
- g) Taikomą teisinę sistemą.
- h) Skundų ir ginčų sprendimo procedūrą.
- i) Ar kvalifikuotų ilgalaikės apsaugos paslaugų atitiktis QPSP buvo įvertinta ir, jeigu taip, tai pagal kokią atitikties įvertinimo schemą.
- j) PSP kontaktinius duomenis.
- k) Bet kokius prieinamumo įsipareigojimus.

Ši informacija yra prieinama MitSoft PSP interneto svetainėje lietuvių ir anglų kalbomis ir gali būti papildyta Abonentinėse sutartyse tarp PSP ir abonentų.

6.3. Informacijos saugumo taisyklės

PSP turi MitSoft direktoriaus patvirtintas informacijos saugumo taisykles, kurios nustato organizacijos informacijos saugumo valdymo metodą.

PSP užtikrina, kad taikomos administracinės ir valdymo procedūros yra adekvačios ir atitinka pripažintą gerąją praktiką. Konfliktuojančios pareigos ir atsakomybės sritys yra atskirtos, siekiant sumažinti galimybes neleistinam ar netyčiam PSP turto modifikavimui ar piktnaudžiavimui.

PSP yra atsakingas už visus kvalifikuotų ilgalaikės apsaugos paslaugų aspektus PSPS apimtyje, nepriklausomai nuo to, ar funkcijos yra perduotos subrangovams ar ne. MitSoft PSP yra atsakingas už visų šalių, dalyvaujančių kvalifikuotų ilgalaikės apsaugos paslaugų teikime, atitinkamų praktikų skelbimą.

Už informacijos saugumo gairių nustatymą, nuolatinę infrastruktūros priežiūrą, dokumentaciją, valdymą ir PSP įrangos, patalpų, sistemų ir informacinio turto saugumo priemonių bei veiklos procedūrų įgyvendinimą, o taip pat informacijos ir kito turto apsaugą yra atsakingas MitSoft direktorius. PSP užtikrina supažindinimą su saugumo gairėmis ir taisyklėmis visų susijusių darbuotojų, kuriems tai yra reikalinga jų darbe.

Įrangos, patalpų, sistemų ir informacinio turto, reikalingų kvalifikuotų ilgalaikės apsaugos paslaugų teikimui, saugumo priemonės ir veiklos procedūros yra dokumentuotos, valdomos ir įgyvendinamos.

Informacijos saugumo infrastruktūra, būtina saugumo užtikrinimui, yra nuolatos prižiūrima. Bet kurie įtakoiantys saugumą pakeitimai yra tvirtinami MitSoft direktoriaus.

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

Profilijų aprašai yra prieinami MitSoft PSP 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.

Saugotinių 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 validavimo 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) yra irgi apsaugos objektai.
- Ar elektroniniai parašai ir elektroniniai spaudai, kurie nėra galiojantys (turintys kitą validavimo statusą nei PASSED), yra irgi 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

PSP laikosi visų praktikų, nurodytų sekančiuose punktuose.

Apsaugos paslaugų teikimas, atsakant į užklausas, yra vykdomas PSP nuožiūra sutinkamai su paslaugų dokumentų ir Abonentinės sutarties nuostatomis.

7.1. Vidinė organizacija

7.1.1. Organizacijos patikimumas

PSP užtikrina, kad MitSoft PSP yra patikima organizacija. Ypač:

- a) PSP yra pagal Lietuvos Respublikos teisę juridinis asmuo, įregistruotas juridinių asmenų registre kaip Uždaroji akcinė bendrovė "MIT-SOFT", įmonės kodas yra 1207920811.
- b) PSP turi kokybės ir informacijos saugumo valdymo sistemą, tinkamą teikiamoms apsaugos paslaugoms.
- c) Ji įdarbinusi pakankamą skaičių darbuotojų, turinčių reikiamą išsilavinimą bei adekvačius mokymus, technines žinias ir patirtį apsaugos paslaugų teikimui.
- d) Taisyklės ir praktikos, pagal kurias PSP veikia, yra paremtos tarptautiniais standartais ir nediskriminuojančios.
- e) PSP paslaugos yra prieinamos visiems naudotojams, kurių veikla patenka į PSP veiklos sritį ir kurie sutinka priimti PSP specifikuotus įsipareigojimus.
- f) PSP turi tinkamas priemones ir resursus, suderinamus su ES Reglamentu Nr. 910/2014 ir nacionaliniais įstatymais, padengti atsakomybei, kylančiai iš jo veiksmų ir veiklos.
- g) PSP turi finansinį stabilumą ir resursus, reikalingus veikti suderinamai su PSPS, įskaitant reikalavimus apsaugos paslaugų teikimo veiklos užbaigimui.
- h) Skundų ir ginčų sprendimo dėl apsaugos paslaugų teikimo ar bet kokiais kitokiais susijusiais klausimais taisyklės ir procedūros yra specifikuotos kaip nustatyta 6.2 skyrelyje „Paslaugų teikimo sąlygos“.
- i) PSP turi dokumentuotus susitarimus ir sutartinius santykius, su paslaugų teikime dalyvaujančiomis trečiosiomis šalimis.

7.1.2. Pareigų atskyrimas

Konfliktuojančios pareigos ir atsakomybės sritys yra atskirtos, kaip tai apibrėžta PSP Informacijos saugumo taisyklėse (žr. 6.3 skyrelį „Informacijos saugumo taisyklės“), siekiant sumažinti galimybes neleistinam ar netyčiam informacijos modifikavimui ar PSP turto piktybiškam naudojimui.

7.2. Žmogiškieji ištekliai

PSP užtikrina, kad personalas ir įdarbinimo praktikos išplečia ir remia PSP veiklos patikimumą. Ypač:

- a) PSP įdarbina asmenis, kurie disponuoja ekspertinėmis žiniomis, patirtimi ir kvalifikacija, būtinomis siūlomoms paslaugoms ir tinkamomis veiklos funkcijoms atlikti.
- b) Darbuotojams, pažeidžiantiems PSP taisykles ir procedūras, yra taikomos drausminės nuobaudos.
- c) Darbuotojų saugumo rolės ir atsakomybės, kaip tai yra nustatyta PSP „Informacijos saugumo taisyklėse“, yra dokumentuotos jų darbo aprašuose. Patikimos rolės, nuo kurių priklauso TSP veikla, yra aiškiai identifikuotos.

- d) PSP darbuotojai (laikini ir pastovūs) turi darbo aprašus, apibrėžtus išeinant iš pareigų atskyrimo ir būtina žinoti principų, nustatant darbo pozicijos jautrumą, remiantis pareigomis ir prieigos lygmenimis, išsilavinimu ir darbuotojo mokymais bei suvokimu. Darbo aprašai apima įgūdžių ir patirties reikalavimus.
- e) Darbuotojai taiko administracines ir valdymo procedūras ir procesus, kurie dera su PSP informacijos saugumo valdymo procedūromis.
- f) PSP įdarbina vadovaujančius darbuotojus, kurie disponuoja:
 - Skaitmeninių parašų kvalifikuotų ilgalaikės apsaugos technologijų žiniomis.
 - Skaitmeninių parašų technologijų žiniomis.
 - Darbuotojų su saugumo atsakomybėmis saugumo procedūrų žinojimu.
 - Informacijos saugumo ir rizikos vertinimo patirtimi.
- g) PSP visi darbuotojai patikimose rolėse neturi interesų konflikto, kuris gali įtakoti PSP veiklos nešališkumą.
- h) Patikimos rolės yra apibrėžtos PSP „Informacijos saugumo taisyklėse“ ir apima roles, įtraukiančias šias atsakomybes:
 - Saugumo pareigūnas: saugumo praktikų įgyvendinimo administravimo bendra atsakomybė.
 - Sistemos administratorius: įgaliotas instaliuoti, konfigūruoti ir prižiūrėti kvalifikuotų ilgalaikės apsaugos paslaugų PSP pasiklojimo sistemą.
 - Sistemos operatorius: atsakingas už PSP pasiklojimo sistemos kasdienį veikimą. Įgaliotas atlikti sistemos atsarginių kopijų išsaugojimą ir atstatymą iš jų.
 - Sistemos auditorius: įgaliotas peržiūrėti PSP pasiklojimo sistemos archyvus ir audito žurnalus.
- i) PSP darbuotojai yra už saugumą atsakingos vadovybės formaliai paskirti atlikti patikimas roles.
- j) Darbuotojai neturi prieigos prie patikimų funkcijų tol, kol nebus atlikti būtini patikrinimai.

MitSoft direktorius yra atsakingas už įdarbinimą darbuotojų, tenkinančių visus šiuos reikalavimus, o taip pat už jų įgūdžių ir patikimumo patikrinimą, darbuotojų rolių apibrėžimą ir aprašymą (įskaitant patikimas funkcijas) jų darbo aprašuose.

Visi darbuotojai gali atlikti tik jų rolėse numatytas veiklas.

7.3. Turto valdymas

PSP užtikrina, kad informacija ir kitas turtas yra tinkamai apsaugoti. Visų pirma, PSP prižiūri viso turto sąrašą ir priskiria šiam turtui klasifikuotus apsaugos reikalavimus sutinkamai su rizikos analize.

Visi informacijos nešėjai yra tvarkomi saugiai pagal informacijos klasifikavimo schemas reikalavimus. Informacijos nešėjai, turintys jautrius duomenis, yra saugiai sunaikinami, kai tampa nebereikalingais.

7.4. Prieigos kontrolė

PSP užtikrina, kad PSP sistemos prieiga yra apribota tik tinkamai įgaliotiems asmenims. Konkrečiai:

- a) Ugniasienė yra naudojama apsaugoti PSP vidinio tinklo sritis nuo neleistinos prieigos, įskaitant abonentų ir trečiųjų šalių prieigą. Ugniasienė yra sukonfigūruota drausti visus nebūtinus PSP veiklai protokolus ir prieigą. Techninis sprendimas yra pateiktas PSP dokumente „Sistemos architektūra ir valdymas“ (angl. „System architecture and management“).

- b) PSP užtikrina efektyvų administravimą naudotojų prieigos, reikalingos operatorių, administratorių ir auditorių darbui. Tokiu būdu palaikomas sistemos saugumas, įskaitant MitSoft PSP naudotojų paskyrų valdymą, auditą ir savalaikį prieigos modifikavimą arba pašalinimą .
- c) Prieiga prie informacijos ir taikomosios sistemos funkcijų yra apribota sutinkamai su prieigos valdymo taisyklėmis, ir PSP sistema užtikrina pakankamą saugumo kontrolę PSP identifikuotų patikimų rolių atskyrimui, įskaitant saugumo administravimo ir eksploatavimo funkcijų atskyrimą. Ypač, yra apribotas ir pilnai kontroliuojamas sistemos tarnybinių programų (utilitų) naudojimas.
- d) PSP darbuotojai yra tinkamai identifikuojami ir autentifikuojami prieš naudojant kritines programas, susijusias su kvalifikuota ilgalaikė apsauga.
- e) PSP darbuotojai yra atskaitingi už savo veiklą; šiuo tikslų, įvykių žurnalai yra išsaugomi (žr. 7.10 skyrelį „Įrodymų surinkimas“).
- f) Jautrūs duomenys yra apsaugoti nuo atskleidimo per pakartotinai naudojamus saugojimo objektus (pvz., pašalintus failus), kurie tampa prieinami neįgalotiems naudotojams.

Kvalifikuotų ilgalaikės apsaugos paslaugų pakankamą saugumo kontrolę užtikrina:

- a) Lokalaus tinklo komponentės (pvz., maršrutizatoriai) yra saugomi saugioje fizinėje aplinkoje ir jų konfigūracija yra periodiškai audituojama PSP specifiškai reikalavimų atitikimui.
- b) Naudojama nuolatinė stebėseną ir signalizacijos įrenginiai, siekiant įgalinti PSP aptikti, registruoti ir laiku reaguoti į bet kokius neleistinus ir/ar neteisėtus prieigos prie resursų mėginimus.

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, kuris laikosi patikimų paslaugų teikėjų, sudarančių kvalifikuotas laiko žymas, taisyklių ir saugumo reikalavimų, geriausios praktikos.

7.6. Fizinis ir aplinkos saugumas

PSP užtikrina, kad fizinė prieiga prie kritinių paslaugų yra kontroliuojama ir fizinė prieiga turtui yra minimizuota. Konkrečiai:

- a) Kvalifikuotoms ilgalaikės apsaugos paslaugoms:
 - Fizinė prieiga prie kvalifikuotų ilgalaikės apsaugos paslaugų yra apribota tik tinkamai autorizuotiems asmenims.
 - Apsaugos priemonės yra įgyvendintos, siekiant išvengti turto praradimo, pažeidimo ar kompromitavimo, informacijos vagystės ar nutekėjimo, verslo veiklą pertraukimo.
 - Apsaugos priemonės yra įgyvendintos, siekiant išvengti informacijos ir informacijos apdorojimo įrangos kompromitavimo ar vagystės.
- b) Be to, kvalifikuotoms ilgalaikės apsaugos paslaugoms yra taikomos šios papildomos apsaugos priemonės:
 - Kvalifikuotų ilgalaikės apsaugos paslaugų įrenginiai veikia aplinkoje, kuri fiziškai apsaugo paslaugas nuo kompromitavimo per neleistiną prieigą prie sistemos ar duomenų.

- Fizinė apsauga yra pasiekama sukūrus aiškiai apibrėžtą kvalifikuotų ilgalaikės apsaugos paslaugų saugumo perimetrą. Šio perimetro viduje nėra patalpų, kuriomis dalinamasi su kitomis organizacijomis.
- Fizinio ir aplinkos saugumo apsaugos priemonės yra įgyvendintos, siekiant apsaugoti sistemos resursų įrenginius, pačius sistemos resursus ir įrenginius, palaikančius jų veikimą. Kvalifikuotų ilgalaikės apsaugos paslaugų sistemos fizinio ir aplinkos saugumo taisyklės apima fizinę prieigos kontrolę, apsaugą nuo gamtinių nelaimių, priešgaisrinės saugos faktorius, palaikančių komunalinių paslaugų (elektros maitinimas, telekomunikacijos) trikius, struktūros griuvimą, vandentiekio nuotėkį, apsaugą nuo vagystės, įsilaužimą, atkūrimą nelaimės atveju.
- Apsaugos priemonės yra įgyvendintos, apsaugant ilgalaikės apsaugos paslaugų įrangą, informaciją, nešėjus, programinę įrangą nuo išnešimo be leidimo.

PSP kvalifikuotų ilgalaikės apsaugos paslaugų įrangą veikia duomenų centre (DC). Tuo pačiu duomenų centro viduje yra apibrėžtas saugumo perimetras, į kurio vidų prieiga nėra galima. Duomenų centro pastatas yra saugomas apsauginių ir saugumo tarnybos. Tokiu būdu, PSP turtas, įskaitant informacijos nešėjus, yra apsaugotas nuo neleistino paėmimo ar kompromitavimo.

Duomenų centre veikia moderni oro kondicionavimo sistema, kuri palaiko reikiamą oro temperatūrą ir valo orą nuo dulkių. Jeigu elektros tiekimas sutrinka, UPS ir dyzeliniai elektros srovės generatoriai palaiko normalų sistemos veikimą 4 val.

Tam, kad būtų išvengta kompromitavimo ir informacijos vagystės, yra imtasi šių priemonių: PSP įrangą, interneto ryšys yra apribotas – tik kvalifikuotų ilgalaikės apsaugos paslaugų teikimui būtinas ryšys yra leistinas. Ugniasienės ir įsilaužimo apsaugos sistemos yra įgyvendintos.

7.7. Veiklos saugumas

Kritinėms paslaugoms, kaip identifikuoja rizikos analizė, PSP naudoja pasiklivimo sistemas ir produktus, kurie yra apsaugoti nuo modifikacijų. PSP užtikrina, kad PSP sistemos komponentės yra saugios ir korektiškai veikia su minimalia trikių rizika.

Konkrečiai:

- a) Saugumo integravimo į IT sistemas tikslu saugumo reikalavimų analizė yra atlikta PSP sistemos kūrimo projekto reikalavimų specifikavimo ir projektavimo etapų metu.
- b) Pakeitimų valdymo procedūros yra taikomos visoms operacinės programinės įrangos laidoms, modifikacijoms ir atsirandantiems programinės įrangos pataisymams ir konfigūracijos pakeitimams, kuriems taikomos PSP „Informacijos saugumo taisyklės“, įskaitant konfigūracijos saugumo patikrinimus. Šios procedūros apima pakeitimų dokumentavimą. Maksimalus intervalas tarp dviejų konfigūracijos saugumo patikrinimų neviršija 12 mėnesių.
- c) PSP sistemos komponentių ir informacijos integralumas yra apsaugotas nuo virusų, kenkėjiškos ir neleistinos programinės įrangos, įdiegtos antivirusinės programinės įrangos pagalba.
- d) PSP pasiklivimo sistemoje naudojami informacijos nešėjai yra saugiai tvarkomi, siekiant apsaugoti nešėjus nuo pažeidimų, vagystės, neteisėtos prieigos ir senėjimo.
- e) Informacijos nešėjų valdymo procedūros yra naudojamos, siekiant apsaugoti informacijos nešėjus nuo pasenimo ir pablogėjimo per visą laikotarpį, kurį įrašus privaloma saugoti.

- f) Procedūros yra parengtos ir įgyvendintos visoms patikimoms ir administracinėms rolėms, kurios įtakoja ilgalaikės apsaugos paslaugų teikimą.
- g) Saugumo pataisymų valdymo procedūros yra naudojamos, siekiant užtikrinti:
 - saugumo pataisymų panaudojimą per pagrįstą laiko tarpą po to, kai jie tampa prieinami;
 - saugumo pataisymai nėra naudojami, jeigu jie iššaukia naujus pažeidžiamumus ar nestabilumą, kas nusveria jų panaudojimo naudą;
 - saugumo pataisymų nenaudojimo priežastys yra dokumentuotos.
- h) Pajėgumų poreikiai yra stebimi ir numatomi būsimi pajėgumų reikalavimai, siekiant, kad adekvataus dydžio apdorojimo galia ir saugykla būtų prieinami.

7.8. Tinklo saugumas

PSP prižiūri ir apsaugo PSP pasiklojimo sistemą, patalpintą Rackray duomenų centre saugiam vidiniame tinkle ir prieinamą tik patikimų rolų darbuotojams. Tos pačios saugumo priemonės yra taikomos visoms sistemos komponentėms, išdėstytoms saugiam vidiniame tinkle:

- a) PSP segmentuoja apsaugos paslaugų sistemos tinklą, remiantis PSP „Informacijos saugumo taisyklių“ reikalavimais, sutinkamai su funkcinėmis, loginėmis ir fizinėmis komponentių priklausomybėmis, kaip pateikta dokumente „Sistemos architektūra ir valdymas“.
- b) PSP apriboja prieigą ir komunikaciją tik tarp zonų, kurios yra būtinos PSP veikimui.
- c) PSP sistemos konfigūracija yra sugriežtinta taip, kad tik būtinos paskyros, programos, paslaugos, protokolai ir portai yra naudojami.
- d) PSP „Informacijos saugumo taisyklės“ identifikuoja patikimas paslaugas ir priskiria atitinkamas atsakomybes tinkle saugumo praktikų įgyvendinimui. PSP reguliariai peržiūri nustatytą saugumo taisyklių aibę.
- e) PSP talpina saugiose zonose visas PSP veikimui kritines posistemes, kaip tai nurodyta dokumente „Sistemos architektūra ir valdymas“.
- f) PSP atskiria IT sistemų administravimui dedikuotą tinklą nuo PSP veiklos saugaus vidinio tinklo.
- g) PSP nenaudoja saugumo taisyklių administravimo sistemų kita paskirtimi.
- h) PSP atskiria PSP paslaugų gamybinę sistemos aplinką nuo kūrimo ir testavimo sistemų aplinkų. Kūrimo ir testavimo sistemos yra patalpintos MitSoft patalpose ir įrenginiuose.
- i) Pagal dokumentą „Sistemos architektūra ir valdymas“ PSP nustato komunikavimą tarp skirtingų posistemių tik patikimais kanalais, kurie yra logiškai skirtingi nuo kitų komunikavimo kanalų ir užtikrina kanalų galinių taškų saugų identifikavimą ir kanalo duomenų apsaugą nuo modifikavimo ir atskleidimo.
- j) Aukštas išorinės prieigos pasiekiamumo lygis prie apsaugos paslaugų nėra reikalaujamas.
- k) PSP atlieka PSP identifikuotų viešų ir privačių IP adresų pažeidžiamumo skenavimą.
- l) PSP atlieka įsiskverbimo į PSP sistemą testavimą, įdiegus PSP sistemą ir po infrastruktūros ar programų atnaujinimo ar modifikavimo, kurie PSP vertinimu yra reikšmingi.
- m) PSP pateikia įrodymus, kad pažeidžiamumo skenavimą ir įsiskverbimo testavimą atliko asmenys, turintys įgūdžius, įrankius, patyrimą ir nepriklausomumą, būtinus patikimos ataskaitos pateikimui.

- n) 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.

7.9. Incidentų valdymas

PSP nuolat stebi prieigos prie PSP paslaugų sistemos ir jos naudojimo veiklas:

- a) Stebėsenos veiklos analizuoja sistemos būseną ir renka techninę informaciją, kuri yra riboto naudojimo pagal MitSoft PSP informacijos klasifikavimo schemą ir yra prieinama tik asmenims patikimose rolėse su saugumo įsipareigojimais.
- b) Nenormalus sistemos veikimas, kuris indikuoja potencialius saugumo pažeidimus, įskaitant galimą įsilaužimą, yra aptinkamas ir pranešamas kaip pavojaus signalas, remiantis stebėsenos funkcionalumu ir sistemos administratoriaus bei sistemos operatoriaus įsipareigojimais.
- c) Stebėseną apima įvykių įrašų registravimo funkcijų darbo pradžią ir pabaigą bei reikiamų paslaugų PSP tinkle prieinamumą ir naudojimą.
- d) PSP veikia savalaikiai ir koordinuotai tam, kad greitai reaguotų į incidentą ir apribotų saugumo pažeidimo poveikį, kaip tai aprašyta „Incidentų valdymo procedūroje“.
- e) PSP pareigybių aprašuose priskiria sistemos administratoriaus patikimos rolės darbuotojams sekimą įspėjimų apie potencialiai kritinius saugumo įvykius ir užtikrinimą, kad apie atitinkamus incidentus būtų pranešama pagal PSP procedūras.
- f) PSP nustato atitinkamų šalių informavimo procedūras pagal taikomas taisykles apie bet kokį saugumo pažeidimą ar integralumo praradimą, kuris turi reikšmingą poveikį patikimų paslaugų teikimui ir saugomiems asmens duomenims per 24 val. nuo pažeidimo identifikavimo.
- g) PSP pagal „Incidentų valdymo procedūrą“ praneša fiziniams ar juridiniams asmenims apie saugumo pažeidimą ar integralumo praradimą be nepagrįsto delsimo, kai saugumo pažeidimas ar integralumo praradimas gali turėti neigiamos įtakos fiziniam ar juridiniam asmeniui, kuriam patikimos paslaugos buvo teikiamos.
- h) PSP sistema yra stebima, įskaitant stebėseną ar reguliarią audito žurnalų peržiūrą, siekiant identifikuoti kenkėjiškos veiklos požymius. PSP įgyvendina automatinius audito žurnalų apdorojimo mechanizmus, kad įspėtų darbuotojus apie galimus kritinius saugumo įvykius. Sistemos auditorius veikia sutinkamai su „Sistemos audito procedūra“.
- i) PSP eliminuoja bet kurį naują kritinį pažeidžiamumą per 48 valandas nuo jo atradimo.
- j) Bet kuriam pažeidžiamumui PSP nustato potencialaus poveikio kainą ir ja remiantis sudaro ir įgyvendina pažeidžiamumo švelninimo planą ar dokumentuoja faktinį pagrindą, kad pažeidžiamumas nereikalauja ištaisymo.
- k) Incidentų pranešimo ir reagavimo procedūros yra taikomos tokiu būdu, kad saugumo incidentų žala ir veikimo sutrikimai būtų minimizuoti.

7.10. Įrodymų surinkimas

PSP užtikrina, kad atitinkama informacija apie ilgalaikės apsaugos paslaugų veikimą yra užrašoma ir saugoma tinkamą laiko tarpą su tikslu pateikti įrodymus teisiniuose nagrinėjimuose. Konkrečiai:

- a) Specifiniai įvykiai ir duomenys, kurie turi būti registruojami, yra dokumentuoti PSP „Informacijos saugumo taisyklėse“, įskaitant klientų kreipinius į operacijų API, paslaugų operacijas ir naudotojų interaktyvius veiksmus.

- b) Einamųjų ir archyvinių įrašų apie ilgalaikės apsaugos paslaugų veiksmus konfidencialumas ir integralumas yra palaikomas.
- c) Įrašai apie kvalifikuotų ilgalaikės apsaugos paslaugų veikimą yra pilnai ir konfidencialiai archyvuojami pagal PSP skelbiamas praktikas.
- d) Įrašai apie kvalifikuotų ilgalaikės apsaugos paslaugų veikimą yra prieinami, jei reikalaujama kvalifikuotų ilgalaikės apsaugos paslaugų korektiško veikimo įrodymo pateikimo teisiniam nagrinėjimui.
- e) Tikslus laikas, kada buvo atliekamas laikrodžio patikslinimas, viršijantis 1 sekundę, yra registruojamas. Laikas, naudojamas fiksuoti įvykius audito žurnaluose, yra sinchronizuojamas su UTC bent kartą per dieną.
- f) Įrašai apie kvalifikuotas ilgalaikės apsaugos paslaugas yra saugomi laiką, tinkamą pateikti būtinus teisinius įrodymus, kaip skelbiama PSP „Paslaugų teikimo sąlygose“.
- g) Įvykiai yra registruojami žurnaluose tokiu būdu, kad negalėtų būti lengvai panaikinti ar sugadinti (išskyrus, kai jie patikimai perduoti į ilgalaikio saugojimo informacijos laikmenas) reikalaujamą išlaikyti laiko tarpą.
- h) Bet kuri apie abonentus išsaugota informacija yra laikoma konfidencialia, išskyrus atvejus, kai gaunamas abonto sutikimas jos platesniam skelbimui.

7.11. Veiklos tęstinumo valdymas

PSP turi atnaujinamą veiklos tęstinumo planą, kuris imamas vykdyti nelaimės atveju. Įvykus nelaimei, veikimas atstatomas per tęstinumo plane numatytą terminą, pašalinant nelaimės priežastis, kurios gali pasikartoti (pvz., saugumo pažeidžiamumas), taikant tinkamas ištaisymų priemonėmis.

PSP užtikrina, kad PSP paslaugų saugumo pažeidimo atveju, atitinkama informacija pranešama abonentams ir pasikliaujančioms šalims.

7.12. PSP veiklos užbaigimas ir užbaigimo planai

PSP užtikrina, kad PSP kvalifikuotų ilgalaikės apsaugos paslaugų teikimo užbaigimo atveju, bus siekiama sudaryti kuo mažiau trikdžių abonentams ir pasikliaujančioms šalims, tolerancijos laikotarpiu prižiūrint informaciją, reikalingą apsaugos objektams išsaugoti ir prieiti prie jų.

PSP turi atnaujinamą veiklos užbaigimo planą, pagal kurį, prieš baigiant kvalifikuotų ilgalaikės apsaugos paslaugų teikimą, yra įvykdomos mažiausiai šios procedūros:

- a) PSP pateikia informaciją apie apsaugos paslaugų veiklos užbaigimą visiems abonentams, pasikliaujančioms šalims ir priežiūros įstaigai, panaudojant turimus kontaktinius duomenis, ne vėliau kaip prieš 3 mėnesius.
- b) PSP visiems subrangovams nutraukia leidimą veikti PSP vardu, atliekant bet kurias funkcijas, susijusias su apsaugos paslaugų teikimo procesu.
- c) PSP patikimai šaliai perduoda įsipareigojimą prižiūrėti įvykių žurnalą ir audito archyvus, būtinus PSP korektiško veikimo demonstravimui pagrįstą laikotarpį.
- d) PSP nenaudoja pasirašymo kriptografijos, todėl neatlieka privalomų baigiamųjų veiksmų jos buvimo atveju.
- e) Prieš PSP užbaigiant paslaugų teikimą, PSP siekia patikimų paslaugų teikimą esamiems klientams pagal galimybes perduoti kitam PSP.
- f) PSP turi susitarimus padengti šių minimalių reikalavimų išpildymo kaštus tam atvejui, jei PSP patiria bankrotą ar dėl kitokių priežasčių negali padengti kaštų pats.
- g) Paslaugų užbaigimo atveju PSP informuos įtakotas esybes ir, jeigu taikytina, perduos PSP įsipareigojimus kitoms šalims.

- h) PSP nepasirašo apsaugos įrodymų. Apsaugos įrodymai yra kvalifikuotos laiko žymų tarnybos pasirašytos laiko žymos.
- i) Užbaigimo planas nustato, kas įvyksta su saugomais apsaugos objektais užbaigus apsaugos paslaugų teikimą.

7.13. Atitiktis

PSP patvirtina, kad MitSoft apsaugos paslaugos atitinka QPSP ir PSPS. Tokiu būdu, PSP prisiima visus QPSP apibrėžtus įpareigojimus ir išpildo visus reikalavimus veikloms.

PSP veiklos atitiktis QPSP ir PSPS yra tikrinama pagal šiuos PSPS ne rečiau kaip kas dvejus metus.

PSP užtikrina atitiktį teisiniams reikalavimams. Konkrečiai:

- a) Atitiktis ES Reglamentui Nr. 910/2014 [eIDAS] yra patvirtinama bent kartą per 24 mėnesius, vykdant akredituotos atitikties vertinimo organizacijos atliekamą auditą.
- b) PSP nenustato specialių naudojimosi paslaugomis reikalavimų, dėl kurių neįgalieji negalėtų naudotis paslaugomis. Vartotojo sąsają pateikia apsaugos paslaugų kliento programinė įranga. Pati apsaugos paslaugų sistema suteikia ribotą vartotojo sąsają administravimo tikslais.
- c) PSP užtikrina, kad būtų laikomasi Europos duomenų apsaugos direktyvos 95/46/EB reikalavimų, kaip ji įgyvendinama Lietuvos teisės aktais:
 - Siekdamas teikti ilgalaikės apsaugos paslaugas, PSP reikalauja pateikti apsaugos užklausa, kaip apibrėžta [TS 119 511], kartu su autentifikavimo duomenimis, jei tai tinka pasirinktam autentifikavimo būdui.
 - PSP apdoroja duomenis kartu su komunikacijos atributais, kad būtų užtikrinta ilgalaikė apsauga ir įvykdyti taikomų standartų reikalavimai, įskaitant saugumo, apskaitos ir pajėgumų planavimo stebėseną.
 - Teikiant paslaugas, jokie kiti duomenys, įskaitant asmens duomenis, nėra renkami ir tvarkomi.
 - Imamasi atitinkamų techninių ir organizacinių priemonių, kad būtų išvengta neleistino ar neteisėto gautų duomenų tvarkymo, atskleidimo, atsitiktinio praradimo, sunaikinimo ar sugadinimo.
 - UAB "MitSoft" turi asmens duomenų tvarkymo taisyklės, dalyvaujantys darbuotojai yra pasirašę konfidencialumo sutartis.
- d) MitSoft PSP apsaugos paslaugų programinė įranga neturi vartotojo sąsajos, ji suteikia API, kuris turėtų būti naudojama iš kliento sistemos.
- e) Veiklos nutraukimo planą turi patvirtinti Lietuvos Respublikos ryšių reguliavimo tarnyba (RRT), atliekanti Nacionalinės kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų priežiūros įstaigos funkcijas.

7.14. Kriptografijos stebėseną

MitSoft PSP kriptografijos stebėseną apima du kriptografinių algoritimų 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 stebėseną yra pagrįsta esama algoritmo patikimumo būseną ir naudojama tik skaitmeninio parašo validavimo metu (atliekama pateikus apsaugos objektą arba pagal užklausa).

Skaitmeninio parašo papildymui naudojamų algoritmų kriptografijos stebėseną yra pagrįsta numatoma algoritmo patikimumo būseną 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 Infrastructures (ESI); Cryptographic Suites" [TS 119 312]. Numatomas kriptografinių algoritmų (jų parametrų ir raktų dydžių), naudojamų naujiems apsaugos įrodymams, atsparumo laikotarpis papildymo metu turėtų būti 3 metai ar daugiau pagal ETSI TS 119 312.

Kriptografinių algoritmų registro peržiūrą ir atnaujinimą atlieka MitSoft PSP sistemos administratorius. 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.

Trūkstanti 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 stebėseną ir reikalingas papildymo planavimas (išsamiau žr. 7.14 skyrių) užtikrina, kad PDS apsaugos tikslas bus pasiektas.

7.16. Eksporto-importo paketas

MitSoft PSP leidžia abonentui, įvardintam MitSoft PSP ilgalaikės apsaugos paslaugos abonentui, 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 abonentui 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 repozitoriuje.

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 saugotinių 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; grąžinti pateiktą elektroninį dokumentą/konteinerį 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; grąžinti pateiktą elektroninį dokumentą /konteinerį 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 teisinę procedūrą 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 pasiekama 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 nepasiekta). 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). Gaunama nauja archyvinė laiko žyma 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 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).