MitSoft

Qualified Long-term Preservation Service

Preservation Practice Statement

QLPS/PS

Unique object ID (OID): **1.3.6.1.4.1.57890.1.4.1**

Version 1.20

Valid since 2024-10-01

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

Approvals

Revision history

Version	Valid since	Description
1.00		First official version of the document for audit
1.10		Adjusted according audit remark
1.11		Fixed minor wording errors when comparing EN and LT versions.
1.12	2023-05-15	CMS signatures in PDF are permitted; clarification for non-valid digital signature preservation
1.20	2024-10-01	General practices common to all qualified trust services transferred to separate document

Approval of the document

	Name	Date	Signature
Reviewed by	Adomas Birštunas	2024-08-13	
Approved by	Antanas Mitašiūnas	2024-08-20	

Table of content

1. INTRODUCTION 5
1.1. Overview 5
1.2. Identification 5
1.3. Users and fields of application of the preservation service 6
1.4. Conformance. Its confirmation and verification 6
1.5. Contact information 6
2. References 8
3. Definitions of terms and abbreviations 9
4. MitSoft PSP: General Concepts 12
4.1. Functional goals of preservation service 12
4.2. Preservation storage models 12
4.2.1. Preservation service with storage (WST) 13
4.2.1.1 Architecture 13
4.2.1.2 Workflow in MitSoft PS 13
4.2.2. Preservation service without storage (WOS) 15
4.2.2.1 Architecture 15
4.2.2.2 Workflow in MitSoft PS 16
5. Risk assessment 18
6. POLICIES AND PRACTICES 19
6.1. Preservation service practice statement 19
6.1.1. PSP obligations 20
6.2. Terms and conditions 20
6.3. Information security policy 21
6.4. Preservation profile 21
6.5. Preservation evidence policy 21
6.6. Signature validation policy 21
6.7. Subscriber agreement 22
7. PSP MANAGEMENT AND OPERATION 23
7.1. Internal organization 23
7.2. Human resources 23
7.3. Asset management 23
7.4. Access control 23
7.5. Cryptographic controls 23
7.6. Physical and environmental security 23
7.7. Operation security 23
7.8. Network security 23
7.9. Incident management 23

7.10. Collection of evidence 24
7.11. Business continuity management....24
7.12. PSP termination and termination plans 24
7.13. Compliance 24
7.14. Cryptographic monitoring 24
7.15. Augmentation of preservation evidences 26
7.16. Export-import package 26
8. Operational and notification protocols 28
8.1. Preservation protocol 28
8.2. Notification protocol....29
9. Preservation process 30
9.1. Storage of preserved data and evidences....30
9.2. Preservation evidences....30
9.3. Preservation of digital signatures 30

1. INTRODUCTION

The joint stock company "MIT-SOFT" (further – the MitSoft) was established on August 1, 1991 and since 1996 is working in software development and services provision for creation and verification of electronic documents having the same legal effect as hand signed paper documents. Information about the MitSoft is available on the website http://www.mitsoft.lt/.

MitSoft has divided its Practice Statements into three parts:

- Qualified Trust Services Practice Statement (QTS PS) describes general practices common to all qualified trust services;
- Preservation Practice Statement (QLPS PS) and Time-Stamping Practice Statement (QTSS PS) describe parts that are specific to each qualified service.

1.1. Overview

The standard ETSI TS 119 511 "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers providing long-term preservation of digital signatures or general data using digital signature techniques" specifies Qualified Long-term preservation service policy for qualified electronic signatures and electronic seals (OID: 0.4.0.19511.1.2). The requirements specified in the policy 0.4.0.19511.1.2 are related neither to concrete technological solutions nor to the organizational structure of the Preservation Service Provider (PSP). Technical solutions, procedures, and personnel policy for the implementation of the policy 0.4.0.19511.1.2 requirements are described in the present MitSoft Qualified Long-term Preservation Service Practice Statement (further – QLPS PS).

The present QLPS PS is based upon the following legal acts and normative documents:

a) The 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 [eIDAS];

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

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

While providing the long-term preservation service, PSP carries out the functions of monitoring and augmentation of the preservation objects.

Note regarding the definitions. Qualified Preservation Service Policy (QPSP) means the policy 0.4.0.19511.1.2. Hereafter preservation service (PS) means MitSoft Qualified Long-term Preservation Service, PSP means MitSoft PSP; QLPS PS means MitSoft QLPS PS, and so on, i.e., everything that is said applies solely to the MitSoft PSP.

1.2. Identification

The unique identifier (OID) of the QLPS PS is 1.3.6.1.4.1.57890.1.4.1; the values of its fields are given in the Table 1.

Table 1. The values of the fields of the unique identifier of the QLPS PS

Name	Value
ISO	1
Organization recognized by ISO	3

U.S. Department of Defence	6
Internet	1
Private company	4
Private company registered by IANA	1
Joint stock company "MIT-SOFT"	57890
Subdivision: Qualified trust services	1
Document type: Qualified long-term preservation service practice statement	4
Document version	1

The version of the QLPS PS in effect is available on the website of MitSoft.

1.3. Users and fields of application of the preservation service

Qualified long-term preservation service allows extension of the validity status of an electronic signature or electronic seal over long periods of time in spite of obsolescence of cryptographic technology such as crypto algorithms, key sizes or hash functions, key compromises or the loss of the ability to check the validity status of public key certificates. The users of the qualified long-term preservation service provided by the PSP can be legal or natural persons needing the services provided by the PSP.

Neither QPSP nor QLPS PS imposes any limitations for using the Qualified long-term preservation services. They can be used when an owner doesn't want to take care by himself about the preservation of validity status of the electronic signatures and seals and delegates it to PSP.

PSP provides public services; however, it can also serve closed user groups.

1.4. Conformance. Its confirmation and verification

PSP confirms that the MitSoft preservation service is EU qualified preservation service and conforms to the QPSP for WOS and WST storage models PDS goal according to defined by PSP preservation profiles and fulfils all the defined requirements for its activities.

The compliance of the PSP 's activities with the QPSP and QLPS PS is verified as defined by the QLPS PS, at least every two years.

1.5. Contact information

The PS is managed by the joint stock company "MIT-SOFT", which contact information is given in the Table 2.

Table 2. Contact information of the PSP

PSP:	The joint stock company "MIT-SOFT"
Address:	Kalvarijų str. 276-100, LT-08316 Vilnius
Phone:	+370 5 233 3922
URL:	https://www.mitsoft.lt/
E-mail:	info@mitsoft.lt

2. References

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

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

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

[ISO 27002] – ISO/IEC 27002:2022: "Information security, cybersecurity and privacy protection – Information security management systems - Requirements".

[ISO 27005] – ISO/IEC 27005:2022: "Information security, cybersecurity and privacy protection – Guidance on managing security risks".

[RFC 3161] – RFC 3161 Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP).

[RFC 5816] – RFC 5816 ESSCertIDv2 Update for RFC 3161.

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

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

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

[QTS PS] - MitSoft "Qualified Trust Services Practice Statement", Version 1.00.

3. Definitions of terms and abbreviations

Archival time stamp: ArchiveTimeStamp for XAdES signatures, archive-time-stamp for CAdES signatures, or DocumentTimeStamp for PAdES signatures.

Compromise: a loss, theft, modification, illegal use, or any other security violation of the confidential data.

Data object: actual binary/octet data being operated on (e.g. transformed, digested, or signed) by an application and which may be associated with additional information like an identifier, the encoding, size or type.

EU qualified preservation service: preservation service that meets the requirements for qualified preservation service for qualified electronic signatures and/or for qualified electronic seals as laid down in Regulation (EU) 910/2014 [eIDAS].

EU qualified time-stamping authority: qualified trust-service provider issuing qualified electronic time stamps as laid down in Regulation (EU) 910/2014 [eIDAS].

Expected evidence duration: for a preservation service with temporary storage or without storage, duration during which the preservation service expects that the preservation evidence can be used to achieve the preservation goal.

Export-import package: information extracted from the preservation service including the submission data object (SubDO), the preservation evidences and preservation-related metadata, allowing another preservation service to import it in order to continue to achieve the preservation goal based on this information.

Long-term: time period during which technological changes may be a concern.

Long-term preservation: extension of the validity status of a digital signature over long periods of time and/or extension of provision of proofs of existence of data over long periods of time, in spite of obsolescence of cryptographic technology such as crypto algorithms, key sizes or hash functions, key compromises or of the loss of the ability to check the validity status of public key certificates.

Metadata: data about other data.

Notification protocol: protocol used by a preservation service to notify the preservation client.

Preservation client: component or a piece of software which interacts with a preservation service via the preservation protocol.

Preservation evidence: evidence produced by the preservation service which can be used to demonstrate that one or more preservation goals are met for a given preservation object.

Preservation evidence policy: set of rules that specify the requirements and the internal process to generate or how to validate a preservation evidence.

Preservation goal: one of the following objectives achieved during the preservation time frame: extending over long periods of time the validity status of digital signatures, providing proofs of existence of data over long periods of time, or augmenting externally provided preservation evidences.

Preservation interface: component implementing the preservation protocol on the side of the preservation service.

Preservation manifest: data object in a preservation object container referring to the preservation data objects or additional information and metadata in the preservation object container.

Preservation object: typed data object which is submitted to, processed by or retrieved from a preservation service.

Preservation object container: container which contains a set of data objects and optionally related metadata providing information about the data objects and optionally preservation manifest(s) specifying its content and relationships.

Preservation period: for a preservation service with storage, duration during which the preservation service preserves the submitted preservation objects and the associated evidences.

Preservation profile: uniquely identified set of implementation details pertinent to a preservation storage model and one or more preservation goals which specifies how preservation evidences are generated and validated.

Preservation protocol: protocol to communicate between the preservation service and a preservation client.

Preservation scheme: generic set of procedures and rules pertinent to a preservation storage model and one or more preservation goals which outlines how preservation evidences are created and validated Note: Different preservation profiles can implement the same preservation scheme.

Preservation service: service capable of extending the validity status of a digital signature over long periods of time and/or of providing proofs of existence of data over long periods of time.

Preservation service provider: trust service provider providing a preservation service.

Preservation service policy: trust service policy for a preservation service.

Preservation service practice statement: trust service practice statement for a preservation service.

Preservation storage model: one of the following ways of implementing a preservation service: with storage, with temporary storage, without storage.

Preservation subscriber: see *Subscriber*.

Proof of existence: evidence that proves that an object existed at a specific date/time.

Repository: an internet place where information of the long-term preservation service is made available for the users.

Signer: entity being the creator of a digital signature.

Submission data object (SubDO): original data object provided by the client.

Subscriber: legal or natural person bound by agreement with a preservation trust service provider to any subscriber obligations.

Time stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time (= electronic time stamp [eIDAS]).

Trusted list: list that provides information about the status and the status history of the trust services from trust service providers regarding compliance with the applicable requirements and the relevant provisions of the applicable legislation.

Validation data: data that is used to validate a digital signature.

ETSI – European Telecommunications Standards Institute
OID – Object identifier
PS - Practice Statement
PSP – Preservation Service Provider
QLPS – Qualified Long-term Preservation Service
QPSP – Qualified Preservation Service Policy
QTS - Qualified Trust Services
QTSP – Qualified Trust Service Provider
QTSS – Qualified Time-Stamping Service

POC – Preservation object container
RRT – Communications Regulatory Authority of the Republic of Lithuania
TSA – Time-stamping authority
SubDO – Submission data object

4. MitSoft PSP: General Concepts

4.1. Functional goals of preservation service

The definition of qualified long-term preservation service by ETSI TS 119 511 foresees three functional goals of preservation services: preservation of digital signatures (PDS), preservation of general data (PGD), augmentation of submitted preservation evidences (AUG). Any combination of these functional goals could be implemented in particular preservation service.

MitSoft PSP provides functional goal - preservation of digital signatures (PDS) within electronic documents/containers of the following formats (specifications): ADOC-V1.0, ADOC-V2.0, EGAS-V1.0, MDOC-V1.0, PDF-LT-V1.0, PDF-RC-V1.0, ASiC-E according to ETSI TS 103174, ASiC-E according to ETSI EN 319162-1, ASiC-S according to ETSI TS 103174, ASiC-S according to ETSI EN 319162-1, PDF with PAdES signature according ETSI TS 103172, PDF with PAdES signature according ETSI EN 319142-1, PDF with CMS signatures.

Preservation service preserves qualified electronic signatures and qualified electronic seals. Preservation service preserves advanced electronic signatures and advanced electronic seals (that are not qualified) only if such a requirement is listed in the Subscriber agreement. Further in this document they are called electronic signatures or seals, or just digital signatures.

Preservation service preserves valid electronic signatures and valid electronic seals. Non-valid electronic signatures and non-valid electronic seals are preserved only if such a requirement is listed in the Subscriber agreement and it is allowed according signature policy.

4.2. Preservation storage models

The definition of qualified long-term preservation service by ETSI TS 119 511 foresees three preservation storage models: preservation service with storage (WST), preservation service with temporary storage (WTS), and preservation service without storage (WOS).

Preservation process involve both sides: preservation client and preservation service provider. A distribution of duties among preservation client and preservation service provider depends on preservation service storage model applied.

Preservation storage model WST allows maximal extent of preservation service delivered by preservation service provider and minimal by preservation client, and contrary, preservation storage model WOS maximally limits preservation service provider’s involvement in total preservation process.

MitSoft PSP uses preservation storage model WST to be able to provide maximal extent of preservation service delivered by preservation service provider. Using preservation storage model WST, the actions of preservation client are limited by submission of submission data object and retrieval of submission data object, preservation object including preservation evidences, when needed. This option suits best for small subscribers of preservation service.

Big subscribers of preservation service may have special needs because of huge total volume of objects to be preserved or for any other reason. Therefore, MitSoft PSP provides preservation service without storage (WOS).

4.2.1. Preservation service with storage (WST)

4.2.1.1 Architecture

General architecture of preservation service with storage (WST) is provided in the figure 1.

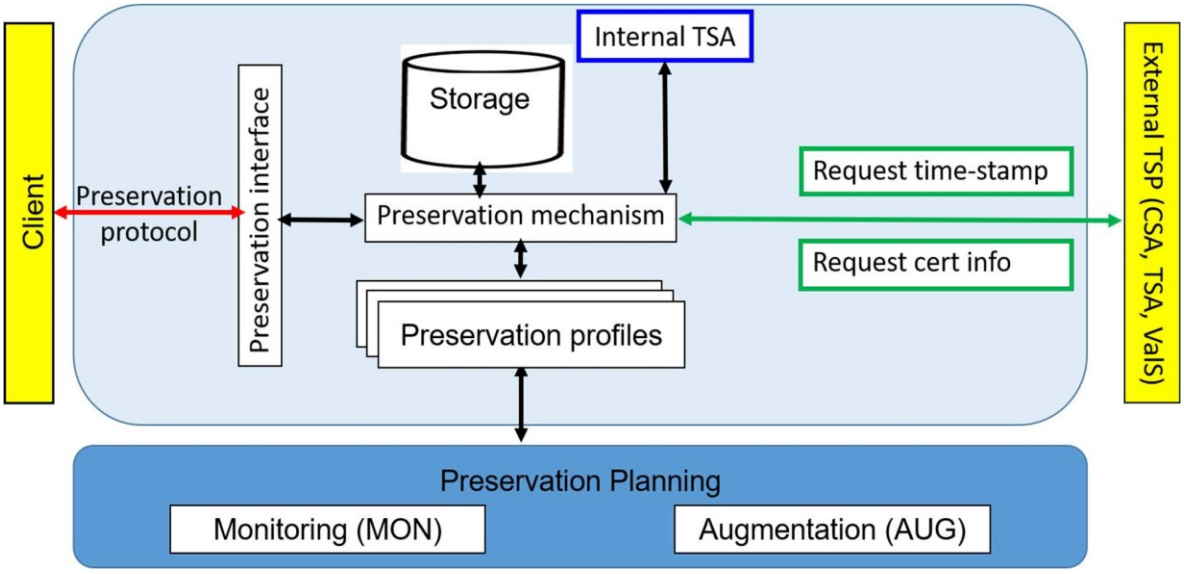


Fig. 1. General architecture of preservation service with storage (WST)

4.2.1.2 Workflow in MitSoft PS

MitSoft qualified long-term preservation service with storage receives electronic documents and containers from preservation clients. Validation is performed by the preservation service when receiving an electronic document/container and later by the explicit request of the client and during the maintenance process of electronic document/container by preservation service. Received electronic document/container is stored in the MitSoft preservation service storage. Augmentation is timely performed by the request of the maintenance process of preservation service. Later client may request preservation service to get stored electronic document/container with included preservation evidences.

Workflow of the electronic document/container in MitSoft preservation service with storage is presented in the figure 2.

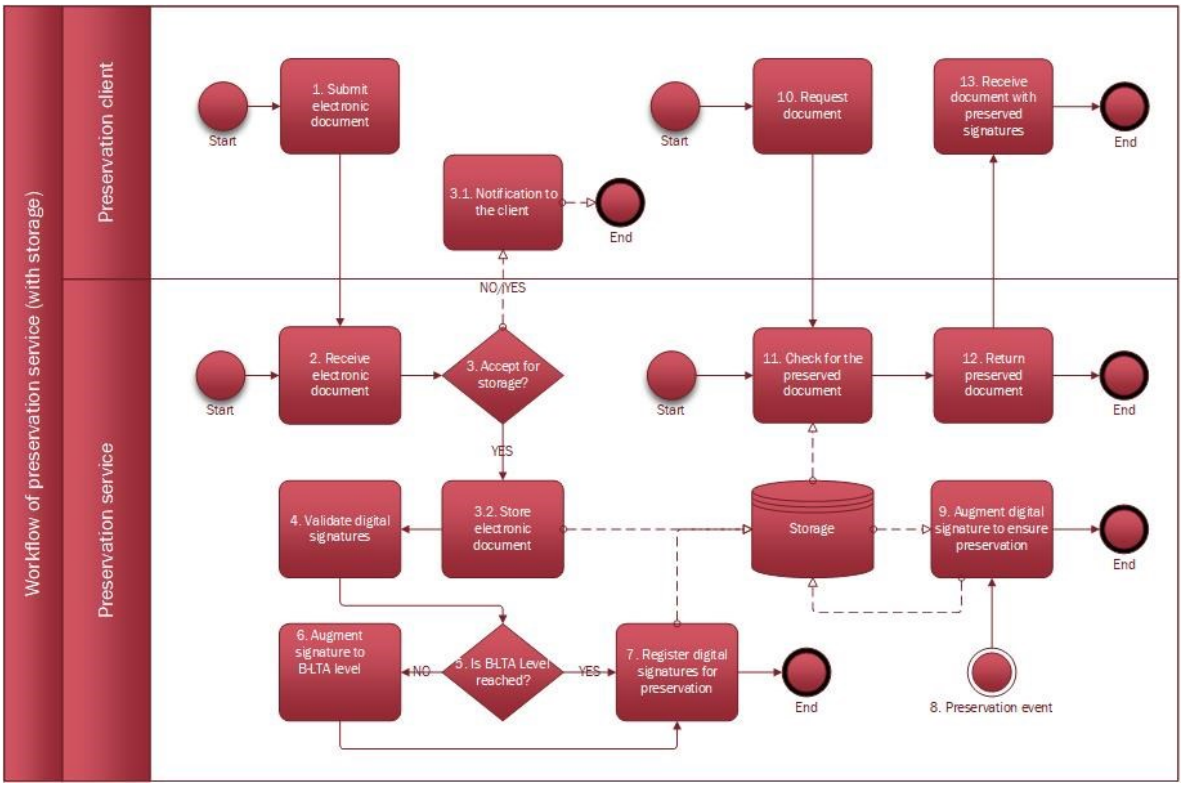


Fig 2. Workflow of electronic document/container in MitSoft preservation service with storage (WST)

1. Preservation client submits electronic document/container to preservation service.
2. Preservation service receives electronic document/container from the client.
3. Preservation service checks if electronic document/container is acceptable. Electronic document/container shall satisfy main format requirements of the electronic document/container specification and shall contain at least one electronic signature or electronic seal. Electronic document/container shall not have viruses, malicious and unauthorized content.
   3.1. Preservation client receives operation response (accepted or not), and, in the case of rejection, reason of the rejection from the preservation service.
   3.2. In the case of acceptance, preservation service stores electronic document/container together with additional metadata.
4. Preservation service validates electronic document/container and electronic signatures and electronic seals within it.
5. Preservation service checks whether every electronic signature and electronic seal to be preserved already reached B-LTA level (or corresponding archival signature format for non-baseline signatures).
6. Preservation service performs augmentation of electronic signatures and electronic seals. After this augmentation every electronic signature/seal to be preserved reaches B-LTA level (or corresponding archival signature format for non-baseline signatures).
7. Preservation service registers electronic signatures and electronic seals to be preserved and contained within electronic document/container for further preservation. For every digital signature registered for preservation additional preservation metadata is collected and stored. Electronic signatures and electronic seals that contain errors preventing to reach B-LTA level (or corresponding archival signature format for non-baseline signatures) will not be registered for preservation.

8. The maintenance process performs the maintenance of preserved electronic signatures/seals within electronic documents/containers. The maintenance process executes the preservation if preserved electronic signature/seal should be augmented to ensure its preservation due to some certificate validity expiration in the near future or possible cryptographic algorithm obsolescence.
9. Preservation service performs digital signature augmentation by adding new archival time stamps to extend their validity status. Preservation evidences are included into the digital signatures presented within the electronic document/container. Upgraded electronic document/container together with updated additional preservation metadata are stored in the MitSoft preservation storage.
10. At some point in time preservation client can decide to request stored electronic document/container.
11. Preservation service checks if requested electronic document/container is stored in the MitSoft preservation storage and checks if service caller has a right to access requested electronic document/container.
12. Preservation service returns requested electronic document/container together with preservation evidences included within digital signatures to the client; or informs client, that the request cannot be fulfilled.
13. Preservation client receives electronic document/container, which contains preserved electronic signatures/seals with incorporated preservation evidences.

Validation is performed for every electronic signature and electronic seal presented in the preserved electronic document/container.

Augmentation is performed for every electronic signature and electronic seal presented in the preserved electronic document/container if it was not recognized as unacceptable for preservation.

4.2.2. Preservation service without storage (WOS)

4.2.2.1 Architecture

General architecture of preservation service without storage (WOS) is provided in the figure 3.

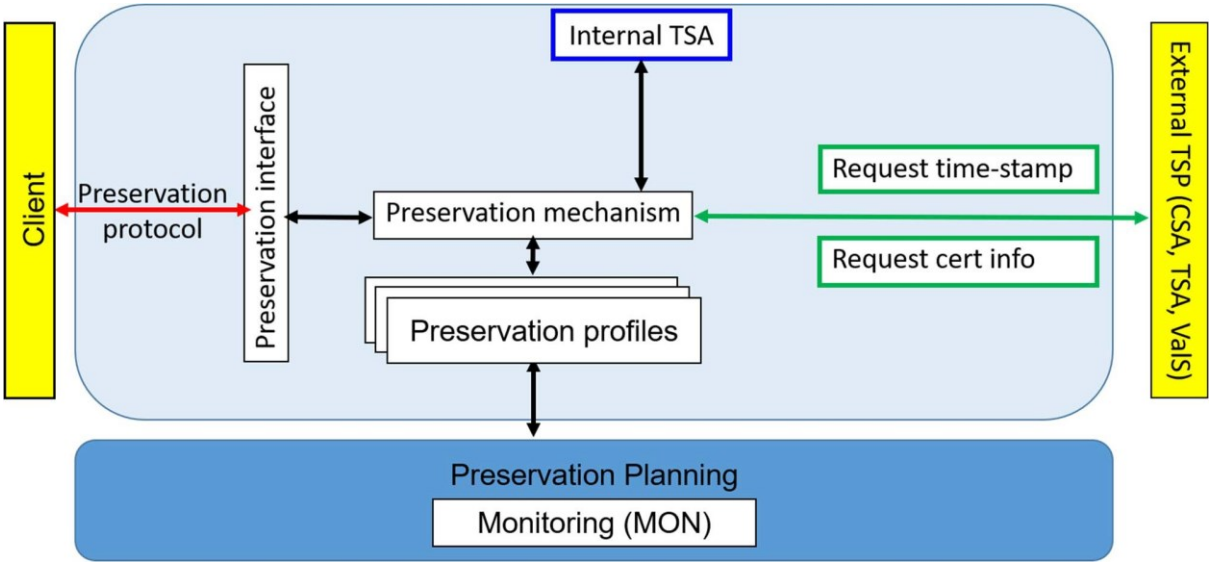


Fig. 3. General architecture of preservation service without storage (WOS)

4.2.2.2 Workflow in MitSoft PS

MitSoft qualified long-term preservation service without storage receives electronic document or container from preservation clients. Validation is performed by the preservation service when receiving an electronic document/container. After validation, augmentation is performed and collected preservation evidences are included into the electronic signatures/seals contained in the preserving electronic document/container. As a preservation evidence upgraded electronic document/container is returned to the preservation client together with calculated expected evidences duration. Neither electronic document/container nor electronic signatures/seals are stored in any MitSoft preservation service storage.

Workflow of the electronic document/container in MitSoft preservation service without storage is presented in the figure 4.

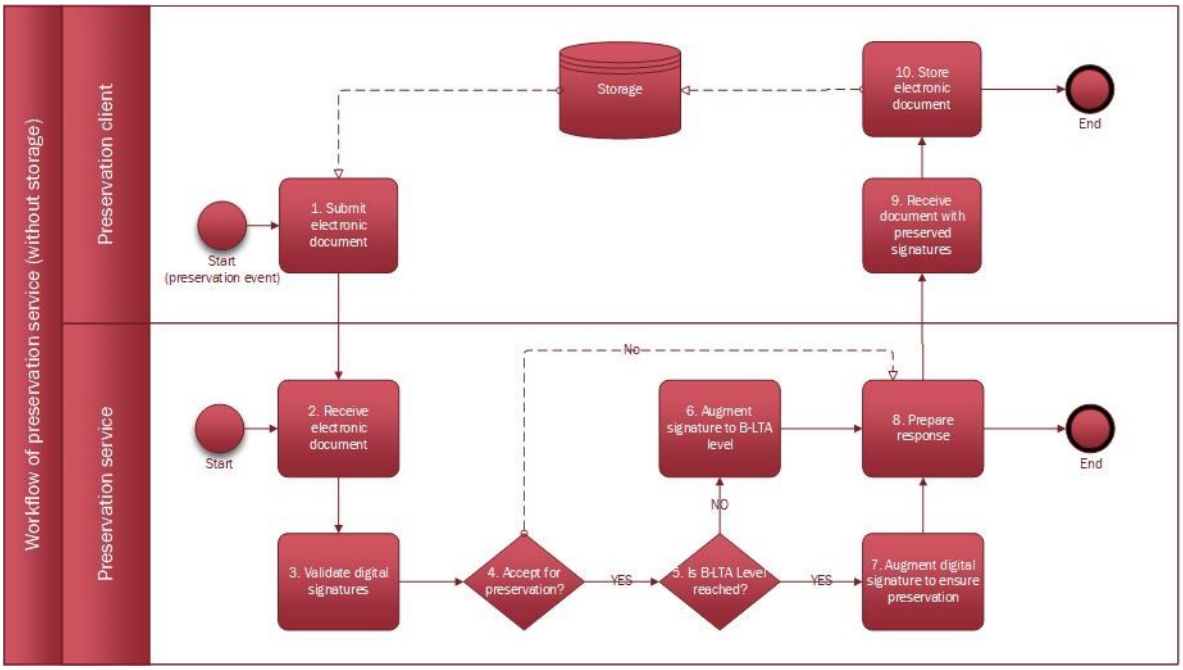


Fig 4. Workflow of electronic document/container in MitSoft preservation service without storage (WOS)

1. Preservation client submits electronic document/container to preservation service when preservation event occurs. Preservation is executed if new electronic document/container preservation should be started, or if already preserving electronic document/container should be re-augmented, since expected evidences (used within digital signatures contained in the preserved electronic document/container) duration is going to expire. The management of the preservation events is performed by the preservation client, not by preservation service.
2. Preservation service receives electronic document/container containing at least one electronic signature or electronic seal.
3. Preservation service validates electronic document/container and electronic signatures and electronic seals within it.
4. Preservation service checks if electronic document/container and electronic signatures and electronic seals to be preserved.
5. Preservation service checks whether every electronic signature and electronic seal to be preserved already reached B-LTA level (or corresponding archival signature format for non-baseline signatures).

6. Preservation service performs augmentation of electronic signatures and electronic seals. After this augmentation every digital signature to be preserved reaches B-LTA level (or corresponding archival signature format for non-baseline signatures).
7. Preservation service performs digital signature augmentation by adding new archival time stamps to extend their validity status. Preservation evidences are included into the digital signatures presented in the electronic document/container. Digital signature augmentation by adding new preservation evidence is performed only if augmentation period is already started, i.e. expected digital signature validity expiration time is in the near future.
8. Preservation service prepares response to the client. Preservation service calculates new expected evidence duration and augmentation period. On success, the response contains upgraded electronic document/container with preservation evidences included within electronic signatures/seals, information about recommended next augmentation time and calculated expected evidence duration. Otherwise, the rejection or failure reason is returned.
9. Preservation client receives updated electronic document/container from the preservation service. It also receives new expected evidence duration and recommended time for the next augmentation.
10. Preservation client stores updated electronic document/container in its own storage. Preservation client should update next augmentation time (and expected evidence duration) for the updated electronic document/container to be able to raise the next preservation event on time.

5. Risk assessment

Refer to clause 5 of [QTS PS].

6. POLICIES AND PRACTICES

6.1. Preservation service practice statement

Refer to clause 6.1 of [QTS PS].

Additionally for providing qualified long-term preservation services:

a) The practices and procedures used to address the requirements identified in the Qualified preservation service policy (QPSP) are described in the present Preservation service practice statement (QLPS PS).

b) The availability of the submitted data objects (SubDO) and the associated preservation evidences is achieved as follows: "Preservation object container (POC) is a submitted electronic document or container, which contains electronic signatures and/or seals (preservation objects) with preservation evidences (time stamps) included by the preservation service. POC is derived from the SubDO, by augmenting preserving digital signatures and timely preservation evidences (time stamps) inclusion. Operations defined by preservation profile accept and return preservation object, which is a whole preservation object container - electronic document or container (together with all preserved digital signature within it), or submission data object. Therefore, the submitted data objects (SubDO) and the associated preservation evidences are contained in the same container during whole preservation period. See for details section 4.8 of Preservation Profile with Storage document.

c) The QLPS PS identifies the obligations of all external organizations supporting the qualified long-term preservation services including the applicable policies and practices. Such external organizations are Qualified time-stamping authorities issuing qualified time stamps and Qualified certification authorities issuing qualified electronic signature certificates or qualified electronic seals certificates and providing OCSP or CRL services for these certificates, according to the Qualified time stamping service policy and Qualified electronic signature certificate policy and Qualified electronic seal certificate policy. OCSP and CRL external services used for status definition of non-qualified certificates are provided by Qualified certification authorities issuing non-qualified electronic signature certificates or non-qualified electronic seals certificates.

QPSP is the only preservation service policy supported by the qualified long-term preservation services:

a) Hashing algorithms that can be used to represent the datum being time-stamped are specified in the section 7.14. Cryptographic monitoring.

b) The MitSoft PSP provides qualified long-term preservation of electronic signatures and electronic seals according to the storage model: Preservation With Storage – WST and Preservation Without Storage – WOS as per QPSP.

c) The MitSoft PSP provides qualified long-term preservation of electronic signatures and electronic seals according to the goal: Preservation Digital Signatures – PDS as per QPSP.

d) The subscriber obligations are specified in the section 6.1.1.3. Subscriber obligations.

e) The relying party obligations are specified in the section 6.1.1.4. Relying party obligations.

f) Information on how to verify the preservation evidences is provided in the section 6.5. Preservation evidence policy.

g) The long-term preservation service of qualified electronic signatures and seals is qualified preservation service as per Regulation (EU) No 910/2014 [eIDAS].

6.1.1. PSP obligations

6.1.1.1. General

The PSP ensures that all requirements on PSP are implemented as applicable to the QPSP. PSP ensures implementation of the following:

a) Procedures defined in the present QLPS PS, including the service of monitoring and augmentation preservation evidences within preservation objects;

b) Adherence to any additional obligations either indicated in the preservation profile or incorporated by reference.

6.1.1.2. PSP obligations towards subscribers

Refer to clause 6.1.1.1 of [QTS PS].

6.1.1.3. Subscriber obligations

When relying upon the long-term preservation evidences, the subscriber shall verify that the preservation evidence has been correctly created and validated (for details, see the section 6.1.1.4. Relying party obligations).

6.1.1.4. Relying party obligations

The relying party, when relying upon a preservation object that includes preservation evidence, shall verify that the qualified archival time stamp has been correctly signed and that the private key used to sign the archival time stamp has not been compromised (disclosed to third-parties or unusable for other reasons) until the time of verification.

The archival time stamp is verified during the TSA's certificate validity period; therefore, the validity of the signing key can be checked by making sure that the TSA's certificate has not been revoked.

Besides that, the relying party shall comply with the constraints on the use of the long-term preservation service defined in the QPSP and take any other measures of precaution.

6.1.1.5. Liability

Refer to clause 6.1.1.2 of [QTS PS].

6.1.1.6. Legal provisions and interpretations

Refer to clause 6.1.1.3 of [QTS PS].

6.1.1.7. Charges

Refer to clause 6.1.1.4 of [QTS PS].

6.1.1.8. Intellectual property rights

Refer to clause 6.1.1.5 of [QTS PS].

6.2. Terms and conditions

Refer to clause 6.2 of [QTS PS].

Additionally, the terms and conditions of qualified long-term preservation service specify the following:

a) The QPSP being applied.

b) Information on how to verify the preservation evidences, and any possible limitations on the validity period associated with it.
c) Whether the qualified long-term preservation service has been assessed to be conformant with the QPSP, and if so through which conformity assessment scheme.
d) Where to find information on the supported preservation profiles.
e) How the request for an export-import package can be done.
f) The strategy that QPSP will follow when it is unable to collect and verify all the validation data.

6.3. Information security policy

Refer to clause 6.3 of [QTS PS].

6.4. Preservation profile

The MitSoft PSP supports the following preservation profiles:

- MitSoftQWST profile – MitSoft electronic document with storage preservation profile for qualified signatures and seals, which is indicated by the unique object identifier (OID):
  - 1.3.6.1.4.1.57890.1.5.1
- MitSoftQWOS profile – MitSoft electronic document without storage preservation profile for qualified signatures and seals, which is indicated by the unique object identifier (OID):
  - 1.3.6.1.4.1.57890.1.5.2

Descriptions of profiles are available on the website of MitSoft.

Submission data objects are electronic documents or containers that contain electronic signatures or electronic seals and actually signed/sealed data. MitSoft PSP does not support submission data objects that contain only hashes of the signed data. Preservation profiles define the actual set of supported submission data object formats.

Details of the preservation objects that will be preserved are listed in the used preservation profile.

6.5. Preservation evidence policy

MitSoft PSP supports the following preservation evidence policy:

- MitSoft Qualified Long-term Preservation Service Preservation Evidence Policy, which is indicated by the unique object identifier (OID):
  - 1.3.6.1.4.1.57890.1.7.1.x

  where x stands for the latest version. Subscribers could find all versions on the repository of MitSoft PSP.

6.6. Signature validation policy

MitSoft PSP supports the following signature validation policy:

- MitSoft Qualified Long-term Preservation Service Signature Policy, which is indicated by the unique object identifier (OID):
  - 1.3.6.1.4.1.57890.1.6.1.x

  where x stands for the latest version. Subscribers could find all versions on the repository of MitSoft PSP.

6.7. Subscriber agreement

MitSoft PSP provides qualified long-term preservation service to the subscribers based on the subscriber agreement that contains the following compulsory clauses:

- An acceptance of the terms and conditions by the subscriber.
- The preservation profile(s) will be used by the subscriber.
- Whether advanced electronic signatures and advanced electronic seals (that are not qualified) are also preserved.
- Whether non-valid electronic signatures and non-valid electronic seals (having validation status other than PASSED) are also preserved (if it is aligned with signature policy).
- The formats (specifications) of electronic documents/containers accepted by preservation service.
- Duration of augmentation period.
- Duration of caution period.
- Subscriber's representative named as subscriber's administrator of MitSoft PSP long-term preservation service.
- Who has the right on behalf of the subscriber to access the preservation objects including submitted data objects and preservation evidences.
- Who has the right on behalf of the subscriber to request the traces on the actions related to the preservation objects.
- What happens to the data at the end of the preservation period.

7. PSP MANAGEMENT AND OPERATION

7.1. Internal organization

Refer to clause 7.1 of [QTS PS].

7.2. Human resources

Refer to clause 7.2 of [QTS PS].

7.3. Asset management

Refer to clause 7.3 of [QTS PS].

7.4. Access control

Refer to clause 7.4 of [QTS PS].

7.5. Cryptographic controls

MitSoft PSP of qualified long-term preservation service does not use any own cryptographic keys nor cryptographic devices for preserving electronic signatures and electronic seals.

MitSoft PSP assures that the time stamps used in preservation process come from EU qualified time-stamping authorities that follows state-of-the-art practices for policy and security requirements for trust service providers issuing time stamps.

7.6. Physical and environmental security

Refer to clause 7.6 of [QTS PS].

7.7. Operation security

Refer to clause 7.7 of [QTS PS].

7.8. Network security

Refer to clause 7.8 of [QTS PS].

Additionally for qualified long-term preservation service:

a) The architecture of preservation service is designed and implemented in such a way that all storage access by the preservation client, changing the content of the storage is done by the preservation service.
b) A high level of availability of external access to the preservation service is not required.

7.9. Incident management

Refer to clause 7.9 of [QTS PS].

7.10. Collection of evidence

Refer to clause 7.10 of [QTS PS].

Additionally:

a) Records concerning qualified long-term preservation service are held for a period of time as appropriate for providing necessary legal evidence and as notified in the PSP terms and conditions.

7.11. Business continuity management

Refer to clause 7.11 of [QTS PS].

7.12. PSP termination and termination plans

Refer to clause 7.12 of [QTS PS].

Additionally, the PSP ensures during tolerance period continued maintenance of information required to enable preservation or access to preservation objects:

a) The termination plan defines what happens with the stored POs at the termination of the preservation service.
b) The PSP does not use own signing cryptography.
c) The PSP does not sign preservation evidences. The preservation evidences are qualified time stamps signed by qualified time stamping authority.

7.13. Compliance

Refer to clause 7.13 of [QTS PS].

Additionally:

- For the purpose of provision of the long-term preservation services, the PSP requires to provide a preservation request as defined in [TS 119 511], together with authentication data if appropriate for the authentication method chosen.

7.14. Cryptographic monitoring

MitSoft PSP cryptographic monitoring covers two sets of cryptographic algorithms used by the preservation service:

- Cryptographic algorithms already used inside submission data objects.
- Cryptographic algorithms used for digital signature augmentation. Digital signature augmentation is performed: if submitted preservation object omits validation data (or part of it) and it is augmented to reach B-LTA level (or corresponding signature format for non-baseline signatures), or if certificate used to sign preservation evidence is going to expire, or cryptographic algorithms used in preservation evidences become less secure.

Cryptographic monitoring for algorithms used inside submission data objects is based on the current algorithm reliability status and is used only during digital signature validation (performed on preservation object submission or by the request).

Cryptographic monitoring for algorithms used for digital signature augmentation is based on the expected algorithm reliability status and is applied for the newly created preservation evidences (time stamps) only.

MitSoft PSP Cryptographic monitoring implementation is based on the Cryptographic algorithm registry and digital signature preservation metadata.

Cryptographic algorithm registry stores information about supported cryptographic algorithms and their reliability status. The stored data cover the following:

- Name of the algorithm.
- Algorithm identifiers (OID and URI).
- Algorithm type (hash function, signature algorithm, canonicalization algorithm).
- Key lengths (for signature algorithms only).
- Algorithm reliability status – is it reliable at the current time and may be used in the submitted data, is it reliable to be used for preservation evidences collected during digital signature augmentation.
- Expected algorithm reliability time – the time it is thought, that algorithm will be still reliable at least at that time. Expected algorithm reliability time may be set and also may be moved forward during Cryptographic algorithm registry revision, if new information about algorithm reliability becomes available.

MitSoft PSP Cryptographic algorithm registry revision and update is performed regularly and reflects the recommendations presented in the standard ETSI TS 119 312 "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites" standard [TS 119 312]. The expected resistance period according to ETSI TS 119 312 of the cryptographic algorithms (their parameters and key sizes) used for new preservation evidences should be 3 years or more at a time of augmentation.

Cryptographic algorithm registry revision and update is performed by the system operator of the MitSoft PSP. In the case cryptographic algorithm defined in the preservation evidence policy was identified to become no more secure enough for new preservation evidence creation, the new version of the Preservation evidence policy is issued.

Digital signature preservation metadata is the data about digital signature preservation status, cryptographic algorithms used in the preservation evidences, planned augmentations and preservation period. Digital signature preservation metadata is collected during submission data object reception, stored separately from the preservation objects in the preservation service storage, and updated during further augmentations. Digital signature preservation metadata cover at least the following:

- Digital signature identifier.
- Current digital signature level (B-B, B-T, B-LT, B-LTA, or corresponding signature format for non-baseline profile signatures).
- Indication if digital signature preservation to be performed or not.
- If digital signature level is B-LTA, the hash algorithm used for the last archival time stamp digest calculation, signature algorithm (with key length) and the hash algorithm used by the timestamping authority to sign time stamp itself.
- The date of the next planned augmentation.
- The end date of the preservation period.

Main rules of the next augmentation date estimation used by the MitSoft PSP:

- If the preservation of digital signature is not performed, then next augmentation date is set to NULL. It means no augmentation will be performed for this digital signature.
- If the level of digital signature is B-B, then next augmentation date is set to current date. It means, that digital signature augmentation should be performed immediately to reach at least B-T level.
- If the level of digital signature is B-T or B-LT, the next augmentation date is set to proof of existence time of the signature value (signature time stamp generation time) + grace period applied by the certification authority (issuer of the signer certificate). If grace period is unknown, default 24 hours grace period is used. It means, that digital signature augmentation

to reach B-LTA level should be performed as soon as suitable validation data become available.

- If the level of digital signature is B-LTA, then next augmentation date is calculated according the last archival time stamp signing certificate expiration date and expected reliability duration of the used cryptographic algorithms. Since augmentation process takes time, and there may be a great number of digital signatures preserved by the time stamps signed using the same timestamping authority certificate, next augmentation date is set within augmentation period and prior to caution period. Augmentation period is a reasonable time period, which starts some time before expected digital signature validity expiration and lasts till the expected digital signature validity expiration date. In order to reduce the risks of possible unavailability of third-party services, the next augmentation date is set prior to caution period. Caution period used by the preservation service is indicated in Subscriber agreement.
- If cryptographic algorithm registry revision recognizes, that some cryptographic algorithm will become less secure earlier than it was expected, then irregular augmentation event is raised. In this case, the next augmentation date is updated according the new expected algorithm reliability time. The digital signatures affected by this event are determined using digital signature preservation metadata.

Digital signature augmentation is performed automatically by the system. Next augmentation date triggers an augmentation event, which puts preserving electronic document or container (with the digital signature to be augmented) into the augmentation queue, which is used by the automatic augmentation process.

7.15. Augmentation of preservation evidences

Preservation goal PDS (extending over long periods of time the validity status of digital signatures) is achieved by timely electronic signatures and electronic seals augmentation.

Used preservation evidences are time stamps that are signed by the directly trusted timestamping authority certificates, which are included into the time stamps. This assures that no additional validation data is needed to augment time stamp itself.

Missing validation data gathering is performed as soon as suitable validation data is available (just after grace-period). Preservation is not performed for electronic signatures and electronic seals, for which suitable validation data is unavailable. For qualified electronic signatures and qualified electronic seals certificate authorities (as qualified trusted service providers issuing qualified certificates) shall ensure, that suitable validation data to be available for every certificate to be validated.

Augmentation is performed not for the separate preservation evidence, but augmentation is performed for the whole digital signature including previously added preservation evidences. Therefore, preservation evidences augmentation is achieved by digital signature augmentation. Cryptographic monitoring and required augmentation planning (see Section 7.14 for details) assures PDS preservation goal to be achieved.

7.16. Export-import package

MitSoft PSP allows the subscriber's representative named as subscriber's administrator of MitSoft PSP long-term preservation service to submit the request for export-import package(s), containing the preserved data, the evidences and all information needed to validate the evidences. The request for export-import package shall be done by e-mail indicating the criteria that to be used to select the preservation objects to be included in the export-import package.

The export-import package is not encrypted and it is delivered to subscriber's administrator of the service using secure data transfer protocol.

MitSoft PSP keeps records of all released export-import packages including:

1) the date of the event;
2) the criteria that has been used to select the set of preservation objects to be included in the export-import package.

The structure of export-import package is defined in the separate document „Export-import package".

The version of the Export-import package definition in effect is available for subscribers on the repository of MitSoft PSP.

8. Operational and notification protocols

8.1. Preservation protocol

Preservation protocol is implemented through preservation profiles and Web service operations supported by them. Operations are implemented as REST web services. Web service caller authentication is used and communication encryption (Secure Sockets Layer) is applied. Only authenticated clients may use/call operations defined in the preservation profiles.

Preservation service is available using one of the available preservation profiles - MitSoftQWST and MitSoftQWOS (see section 6.4). Both preservation profiles support the following operation:

- `RetrieveInfo` (defined in the ETSI TS 119 512): allows to retrieve information about the currently and previously supported preservation profiles.

Preservation profile MitSoftQWST supports the following operations:

- `Store` (defined in the preservation profile MitSoftQWST): allows to pass electronic document/container signed with electronic signature(-s)/seal(-s) together with additional metadata to the preservation service for its further preservation and storage in the MitSoft preservation service; supported submission data objects and their formats are defined in the MitSoftQWST profile. If a preservation object with provided identifier already exists in the preservation service, it is replaced by the submitted data object.
- `Status` (defined in the preservation profile MitSoftQWST): allows to get current status of the electronic document/container and preserving electronic signatures/seals within it.
- `Download` (defined in the preservation profile MitSoftQWST): allows to download the electronic document/container together with preserving electronic signatures/seals and preservation evidences within it.
- `Remove` (defined in the preservation profile MitSoftQWST): allows to remove currently preserving electronic document/container together with preserving electronic signatures/seals and preservation evidences within it; associated metadata is also removed; electronic document/container preservation is to be stopped. The corresponding submission data object is not preserved by the MitSoft preservation service.
- `PreservePO` (defined in the ETSI TS 119 512): allows to pass electronic document/container signed with electronic signature(-s)/seal(-s) to the preservation service for its further preservation and storage in the MitSoft preservation service. Supported submission data objects and their formats are defined in the MitSoftQWST profile. If a preservation object with provided identifier already exists in the preservation service, it is replaced by the submitted data object
- `RetrievePO` (defined in the ETSI TS 119 512): allows to retrieve the electronic document/container together with preserving electronic signatures/seals and preservation evidences within it.
- `DeletePO` (defined in the ETSI TS 119 512): allows to delete currently preserving electronic document/container together with preserving electronic signatures/seals and preservation evidences within it; associated metadata is also removed; electronic document/container preservation is to be stopped. The corresponding submission data object is not preserved by the MitSoft preservation service.
- `RetrieveTrace` (defined in the ETSI TS 119 512): allows to retrieve the audit trail of the electronic document/container and preserving electronic

signatures/seals within it. Audit trail contains information about preservation actions performed with the preservation object.

- `Search` (defined in the ETSI TS 119 512): allows to search among the set of preservation objects that are accessible by the client.

Preservation profile MitSoftQWOS supports the following operations:

- `Augment` (defined in the preservation profile MitSoftQWOS): allows to perform preservation action for the provided electronic document/container signed with electronic signature(-s)/seal(-s); preservation action covers preserving digital signatures validation and augmentation; provided electronic document/container with augmented electronic signature(-s)/seal(-s) and preservation evidences within them to be returned; supported submission data objects and their formats are defined in the MitSoftQWOS profile. Calculated expected evidence duration and recommended time of the next augmentation are also returned.
- `Download` (defined in the preservation profile MitSoftQWOS): allows to download the electronic document/container previously augmented with Augment operation. It is used for efficient retrieving result of the Augment operation only.
- `PreservePO` (defined in the ETSI TS 119 512): allows to perform preservation action for the provided electronic document/container signed with electronic signature(-s)/seal(-s); preservation action covers preserving digital signatures validation and augmentation; provided electronic document/container with augmented electronic signature(-s)/seal(-s) and preservation evidences within them to be returned; submission data objects and their formats are defined in the MitSoftQWOS profile. Calculated expected evidence duration and recommended time of the next augmentation are also returned.

The details of the supported operations and used preservation protocol are fully described in the preservation profiles documents (see section 6.4 for references to documents).

8.2. Notification protocol

Not applicable.

9. Preservation process

9.1. Storage of preserved data and evidences

MitSoft PSP stores preservation objects during whole preservation period, or till the explicit request for removal. Preservation objects provided to preservation service are not stored within PSP storage in the case profile without storage (WOS) is used. All preservation evidences are incorporated into the preservation objects and they are stored and deleted together with preservation objects and submission data objects.

Most subscribers have legal obligations to perform their own legal procedures before physical deletion of preserved electronic document, even after the preservation period. Therefore, preservation objects are stored in the PSP storage until they are removed by the subscriber. Subscriber agreements between the PSP and the subscribers define the exact period of the preservation object and its metadata storage after elapsed preservation period.

If preservation period elapsed, no preservation actions (augmentation) will be performed any more.

9.2. Preservation evidences

The only preservation evidences used are qualified electronic time stamps that are aligned with the following standards:

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

There are used only qualified electronic time stamps that satisfies the following requirements:

- It is qualified electronic time stamp as per eIDAS Regulation [eIDAS].
- It is issued by the EU qualified time-stamping authority.
- Certificate used to sign qualified electronic time stamp is presented within time stamp.
- Certificate used to sign qualified electronic time stamp itself is listed in the EU Trusted List.

These requirements assure, that no more additional validation data is needed to validate time stamp itself.

Every preservation evidence (time stamp) is stored within preserving electronic signature or electronic seal, since it is included as appropriate time stamp attribute.

9.3. Preservation of digital signatures

Preservation of digital signatures is achieved by timely digital signature augmentation. This is performed through 3 stages:

- B-T level assurance. It is performed at the time of submission, if valid signature time stamp is missing in the digital signature. New signature time stamp is obtained and included into the digital signature. This provides the proof of existence for the digital signature.
- B-LTA level assurance. It is performed immediately after grace-period elapsed (or at the time of submission, if grace-period is already elapsed), if validation data or part of it is missing, or all covering time stamp is not presented within digital signature (B-LTA level is not reached). Missing

validation data is collected and included into the digital signature. This assures, that all required validation data is collect at the time it is still available and still suitable for validation. New archival time stamp, which covers all digital signature data, validation data and actually signed data, is obtained and included into the digital signature. This provides the proof of existence for validation data, previously added time stamps and also for actually signed data. Supported preservation object formats assures, that archival time stamp directly covers the signed data even if detached signatures are used.

- B-LTA level preservation assurance. It is performed when preservation event is raised by the maintenance process (see clause 7.14). New archival time stamp is obtained and included into the digital signature. This provides the new proof of existence for previously added time stamps, validation data, signed data and protection against certificate expiration and possible future obsolescence of the used cryptographic algorithms.

Digital signature augmentation (and validation) is based on the standard ETSI EN 319 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation [EN 319 102-1] and is performed according Signature validation policy of MitSoft PS.

Supported preservation object formats assures, that signed data will be provided to the preservation service together with the digital signature. Detached signatures with only hashes of the signed data (without signed data itself) is not supported by MitSoft PSP.