MitSoft

Kvalifikuotos ilgalaikės apsaugos paslaugos

Apsaugos profilis be saugyklos

QLPS/PP-WOS-LT

Unikalus objekto ID (OID): **1.3.6.1.4.1.57890.1.5.2**

Dokumento versija 1.02

Galioja nuo 2023-05-15

UAB „MIT-SOFT“, Kalvarijų st. 276-100, LT-08316 Vilnius, Tel. +370 233 3922, Fax +370 5 213 6191, www.mitsoft.lt, info@mitsoft.lt, Company ID 120792080, VAT payer code LT207920811

Patvirtinimai

Versijų istorija

Versija	Galioja nuo	Aprašas
1.00		Pirma oficiali dokumento versija
1.01		Ištaisytos smulkios formulavimo klaidos
1.02	2023-05-15	Leidžiami CMS parašai PDF dokumente; išaiškinimas dėl skaitmeninių parašų, kurie nėra galiojantys, ilgalaikės apsaugos

Dokumento patvirtinimas

	Vardas Pavardė	Data	Parašas
Peržiūrėjo	Adomas Birštunas	2023-04-04	
Patvirtino	Antanas Mitašiūnas	2023-05-15	

Turinys

1. Įvadas

UAB "MIT-SOFT" (toliau – MitSoft) yra kvalifikuotų ilgalaikės apsaugos paslaugų teikėjas (toliau – PSP).

Šis dokumentas apibrėžia vieną iš apsaugos profilių, kurį palaiko MitSoft PSP. Šiame dokumente apibrėžiamo apsaugos profilio pavadinimas yra:

- MitSoftQWOS profilis – kvalifikuotų elektroninių parašų ir spaudų MitSoft apsaugos profilis be saugyklos.

MitSoftQWOS profilis turi būti naudojamas, kai kvalifikuoti elektroniniai parašai, pažangūs elektroniniai parašai, kvalifikuoti elektroniniai spaudai, pažangūs elektroniniai spaudai, esantys elektroniniuose dokumentuose ar konteineriuose, yra saugomi už MitSoft PSP ribų (abonento saugykloje), bet MitSoft PSP apsaugos paslaugos yra naudojamos elektroninių parašų ir (arba) elektroninių spaudų apsaugai.

Apsaugos saugyklos modelis, apsaugos tikslai, MitSoftQWOS profilio palaikomos operacijos ir apsaugos protokolas yra aprašyti šiame dokumente.

2. Nuorodos

[ADOC-V1.0] – Lietuvos vyriausiasis archyvaras. "Elektroniniu parašu pasirašyto elektroninio dokumento specifikacija ADOC-V1.0".

[ADOC-V2.0] – Lietuvos vyriausiasis archyvaras. "Elektroninio dokumento specifikacija ADOC-V2.0".

[EGAS-V1.0] – Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos direktoriaus įsakymas "Dėl elektroninės gyventojų aptarnavimo sistemos naudojimo taisyklių ir elektroninės gyventojų aptarnavimo sistemos elektroniniu parašu pasirašyto dokumento specifikacijos EGAS-V1.0 patvirtinimo".

[eIDAS] – Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[EN 319 122-1] – ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[EN 319 132-1] – ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[EN 319 142-1] – ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[EN 319 162-1] – ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers".

[MDOC-V1.0] – Lietuvos vyriausiasis archyvaras. "Elektroniniu parašu pasirašyto kompiuterio skaitomo elektroninio dokumento specifikacija MDOC-V1.0".

[PDF-LT-V1.0] – Lietuvos vyriausiasis archyvaras. "Elektroninio dokumento PDF-LT-V1.0 specifikacija".

[PDF-RC-V1.0] – Valstybės įmonė Registrų centras. „Elektroninio dokumento specifikacija PDF-RC-V1.0".

[DSS Core 2.0] - OASIS: "Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0", Committee Specification 02, 11 December 2019.

[TS 101 733] – ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[TS 101 903] – ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[TS 102 778-2] - ETSI TS 102 778-2: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1".

[TS 102 778-4] – ETSI TS 102 778-4: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile".

[TS 103 171] – ETSI TS 103 171: "Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile".

[TS 103 172] – ETSI TS 103 172: "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile".

[TS 103 173] – ETSI TS 103 173: "Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile".

[TS 103 174] – ETSI TS 103 174: "Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile".

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

[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 abonento įsipareigojimus su apsaugos patikimų paslaugų teikėju.

Apsaugos interfeisas: apsaugos paslaugos komponentė, įgyvendinanti apsaugos protokolą.

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

Apsaugos įrodymų taisyklės: aibė taisyklių, kurios 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, kurį apsaugos paslauga apsaugo pateiktus apsaugos objektus ir susijusius įrodymus.

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

PASTABA: Tai apima pateikimo duomenų objektus, apsaugos objektų konteinerius ir apsaugos įrodymus.

Apsaugos objekto identifikatorius: unikalus apsaugos objekto (aibės apsaugos objektų) identifikatorius, pateiktas apsaugos paslaugai.

Apsaugos objekto konteineris: konteineris, turintis savyje aibę duomenų objektų ir galimai susijusius metaduomenis, pateikiančią informaciją apie duomenų objektus ir galimai apsaugos manifestą, specifikuojantį jo turinį ir sąryšius.

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

Apsaugos paslaugos teikėjas: patikimų paslaugų teikėjas, teikiantis apsaugos paslaugą.

Apsaugos profilis: su apsaugos saugyklos modeliu ir vienu ar daugiau apsaugos tikslų susijęs unikaliai identifikuotas įgyvendinimo detalių rinkinys, kuris specifikuoja, kaip apsaugos įrodymai yra generuojami ir validuojami.

Apsaugos protokolas: apsaugos paslaugos ir apsaugos kliento komunikavimo protokolas.

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

Apsaugos schema: su apsaugos saugyklos modeliu ir vienu ar daugiau apsaugos tikslų susijęs bendrinių procedūrų ir taisyklių rinkinys, nurodantis, kaip kuriami ir validuojami apsaugos įrodymai.

PASTABA: Skirtingi apsaugos profiliai gali įgyvendinti tą pačią apsaugos schemą.

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

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).

Ilgalaikė apsauga: skaitmeninių parašų galiojimo statuso pratęsimas per ilgą laikotarpį ir/ar duomenų egzistavimo įrodymų pateikimo pratęsimas per ilgą laikotarpį, nepaisant senėjimo kriptografinių technologijų, tokių kaip kriptografiniai algoritmai, raktų

ilgiai ar santraukų funkcijos, raktų kompromitavimas ar praradimas galimybės patikrinti viešųjų raktų sertifikatų galiojimo statusą.

Ilgalaikis: laikotarpis, kurio eigoje gali įvykti technologiniai pokyčiai.

Konteineris: duomenų objektas, turintis savyje aibę duomenų objektų ir galimai papildomą informaciją, aprašančią turimus duomenų objektus ir galimai jų turinį ir tarpusavio ryšius.

Parašo papildymas (angl. augmentation)**:** informacijos įtraukimo į elektroninį parašą arba elektroninį spaudą procesas, siekiant išlaikyti to parašo / antspaudo galiojimo statusą artimiausiu metu ir (arba) ilgą laikotarpį.

Parašo taisyklės: parašo kūrimo taisyklės, parašo papildymo taisyklės, parašo validavimo taisyklės arba bet koks jų derinys, taikomas tam pačiam parašui ar parašų rinkiniui.

Parašo validavimo apribojimas: techniniai kriterijai, pagal kuriuos galima validuoti elektroninį parašą arba elektroninį spaudą

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

Sukompromitavimas: praradimas, vagystė, modifikavimas, neteisėtas naudojimas ar kitas konfidencialių duomenų saugumo pažeidimas.

Kitos sąvokos naudojamos taip, kaip jos apibrėžtos Reglamente (EU) 910/2014 [eIDAS].

ETSI – Europos Telekomunikacijų Standartų Institutas (angl. *European Telecommunications Standards Institute*)

OID – Objekto identifikatorius (angl. *Object identifier*)

PO – Apsaugos objektas (angl. *Preservation object*)

POC – Apsaugos objekto konteineris (angl. *Preservation object container*)

PSP – Apsaugos paslaugų teikėjas (angl. *Preservation service provider*)

SubDO – Pateikimo duomenų objektas (angl. *Submission data object*)

4. Kvalifikuotų elektroninių parašų ir spaudų MitSoft apsaugos profilis be saugyklos

4.1. Aprašymas

MitSoftQWOS profilis apibrėžia MitSoft apsaugos paslaugų eksploatacines detales, kai jos naudojamos be integruotos elektroninių dokumentų saugyklos. Apsaugos objektai saugomi apsaugos paslaugų išorėje (kokioje nors abonento saugykloje). Apsaugos paslaugų naudojant MitSoftQWOS profilį tikslas – ilgą laiką išsaugoti galimybę validuoti elektroninius parašus ir elektroninius spaudus, palaikyti jų galiojimo būseną ir gauti susijusių pasirašytų duomenų egzistavimo įrodymus.

Apsaugos paslaugų apsaugomi apsaugos objektai yra kvalifikuoti elektroniniai parašai ir kvalifikuoti elektroniniai spauda. Apsaugos paslaugos apsaugo pažangius elektroninius parašus ir pažangius elektroninius spaudus (kurie nėra kvalifikuoti) tik tuo atveju, jei toks reikalavimas yra nurodytas Abonento sutartyje. Toliau šiame dokumente jie vadinami elektroniniais parašais ar spaudais arba 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 taisykles.

Apsaugos paslaugos nepriima elektroninių parašų ar elektroninių spaudų, kurie nėra pateikto elektroninio dokumento ar konteinerio dalis. Kiekviename pateiktame elektroniniame dokumente ar konteineryje turi būti duomenys, pasirašyti apsaugomu elektroniniu parašu arba užantspauduoti saugomu elektroniniu spaudu (abonentams neleidžiama pateikti tik pasirašytų duomenų santraukų reikšmes). Palaikomos elektroninių dokumentų specifikacijos ir konteinerių standartai yra pateikti 4.12 skyrelyje. Apsaugos objektai, apsaugomi šiame profilyje, yra pateikti 4.8 skyrelyje.

Šis profilis turi būti naudojamas, kai pasirašyti/užantspauduoti elektroniniai dokumentai/konteineriai yra saugomi abonento saugykloje, bet jų apsaugą užtikrina MitSoft apsaugos paslaugos. Abonentas atsakingas už išsaugojimą ir priežiūrą elektroninių parašų ir elektroninių spaudų, esančių pasirašytuose/užantspauduotuose elektroniniuose dokumentuose/konteineriuose. Abonentas taip pat atsakingas už savalaikius kreipinius į MitSoft apsaugos paslaugas, kad elektroninius parašus/spaudus papildytų apsaugos įrodymais ir gautų numatomą įrodymų galiojimo trukmę. Apsaugos paslaugos yra atsakingos už pateiktų elektroninių parašų ir elektroninių spaudų apsaugą. Apsaugos paslaugos užtikrina elektroninių parašų/spaudų apsaugą, juos validuodamos, surinkdamos validavimo duomenis ir apsaugos įrodymus, papildydamos elektroninius parašus/spaudus ir įvertindamos numatomą įrodymų galiojimo trukmę. Kadangi pagal šį profilį apsaugos paslaugos nesaugo elektroninių dokumentų/konteinerių, apsaugos paslaugos neseka kada turi būti atlikti apsaugos veiksmai.

MitSoftQWOS profilis pateikia operacijas:

- elektroninių parašų/spaudų, esančių pateiktuose elektroniniuose dokumentuose/konteineriuose, apsaugos veiksmų (validavimo ir papildymo, įtraukiant apsaugos įrodymus) atlikimui (žr. Augment, PreservePO operacijas),

4.2. Identifikavimas

MitSoftQWOS profilio unikalus identifikatorius (OID) yra:

- Identifikatorius OID forma yra
  - 1.3.6.1.4.1.57890.1.5.2;

  Jo laukų reikšmės yra pateiktos 1 lentelėje.

- Identifikatorius URI forma yra
  - `http://uri.mitsoft.lt/preservation/profile/qwos/2`

1 lentelė. MitSoftQWOS profilio unikalaus identifikatoriaus laukų reikšmės

Name	Value
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 (apsaugos profilis)	5
Apsaugos profilio identifikatorius	2

4.3. Galiojimo laikotarpis

Šis apsaugos profilis taps aktyviu nuo 2022-12-01. Tas pats apsaugos profilis taikomas visą apsaugos laikotarpį.

4.4. Apsaugos schema

MitSoftQWOS profilis įgyvendina tokią apsaugos schemą:

- apsaugos schema su parašo papildymu be saugyklos, apibrėžta ETSI TS 119 512 [TS 119 512] F.4 priede ir nurodoma identifikatoriumi:
  - `http://uri.etsi.org/19512/scheme/pds+wos+aug`

4.5. Apsaugos tikslas

MitSoftQWOS profilis palaiko tokį apsaugos tikslą:

- PDS – skaitmeninių parašų galiojimo statuso pratęsimas ilgą laikotarpį ETSI TS 119 512 [TS 119 512], nurodomą URI:
  - `http://uri.etsi.org/19512/goal/pds`

4.6. Apsaugos saugyklos modelis

MitSoftQWOS profilis palaiko apsaugos paslaugas be saugyklos – WOS pagal ETSI TS 119 512 [TS 119 512].

4.7. Palaikomos operacijos

Šis apsaugos profilis palaiko tokias operacijas:

- Augment,
- Download,
- RetrieveInfo,
- PreservePO.

4.8. Pateikimo duomenų objektai ir apsaugos objektai

MitSoftQWOS apsaugo elektroninius parašus ir elektroninius spaudus, esančius elektroniniame dokumente ar konteineryje.

Pateikimo duomenų objektas (SubDO) yra elektroninis dokumentas/konteineris, pateiktas kaip vienas failas, kuris:

- turi bent vieną elektroninį parašą ar elektroninį spaudą,
- turi visus duomenų objektus, pasirašytus elektroniniu parašu ar užantspauduotus elektroniniu spaudu, ir
- gali turėti savo metaduomenis.

Palaikomi SubDO yra apibrėžti 4.12 skyrelyje.

MitSoft PSP apsaugos objektas (PO) yra elektroninis parašas ar elektroninis spaudas, atitinkantis B-LTA parašo lygmenį (ar atitinkamą archyvinio parašo formatą parašams, kurie nėra baziniai parašai).

Apsaugos paslaugos apsaugo kvalifikuotus elektroninius parašus ir kvalifikuotus elektroninius spaudus. Apsaugos paslaugos apsaugo pažangius elektroninius parašus ir pažangius elektroninius spaudus (kurie nėra kvalifikuoti) tik tuo atveju, jei toks reikalavimas yra nurodytas Abonento sutartyje.

Apsaugos paslaugos saugo galiojančius elektroninius parašus ir galiojančius elektroninius spaudus (turinčius validavimo statusą PASSED). Apsaugos paslaugos saugo elektroninius parašus ir elektroninius spaudus, kurie nėra galiojantys (turintys kitą validavimo statusą nei PASSED), tik tuo atveju, jei validavimo rezultate nėra validavimo klaidų, kurios neleidžia atlikti skaitmeninio parašo papildymo pagal parašo taisykles, ir jei toks reikalavimas yra nurodytas Abonento sutartyje. Tikslus validavimo klaidų subindikacijų, kurios netrukdo atlikti skaitmenio parašo papildymo, sąrašas yra pateiktas parašo taisyklėse.

MitSoft PSP saugomas apsaugos objektas yra gaunamas iš pateikimo duomenų objekto, papildant SubDO esančius elektroninius parašus ir elektroninius spaudus. Papildymas atliekamas siekiant B-LTA parašo lygmens (ar atitinkamo archyvinio parašo formato parašams, kurie nėra baziniai parašai). Papildymas apima validavimo duomenų ir laiko žymų gavimą ir jų įtraukimą į skaitmeninį parašą. Elektroninių parašų ir elektroninių spaudų apsauga yra nevykdoma, jei pasiekti B-LTA parašo lygmens (ar atitinkamo archyvinio parašo formato parašams, kurie nėra baziniai parašai) neįmanoma (dėl jų nekorektiškumo ar nesant galimybės gauti patikimus trūkstamus validavimo duomenis).

Kai pateikimo duomenų objektai neturi saugotinų elektroninių parašų ar elektroninių spaudų, apsaugos veiksmai su tokiais SubDO neatliekami, bet validavimo duomenys gali būti įtraukti į skaitmeninius parašus. Tai leidžia neprarasti surinktų validavimo duomenų, kurie yra galimi pateikto skaitmeninio parašo negaliojimo įrodymai.

Elektroninių parašų ir elektroninių spaudų apsauga yra užtikrinama naujais apsaugos įrodymais (archyvinėmis laiko žymomis). Kai SubDO esantis elektroninis parašas ar elektroninis spaudas jau yra B-LTA lygmens, nauji apsaugos įrodymai (archyvinės laiko žymos) bus pridėti tik, jei papildymo laikotarpis jau prasidėjęs (žr. 4.8.2 skyrelį). Kitu atveju nauji apsaugos įrodymai nebus įtraukti į PO ir bus pateikta tik informacija apie sekančio papildymo laiką (įskaitant apskaičiuotą numatomą įrodymų galiojimo trukmę). Apsaugos paslaugos apskaičiuoja numatomą įrodymų galiojimo trukmę ir grąžina ją klientui kaip apsaugos operacijos rezultatą. Detaliau žr. 4.8.1 skyrelyje.

Elektroninių dokumentų kontekste skaitmeninio parašo naudojimas (ir apsauga) be elektroninio dokumento/konteinerio, kuriam jis priklauso (ir faktiškai pasirašo), yra beprasmis. Todėl visos operacijos dirba su apsaugos objekto konteineriu, o ne su atskiru apsaugos objektu, apsaugomu MitSoft PSP.

Apsaugos objekto konteineris (POC) yra pateiktas elektroninis dokumentas arba konteineris, turintis elektroninius parašus ir (arba) spaudus (apsaugos objektus) su apsaugos paslaugų pridėtais apsaugos įrodymais (laiko žymomis). POC gaunamas iš

SubDO, papildant apsaugomus skaitmeninius parašus apsaugos įrodymais (laiko žymomis). Atskiru atveju, kai SubDO nėra apsaugomų skaitmeninių parašų, POC gali būti tas pats nepakeistas SubDO.

Šiame profilyje apibrėžtos operacijos priima ir grąžina apsaugos objektus, kurie yra visas apsaugos objekto konteineris – elektroninis dokumentas ar konteineris (su jame esančiais apsaugomais skaitmeniniais parašais ir apsaugos įrodymais) arba pateikimo duomenų objektas. Naudojant šio profilio operacijas negalima dirbti su atskiru elektroniniu parašu ar spaudu.

4.8.1. Numatoma įrodymų galiojimo trukmė

Pagal MitSoftQWOS profilį pateikimo duomenų objektai ir apsaugos objektai saugomi kliento saugykloje, todėl klientas yra atsakingas už apsaugos objektų priežiūrą ir inicijavimą apsaugos veiksmų. Kad klientas galėtų nustatyti tinkamą kito apsaugos veiksmo laiką, MitSoft PSP apskaičiuoja numatomą apsaugos įrodymų galiojimo trukmę.

Numatoma apsaugos įrodymų galiojimo trukmė apskaičiuojama kiekvienam apsaugomam elektroniniam parašui ar elektroniniam spaudui. Kadangi apsauga atliekama tik B-LTA parašo lygmens (ar atitinkamo archyvinio parašo formato parašams, kurie nėra baziniai parašai) skaitmeniniams parašams, numatoma apsaugos įrodymų galiojimo trukmė apskaičiuojama pagal paskutinės galiojančios laiko žymos sertifikatą ir jo kūrimui naudotus kriptografinius algoritmus.

Numatomą apsaugos įrodymų galiojimo trukmę riboja vienas iš šių veiksnių (kuris ankstesnis):

- paskutinei galiojančiai laiko žymai pasirašyti naudoto laiko žymų tarnybos sertifikato galiojimo pabaigos data,
- minimalus numatomas paskutinei galiojančiai laiko žymai naudotų kriptografinių algoritmų patikimumo laikotarpis.

Numatomus kriptografinių algoritmų patikimumo laikotarpius palaiko apsaugos paslaugų kriptografinė stebėsena. MitSoft PSP „Veiklos nuostatų" 7.14 skyrelyje detaliai aprašyta, kaip nustatomas ir prižiūrimas numatomas kriptografinio algoritmo patikimumo laikotarpis.

Jei reikia nustatyti bendrą viso POC (elektroninio dokumento ar konteinerio) numatomą įrodymų galiojimo trukmę, ji turi būti minimali POC esančių elektroninių parašų/spaudų numatoma įrodymų galiojimo trukmė. Pastebėkime, kad normaliu atveju ta pati laiko žymų tarnyba ir tie patys kriptografiniai algoritmai naudojami archyvinių laiko žymų kūrimui, todėl visų skaitmeninių parašų numatoma įrodymų galiojimo trukmė paprastai bus ta pati.

Apskaičiuota numatoma įrodymų galiojimo trukmė yra vienas iš operacijų grąžinamo rezultato laukų: *Augment* (*AugmentNotAfter* laukas, žr. 4.9.2 skyrelį) ir *PreservePO* (*eed* atributas, žr. 4.9.4 skyrelį).

4.8.2. Apsaugos įvykio laiko nustatymas

Apsaugos veiksmai turi būti atliekami kart nuo karto, siekiant užtikrinti PO galiojimą apsaugos laikotarpiu. Kadangi PSP klientas saugo PO savo saugykloje (pagal MitSoftQWOS profilį), tai jis yra atsakingas už apsaugos veiksmo inicijavimą tinkamu laiku. Tinkamas laikas neturėtų būti nei per anksti, nei per vėlai. Apsaugos veiksmas yra per vėlus, jei skaitmeninio parašo galiojimas jau baigėsi, arba yra rizika nesugebėti pratęsti skaitmeninio parašo galiojimo dėl didelio apsaugos veiksmų kiekio ir/arba laikino trečiųjų šalių paslaugų neprieinamumo. Apsaugos veiksmas yra per ankstus, jei naujų apsaugos įrodymų (archyvinės laiko žymos) įtraukimas į skaitmeninį parašą yra perteklinis. Apsaugos paslaugos padeda klientui suplanuoti tinkamą laiką sekančiam apsaugos veiksmui. Tinkamas sekančio apsaugos veiksmo laikas yra apibrėžiamas naudojant numatomą įrodymų galiojimo trukmę, papildymo laikotarpį ir atsargumo laikotarpį.

Apsaugos įrodymų galiojimą riboja laiko žymų tarnybos sertifikato galiojimo pabaiga ir numatomas kriptografinių algoritmų patikimumo laikotarpis. Kadangi daug apsaugomų skaitmeninių parašų turės apsaugos įrodymus su tuo pačiu galiojimo laikotarpiu, svarbu užtikrinti, kad visi tokie skaitmeniniai parašai būtų papildyti (atlikti apsaugos veiksmai) prieš jų galiojimo pabaigos laiką. Todėl skaitmeniniai parašai turi būti papildyti prieš atsargumo laikotarpį – šiek tiek laiko iki galiojimo pabaigos. Apsaugos paslaugos negarantuoja, kad pateiktas skaitmeninis parašas bus sėkmingai atnaujintas naujais apsaugos įrodymais, jei atsargumo laikotarpis jau prasidėjęs. MitSoftQWOS profilio naudojamas atsargumo laikotarpis nurodomas Abonento sutartyje.

Tuo atveju, kai SubDO jau turi B-LTA lygmens skaitmeninį parašą, kurio galiojimas nesibaigs artimiausioje ateityje, naujos archyvinės laiko žymos įtraukimas į skaitmeninį parašą gali būti perteklinis. Todėl nauji apsaugos įrodymai bus įtraukti į skaitmeninį parašą tik, jei papildymo laikotarpis jau prasidėjęs. Papildymo laikotarpis yra pagrįstas laikotarpis, kuris prasideda šiek tiek laiko iki numatomos skaitmeninio parašo galiojimo pabaigos ir tęsiasi iki numatomos skaitmeninio parašo galiojimo pabaigos. Tikslus naudojamas papildymo laikotarpis nurodomas Abonento sutartyje.

Tokie elementai (tarp kitų) bus grąžinami kaip apsaugos operacijų rezultatas:

- *AugmentNotBefore* – papildymo laikotarpio pradžios data; nauji apsaugos įrodymai bus įtraukti į skaitmeninį parašą tik, jei *AugmentNotBefore* yra anksčiau nei dabartinis laikas,
- *AugmentAt* – sekančio apsaugos įvykio rekomenduojamas laikas; tai laikas papildymo laikotarpyje, bet prieš atsargumo laikotarpio pradžią,
- *AugmentNotAfter* – tai papildymo laikotarpio pabaiga, lygi numatomos įrodymų galiojimo trukmės pabaigai; skaitmeninis parašas gali prarasti galiojimą, jei sėkmingi apsaugos veiksmai nebus atlikti iki *AugmentNotAfter*.

Rekomenduojama, kad sekantys apsaugos veiksmai su tuo pačiu PO būtų atliekami laiku (ar beveik), kurį rekomendavo ankstesnė apsaugos operacija (*AugmentAt*).

Pastebėkime, kad numatomas kriptografinio algoritmo patikimumo laikotarpis laikui bėgant gali pailgėti (arba sutrumpėti). Todėl apsaugos operacijos grąžinami papildymo laikotarpis ir numatoma įrodymų galiojimo trukmė gali skirtis nuo ankstesnės operacijos grąžintų. Operacijos (*AugmentAt*) vykdymas ankstesnės operacijos rekomenduotu laiku gali pratęsti skaitmeninio parašo galiojimą, įtraukiant naujus apsaugos įrodymus, arba gali apskaičiuoti ir grąžinti patikslintą papildymo laikotarpį ir naują rekomenduojamą papildymo laiką.

4.9. Apsaugos protokolas

Šis skyrelis aprašo palaikomų operacijų sintaksę ir semantiką. Operacijos įgyvendintos kaip REST žiniatinklio paslaugos (angl. web services). Turi būti naudojamas žiniatinklio paslaugos naudotojo autentifikavimas ir ryšio šifravimas (Secure Sockets Layer).

ETSI TS 119 512 apibrėžtos operacijos yra trumpai pristatomos šiame skyrelyje su nuorodomis į standartą ir apibrėžiant tik specifinius momentus. Kitų specifinių operacijų sintaksė ir semantika yra pilnai apibrėžiama šiame skyrelyje. Aprašyti tik pagrindiniai laukai, laukų pavadinimai yra neformalūs, laukų tipai ir kardinalumai praleisti. Tikslus apsaugos interfeisas – užklausų ir atsakymų laukai – aprašyti atskirai, naudojant JSON formatą (žr. 4.9.5 skyrelį).

MitSoftQWOS profilis palaiko tokias operacijas:

4.9.1. RetrieveInfo

RetrieveInfo operacija naudojama palaikomų apsaugos profilių aibei gauti. Operacija grąžina palaikomų apsaugos profilių sąrašą.

RetrieveInfo operacijos sintaksė ir semantika yra pilnai apibrėžta ETSI TS 119 512 skyrelyje 5.3.2. Šis profilis palaiko šią operaciją tik naudojant JSON sintaksę.

4.9.2. Augment

Augment operacija yra analogiškos ETSI TS 119 512 apibrėžtos *PreservePO* operacijos išplėtimas. *Augment* operacija yra naudojama apsaugoti apsaugos objektą, kuris yra naujas pateikimo duomenų objektas, ar apsaugos objekto konteinerį, anksčiau gautą atliekant šią operaciją. Pateiktas apsaugos objektas yra elektroninis dokumentas ar konteineris su elektroniniais parašais ar elektroniniais spaudais. Šiai operacijai turi būti pateiktas apsaugos objektas. Apsauga atliekama, papildant elektroninius parašus ir elektroninius spaudus. Tai apima kūrimą/rinkimą validavimo duomenų (jei jų nebuvo) ir apsaugos įrodymų bei jų įtraukimą į apsaugos objektus – elektroninius parašus ar elektroninius spaudus.

Jei elektroninis parašas ar spaudas jau pasiekęs B-LTA parašo lygmenį (ar atitinkamą archyvinio parašo formatą parašams, kurie nėra baziniai parašai) operacijos veiksmai priklauso nuo papildymo ir atsargumo laikotarpių (žr. 4.8.2 skyrelį):

- jei opera operacija vykdoma prieš papildymo laikotarpio pradžią (numatoma skaitmeninio parašo galiojimo pabaiga yra tolimoje ateityje), nauji apsaugos įrodymai (archyvinė laiko žyma) nebus įtraukti, tik bus apskaičiuoti ir grąžinti papildymo laikotarpis ir numatoma įrodymų galiojimo trukmė,
- jei operacija vykdoma papildymo laikotarpiu ir prieš atsargumo laikotarpio pradžią (numatoma skaitmeninio parašo galiojimo pabaiga yra artimoje ateityje), nauji apsaugos įrodymai (archyvinė laiko žyma) bus įtraukti bei apskaičiuoti ir grąžinti papildymo laikotarpis ir numatoma įrodymų galiojimo trukmė,
- jei operacija vykdoma atsargumo laikotarpiu ir po papildymo laikotarpio pabaigos (skaitmeninio parašo galiojimas jau gali būti pasibaigęs), apsaugos paslaugos stengsis įtraukti naujus apsaugos įrodymus (archyvinę laiko žymą) tik, jei skaitmeninio parašo galiojimas dar nesibaigė, ir pavykus bus grąžinti naujas papildymo laikotarpis, numatoma įrodymų galiojimo trukmė ir rekomenduojamas sekančio papildymo laikas.

Jei elektroninis parašas ar spaudas yra B-T ar B-LT parašo lygmens, operacija bandys surinkti tinkamus validavimo duomenis:

- jei tinkami validavimo duomenys šiuo metu neprieinami (pvz., atšaukimo duomenys per seni dėl atidėjimo laikotarpio), nauji apsaugos įrodymai (archyvinė laiko žyma) nebus įtraukti, tik bus apskaičiuotas ir grąžintas sekančio papildymo laikas, atitinkantis atidėjimo laikotarpį,
- jei tinkami validavimo duomenys šiuo metu prieinami, surinkti validavimo duomenys ir nauji apsaugos įrodymai (archyvinė laiko žyma) bus įtraukti bei apskaičiuoti ir grąžinti naujas papildymo laikotarpis, numatoma įrodymų galiojimo trukmė ir rekomenduojamas sekančio papildymo laikas

Jei elektroninis parašas ar spaudas yra B-B parašo lygmens, operacija *Augment* pirmiausia įtrauks parašo reikšmės (angl. signature value) egzistavimo įrodymą (parašo laiko žymą), o tada elgsis kaip B-LT lygmens atveju (žr. aukščiau).

Ši operacija palaiko 4.12 skyrelyje išvardintus pateikimo duomenų objektų formatus. SubDO ir iš jo gauti apsaugos objektai neišsaugomi PSP saugykloje, bet išsaugoma informacija apie atliktus veiksmus (veiksmų sekos). Veiksmų sekose SubDO ir apsaugos objektai bus identifikuojami šios operacijos suteiktu *DocumentTicket* elementu.

Šis profilis palaiko šią operaciją naudojant JSON sintaksę. JSON schema ir OpenAPI dokumentas pateikti 4.9.5 skyrelyje.

4.9.2.1 Augment užklausa

Augment užklausa turi priimti pateikimo duomenų objektą ir papildomus parametrus.

Užklausoje turi būti nurodyti tokie laukai:

- *client ID*. Jame turi būti apsaugos kliento, kviečiančio operaciją, identifikatorius.
- *document file*. Jame turi būti SubDO turinys, pateiktas kaip failas. Turinys turi būti pateikiamas originaliu formatu be kodavimo ar transformacijos.

Užklausoje gali būti tokie laukai:

- neprivalomas *document specification*. Jei pateiktas, jame turi būti dokumento specifikacijos identifikatorius, apibrėžiantis SubDO turinio tipą. Identifikatorius turi atitikti vieną iš specifikacijų, išvardintų 4.12 skyrelyje. Jei šis parametras praleistas, SubDO tipas nustatomas pagal jo failo vardą ar turinį.
- neprivalomas *signature filters*. Jei pateiktas, jame turi būti elektroninių parašų ar elektroninių spaudų, kuriuos turi apdoroti ši papildymo operacija, filtrai. Filtrai gali būti apibrėžti kaip skaitmeninių parašų identifikatorių sąrašas arba parašo paskirčių, jei taikoma, sąrašas.
- neprivalomas *time to live*. Jei pateiktas, jame turi būti laikas sekundėmis, kiek apsaugos objektas turi būti saugomas apsaugos paslaugų sistemos atmintyje, kol jį pasiims apsaugos klientas. Pasibaigus šiam laikotarpiui, apsaugos paslaugos sunaikina apsaugos objektą ir apsaugos klientas nebegali jo pasiimti.

Aprašyti laukai turi būti perduodami kaip HTTP multi-part POST užklausos parametrai:

Laukas	Aprašymas	HTTP užklausos parametras
Client ID	Apsaugos kliento identifikatorius	cid
Document file	Pateikimo duomenų objekto turinys	docFile
Document specification	Pateikimo duomenų objekto tipą apibrėžiančios specifikacijos identifikatorius	docSpecId
Signatures filters	Sąrašas SubDO skaitmeninių parašų arba parašų tipų, kurie turi būti apdoroti papildymo metu	sigIds, sigPurposes
Time to live	Laikas sekundėmis, kiek apsaugos objektas turi būti saugomas apsaugos paslaugų sistemos atmintyje po papildymo	ttl

4.9.2.2 Augment atsakymas

Augment atsakyme nurodoma operacijos įvykdymo būsena, ar operacija buvo sėkminga ar ne, ir klaidos nesėkmės atveju.

Sėkmės atveju pateikiamas HTTP atsakymas su būsenos kodu 200 ir informacija apie atliktą papildymą.

Klaidos, įskaitant klaidas apdorojant pateiktą SubDO, atveju pateikiamas HTTP atsakymas su būsenos kodu, skirtingu nuo 200, ir klaidos pranešimu.

Sėkmingame atsakyme turi būti pateikiami tokie elementai:

- *AugmentationStatus* elementas. Jame turi būti reikšmė, nurodanti ar apsaugos objekto elektroniniai parašai ir/ar elektroniniai spaudai buvo papildyti ar nepakeisti.
- *DocumentSpecificationId* elementas. Jame turi būti dokumento specifikacijos identifikatorius, apibrėžiantis SubDO turinio tipą. Identifikatorius turi atitikti vieną iš specifikacijų, išvardintų 4.12 skyrelyje.
- *AugmentAt* elementas. Jame turi būti data ir laikas, nurodantys, kada sekantis apsaugos objekto papildymas turėtų būti atliekamas. Jei šio papildymo metu sekančio papildymo laikas negali būti nustatytas, šio elemento reikšmė turi būti *null*. Ji apskaičiuojama pagal PO atskirų apsaugomų parašų *AugmentAt* elementus. Ji turi būti naudojama kaip laiko sekančiam apsaugos veiksmui rekomendacija.
- *DocumentAvailableUntil* elementas. Jame turi būti data ir laikas, nurodantys, iki kada apsaugos objektas laikomas apsaugos paslaugų sistemos atmintyje. Po šio momento apsaugos objektas yra sunaikinamas ir nebegali būti pasiimtas. Jei apsaugos objektas papildymo metu nebuvo atnaujintas ir apsaugos klientas negali jo atsiimti, šio elemento reikšmė turi būti *null*.
- *DocumentTicket* elementas. Jame turi būti apsaugos objekto identifikatorius, kurį jam suteikė apsaugos paslaugos. Jį turi naudoti apsaugos klientas pasiėmimui apsaugos objekto, kai keli ar visi jo elektroniniai parašai ar elektroniniai spaudai yra papildyti. Kad pasiimtų apsaugos objektą po papildymo, apsaugos klientas turi iškviesti *Download* operaciją, iš karto gavęs *Augment* atsakymą, bet ne vėliau nei laikas nurodytas *DocumentAvailableUntil* elemente.

  Pastaba: Šis elementas taip pat naudojamas kaip apsaugos objekto (SubDO ir iš jo gauto apsaugos objekto konteinerio) identifikatorius atliktų apsaugos veiksmų sekose.
- *Signatures* elementas. Jame turi būti *Signature* elementų masyvas. Šio masyvo elementai atitinka visus apsaugos objekte esančius elektroninius prašus ir elektroninius spaudus.

Signature komponentas turi turėti tokius elementus:

- *AugmentationValidation* elementas. Jame turi būti kodas, nurodantis papildymo metu atliktos elektroninio parašo ar elektroninio spaudo validavimo būseną.
- *AugmentNotBefore* elementas. Jame turi būti data ir laikas, nurodantys kito papildymo laikotarpio pradžią. Nauji apsaugos įrodymai bus įtraukti į skaitmeninį parašą, jei operacija bus atliekama papildymo laikotarpiu, todėl sekantis operacijos vykdymas (apsaugos veiksmai) turi būti atliekamas ne anksčiau nei šiuo elementu grąžinamas laikas. Jei skaitmeninio parašo apsauga neatliekama ar B-LTA prašo lygmuo (ar atitinkamas archyvinio parašo formatas parašams, kurie nėra baziniai parašai) nepasiektas, šio elemento reikšmė turi būti *null*.
- *AugmentAt* elementas. Jame turi būti data ir laikas, nurodantys, kada sekantis skaitmeninio parašo papildymas turėtų būti vykdomas. Jei papildymo metu sekančio papildymo laikas negali būti nustatytas, šio elemento reikšmė turi būti *null*. Klientas ją turėtų naudoti kaip rekomendaciją sekančio apsaugos veiksmo iškvietimui.
- *AugmentNotAfter* elementas. Jame turi būti data ir laikas, nurodantys numatomą skaitmeninio parašo galiojimo pabaigos laiką, kuris taip pat nurodo šio skaitmeninio parašo numatomą apsaugos įrodymų galiojimo trukmę. Jei skaitmeninio parašo apsauga neatliekama ar B-LTA prašo lygmuo (ar atitinkamas archyvinio parašo formatas parašams, kurie nėra baziniai parašai) nepasiektas, šio elemento reikšmė turi būti *null*.

- *Info* elementas. Jame turi būti elektroninio parašo ar elektroninio spaudo informacija: pasirašančiojo sertifikato informacija (sertifikato išdavėjas, sertifikato subjektas ir galiojimo data bei laikas), pasirašymo laikas, parašo laiko žyma, jei yra, parašo lygmuo ir formatas.
- *Validation* elementas. Jame turi būti skaitmeninio parašo validavimo būsena ir masyvas validavimo klaidų, jei rasta.

Augment atsakymo JSON objektas turi būti apibrėžtas kaip JSON schema faile (signa-arch-api-schema.json), pateiktame 4.9.5.1 skyrelyje. JSON schemos elementai turi įgyvendinti *Augment* atsakymo elementus pagal vardus, kaip pateikta lentelėje:

Elementas	Aprašymas	JSON nario pavadinimas
AugmentationStatus	Papildymo operacijos vykdymo būsena	augmentStatus
DocumentSpecificationId	SubDO turinį apibrėžiančios specifikacijos identifikatorius	docSpecId
AugmentAt	Sekančio apsaugos veiksmo vykdymo data ir laikas	augmentAt
DocumentAvailableUntil	Laikas, iki kurio apsaugos klientas gali pasiimti papildytą apsaugos objektą	docAvailableUntil
DocumentTicket	Unikalus kodas, kurį apsaugos klientas turėtų naudoti papildyto apsaugos objekto pasiėmimui	docTicket
Signatures	"Signature" objektų masyvas su informacija apie kiekvieną skaitmeninį parašą ir jo papildymo būseną	signatures
Signature elementas		
AugmentationValidation	Elektroninio parašo ar elektroninio spaudo papildymo operacijos metu atlikto validavimo būsena	augmentValidation
AugmentNotBefore	Papildymo laikotarpio sekančio apsaugos veiksmo vykdymui pradžios data ir laikas	augmentNotBefore
AugmentAt	Elektroninio parašo ar elektroninio spaudo sekančio apsaugos veiksmo data ir laikas	augmentAt

AugmentNotAfter	Papildymo laikotarpio sekančio apsaugos veiksmo vykdymui pabaigos data ir laikas	augmentNotAfter
Info	Elektroninio parašo ar elektroninio spaudo informacija	info
Validation	Elektroninio parašo ar elektroninio spaudo validavimo būsena ir klaidų pranešimų masyvas, jei rasta	validation

4.9.3. Download

Download operacija grąžins apsaugos objektą prieš tai papildytą su *Augment* operacija. Ši operacija turi būti iškviesta iš karto gavus *Augment* operacijos atsakymą su *DocumentTicket* reikšme, tokiu būdu leidžiant apsaugos klientui gauti apsaugos objekto turinį. Klientas turi iškviesti *Download* operaciją prieš laiką, nurodytą *Augment* atsakymo *DocumentAvailableUntil* elemente, po kurio apsaugos objektas nebebus prieinamas.

4.9.3.1 Download užklausa

Download užklausoje turi būti nurodyti tokie laukai:

- *document ticket*. Jame turi būti anksčiau apsaugos paslaugų šiam apsaugos objektui priskirtas identifikatorius. Jo reikšmė turi būti tokia pati kaip ir anksčiau vykdytos *Augment* atsakyme (*DocumentTicket*).

Užklausoje gali būti tokie laukai:

- *client ID*. Jame turi būti apsaugos kliento, kviečiančio operaciją, identifikatorius. Jei pateiktas, jo reikšmė turi būti tokia pati kaip ir anksčiau vykdytos *Augment* užklausos.

Aprašyti laukai turi būti įgyvendinti kaip atitinkami HTTP GET užklausos parametrai:

Laukas	Aprašymas	JSON nario pavadinimas
Client ID	Apsaugos kliento identifikatorius	cid
Document ticket	Apsaugos objekto, kurį reikia gauti, identifikatorius	docTicket

4.9.3.2 Download atsakymas

Download operacijos atsakymas grąžinamas kaip HTTP atsakymas su būsenos kodu 200 ir apsaugos objekto turiniu. Apsaugos objekto turinys gražinamas be kodavimo ir transformacijos.

Nesėkmės atveju pateikiamas HTTP atsakymas, kurio būsenos kodas skiriasi nuo 200, ir turinys su klaidos pranešimu.

4.9.4. PreservePO

PreservePO operacija yra naudojama apsaugoti pateiktą apsaugos objektą, kuris yra naujas pateikimo duomenų objektas, ar apsaugos objekto konteinerį, anksčiau gautą atliekant šią operaciją. Pateiktas apsaugos objektas yra elektroninis dokumentas ar konteineris su elektroniniais parašais ar elektroniniais spaudais. Šiai operacijai turi būti pateiktas apsaugos objektas. Apsauga atliekama, papildant elektroninius parašus ir

elektroninius spaudus. Tai apima kūrimą/rinkimą validavimo duomenų (jei jų nebuvo) ir apsaugos įrodymų bei jų įtraukimą į apsaugos objektus – elektroninius parašus ar elektroninius spaudus.

B-B, B-L, B-LT ir B-LTA lygmens elektroniniai parašai ar spaudai yra papildomi ir apskaičiuojami ir grąžinami numatoma įrodymų galiojimo trukmė bei rekomenduojamas sekančio papildymo laikas pagal tuos pačius principus kaip *Augment* operacijoje (4.9.2 skyrelis).

Ši operacija palaiko 4.12 skyrelyje išvardintus pateikimo duomenų objektų formatus. SubDO ir iš jo gauti apsaugos objektai neišsaugomi PSP saugykloje, bet išsaugoma informacija apie atliktus veiksmus (veiksmų sekos). Veiksmų sekose SubDO ir apsaugos objektai bus identifikuojami šios operacijos suteiktu apsaugos objekto identifikatoriumi (id).

PreservePO operacijos sintaksė ir semantika yra apibrėžta ETSI TS 119 512 skyrelyje 5.3.3. Šis profilis palaiko šią operaciją tik naudojant JSON sintaksę.

PreservePO operacija turi priimti tokius *OptionalInputs* elementus, kaip apibrėžta OASIS DSS-X Core 2.0 [DSS Core 2.0] 4.2.8 skyrelyje:

- neprivalomas *lang* elementas. Jei pateiktas, jame turi būti apsaugos paslaugų pranešimų kalbos kodas.
- *other* elementas. Jame turi būti masyvas iš vieno elemento su atributais:
  - *ID* atributas. Jame turi būti fiksuota reikšmė "cid".
  - *value* atributas. Jame turi būti Base64 užkoduotas apsaugos kliento identifikatorius.

PreservePO operacija turi būti prieinama apsaugos klientams, kuriuos gali identifikuoti apsaugos paslaugos. Kad būtų galima identifikuoti apsaugos klientą, *PreservePO* operacijos užklausoje turi būti nurodytas kliento identifikatorius naudojant *other* elementą, kaip aprašyta aukščiau.

PreservePO operacijos rezultatas turi apimti tokius elementus iš *OptionalOutput* elemento, kaip apibrėžta OASIS DSS-X Core 2.0 [DSS Core 2.0] 4.2.9 skyrelyje:

- *other* elementas su elementų masyvu. Kiekvienam PO šis masyvas gali turėti du elementus:
  - Elementas, nurodantis *numatomos įrodymų galiojimo trukmės* laiką. Šis laikas apskaičiuojamas imant minimalų iš visų pateikto PO skaitmeninių parašų numatomą įrodymų galiojimo trukmę.

    Šio elemento *ID* atributas turi turėti fiksuotą reikšmę "eed". *value* atributas turi turėti Base64 užkoduotą laiką (ISO Date Time Format). *idRef* atributas turi turėti PO identifikatoriaus reikšmę (id).
  - Elementas, nurodantis s*ekančio papildymo* laiką. Jame turi būti laikas, nurodantis, kada atitinkamo PO sekantis papildymas turi būti vykdomas. Klientas jį turi naudoti kaip rekomenduojamą laiką sekančio apsaugos veiksmo iškvietimui. Šis laikas apskaičiuojamas imant minimalų visų šio PO apsaugomų skaitmeninių parašų sekančio papildymo laiką.

    Šio elemento *ID* atributas turi turėti fiksuotą reikšmę "aat". *value* atributas turi turėti Base64 užkoduotą laiką (ISO Date Time Format). *idRef* atributas turi turėti PO identifikatoriaus reikšmę (id).

Jei PO negali būti nustatytas *numatomos įrodymų galiojimo trukmės* arba s*ekančio papildymo* laikas, atitinkamas *other* elemento elementas turi būti praleistas.

4.9.5. JSON schemos ir OpenAPI dokumentai

4.9.5.1 JSON schemos failai

JSON schemos apibrėžimai *Augment* ir *Download* operacijoms pateikti:

- https://qtsp.mitsoft.lt/repo/qlps/arch-protocol/v1/signa-arch-api-schema.json

JSON schemos apibrėžimai *RetrieveInfo* ir *PreservePO* operacijoms pateikti:

- https://qtsp.mitsoft.lt/repo/qlps/preserv-protocol/v1/signa-19512-preservation-api-schema.json

4.9.5.2 OpenAPI specifikacijos

OpenAPI specifikacijos *Augment* ir *Download* operacijoms pateiktos:

- https://qtsp.mitsoft.lt/repo/qlps/arch-protocol/v1/signa-arch-api-openapi.json

OpenAPI specifikacijos *RetrieveInfo* ir *PreservePO* operacijoms pateiktos:

- https://qtsp.mitsoft.lt/repo/qlps/preserv-protocol/v1/signa-19512-preservation-api-openapi.json

4.10. Apsaugos protokolo naudojimo gairės

4.8 ir 4.9 skyreliai detaliai aprašo pateikimo duomenų objekte esančių elektroninių parašų ir elektroninių spaudų papildymo procesą. Juose taip pat paaiškinta, kaip nustatoma numatoma įrodymų galiojimo trukmė ir kaip, pasirenkant sekančio papildymo laiką, naudojami papildymo laikotarpis ir atsargumo laikotarpis. Apsaugos operacijos turi būti naudojamos, atsižvelgiant į šią informaciją.

Abonentas turi naudoti apsaugos operacijas pagal šias gaires:

- MitSoft PSP primygtinai rekomenduoja sekančio kreipinio į apsaugos paslaugas laiką planuoti, kaip nurodytą apsaugos operacijų (*augment*, *PreservePO*) rezultatuose viso apsaugos objekto lygyje (*AugmentAt*, *aat*).
- Jei apsaugos klientas ignoruoja rekomenduojamą sekančio papildymo laiką, jis turėtų planuoti sekantį kreipinį į apsaugos paslaugų operacijas tokiu būdu:
    - Planuoti sekantį apsaugos operacijų kreipinį laiko intervale tarp papildymo laikotarpio pradžios ir atsargumo laikotarpio pradžios.
    - Nustatyti tikslius papildymo laikotarpio pradžios ir atsargumo laikotarpio pradžios laikus pateikimo objektui, remiantis ankstesnio apsaugos operacijos kreipinio *numatomos įrodymų galiojimo trukmės* laiku ir papildymo laikotarpiu bei atsargumo laikotarpiu, nurodytais Abonentinėje sutartyje.
    - Vengti apsaugos operacijų kreipinių prieš papildymo laikotarpio pradžią. Apsaugos paslaugos ignoruos tokį kreipinį, nebent jis būtinas dėl pasikeitusios numatomos įrodymų galiojimo trukmės (žr. žemiau).
    - Vengti apsaugos operacijų kreipinių atsargumo laikotarpiu. Nors tokie kreipiniai gali būti sėkmingi, tai kelia pavojų praleisti objekto apsaugą, sutrikus apsaugos paslaugoms ar kitoms susijusioms paslaugoms.
- Jei apsaugos operacijų kreipinys nesėkmingas dėl sutrikusių apsaugos paslaugų (paslauga nepasiekiama, programinės įrangos klaidos, nepasiekiamos susijusios paslaugos), apsaugos klientas kartos apsaugos operacijų kreipinius, kol apsaugos paslaugos taps pasiekiamos.
- Apsaugos klientas turi įgyvendinti galimybę kreiptis į apsaugos paslaugas prieš planuotą sekančio papildymo laiką. Pavyzdžiui, gavus informaciją, kad

apsaugos objektų apsauga turi būti atlikta anksčiau nei planuota dėl (netikėto) kriptografinių algoritmų patikimumo laikotarpio pasikeitimo.

4.11. Taikomos taisyklės

MitSoftQWOS profilis palaiko tokias apsaugos įrodymų taisykles:

- MitSoft Kvalifikuotos ilgalaikės apsaugos paslaugų apsaugos įrodymų taisyklės, kurias nurodo unikalus objekto identifikatorius (OID):
  - 1.3.6.1.4.1.57890.1.7.1.X

  kur x žymi naujausią versiją. Visos versijos yra prieinamos abonentams MitSoft PSP saugykloje. Kiekvienoje versijoje nurodytas momentas, nuo kurio ši taisyklių versija tapo arba bus aktyvi. Versijos galiojimo laikas baigiasi, kai tampa aktyvi nauja versija.

MitSoftQWOS profilis palaiko tokias apsaugos parašo taisykles:

- MitSoft Kvalifikuotos ilgalaikės apsaugos paslaugų parašo taisyklės, kurias nurodo unikalus objekto identifikatorius (OID):
  - 1.3.6.1.4.1.57890.1.6.1.X

  kur x žymi naujausią versiją. Visos versijos yra prieinamos abonentams MitSoft PSP saugykloje. Kiekvienoje versijoje nurodytas momentas, nuo kurio ši taisyklių versija tapo arba bus aktyvi. Versijos galiojimo laikas baigiasi, kai tampa aktyvi nauja versija.

4.12. Palaikomi pateikimo duomenų objektai

Apsaugos paslaugos priima elektroninius dokumentus ar konteinerius, pasirašytus elektroniniais parašais arba patvirtintus elektroniniais spaudais. Kiekviename pateiktame elektroniniame dokumente ar konteineryje turi būti duomenys, pasirašyti elektroniniu parašu arba patvirtinti elektroniniu spaudu.

Kiekviename pateikimo duomenų objekte turi būti bent vienas elektroninis parašas ar elektroninis spaudas.

Šio apsaugos profilio palaikomi pateikimo duomenų objektų formatai apibrėžti lentelėje:

Pateikimo duomenų objekto formatas (elektroninio dokumento specifikacija ar konteinerio standartas)	**Elektroninio parašo/spaudo formatas**	**Pateikimo duomenų objekto (specifikacijos) identifikatorius**
ADOC-V1.0 elektroninis dokumentas	XAdES	ADOC-V1.0
ADOC-V2.0 elektroninis dokumentas	XAdES baseline	ADOC-V2.0
EGAS-V1.0 elektroninis dokumentas	XAdES	EGAS-V1.0
MDOC-V1.0 elektroninis dokumentas	XAdES	MDOC-V1.0
PDF-LT-V1.0 elektroninis dokumentas	PAdES baseline	PDF-LT-V1.0
PDF-RC-V1.0 elektroninis dokumentas	PAdES baseline	PDF-RC-V1.0
ASiC-E konteineris pagal ETSI TS 103 174	XAdES baseline	ASiC-E-XAdES-TS
ASiC-E konteineris pagal ETSI EN 319 162-1	XAdES baseline	ASiC-E-XAdES-EN

ASiC-S konteineris pagal ETSI TS 103 174	XAdES baseline	ASiC-S-XAdES-TS
	CAdES baseline	ASiC-S-CAdES-TS
ASiC-S konteineris pagal ETSI EN 319 162-1	XAdES baseline	ASiC-S-XAdES-EN
	CAdES baseline	ASiC-S-CAdES-EN
PDF dokumentas su PAdES parašais pagal ETSI TS 103 172	PAdES baseline	PDF-PAdES-TS
PDF dokumentas su PAdES parašais pagal to ETSI EN 319 142-1	PAdES baseline	PDF-PAdES-EN
PDF dokumentas su CMS parašais	PAdES	PDF-PAdES-CMS

Palaikomų pateikimo duomenų objektų aibė konkrečiam abonentui gali būti susiaurinta Abonentinėje sutartyje tarp apsaugos paslaugų abonento ir MitSoft PSP.

4.12.1. ADOC-V1.0 elektroniniai dokumentai

ADOC-V1.0 elektroninis dokumentas [ADOC-V1.0], kuriame yra bent vienas XAdES elektroninis parašas ar elektroninis spaudas, atitinkantis XAdES standartą ETSI TS 101 903 [TS 101 903].

Šis pateikimo duomenų objektas identifikuojamas tokiu identifikatoriumi:

- `ADOC-V1.0`

Šis pateikimo duomenų objektas identifikuojamas tokiu URI identifikatoriumi:

- `http://uri.mitsoft.lt/specification/type/adoc-v1.0`

Šio pateikimo duomenų objekto MIME tipas yra:

- `application/vnd.lt.archyvai.adoc-2008`

4.12.2. ADOC-V2.0 elektroniniai dokumentai

ADOC-V2.0 elektroninis dokumentas [ADOC-V2.0], kuriame yra bent vienas XAdES elektroninis parašas ar elektroninis spaudas, atitinkantis XAdES bazinio profilio standartą ETSI TS 103 171 [TS 103 171].

Šis pateikimo duomenų objektas identifikuojamas tokiu identifikatoriumi:

- `ADOC-V2.0`

Šis pateikimo duomenų objektas identifikuojamas tokiu URI identifikatoriumi:

- `http://uri.mitsoft.lt/specification/type/adoc-v2.0`

Šio pateikimo duomenų objekto MIME tipas yra:

- `application/vnd.etsi.asic-e+zip`

4.12.3. EGAS-V1.0 elektroniniai dokumentai

EGAS-V1.0 elektroninis dokumentas [EGAS-V1.0], kuriame yra bent vienas XAdES elektroninis parašas ar elektroninis spaudas, atitinkantis XAdES standartą ETSI TS 101 903 [TS 101 903].

Šis pateikimo duomenų objektas identifikuojamas tokiu identifikatoriumi:

- `EGAS-V1.0`

Šis pateikimo duomenų objektas identifikuojamas tokiu URI identifikatoriumi:

- `http://uri.mitsoft.lt/specification/type/egas-v1.0`

Šio pateikimo duomenų objekto MIME tipas yra:

- `application/vnd.lt.sodra.egas-2009`

4.12.4. MDOC-V1.0 elektroniniai dokumentai

MDOC-V1.0 elektroninis dokumentas [MDOC-V1.0], kuriame yra bent vienas XAdES elektroninis parašas ar elektroninis spaudas, atitinkantis XAdES standartą ETSI TS 101 903 [TS 101 903].

Šis pateikimo duomenų objektas identifikuojamas tokiu identifikatoriumi:

- `MDOC-V1.0`

Šis pateikimo duomenų objektas identifikuojamas tokiu URI identifikatoriumi:

- `http://uri.mitsoft.lt/specification/type/mdoc-v1.0`

Šio pateikimo duomenų objekto MIME tipas yra:

- `application/vnd.lt.archyvai.mdoc-2010`

4.12.5. PDF-LT-V1.0 elektroniniai dokumentai

PDF-LT-V1.0 elektroninis dokumentas [PDF-LT-V1.0], kuriame yra bent vienas PAdES elektroninis parašas ar elektroninis spaudas, atitinkantis PAdES bazinio profilio standartą ETSI TS 103 172 [TS 103 172].

Šis pateikimo duomenų objektas identifikuojamas tokiu identifikatoriumi:

- `PDF-LT-V1.0`

Šis pateikimo duomenų objektas identifikuojamas tokiu URI identifikatoriumi:

- `http://uri.mitsoft.lt/specification/type/pdf-lt-v1.0`

Šio pateikimo duomenų objekto MIME tipas yra:

- `application/pdf`

4.12.6. PDF-RC-V1.0 elektroniniai dokumentai

PDF-RC-V1.0 elektroninis dokumentas [PDF-RC-V1.0], kuriame yra bent vienas PAdES elektroninis parašas ar elektroninis spaudas, atitinkantis PAdES bazinio profilio standartą ETSI EN 319 142-1 [EN 319 142-1].

Šis pateikimo duomenų objektas identifikuojamas tokiu identifikatoriumi:

- `PDF-RC-V1.0`

Šis pateikimo duomenų objektas identifikuojamas tokiu URI identifikatoriumi:

- `http://uri.mitsoft.lt/specification/type/pdf-rc-v1.0`

Šio pateikimo duomenų objekto MIME tipas yra:

- `application/pdf`

4.12.7. ASiC-E konteineris pagal ETSI TS 103 174

ASiC-E konteineris, kuris atitinka ASiC bazinio profilio standartą [TS 103 174] ir kuriame yra bent vienas XAdES elektroninis parašas ar elektroninis spaudas, atitinkantis XAdES bazinio profilio standartą ETSI TS 103 171 [TS 103 171].

Šis pateikimo duomenų objektas identifikuojamas tokiu identifikatoriumi:

- `ASiC-E-XAdES-TS`

Šis pateikimo duomenų objektas identifikuojamas tokiu URI identifikatoriumi:

- `http://uri.mitsoft.lt/ades/type/asic-e/xades/ts`

Šio pateikimo duomenų objekto MIME tipas yra:

- `application/vnd.etsi.asic-e+zip`

4.12.8. ASiC-E konteineris pagal ETSI EN 319 162-1

ASiC-E konteineris, kuris atitinka Sudedamųjų dalių ir ASiC bazinių konteinerių standartą ETSI EN 319 162-1 [EN 319 162-1] ir kuriame yra bent vienas XAdES elektroninis parašas ar elektroninis spaudas, atitinkantis Sudedamųjų dalių ir XAdES bazinių parašų standartą ETSI EN 319132-1 [EN 319 132-1].

Šis pateikimo duomenų objektas identifikuojamas tokiu identifikatoriumi:

- `ASiC-E-XAdES-EN`

Šis pateikimo duomenų objektas identifikuojamas tokiu URI identifikatoriumi:

- `http://uri.mitsoft.lt/ades/type/asic-e/xades/en`

Šio pateikimo duomenų objekto MIME tipas yra:

- `application/vnd.etsi.asic-e+zip`

4.12.9. ASiC-S konteineris su XAdES parašais pagal ETSI TS 103 174

ASiC-S konteineris, kuris atitinka ASiC bazinio profilio standartą ETSI TS 103 174 [TS 103 174] ir kuriame yra bent vienas XAdES elektroninis parašas ar elektroninis spaudas, atitinkantis XAdES bazinį profilį pagal ETSI TS 103 171 [TS 103 171].

Šis pateikimo duomenų objektas identifikuojamas tokiu identifikatoriumi:

- `ASiC-S-XAdES-TS`

Šis pateikimo duomenų objektas identifikuojamas tokiu URI identifikatoriumi:

- `http://uri.mitsoft.lt/ades/type/asic-s/xades/ts`

Šio pateikimo duomenų objekto MIME tipas yra:

- `application/vnd.etsi.asic-s+zip`

4.12.10. ASiC-S konteineris su CAdES parašais pagal ETSI TS 103 174

ASiC-S konteineris, kuris atitinka ASiC bazinio profilio standartą ETSI TS 103 174 [TS 103 174] ir kuriame yra bent vienas CAdES elektroninis parašas ar elektroninis spaudas, atitinkantis CAdES bazinį profilį pagal ETSI TS 103 173 [TS 103 173].

Šis pateikimo duomenų objektas identifikuojamas tokiu identifikatoriumi:

- `ASiC-S-CAdES-TS`

Šis pateikimo duomenų objektas identifikuojamas tokiu URI identifikatoriumi:

- `http://uri.mitsoft.lt/ades/type/asic-s/cades/ts`

Šio pateikimo duomenų objekto MIME tipas yra:

- `application/vnd.etsi.asic-s+zip`

4.12.11. ASiC-S konteineris su XAdES parašais pagal ETSI EN 319 162-1

ASiC-S konteineris, kuris atitinka Sudedamųjų dalių ir ASiC bazinių konteinerių standartą ETSI EN 319 162-1 [EN 319 162-1] ir kuriame yra bent vienas XAdES elektroninis parašas ar elektroninis spaudas, atitinkantis Sudedamųjų dalių ir XAdES bazinių parašų standartą ETSI EN 319 132-1 [EN 319 132-1].

Šis pateikimo duomenų objektas identifikuojamas tokiu identifikatoriumi:

- `ASiC-S-XAdES-EN`

Šis pateikimo duomenų objektas identifikuojamas tokiu URI identifikatoriumi:

- `http://uri.mitsoft.lt/ades/type/asic-s/xades/en`

Šio pateikimo duomenų objekto MIME tipas yra:

- `application/vnd.etsi.asic-s+zip`

4.12.12. ASiC-S konteineris su CAdES parašais pagal ETSI EN 319 162-1

ASiC-S konteineris, kuris atitinka Sudedamųjų dalių ir ASiC bazinių konteinerių standartą [EN 319 162-1] ir kuriame yra bent vienas CAdES elektroninis parašas ar elektroninis spaudas, atitinkantis Sudedamųjų dalių ir CAdES bazinių parašų standartą ETSI EN 319 122-1 [EN 319 122-1].

Šis pateikimo duomenų objektas identifikuojamas tokiu identifikatoriumi:

- `ASiC-S-CAdES-EN`

Šis pateikimo duomenų objektas identifikuojamas tokiu URI identifikatoriumi:

- `http://uri.mitsoft.lt/ades/type/asic-s/cades/en`

Šio pateikimo duomenų objekto MIME tipas yra:

- `application/vnd.etsi.asic-s+zip`

4.12.13. PDF dokumentai su PAdES parašais pagal ETSI TS 103 172

PDF elektroninis dokumentas su PAdES elektroniniu parašu ar elektroniniu spaudu, atitinkančiu PAdES bazinio profilio standartą ETSI TS 103 172 [TS 103 172].

Šis pateikimo duomenų objektas identifikuojamas tokiu identifikatoriumi:

- `PDF-PAdES-TS`

Šis pateikimo duomenų objektas identifikuojamas tokiu URI identifikatoriumi:

- `http://uri.mitsoft.lt/ades/type/pdf/pades/ts`

Šio pateikimo duomenų objekto MIME tipas yra:

- `application/pdf`

4.12.14. PDF dokumentai su PAdES parašais pagal ETSI EN 319 142-1

PDF elektroninis dokumentas su PAdES elektroniniu parašu ar elektroniniu spaudu, atitinkančiu Sudedamųjų dalių ir PAdES bazinių parašų standartą ETSI EN 319 142-1 [EN 319 142-1].

Šis pateikimo duomenų objektas identifikuojamas tokiu identifikatoriumi:

- `PDF-PAdES-EN`

Šis pateikimo duomenų objektas identifikuojamas tokiu URI identifikatoriumi:

- `http://uri.mitsoft.lt/ades/type/pdf/pades/en`

Šio pateikimo duomenų objekto MIME tipas yra:

- `application/pdf`

4.12.15. PDF dokumentai su CMS parašais

PDF elektroninis dokumentas su PAdES elektroniniu parašu ar elektroniniu spaudu, atitinkančiu CMS parašų PDF dokumente profilį apibrėžtą ETSI TS 102 778-2 standarte „PDF pažangiųjų elektroninių parašų profilis; 2 dalis: PAdES Basic – Profilis ISO 32000-1 pagrindu“ [TS 102 778-2]. Šio profilio ilgo galiojimo forma apibrėžta ETSI TS 102 778-4 standarte „PDF pažangiųjų elektroninių parašų profilis; 4 dalis: Ilgo galiojimo PAdES – PAdES LTV profilis“ [TS 102 778-4].

Šis pateikimo duomenų objektas identifikuojamas tokiu identifikatoriumi:

- `PDF-PAdES-CMS`

Šis pateikimo duomenų objektas identifikuojamas tokiu URI identifikatoriumi:

- `http://uri.mitsoft.lt/ades/type/pdf/pades/cms`

Šio pateikimo duomenų objekto MIME tipas yra:

- `application/pdf`

4.13. Palaikomi apsaugos įrodymų formatai

Šis apsaugos profilis palaiko tokius apsaugos įrodymų formatus: XAdES archyvinė laiko žyma, CAdES archyvinė laiko žyma V3, PAdES dokumento laiko žyma.

4.13.1. XAdES archyvinė laiko žyma

XML formato *Archive Time Stamp* atributas pagal ETSI TS 101 903 [TS 101 903] ir ETSI EN 319 162-1 [EN 319 162-1] naudojamas apsaugai XAdES skaitmeninių parašų ADOC-V1.0, ADOC-V2.0, EGAS-V1.0, MDOC-V1.0 elektroniniuose dokumentuose ir ASiC-E, ASiC-S konteineriuose su XAdES skaitmeniniais parašais.

4.13.2. CAdES archyvinė laiko žyma V3

ASN.1 formato *Archive Time Stamp V3* atributas pagal ETSI TS 101 733 [TS 101 733] ir ETSI EN 319 122-1 [EN 319 122-1] naudojamas apsaugai CAdES skaitmeninių parašų ASiC-S konteineriuose su CAdES skaitmeniniais parašais.

4.13.3. PAdES dokumento laiko žyma

Document Time-Stamp atributas pagal ETSI TS 102 778-4 [TS 102 778-4] ir ETSI EN 319 142-1 [EN 319 142-1] naudojamas apsaugai PAdES skaitmeninių parašų PDF-LT-V1.0, PDF-RC-V1.0 elektroniniuose dokumentuose ir PDF dokumentuose su PAdES skaitmeniniais parašais.