mitsoft

Qualified Long-term Preservation Service

Preservation Evidence Policy

QLPS/PEP

Unique object ID (OID): **1.3.6.1.4.1.57890.1.7.1.1**

Version 1.01

Valid since 2026-09-01

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

Approvals

Revision history

Version	Valid since	Description
1.00	2023-05-15	First official version of the document
1.01	2026-09-01	Algorithms ecdsa-with-SHA256 and ecdsa-with-SHA512 supported for time stamp signing; reference to ENISA

Approval of the document

	Name	Date	Signature
Reviewed by	Adomas Birštunas	2026-05-20	
Approved by	Antanas Mitašiūnas	2026-05-20	

Table of content

1. Introduction 4
1.1. Overview 4
1.2. Scope of preservation evidence policy 4
1.3. Preservation evidence policy document identifier 4
2. References 6
3. Definitions of terms and abbreviations 7
4. Preservation evidence policy requirements 8
4.1. Preservation evidence creation and usage 8
4.2. Preservation evidences 8
4.3. Cryptographic suites 9
4.4. Trusted service providers 10
4.5. Preservation evidence validation 10
4.6. Preservation evidence policy identification in the preservation evidences 10

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 power as hand signed paper documents. Information about the MitSoft is available on the website http://www.mitsoft.lt/.

1.1. Overview

The present document defines MitSoft Qualified Long-term Preservation Service preservation evidence policy in a human readable form. Preservation evidence policy is created to define the set of rules that specify the requirements and the internal process to generate and how to validate a preservation evidence.

The present preservation evidence policy document is aligned with the requirements for the preservation evidence policy listed in the section 6.5 of the ETSI TS 119 511 Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques [TS 119 511].

Note regarding the definitions. Hereafter preservation evidence policy means Preservation evidence policy for MitSoft Qualified Long-term Preservation Service.

In all cases this human readable English version of Preservation evidence policy has priority.

1.2. Scope of preservation evidence policy

The present preservation evidence policy is applied only by MitSoft Qualified Long-term Preservation Service to ensure long-term preservation of the electronic documents or containers signed by qualified electronic signatures or qualified electronic seals.

1.3. Preservation evidence policy document identifier

The unique identifier (OID) of the preservation evidence policy is 1.3.6.1.4.1.57890.1.7.1.1; the values of its fields are given in the Table 1.

Table 1. The values of the fields of the unique identifier of the Preservation evidence policy

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 MitSoft	1
Document type (preservation evidence policy)	7
Preservation evidence policy identifier	1

Document version	1

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.

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

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

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

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

[RFC 5816] – IETF RFC 5816 (2010): "ESSCertIDv2 Update for RFC 3161".

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

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

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

3. Definitions of terms and abbreviations

Cryptographic suite: combination of a signature scheme with a padding method and a cryptographic hash function

Digital signature: data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.

Note: In the present document digital signature is a technical term, which is used to define electronic signature, advanced electronic signature, qualified electronic signature, electronic seal, advanced electronic seal, and qualified electronic seal as per eIDAS Regulation [eIDAS].

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.

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 augmentation: addition of data to an existing preservation evidence to extend the validity period of that evidence

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

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.

Time-stamping authority: trust service provider which issues electronic time stamps using one or more time-stamping units.

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.

Acronyms

ETSI – European Telecommunications Standards Institute
OID – Object identifier
QLURNPS – Qualified long-term preservation service
TSA – Time-stamping authority
URN – Uniform Resource Number

4. Preservation evidence policy requirements

4.1. Preservation evidence creation and usage

MitSoft Qualified Long-term Preservation Service uses qualified electronic time stamps as preservation evidences.

The process of the qualified electronic time stamp creation and usage is as follows:

- Preservation service creates message digest of the data to be timestamped. Data to be timestamped depends on the time stamp attribute to be created – according XAdES, CAdES, PAdES electronic signature standards requirements for the appropriate time stamp attribute (see [TS 101 903], [TS 101 733], [TS 102 778-4], [EN 319 132-1], [EN 319 122-1], [EN 319 142-1]). Algorithms used for the digest calculations are presented in the clause 4.3.
- Preservation service creates time stamp request according RFC 3161 [RFC 3161] and sends it to the timestamping authority using time stamp protocol via HTTP as defined in the RFC 3161. Created time stamp request contains field `certReq` set to true (signing certificate is requested to be included into the time stamp response).
- TSA creates time stamp response with an electronic time stamp in it. Created time stamp response is returned to the preservation service.
- Preservation service validates just obtained time stamp (see clause 4.5).
- Preservation service constructs time stamp attribute using obtained electronic time stamp and incorporates attribute into the XAdES, CAdES, PAdES signature according requirements presented in the XAdES, CAdES, PAdES standards (see [TS 101 903], [TS 101 733], [TS 102 778-4], [EN 319 132-1], [EN 319 122-1], [EN 319 142-1]).

Preservation evidences (time stamps) are stored within digital signatures as signature attributes. Digital signatures are integral part of the preserved electronic documents.

4.2. Preservation evidences

Preservation evidences are time stamp attributes incorporated into the digital signatures:

- For XAdES signatures XML-based Archive Time Stamp property according ETSI TS 101 903 [TS 101 903] and ETSI EN 319 132-1 [EN 319 132-1] is used.
- For CAdES signatures ASN.1-based Archive Time Stamp V3 attribute according ETSI TS 101 733 [TS 101 733] and ETSI EN 319 122-1 [EN 319 122-1] is used.
- For PAdES signatures Document Time Stamp attribute according ETSI TS 102 778-4 [TS 102 778-4] and ETSI EN 319 142-1 [EN 319 142-1] is used.

Every created time stamp attribute contains qualified electronic time stamp, which is 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, those satisfies the following requirements:

- It is qualified electronic time stamp as per eIDAS Regulation [eIDAS].
- It is issued by the qualified trust service provider, which confirms eIDAS Regulation requirements.
- 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.

4.3. Cryptographic suites

Cryptographic algorithms and key lengths for preservation evidences are selected based on the ETSI TS 119 312 Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites [TS 119 312] and are compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [ENISA].

For every created electronic time stamp (new preservation evidence), preservation service uses the following cryptographic algorithms:

- Canonicalization algorithms (for XML based time stamps only) used for message digest calculation:
  - Canonical XML 1.0 (omits comments) (URN http://www.w3.org/TR/2001/REC-xml-c14n-20010315), or
  - Exclusive XML Canonicalization 1.0 (omits comments) (URN http://www.w3.org/2001/10/xml-exc-c14n#).
- Digest algorithms used for message digest calculation:
  - SHA256 (OID 2.16.840.1.101.3.4.2), or
  - SHA512 (OID 2.16.840.1.101.3.4.3).
- Signature algorithms used by timestamping authority for time stamp signing:
  - sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11), and key length ≥ 2 048, or
  - sha512WithRSAEncryption (OID 1.2.840.113549.1.1.13), and key length ≥ 2 048, or
  - ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2) with P-256 (OID 1.2.840.10045.3.1.7), P-384 (OID 1.3.132.0.34) or P-521 (OID 1.3.132.0.35) elliptic curves, or
  - ecdsa-with-SHA512 (OID 1.2.840.10045.4.3.4) with P-256 (OID 1.2.840.10045.3.1.7), P-384 (OID 1.3.132.0.34) or P-521 (OID 1.3.132.0.35) elliptic curves.

Requirements for the cryptographic algorithms applied for the preservation evidences, those are already presented in the digital signatures, are based on the ETSI TS 119 312 Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites [TS 119 312] and are compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [ENISA]. National electronic document specifications suppress requirements for allowed cryptographic algorithms. Requirements are defined in detail in the MitSoft Qualified Long-term Preservation Service signature policy.

4.4. Trusted service providers

This preservation evidence policy supports only qualified electronic time stamps, those are issuer by the qualified trust service providers, those confirms eIDAS Regulation requirements [eIDAS]. Trusted service provider certificate used for time stamp signing shall be listed as qualified electronic time stamp provider certificate in the EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml).

4.5. Preservation evidence validation

Preservation evidences (electronic time stamps) validation is performed according time stamps validation procedures described in ETSI EN 319 102-1 Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation [EN 319 102-1].

Time stamp attribute validation covers:

- Time stamp attribute validation according requirements listed in the corresponding digital signature standard:
  - for XAdES signatures - ETSI TS 101 903 [TS 101 903] and ETSI EN 319 132-1 [EN 319 132-1].
  - for CAdES signatures - ETSI TS 101 733 [TS 101 733] and ETSI EN 319 122-1 [EN 319 122-1].
  - for PAdES signatures - ETSI TS 102 778-4 [TS 102 778-4] and ETSI EN 319 142-1 [EN 319 142-1].
- Validation if calculated message digest is equal to the message digest presented in the time stamp.
- Time stamp signing certificate validation. Requirements for trusted service providers described in the clause 4.4.
- Cryptographic algorithms validation according cryptographic suites validation (see clause 4.3).

Preservation service uses only time stamps attributes incorporated into the digital signatures. Therefore, digital signature augmentation at the same time is also augmentation of the preservation evidences.

4.6. Preservation evidence policy identification in the preservation evidences

There is no preservation service, preservation profile or preservation evidence policy identification presented in used preservation evidences.