MitSoft

Kvalifikuotos ilgalaikės apsaugos paslaugos

Apsaugos profilis su saugykla

QLPS/PP-WST-LT

Unikalus objekto ID (OID): **1.3.6.1.4.1.57890.1.5.1**

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 5
2. Nuorodos 6
3. Sąvokų ir santrumpų apibrėžimas 8
4. Kvalifikuotų elektroninių parašų ir spaudų MitSoft apsaugos profilis su saugykla 10
4.1. Aprašymas 10
4.2. Identifikavimas 10
4.3. Galiojimo laikotarpis 11
4.4. Apsaugos schema 11
4.5. Apsaugos tikslas 11
4.6. Apsaugos saugyklos modelis 11
4.7. Palaikomos operacijos 11
4.8. Pateikimo duomenų objektai ir apsaugos objektai 12
4.9. Apsaugos protokolas 13
4.9.1. RetrieveInfo 13
4.9.2. Store 13
4.9.2.1 Store užklausa 14
4.9.2.2 Store atsakymas 14
4.9.3. Status 15
4.9.3.1 Status užklausa 15
4.9.3.2 Status atsakymas 16
4.9.4. Download 17
4.9.4.1 Download užklausa 18
4.9.4.2 Download atsakymas 18
4.9.5. Remove 18
4.9.5.1 Remove užklausa 18
4.9.5.2 Remove atsakymas 19
4.9.6. PreservePO 19
4.9.7. RetrievePO 20
4.9.8. DeletePO 20
4.9.9. RetrieveTrace 21
4.9.10. Search 21
4.9.11. JSON schemos ir OpenAPI dokumentai 22
4.9.11.1 JSON schemos failai 22
4.9.11.2 OpenAPI specifikacijos 22
4.10. Apsaugos protokolo naudojimo gairės 22

4.11. Taikomos taisyklės 23
4.12. Palaikomi pateikimo duomenų objektai 23
4.12.1. ADOC-V1.0 elektroniniai dokumentai 24
4.12.2. ADOC-V2.0 elektroniniai dokumentai 24
4.12.3. EGAS-V1.0 elektroniniai dokumentai 25
4.12.4. MDOC-V1.0 elektroniniai dokumentai 25
4.12.5. PDF-LT-V1.0 elektroniniai dokumentai 25
4.12.6. PDF-RC-V1.0 elektroniniai dokumentai 25
4.12.7. ASiC-E konteineris pagal ETSI TS 103 174 26
4.12.8. ASiC-E konteineris pagal ETSI EN 319 162-1 26
4.12.9. ASiC-S konteineris su XAdES parašais pagal ETSI TS 103 174 26
4.12.10. ASiC-S konteineris su CAdES parašais pagal ETSI TS 103 174 26
4.12.11. ASiC-S konteineris su XAdES parašais pagal ETSI EN 319 162-1 27
4.12.12. ASiC-S konteineris su CAdES parašais pagal ETSI EN 319 162-1 27
4.12.13. PDF dokumentai su PAdES parašais pagal ETSI TS 103 172 27
4.12.14. PDF dokumentai su PAdES parašais pagal ETSI EN 319 142-1 27
4.12.15. PDF dokumentai su CMS parašais 28
4.13. Palaikomi apsaugos įrodymų formatai 28
4.13.1. XAdES archyvinė laiko žyma 28
4.13.2. CAdES archyvinė laiko žyma V3 28
4.13.3. PAdES dokumento laiko žyma 28
4.14. Kriptografinis monitoringas 28

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:

- MitSoftQWST profilis – kvalifikuotų elektroninių parašų ir spaudų MitSoft apsaugos profilis su saugykla.

MitSoftQWST profilis turi būti naudojamas, kai kvalifikuoti elektroniniai parašai, pažangūs elektroniniai parašai, kvalifikuoti elektroniniai spaudai, pažangūs elektroniniai spaudai, esantys elektroniniuose dokumentuose ar konteineriuose, turi būti apsaugomi MitSoft PSP, išsaugojus PSP saugykloje.

Apsaugos saugyklos modelis, apsaugos tikslai, MitSoftQWST 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 119 512] – 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 / spaudo 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 su saugykla

4.1. Aprašymas

MitSoftQWST profilis apibrėžia MitSoft apsaugos paslaugų eksploatacines detales, kai jos naudojamos su integruota elektroninių dokumentų saugykla. Apsaugos objektai saugomi PSP saugykloje. Apsaugos paslaugų naudojant MitSoftQWST profilį tikslas – ilgą laiką išsaugoti galimybę patvirtinti elektroninius parašus ir elektroninius spaudus, palaikyti jų galiojimo būseną ir gauti susijusių pasirašytų duomenų egzistavimo įrodymus.

Apsaugos paslaugose saugomi apsaugos objektai yra kvalifikuoti elektroniniai parašai ir kvalifikuoti elektroniniai spaudai, esantys pasirašytuose/patvirtintuose elektroniniuose dokumentuose ar konteineriuose. Apsaugos paslaugos saugo 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 saugomu elektroniniu parašu arba patvirtinti 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, saugomi šiame profilyje, yra pateikti 4.8 skyrelyje.

Šis profilis turi būti naudojamas, kai pasirašyti/patvirtinti elektroniniai dokumentai/konteineriai yra saugomi MitSoft apsaugos paslaugose. Apsaugos paslaugos yra atsakingos už elektroninių parašų ir elektroninių spaudų, esančių pasirašytuose/patvirtintuose elektroniniuose dokumentuose/konteineriuose, priežiūrą ir apsaugą per apsaugos laikotarpį.

MitSoftQWST profilis pateikia operacijas:

- elektroninių dokumentų/konteinerių pateikimui MitSoft apsaugos paslaugoms ir jų patalpinimui MitSoft apsaugos paslaugų saugykloje (žr. Store, PreservePO operacijas),
- elektroninių dokumentų/konteinerių parsisiuntimui iš MitSoft apsaugos paslaugų saugyklos (žr. Download, RetrievePO operacijas),
- elektroninių dokumentų/konteinerių pašalinimui iš MitSoft apsaugos paslaugų saugyklos (žr. Remove, DeletePO operacijas),
- gavimui informacijos apie saugomų elektroninių dokumentų/konteinerių einamąją būseną (žr. Status ir RetrieveTrace operacijas).

MitSoft apsaugos paslaugos elektroninių parašų ir elektroninių spaudų, esančių saugomuose elektroniniuose dokumentuose, apsaugą atlieka automatiškai ir laiku.

4.2. Identifikavimas

MitSoftQWST profilio unikalus identifikatorius (OID) yra:

- Identifikatorius OID forma yra
  - 1.3.6.1.4.1.57890.1.5.1;

Jo laukų reikšmės yra pateiktos 1 lentelėje.

- Identifikatorius URI forma yra
  - `http://uri.mitsoft.lt/preservation/profile/qwst/1`

1 lentelė. MitSoftQWST profilio 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 (apsaugos profilis)	5
Apsaugos profilio identifikatorius	1

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

MitSoftQWST profilis įgyvendina tokią apsaugos schemą:

- apsaugos schema su parašo papildymu ir saugykla, apibrėžta ETSI TS 119 512 [TS 119 512] F.3 priede ir nurodoma identifikatoriumi:
  - `http://uri.etsi.org/19512/scheme/pds+wst+aug`

4.5. Apsaugos tikslas

MitSoftQWST 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

MitSoftQWST profilis palaiko apsaugos paslaugas su saugykla – WTS pagal ETSI TS 119 512 [TS 119 512].

4.7. Palaikomos operacijos

Šis apsaugos profilis palaiko tokias operacijas:

- RetrieveInfo,
- Store,
- Status,

- Download,
- Remove,
- PreservePO,
- RetrievePO,
- DeletePO,
- RetrieveTrace,
- Search.

4.8. Pateikimo duomenų objektai ir apsaugos objektai

MitSoftQWST 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 patvirtintus 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 saugo kvalifikuotus elektroninius parašus ir kvalifikuotus elektroninius spaudus. Apsaugos paslaugos saugo 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).

Priimti pateikimo duomenų objektai, neturintys jokių elektroninių parašų ar elektroninių spaudų, yra išsaugomi PSP saugykloje, bet apsaugos veiksmai jiems neatliekami. Tokie SubDO gali būti pašalinti iš MitSoft PSP dokumentų saugyklos, klientui iškvietus atitinkamas operacijas (*Remove*, *DeletePO*).

Elektroninių parašų ir elektroninių spaudų apsauga yra užtikrinama uždedant naujas archyvines laiko žymas. PSP apsaugos mechanizmas užtikrina, kad nauji apsaugos įrodymai (archyvinės laiko žymos) bus pridėti, kai baigsis paskutinės archyvinės laiko žymos sertifikato galiojimas ar kažkuris kriptografinis algoritmas taps nepakankamai saugiu, kad užtikrintų apsaugos įrodymų patikimumą artimiausioje

ateityje. Nauja apsaugos įrodymų taisyklių versija gali būti parengta ir pradėta naudoti, jei dabartinės apsaugos įrodymų taisyklės nebegali užtikrinti reikiamo patikimumo lygio.

Jei elektroninių parašų ir elektroninių spaudų apsauga negali būti atlikta dėl nepasiekiamų validavimo duomenų ir (arba) laiko žymų tarnybos, bandymai papildyti bus kartojami pagrįstą laikotarpį.

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, saugomu 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 saugomus 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.

Apsaugos objekto identifikatorius identifikuoja vieną elektroninį dokumentą/konteinerį (POC) ir jame esantį kiekvieną apsaugomą skaitmeninį parašą.

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. 4.9.11 skyrelį).

MitSoftQWST profilis palaiko tokias operacijas:

4.9.1. RetrieveInfo

RetrieveInfo operacija naudojama palaikomų apsaugos profilių sąrašui gauti.

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. Store

Store operacija yra analogiškos ETSI TS 119 512 apibrėžtos *PreservePO* operacijos išplėtimas. *Store* operacija naudojama pateikimo duomenų objekto (SubDO) pateikimui apsaugos paslaugoms. Šiai operacijai turi būti perduotas pateikimo duomenų objektas. Taip pat šiai operacijai gali būti pateikta neprivaloma papildoma informacija. Apsaugos paslaugos yra atsakingos už gauto pateikimo duomenų objekto išsaugojimą ir SubDO esančių apsaugos objektų apsaugą, papildant elektroninius parašus/spaudus. Išsami informacija apie apsaugos objektus ir tai, kaip jie gaunami iš SubDO, aprašyta 4.8 skyrelyje. Apsaugos paslaugos saugo papildomus duomenis tokius, kokie yra, ir apsaugos paslaugos nėra atsakingos už tokių duomenų egzistavimo įrodymų teikimą.

Ši operacija palaiko 4.12 skyrelyje išvardintus pateikimo duomenų objektų formatus.

Šis profilis palaiko šią operaciją naudojant JSON sintaksę. JSON schema ir OpenAPI dokumentas pateikti 4.9.11 skyrelyje.

4.9.2.1 Store užklausa

Store 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 *external identifier*. Jei pateiktas, jame turi būti apsaugos kliento suteiktas SubDO identifikatorius. Identifikatorius turi būti unikalus tarp to apsaugos kliento SubDO.

  Jei kitas šio kliento PO su tokiu identifikatoriumi jau saugomas apsaugos paslaugose, tai jis bus pakeistas pateiktu SubDO.
- neprivalomas *preserve till*. Jei pateiktas, jame turi būti data, iki kurios apsaugos paslaugos turi saugoti SubDO esančius apsaugos objektus. Jei jis praleistas ar jo reikšmė *null*, apsaugos objektas bus saugomas neribotą laiką.

Užklausa gali turėti papildomus laukus, kuriuose pateikiami su pateikimo duomenų objektu susiję metaduomenys išsaugojimui apsaugos paslaugose (apsaugos objekto pavadinimas, tipas, data, numeris ir kt.). Žiūrėti JSON sintaksės failą (4.9.11 skyrelyje).

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
External identifier	Kliento sistemoje naudojamas SubDO identifikatorius	extCode
Preserve till	Data, iki kurios apsaugos objektas turėtų būti saugomas	maintainableUntil

4.9.2.2 Store atsakymas

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

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

Sėkmės atveju pateikiamas HTTP atsakymas su būsenos kodu 200. Atsakyme turi būti pateikiami tokie elementai:

- *operation status* elementas. Jame turi būti reikšmė „success", nurodanti operacijos sėkmę.
- *external identifier* elementas. Jame turi būti apsaugos objekto identifikatorius apsaugos paslaugose. Jei *external identifier* buvo pateiktas operacijos užklausoje, grąžinama ta pati reikšmė. Jei *external identifier* buvo praleistas ar jo reikšmė buvo *null*, grąžinama apsaugos paslaugų suteikta nauja identifikatoriaus reikšmė. Ją turėtų naudoti apsaugos klientas apsaugos objekto nurodymui paskesniuose apsaugos paslaugų operacijų kreipiniuose.

Store atsakymo JSON objektas turi būti apibrėžtas kaip JSON schema faile (signa-arch-api-schema.json), pateiktame 4.9.11.1 skyrelyje. JSON schemos elementai turi įgyvendinti *Store* atsakymo elementus pagal vardus, kaip pateikta lentelėje:

Elementas	Aprašymas	JSON nario pavadinimas
Operation status	Operacijos įvykdymo būsena	status
External identifier	Apsaugos objekto identifikatorius apsaugos paslaugose	extCode

4.9.3. Status

Status operacija yra analogiškos ETSI TS 119 512 apibrėžtos *RetrieveTrace* operacijos išplėtimas. *Status* operacija naudojama gavimui informacijos apie saugomą apsaugos objektą (elektroninį dokumentą/konteinerį), bet ne apie patį apsaugos objektą. Šiai operacijai turi būti pateiktas apsaugos objekto identifikatorius. Operacija grąžina einamąją būseną anksčiau pateikto elektroninio dokumento/konteinerio, jo pagrindinių duomenų ir jame esančių elektroninių parašų ir elektroninių spaudų galiojimo būseną. Operacija turi gražinti būsenos informaciją tik apsaugos objektų, kurie prieinami apsaugos klientui.

Šis profilis palaiko šią operaciją naudojant JSON sintaksę. JSON schema ir OpenAPI dokumentas pateikti 4.9.11 skyrelyje.

4.9.3.1 Status užklausa

Status užklausoje turi būti nurodyti tokie laukai:

- *client ID*. Jame turi būti apsaugos kliento, kviečiančio operaciją, identifikatorius.
- *identifier*. Jame turi būti nuoroda į apsaugos objektą, kurį klientas anksčiau pateikė apsaugos paslaugoms (žr. *store* operaciją ir jos *external identifier* lauką).

Užklausoje gali būti tokie laukai:

- neprivalomas *mode*. Jei pateiktas, jame turi būti nurodyta kliento pageidaujamų duomenų apie apsaugos objektą apimtis. Jis gali nurodyti tik patikrinti apsaugos objekto buvimą apsaugos paslaugose, gauti daugiau duomenų apie jo būseną apsaugos paslaugose ar gauti informaciją apie saugomo objekto turinį ir skaitmeninių parašų validavimą. Žiūrėti JSON sintaksės failą (4.9.11 skyrelyje).

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

Laukas	Aprašymas	JSON nario pavadinimas
Client Id	Kliento identifikatorius	cid
Identifier	Apsaugos objekto identifikatorius	extCode
Mode	Režimas, apibrėžiantis grąžinamų duomenų apimtį	mode

4.9.3.2 Status atsakymas

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

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

Sėkmės atveju pateikiamas HTTP atsakymas su būsenos kodu 200 ir jame yra apsaugos objekto būsenos informacija.

Atsakyme turi būti pateikiami tokie elementai:

- *status* elementas. Jame turi būti nurodoma, ar apsaugos objektas yra apsaugos paslaugoje, jis validus ar turi klaidų.
- *document identifier* elementas. Jame turi būti apsaugos objekto identifikatorius.

Priklausomai nuo *mode* parametro reikšmės, nurodytos Status užklausoje, atsakyme gali būti tokie papildomi elementai:

- *document specification* elementas. Jei pateiktas, jame turi būti dokumento specifikacijos identifikatorius, apibrėžiantis pateikimo duomenų objekto turinio tipą. Identifikatorius atitinka vieną iš specifikacijų, išvardintų 4.12 skyrelyje.
- *maintainable until* elementas. Jei pateiktas, jis turi nurodyti datą, iki kurios apsaugos paslaugos saugos apsaugos objektą.
- *next update date* elementas. Jei pateiktas, jame turi būti data ir laikas, kada apsaugos paslaugos atliks apsaugos objekto ir jo skaitmeninių parašų analizę.
- *last augment date* elementas. Jei pateiktas, jame turi būti data ir laikas, kada apsaugos paslaugos paskutinį kartą atliko apsaugos objekte esančių skaitmeninių parašų papildymą.
- *last augment status* element. Jei pateiktas, jame turi būti paskutinės apsaugos objekto skaitmeninių parašų papildymo operacijos būsena.
- *next augment date* element. Jei pateiktas, jame turi būti data ir laikas, kada apsaugos paslaugos planuoja atlikti kitą apsaugos objekto ir jo skaitmeninių parašų papildymą.
- *events* element. Jei pateiktas, jame turi būti sąrašas veiksmų, kuriuos su apsaugos objektu atliko apsaugos klientas ar apsaugos paslaugos.
- *structure* element. Jei pateiktas, jame turi būti apsaugos objekto struktūros validavimo būsena ir sąrašas klaidų, jei tokių nustatyta.
- *packaging* element. Jei pateiktas, jame turi būti apsaugos objekto paketo (pvz., elektroninio dokumento failo) validavimo būsena ir sąrašas klaidų, jei tokių nustatyta.
- *signature* element. Jei pateiktas, jame turi būti sąrašas apsaugos objekto skaitmeninių parašų. Sąrašo elementą sudaro skaitmeninio parašo validavimo būsena, validavimo klaidos (jei nustatyta) ir informacija apie skaitmeninį parašą bei pasirašiusio sertifikatą.

- *content* element. Jei pateiktas, jame turi būti sąrašas POC turinio elementų (jame esančių pasirašytų ir/ar nepasirašytų duomenų failų), jų validavimo būsena ir sąrašas klaidų, jei tokių nustatyta.
- *metadata* element. Jei pateiktas, jame turi būti sąrašas SubDO metaduomenų, jų validavimo būsena ir sąrašas klaidų, jei tokių nustatyta.

Status atsakymo JSON objektas turi būti apibrėžtas kaip JSON schema faile (signa-arch-api-schema.json), pateiktame 4.9.11.1 skyrelyje. JSON schemos elementai turi įgyvendinti *Status* atsakymo elementus pagal vardus, kaip pateikta lentelėje:

Laukas	Aprašymas	JSON nario pavadinimas
Status	Bendra apsaugos objekto apsaugos paslaugose būsena	status
Document identifier	Apsaugos objekto apsaugos paslaugose identifikatorius	extCode
Document specification	Apsaugos objekto tipo identifikatorius	docSpecId
Maintainable until	Data, iki kurios apsaugos objektas bus saugomas apsaugos paslaugose	maintainableUntil
Next update date	Laikas, kada apsaugos paslaugos atnaujins apsaugos objekto informaciją	nextUpdateDate
Last augment date	Data ir laikas, kada paskutinį kartą apsaugos paslaugos papildė apsaugos objektą	lastAugmentDate
Last augment status	Paskutinio apsaugos objekto papildymo būsenos kodas	lastAugmentStatus
Next augment date	Laikas, kada apsaugos paslaugos papildys apsaugos objektą	nextAugmentDate
Events	Sąrašas veiksmų, kuriuos su apsaugos objektu atliko apsaugos klientas ar apsaugos paslaugos	events
Structure	Apsaugos objekto struktūros validavimo būsena	structure
Packaging	Apsaugos objekto paketo validavimo būsena	packaging
Signatures	Sąrašas apsaugos objekto skaitmeninių parašų su skaitmeninių parašų informacija ir validavimo būsena	signatures
Content	Sąrašas POC turinio elementų (failų) ir validavimo būsena	content
Metadata	Sąrašas POC metaduomenų ir validavimo būsena	metadata

4.9.4. Download

Download operacija yra analogiškos ETSI TS 119 512 apibrėžtos *RetrievePO* operacijos išplėtimas. *Download* operacija naudojama gavimui patalpinto apsaugos objekto su jame esančiais apsaugos įrodymais. Šiai operacijai turi būti pateiktas

apsaugos objekto identifikatorius. Grąžinamo apsaugos objekto formatas yra vienas iš formatų, išvardintų 4.12 skyrelyje. Operacija turi gražinti tik apsaugos objektus, kurie prieinami apsaugos klientui.

Šis profilis palaiko šią operaciją naudojant JSON sintaksę. JSON schema ir OpenAPI dokumentas pateikti 4.9.11 skyrelyje.

4.9.4.1 Download užklausa

Download užklausoje turi būti nurodyti tokie laukai:

- *client ID*. Jame turi būti apsaugos kliento, kviečiančio operaciją, identifikatorius.
- *identifier*. Jame turi būti nuoroda į apsaugos objektą, kurį klientas anksčiau pateikė apsaugos paslaugoms (žr. *store* operaciją ir jos *external identifier* lauką).

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

Laukas	Aprašymas	JSON nario pavadinimas
Client ID	Kliento identifikatorius	cid
Identifier	Apsaugos objekto identifikatorius apsaugos paslaugose	extCode

4.9.4.2 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.

4.9.5. Remove

Remove operacija yra analogiškos ETSI TS 119 512 apibrėžtos *DeletePO* operacijos išplėtimas. *Remove* operacija naudojama apsaugos objekto pašalinimui iš PSP saugyklos. Šiai operacijai turi būti pateiktas apsaugos objekto identifikatorius.

Kai apsaugos objektas pašalinamas, atitinkamas SubDO ir apsaugos įrodymai irgi pašalinami. Su apsaugos objektu atliktų veiksmų įrašai nebus pašalinti. Operacija turi leisti pašalinti tik apsaugos objektus, kurie prieinami apsaugos klientui.

Šis profilis palaiko šią operaciją naudojant JSON sintaksę. JSON schema ir OpenAPI dokumentas pateikti 4.9.11 skyrelyje.

4.9.5.1 Remove užklausa

Remove užklausoje turi būti nurodyti tokie laukai:

- *client ID*. Jame turi būti apsaugos kliento, kviečiančio operaciją, identifikatorius.
- *identifier*. Jame turi būti nuoroda į apsaugos objektą, kurį klientas anksčiau pateikė apsaugos paslaugoms (žr. *store* operaciją ir jos *external identifier* lauką).
- *actor name*. Jame nurodomas šio apsaugos objekto pašalinimo prašytojo vardas. Jis privalomas, jei pašalinti apsaugos objektą prašoma nepasibaigus jo apsaugos laikotarpiui.

- *reason*. Jame nurodomas šio apsaugos objekto pašalinimo priežastis. Jis privalomas, jei pašalinti apsaugos objektą prašoma nepasibaigus jo apsaugos laikotarpiui.

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

Laukas	Aprašymas	JSON nario pavadinimas
Client ID	Apsaugos kliento identifikatorius	cid
Identifier	Pašalinamo apsaugos objekto identifikatorius	extCode
Actor name	Šios operacijos prašytojo vardas	actorName
Reason	Apsaugos objekto pašalinimo priežastis	reason

4.9.5.2 Remove atsakymas

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

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

Sėkmės atveju pateikiamas HTTP atsakymas su būsenos kodu 200.

Atsakyme turi būti pateikiami tokie elementai:

- *operation status* elementas. Jame turi būti reikšmė „success", nurodanti operacijos sėkmę.
- *external identifier* elementas. Jame turi būti pašalinto apsaugos objekto identifikatorius.

Remove atsakymo JSON objektas turi būti apibrėžtas kaip JSON schema faile (signa-arch-api-schema.json), pateiktame 4.9.11.1 skyrelyje. JSON schemos elementai turi įgyvendinti *Remove* atsakymo elementus pagal vardus, kaip pateikta lentelėje:

Elementas	Aprašymas	JSON nario pavadinimas
Operation status	*Remove* operacijos įvykdymo būsena	status
External identifier	Pašalinto apsaugos objekto identifikatorius	extCode

4.9.6. PreservePO

PreservePO operacija naudojama pateikimo duomenų objekto (SubDO) pateikimui apsaugos paslaugoms. Šiai operacijai turi būti perduotas pateikimo duomenų objektas. Apsaugos paslaugos yra atsakingos už gauto pateikimo duomenų objekto išsaugojimą ir SubDO esančių apsaugos objektų apsaugą, papildant elektroninius parašus/spaudus. Išsami informacija apie apsaugos objektus ir tai, kaip jie gaunami iš SubDO, aprašyta 4.8 skyriuje.

Ši operacija palaiko 4.12 skyrelyje išvardintus pateikimo duomenų objektų formatus.

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.

4.9.7. RetrievePO

RetrievePO operacija naudojama gavimui patalpinto apsaugos objekto su jame esančiais apsaugos įrodymais. Šiai operacijai turi būti pateiktas apsaugos objekto identifikatorius.

Grąžinamo apsaugos objekto formatas turi būti vienas iš formatų, išvardintų 4.12 skyrelyje. Operacija turi gražinti tik apsaugos objektus, kurie prieinami apsaugos klientui.

RetrievePO operacijos sintaksė ir semantika yra apibrėžta ETSI TS 119 512 skyrelyje 5.3.4. Šis profilis palaiko šią operaciją tik naudojant JSON sintaksę.

RetrievePO 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.

RetrievePO operacija palaiko tokius elementus, apibrėžtus ETSI TS 119 512 standarto 5.3.4 skyrelyje, su tokiais patikslinimais:

- *POID* elementas. Jis turi būti pateiktas ir jame turi būti identifikatorius apsaugos objekto, kurį reikia gauti.
- *SubjectOfRetrieval* elementas. Jei pateiktas, jame turi būti reikšmė "POwithEmbeddedEvidence".
- *POFormat* elementas. Jei pateiktas, jame turi būti apsaugos objekto formatą identifikuojantis URI, atitinkantis apsaugos paslaugose ir šia operacija gaunamo saugomo apsaugos objekto formatą.
- *EvidenceFormat* elementas. Jis turi būti praleistas. Jei jis pateiktas, operacija turi grąžinti klaidos pranešimą apie nepalaikomą elementą.

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

4.9.8. DeletePO

DeletePO operacija naudojama apsaugos objekto pašalinimui iš PSP saugyklos. Šiai operacijai turi būti pateiktas apsaugos objekto identifikatorius. Apsaugos objektas bus pašalintas kartu su atitinkamu pateikimo duomenų objektu, apsaugos įrodymais ir visais atitinkamais metaduomenimis. Su apsaugos objektu atliktų veiksmų įrašai nebus

pašalinti. Operacija turi leisti pašalinti tik apsaugos objektus, kurie prieinami apsaugos klientui.

DeletePO operacijos sintaksė ir semantika yra apibrėžta ETSI TS 119 512 skyrelyje 5.3.5. Šis profilis palaiko šią operaciją tik naudojant JSON sintaksę.

DeletePO 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.

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

4.9.9. RetrieveTrace

RetrieveTrace operacija naudojama su apsaugos objektu atliktų veiksmų įrašų gavimui. Šiai operacijai turi būti pateiktas apsaugos objekto identifikatorius.

Operacija turi grąžinti informaciją tik apsaugos objektams, kurie prieinami apsaugos klientui.

RetrieveTrace operacijos sintaksė ir semantika yra apibrėžta ETSI TS 119 512 skyrelyje 5.3.7. Šis profilis palaiko šią operaciją tik naudojant JSON sintaksę.

RetrieveTrace 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.

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

4.9.10. Search

Search operacija naudojama paieškai tarp PSP saugykloje saugomų apsaugos objektų. Šiai operacijai turi būti pateiktas apsaugos objektų filtras. Operacija grąžins apsaugos objektų identifikatorių sąrašą.

Operacija turi grąžinti identifikatorius tik apsaugos objektams, kurie prieinami apsaugos klientui.

Search operacijos sintaksė ir semantika yra apibrėžta ETSI TS 119 512 skyrelyje 5.3.9. Šis profilis palaiko šią operaciją tik naudojant JSON sintaksę.

Search 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.

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

4.9.11. JSON schemos ir OpenAPI dokumentai

4.9.11.1 JSON schemos failai

JSON schemos apibrėžimai *Store*, *Status*, *Download* ir *Remove* operacijoms pateikti:

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

JSON schemos apibrėžimai *RetrieveInfo*, *PreservePO*, *RetrievePO*, *DeletePO*, *RetrieveTrace* ir *Search* operacijoms pateikti:

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

4.9.11.2 OpenAPI specifikacijos

OpenAPI specifikacijos *Store*, *Status*, *Download* ir *Remove* operacijoms pateiktos:

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

OpenAPI specifikacijos *RetrieveInfo*, *PreservePO*, *RetrievePO*, *DeletePO*, *RetrieveTrace* ir *Search* operacijoms pateiktos:

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

4.10. Apsaugos protokolo naudojimo gairės

Apsaugos klientas gali nuspręsti pašalinti pateikimo duomenų objektą (SubDO) iš savo saugyklos, kai tik jis patalpintas į apsaugos paslaugas su saugykla. Kad būtų išvengta bet kokių duomenų praradimų, apsaugos klientui rekomenduojama palaikyti savo SubDO saugykloje kurį laiką po pateikimo apsaugos paslaugoms, kol jis bus saugiai išsaugotas apsaugos paslaugų saugykloje.

Abonentas turi naudoti apsaugos operacijas pagal šias gaires:

- Apsaugos klientas pateikia SubDO apsaugos paslaugoms (*store*, *PreservePO* operacijos).
  - Jei apsaugos klientas pateikia SubDO naudodamas *store* operaciją, jis gali nurodyti apsaugos laikotarpį.
  - Jei apsaugos laikotarpis nenurodytas arba SubDO pateiktas su *PreservePO* operacija, apsaugos laikotarpis yra neribotas.
  - SubDO apsauga bei elektroninių parašų ir elektroninių spaudų papildymas neatliekami po apsaugos laikotarpio. Apsaugos klientas turi nurodyti apsaugos laikotarpį, tik jei jis žino, kad SubDO apsauga po nurodyto laikotarpio yra nebūtina.
- Apsaugos klientas pasaugo SubDO originalią kopiją savo saugykloje laikotarpį, kuris nurodytas Abonentinėje sutartyje.

- Po šio laikotarpio apsaugos klientas pasitikrina apsaugos paslaugose pateikto SubDO būseną (*status*, *RetrieveTrace* operacijos). Jei apsaugos paslaugose SubDO yra, apsaugos klientas gali pašalinti jį iš savo saugyklos.
- Jei apsaugos klientas pateikia SubDO su identifikatoriumi, atitinkančiu anksčiau apsaugos paslaugoms pateiktą SubDO, tai naujas pakeičia ankstesnį SubDO. Ankstesnis SubDO su surinktais įrodymų duomenimis prarandamas. Kad išvengtų duomenų praradimo pateikdamas SubDO atnaujinimą, apsaugos klientas turi:
    - Paimti SubDO iš apsaugos paslaugų, prieš atnaujindamas jį savo sistemoje (pavyzdžiui, pridėdamas elektroninį parašą).
    - Patalpinti atnaujintą SubDO apsaugos paslaugose su tuo pačiu identifikatoriumi.

4.11. Taikomos taisyklės

MitSoftQWST 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.

MitSoftQWST 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.

4.14. Kriptografinis monitoringas

Algoritmų, panaudotų pateikimo duomenų objektuose, kriptografinis monitoringas remiasi einamąja algoritmo patikimumo būsena ir naudojamas tik validuojant skaitmeninį parašą (atliekama gavus apsaugos objektą arba pagal pareikalavimą).

Algoritmų, naudojamų skaitmeninių parašų papildymui, kriptografinis monitoringas remiasi numatoma algoritmo patikimumo būsena ir naudojamas tik naujai kuriamiems apsaugos įrodymams (laiko žymoms).

MitSoft PSP kriptografinio monitoringo realizacija remiasi Kriptografinių algoritmų registru ir skaitmeninių parašų apsaugos metaduomenimis.

Kriptografinių algoritmų registre saugoma informacija apie palaikomus kriptografinius algoritmus ir jų patikimumo būseną. Saugomi duomenis apima:

- Algoritmo pavadinimą.

- Algoritmo identifikatorių (OID ir URI).
- Algoritmo tipą (santraukos funkcija, parašo algoritmas, kanonizavimo algoritmas).
- Rakto ilgį (tik parašų algoritmams).
- Algoritmo patikimumo būseną – ar jis šiuo metu patikimas ir gali būti naudojamas pateikimo duomenų objektuose, ar jis 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 taip pat pailgintas Kriptografinių algoritmų registro peržiūros metu, jei atsiranda naujos informacijos apie algoritmo patikimumą.

MitSoft PSP Kriptografinių algoritmų registro peržiūra ir atnaujinimas atliekami reguliariai ir atitinka standarte ETSI TS 119 312 "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites" standarto [TS 119 312] rekomendacijas. Naujiems apsaugos įrodymams naudojamų kriptografinių algoritmų (jų parametrų ir raktų ilgių) numatomas atsparumo laikotarpis papildymo metu pagal ETSI TS 119 312 turi būti 3 metai ar daugiau.

Kriptografinių algoritmų registro peržiūrą ir atnaujinimą atlieka MitSoft PSP sistemos administratorius. Jei Apsaugos įrodymų taisyklėse apibrėžtas kriptografinis algoritmas tampa nepakankamai saugiu naujų apsaugos įrodymų kūrimui, išleidžiama nauja Apsaugos įrodymų taisyklių versija.