mitsoft

Qualified Long-term Preservation Service

Signature Policy

QLPS/SP

Unique object ID (OID): **1.3.6.1.4.1.57890.1.6.1.1**

Version 1.02

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		First official version of the document
1.01	2023-05-15	CMS signatures in PDF are permitted; clarification for non-valid digital signature preservation
1.02	2026-09-01	Compliance with new implementing acts

Approval of the document

	Name	Date	Signature
Reviewed by	Adomas Birštunas	2026-06-18	
Approved by	Antanas Mitašiūnas	2026-06-19	

Table of content

1. INTRODUCTION 6
1.1. Overview 6
1.2. Business or Application Domain 6
1.2.1. Scope and boundaries of signature policy 6
1.2.2. Domain of applications 6
1.2.3. Transactional context 6
1.3. Document and policy(ies) names, identification and conformance rules 7
1.3.1. Signature policy document and signature policy(ies) names 7
1.3.2. Signature policy document and signature policy identifiers 7
1.3.3. Conformance rules 7
1.3.4. Distribution points 8
1.4. Signature policy document administration 8
1.4.1. Signature policy authority 8
1.4.2. Contact person 9
1.4.3. Approval procedures 9
1.5. Definitions and Acronyms 9
1.5.1. Definitions 9
1.5.2. Acronym 10
1.5.3. References 10
2. Signature application practices statements 13
3. BUSINESS SCOPING PARAMETERS 14
3.1. BSPs mainly related to the concerned application/business 14
3.1.1. BSP (a): Workflow (sequencing and timing) of signatures 14
3.1.1.1 Workflow of the MitSoft preservation service with storage 14
3.1.1.2 Workflow of the MitSoft preservation service without storage 15
3.1.1.3 Performing signature validation 16
3.1.1.4 Performing signature augmentation 16
3.1.2. BSP (b): Data to be signed 17
3.1.3. BSP (c): The relationship between signed data and signature(s) 19
3.1.4. BSP (d): Targeted community 21
3.1.5. BSP (e): Allocation of responsibility for signature validation and augmentation 21
3.2. BSPs mainly influenced by the legal/regulatory provisions 22
3.2.1. BSP (f): Legal type of the signatures 22
3.2.2. BSP (g): Commitment assumed by the signer 22
3.2.3. BSP (h): Level of assurance on timing evidences 23
3.2.4. BSP (i): Formalities of signing 24
3.2.5. BSP (j): Longevity and resilience to change 24

3.2.6. BSP (k): Archival 24
3.3. BSPs mainly related to the actors involved in creating/augmenting/validating signatures 25
3.3.1. BSP (l): Identity (and roles/attributes) of the signers 25
3.3.2. BSP (m): Level of assurance required for the authentication of the signer 26
3.3.3. BSP (n): Signature creation devices 26
3.4. Other BSPs 26
3.4.1. BSP (o): Other information to be associated with the signature 26
3.4.2. BSP (p): Cryptographic suites 26
3.4.2.1 Requirements for the Cryptographic algorithms used in the submitted signatures 27
3.4.2.2 Requirements for the Cryptographic algorithms used for augmentation 27
3.4.3. BSP (q): Technological environment 28
4. Requirements / statements on technical mechanisms and standards implementation 29
4.1. Technical counterparts of BSPs - Statement summary 29
4.1.1. Statement summary for ADOC-V1.0 electronic documents 29
4.1.2. Statement summary for ADOC-V2.0 electronic documents 31
4.1.3. Statement summary for EGAS-V1.0 electronic documents 33
4.1.4. Statement summary for MDOC-V1.0 electronic documents 35
4.1.5. Statement summary for PDF-LT-V1.0 electronic documents 37
4.1.6. Statement summary for PDF-RC-V1.0 electronic documents 39
4.1.7. Statement summary for ASiC baseline containers 41
4.1.8. Statement summary for PAdES baseline signatures 43
4.1.9. Statement summary for CMS signatures in PDF (PAdES-Basic) 45
4.2. Input and output constraints for signature creation, augmentation and validation procedures 47
4.2.1. Input constraints to be used when generating, augmenting and/or validating signatures in the context of the identified signature policy 47
4.2.1.1 Input constraints for ADOC-V1.0 electronic documents 47
4.2.1.2 Input constraints for ADOC-V2.0 electronic documents 52
4.2.1.3 Input constraints for EGAS-V1.0 electronic documents 58
4.2.1.4 Input constraints for MDOC-V1.0 electronic documents 63
4.2.1.5 Input constraints for PDF-LT-V1.0 electronic documents 68
4.2.1.6 Input constraints for PDF-RC-V1.0 electronic documents 73
4.2.1.7 Input constraints for ASiC baseline containers 78
4.2.1.8 Input constraints for PAdES baseline signatures 82
4.2.1.9 Input constraints for CMS signatures in PDF (PAdES-Basic) 86
4.2.2. Output constraints to be used when validating signatures in the context of the identified signature policy 90

4.2.3. Output constraints to be used for generating/augmenting signatures in the context of the identified signature policy 90
5. Other business and legal matters 91
6. Other business and legal matters Compliance audit and other assessments 92

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 signature policy is created to define the set of rules related to validation and augmentation of signatures contained in the preserved electronic documents or electronic containers.

The present signature policy covers the following aspects related to the management of the signatures to which it applies:

- a signature validation policy,
- a signature augmentation policy.

The present signature policy is created to be used by the MitSoft Qualified Long-term Preservation Service to determine the validity status of the electronic signatures, those signs preserved electronic documents or electronic containers.

The present signature policy 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 TS 119 172-1 "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents";

Note regarding the definitions. Hereafter signature policy, signature validation policy, signature augmentation policy or just policy means Signature policy for MitSoft Qualified Long-term Preservation Service.

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

1.2. Business or Application Domain

1.2.1. Scope and boundaries of signature policy

The scope of the present signature policy is MitSoft Qualified Long-term Preservation Service. The present policy document is used for augmentation and validation of signatures to ensure electronic document or container long-term preservation.

1.2.2. Domain of applications

Not applicable.

1.2.3. Transactional context

MitSoft Qualified Long-term Preservation Service uses signature validation policy to determine the validity status of the electronic documents or containers provided to the service for further preservation. Augmentation of the preserved qualified electronic signatures, qualified electronic seals, advanced electronic signatures and advanced electronic seals are also performed according the present signature augmentation policy.

1.3. Document and policy(ies) names, identification and conformance rules

1.3.1. Signature policy document and signature policy(ies) names

MitSoft Qualified Long-term Preservation Service signature policy.

1.3.2. Signature policy document and signature policy identifiers

The unique identifier (OID) of the MitSoft Qualified Long-term Preservation Service signature policy is as follows:

- identifier presented as OID is
  - 1.3.6.1.4.1.57890.1.6.1.1;

  the values of its fields are given in the Table 1.
- Identifier presented as URI is
  - `http:/uri.mitsoft.lt/preservation/policy/1.1`.

Table 1. The values of the fields of the unique identifier of the signature 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 (signature policy)	6
Signature policy identifier	1
Document version	1

The version of the signature policy in effect is available on the repository of MitSoft PSP: https://www.mitsoft.lt/qtsp-repo/qlps-subscriber-area/.

1.3.3. Conformance rules

The present signature policy describes the set of rules for qualified electronic signature, qualified electronic seals, advanced electronic signature and advanced electronic seals augmentation and validation processes, those meets requirements laid down in:

- 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];
- 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].

- ETSI TS 119 172-4 "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists".

Qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals augmentation process shall use qualified electronic time stamps obtained from the qualified timestamping authorities, those are conformant to Regulation (EU) No 910/2014 [eIDAS].

1.3.4. Distribution points

The present signature policy in a human readable form is available on the MitSoft PSP repository: https://www.mitsoft.lt/qtsp-repo/qlps-subscriber-area/. The present signature policy is not available in a machine processable format.

1.4. Signature policy document administration

1.4.1. Signature policy authority

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

Table 2. Contact information of the signature policy authority

Name:	The joint stock company "MIT-SOFT"
Registration number:	120792080
Address:	Kalvarijų str. 276-100, LT-08316 Vilnius
Phone:	+370 5 233 3922
URL:	http://www.mitsoft.lt/
E-mail:	info@mitsoft.lt

The present signature policy document is signed by the director of the joint stock company "MIT-SOFT". Main information of the public key certificate, used to sign the present document is given in the Table 3.

Table 3. Information of the public key certificate used to sign the present document

Owner:	ANTANAS, MITAŠIŪNAS, LT
DN:	C=LT CN=ANTANAS,MITAŠIŪNAS SN=MITAŠIŪNAS GIVENNAME=ANTANAS SERIALNUMBER= PNOLT-35201290142
Serial number:	281106941581223758063334190748323213 61 (0x1525ec3a3d4e7bc164219d4757f04b51)
Issue DN:	C=EE CN = EID-SK 2016 O= AS Sertifitseerimiskeskus organizationIdentifier=NTREE-10747013

Valid from:	2023-03-27 16:42:31
Valid To:	2028-03-25 23:59:59

1.4.2. Contact person

Contact person information is given in the Table 4.

Table 4. Contact person information

Name:	Adomas Birštunas
E-mail:	info@mitsoft.lt
Phone:	+370-5-2333922

1.4.3. Approval procedures

The present signature policy document is approved by the director of the joint stock company "MIT-SOFT".

1.5. Definitions and Acronyms

1.5.1. Definitions

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].

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.

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.

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

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

Signer: entity being the creator of a digital signature.

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

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

Time-stamping service: trust service for issuing time-stamps.

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

Other definitions are used as in Regulation (EU) 910/2014 [eIDAS].

1.5.2. Acronym

CA	–	Certificate authority
ETSI	–	European Telecommunications Standards Institute
OID	–	Object identifier
PS	–	Qualified long-term preservation service
PSP	–	Preservation service provider
PSPS	–	Qualified long-term preservation service practice statement
TSA	–	Time-stamping authority
QSCD	–	Qualified Signature Creation Device

1.5.3. References

[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.

[CID 2013/662] – 2013/662/EU: Commission Implementing Decision of 14 October 2013 amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States.

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

[EN 319 412-5] – ETSI EN 319 412-5: "Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

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

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

[MitSoft PS] – MitSoft Qualified Long-term Preservation Service Practice Statement.

[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".

[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 102 778-2] - 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 119 101] - ETSI TS 119 101: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation".

[TS 119 172-4] - ETSI TS 119 172-4: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists".

[TS 119 612] - ETSI TS 119 612: "Electronic Signatures and Trust Infrastructures (ESI); Trusted Lists".

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

2. Signature application practices statements

Signature application, which uses the present signature policy is MitSoft Qualified Long-term Preservation Service, which defines the following practice statement document:

- MitSoft Qualified Long-term Preservation Service Practice Statement, which is indicated by the unique object identifier (OID):
  - 1.3.6.1.4.1.57890.1.4.1.

MitSoft Qualified Long-term Preservation Service ensures, that signature validation and augmentation is performed according this signature policy, and signature validation application is compliant with [TS 119 101].

3. BUSINESS SCOPING PARAMETERS

3.1. BSPs mainly related to the concerned application/business

3.1.1. BSP (a): Workflow (sequencing and timing) of signatures

MitSoft Qualified Long-term Preservation Service receives electronic documents or containers from its clients. Validation is performed by the MitSoft Qualified Long-term Preservation Service on the time of receiving an electronic document or container, or later on the time of explicit request by the client or preservation service maintenance process. Augmentation is timely performed by the request of the MitSoft Qualified Long-term Preservation Service maintenance process.

The present signature policy is used by the MitSoft PSP for ensuring service with two profiles:

- MitSoft preservation service with storage (WST),
- MitSoft preservation service without storage (WOS).

Every service defines its own workflow of the electronic document/container and their digital signatures.

3.1.1.1 Workflow of the MitSoft preservation service with storage

Workflow of the electronic document/container and its digital signatures used in MitSoft preservation service with storage is presented in the figure 1.

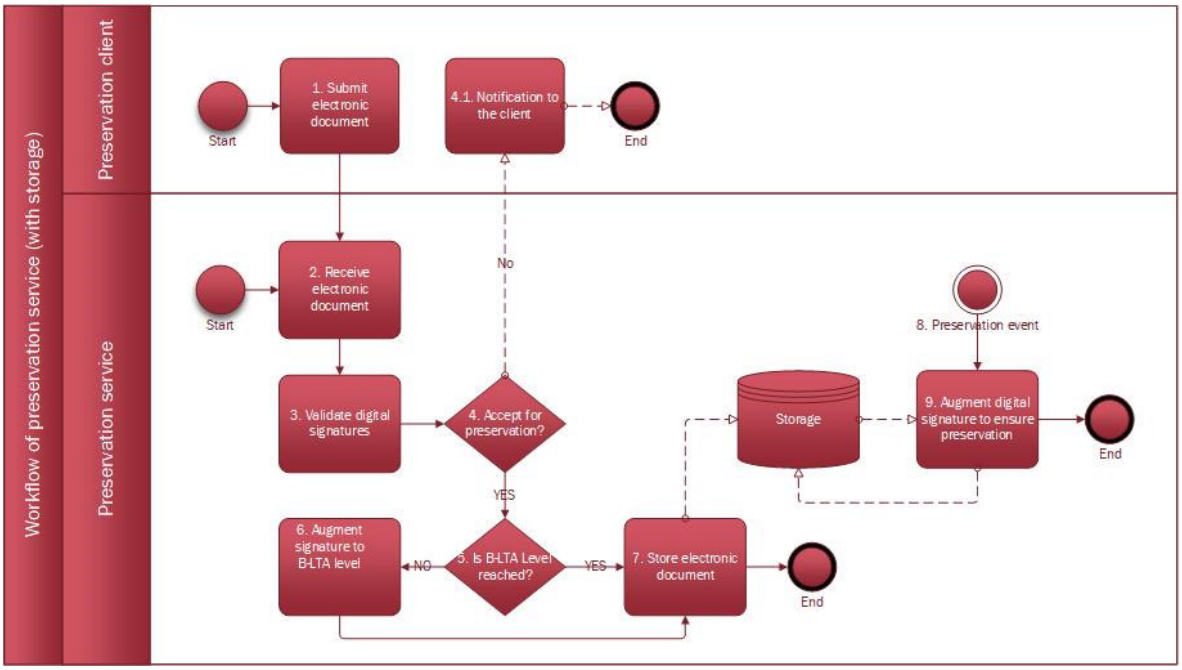


Fig. 1. Electronic document/*container* workflow for MitSoft preservation service with storage (WST)

1. Preservation client submits electronic document or container to preservation service.
2. Preservation service receives electronic document or container, which contains electronic signatures or electronic seals.
3. Preservation service validates electronic document/container and electronic signatures and/or electronic seals contained in it. The present signature policy document is used for digital signature validation.

4. Preservation service checks if electronic document/container and electronic signatures and/or electronic seals to be preserved.
   4.1. Preservation client receives notification and reason of the rejection from the preservation service.
5. Preservation service checks if every electronic signature and electronic seal to be preserved already reached B-LTA level (or corresponding archival signature format for non-baseline signatures) or not.
6. Preservation service perform electronic signatures and/or electronic seals augmentation. After this augmentation every digital signature to be preserved will reach B-LTA level (or corresponding archival signature format for non-baseline signatures). The present signature policy document is used for digital signature augmentation.
7. Preservation service stores electronic document/container together with preservation metadata into the storage.
8. Preservation service maintenance process maintains preserved electronic documents/containers and digital signatures contained in them. Preservation service maintenance process raises preservation event if preserved digital signatures should be augmented to ensure their 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 archive time stamps (or DocumentTimeStamp for PAdES signatures) to extend their preservation period. The present signature policy document is used for digital signature augmentation.

3.1.1.2 Workflow of the MitSoft preservation service without storage

Workflow of the electronic document/container and its digital signatures used in MitSoft preservation service without storage is presented in the figure 2.

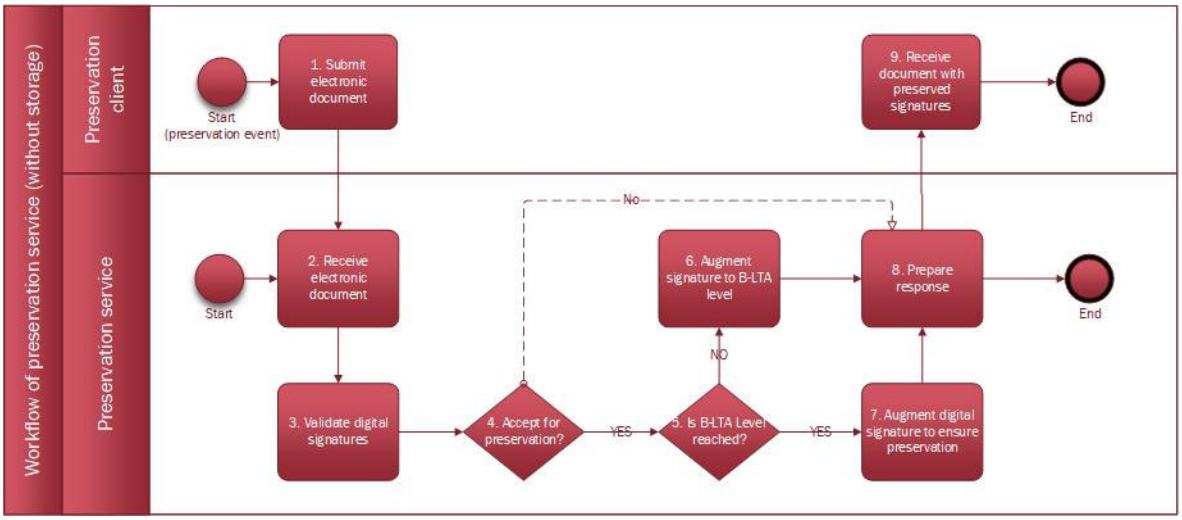


Fig. 2. Electronic document/container workflow for MitSoft preservation service without storage (WOS)

1. Preservation client submits electronic document or container to preservation service.
2. Preservation service receives electronic document or container, which contains electronic signatures or electronic seals.
3. Preservation service validates electronic document/container and electronic signatures and/or electronic seals contained in it. The present signature policy document is used for digital signature validation.

4. Preservation service checks if electronic document/container and electronic signatures and/or 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/or electronic seals. After this augmentation every electronic signature or electronic seal to be preserved reaches B-LTA level (or corresponding archival signature format for non-baseline signatures). The present signature policy document is used for digital signature augmentation.
7. Preservation service performs digital signature augmentation by adding new archive time stamps to extend their preservation period. Preservation evidences are included into the digital signatures/seals presented in the electronic document/container. The present signature policy document is used for digital signature augmentation.
8. Preservation service prepares response to the client. On success, the response contains upgraded electronic document/container with preservation evidences included within digital signatures/seals. Otherwise, the rejection or failure reason is returned.
9. Preservation client receives updated electronic document/container from the preservation service.

3.1.1.3 Performing signature validation

Validation is performed according standard ETSI EN 319 102-1 ”Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation” [EN 319 102-1].

Validation, whether a digital signature is fit for meeting the requirements of EU qualified electronic signature or qualified electronic seal, is performed taking into account the EU Member States trusted lists and is compliant with the requirements defined in the standard ETSI EN 119 172-4 “Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists” [EN 119 172-4].

Validation is performed for every qualified electronic signature, qualified electronic seal, advanced electronic signature and advanced electronic seal contained within the electronic document/container. The validation result is also used to decide if digital signature shall be preserved (and registered for augmentation) or not.

Validation of every digital signature is performed separately and independently of other digital signatures contained in the same electronic document or container. Digital signature being a counter signature, or countersigned signature does not impact validation process and its validity status. Only detached countersignatures are allowed, XAdES and CAdES CounterSignature attribute is forbidden.

Every document time stamp presented within PDF document is also some kind of a time stamp for every PAdES signature. Therefore, the same document time stamp will be used during every PAdES signature validation.

No special timing constraints are applied for validation.

3.1.1.4 Performing signature augmentation

Augmentation is performed according standard ETSI EN 319 102-1 ”Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation” [EN 319 102-1].

Augmentation is performed for qualified electronic signatures and qualified electronic seals contained within the preserving electronic document/container. Augmentation for advanced electronic signatures and advanced electronic seals (that

are not qualified) is performed only if such a requirement is listed in the Subscriber agreement. Electronic signatures or electronic seals, whose are not advanced electronic signatures or advanced electronic seals, are not preserved by the MitSoft Qualified Long-term Preservation Service and, therefore, their augmentation (even if performed) is not regulated by the present signature policy document.

Augmentation is performed for valid electronic signatures and valid electronic seals (having validation status PASSED). Non-valid electronic signatures and non-valid electronic seals (having validation status other than PASSED) are augmented if only validation errors do not prevent digital signature from the augmentation, and if such a requirement (to preserve and augment non-valid digital signatures) is listed in the Subscriber agreement.

Which validation error does not prevent digital signature from the augmentation, and which does prevent, is defined in terms of subindications returned by the validation process according standard ETSI EN 319 102-1 [EN 319 102-1].

The present signature policy defines the following list of subindications according ETSI EN 319 102-1 [EN 319 102-1], that do not prevent digital signature from the augmentation:

- SIG_CONSTRAINTS_FAILURE,
- CRYPTO_CONSTRAINTS_FAILURE_NO_POE,
- CRYPTO_CONSTRAINTS_FAILURE,
- CUSTOM.

Augmentation for non-valid digital signature will not be performed if validation result contains an error having any subindication other than the listed above.

Augmentation is performed if only required validation data is still available, required validation data is relevant and it is possible to collect it by automatic means. Partial augmentation (till level T, or LT, instead of required LTA) is allowed.

Augmentation of every XAdES or CAdES signature is performed separately and independently of other digital signatures contained in the same electronic document or container. Augmentation of PAdES signatures may be performed separately or together with other PAdES signatures contained in the same PDF document to reduce the amount of electronic time stamps applied to the PDF document.

No special timing constraints are applied for augmentation.

3.1.2. BSP (b): Data to be signed

Validated electronic signatures and seals are part of the electronic document or container and should sign content inside them. Supported electronic document and container formats and corresponding data to be signed are listed in the Table 5.

Table 5. Signed data and formats

Electronic document, or container specification	Signed data	Allowed data to be signed formats
ADOC-V1.0 electronic documents [ADOC-V1.0]	Every signature may sign every or only part of the content files, signed metadata files or their parts, or other signatures (using counter signature) presented within electronic document container as defined in [ADOC-V1.0]	As defined in [ADOC-V1.0]

ADOC-V2.0 electronic documents [ADOC-V2.0]	Every signature may sign every or only part of the content files, signed metadata files or their parts, or other signatures (using counter signature) presented within electronic document container as defined in [ADOC-V2.0]	As defined in [ADOC-V2.0]
EGAS-V1.0 electronic document [EGAS-V1.0]	Every signature may sign every or only part of the content files, signed metadata files or their parts, or other signatures (using counter signature) presented within electronic document container as defined in [EGAS-V1.0]	As defined in [EGAS-V1.0]
MDOC-V1.0 electronic document [MDOC-V1.0]	Every signature may sign every or only part of the content files, signed metadata files or their parts, or other signatures (using counter signature) presented within electronic document container as defined in [MDOC-V1.0]	As defined in [MDOC-V1.0]
PDF-LT-V1.0 electronic document [PDF-LT-V1.0]	Every signature shall sign whole PDF file	PDF/A-2 file satisfying requirements in [PDF-LT-V1.0]
PDF-RC-V1.0 electronic document [PDF-RC-V1.0]	Every signature shall sign whole PDF file	PDF/A-3 file satisfying requirements in [PDF-RC-V1.0]
ASiC-E container according to ETSI TS 103 174 [TS 103 174]	Every signature may sign every or only part of the files, or other signatures (using counter signature) presented within ASiC container	Any format aligned with MIME type defined within ASiC container
ASiC-E container according to ETSI EN 319 162-1 [EN 319 162-1]	Every signature may sign every or only part of the files, or other signatures (using counter signature) presented within ASiC container	Any format aligned with MIME type defined within ASiC container
ASiC-S container according to ETSI TS 103 174 [TS 103 174]	Every signature shall sign the only content file presented within ASiC-S container together or without other signatures (using counter signature)	Any format aligned with MIME type defined within ASiC container
ASiC-S container according to ETSI EN 319 162-1 [EN 319 162-1]	Every signature shall sign the only content file presented within ASiC-S container together or without other signatures (using counter signature)	Any format aligned with MIME type defined within ASiC container
PDF with PAdES signature according ETSI TS 103 172 [TS 103 172]	Every signature shall sign whole PDF file	PDF file, including PDF/A-1, PDF/A-2, PDF/A-3

PDF with PAdES signature according ETSI EN 319 142-1 [EN 319 142-1]	Every signature shall sign whole PDF file	PDF file, including PDF/A-1, PDF/A-2, PDF/A-3
PDF document with CMS signatures	Every signature shall sign whole PDF file	PDF file, including PDF/A-1, PDF/A-2, PDF/A-3

The mime types of the signed data files shall be indicated in the electronic documents conformant to ADOC-V1.0, ADOC-V2.0, EGAS-V1.0, MDOC-V1.0 specifications or in the ASiC-S, ASiC-E containers.

3.1.3. BSP (c): The relationship between signed data and signature(s)

Signed data referencing mechanisms are defined in ASiC, XMLDSIG and PAdES standards and further detailed in the corresponding electronic document specifications. The relationship between the signed data and the signatures, and supported signature levels and formats are listed in the Table 6.

Table 6. Relationship between signed data and signatures; supported signature levels

Electronic document, or container specification	Signature format	Signature and its signed data	Signature formats or levels
ADOC-V1.0 electronic documents [ADOC-V1.0]	Detached XAdES signatures conformant to XAdES standard [TS 101 903]	One or more content or metadata files, or metadata file parts presented within electronic document container	XAdES-EPES, XAdES-T, XAdES-C, XAdES-X-L, XAdES-A formats
ADOC-V2.0 electronic documents [ADOC-V2.0]	Detached XAdES signatures conformant to XAdES baseline profile standard [TS 103 171]	One or more content or metadata files, or metadata file parts presented within electronic document container	B-B, B-T, B-LT, B-LTA levels
EGAS-V1.0 electronic document [EGAS-V1.0]	Detached XAdES signatures conformant to XAdES standard [TS 101 903]	One or more content or metadata files, or metadata file parts presented within electronic document container	XAdES-EPES, XAdES-T, XAdES-C, XAdES-X-L, XAdES-A formats
MDOC-V1.0 electronic document [MDOC-V1.0]	Detached XAdES signatures conformant to XAdES standard [TS 101 903]	One or more content or metadata files, or metadata file parts presented within electronic document container	XAdES-EPES, XAdES-T, XAdES-C, XAdES-X-L, XAdES-A formats

PDF-LT-V1.0 electronic document [PDF-LT-V1.0]	Enveloped PAdES signatures conformant to PAdES baseline profile standard [TS 103 172]	One whole PDF file	B-B, B-T, B-LT, B-LTA levels
PDF-RC-V1.0 electronic document [PDF-RC-V1.0]	Enveloped PAdES signatures conformant to Building blocks and PAdES baseline signatures standard [EN 319 142-1]	One whole PDF file	B-B, B-T, B-LT, B-LTA levels
ASiC-E container according to ETSI TS 103 174 [TS 103 174]	Detached XAdES signatures conformant to XAdES baseline profile standard [TS 103 171]	One or more files presented within ASiC container	B-B, B-T, B-LT, B-LTA levels
ASiC-E container according to ETSI EN 319 162-1 [EN 319 162-1]	Detached XAdES signature conformant to Building blocks and XAdES baseline signatures standard [EN 319 132-1]	One or more files presented within ASiC container	B-B, B-T, B-LT, B-LTA levels
ASiC-S container according to ETSI TS 103 174 [TS 103 174]	Detached XAdES signature conformant to XAdES baseline profile according [TS 103 171], or detached CAdES signature conformant to CAdES baseline profile according [TS 103 173]	One file presented within ASiC container	B-B, B-T, B-LT, B-LTA levels
ASiC-S container according to ETSI EN 319 162-1 [EN 319 162-1]	Detached XAdES signature conformant to Building blocks and XAdES baseline signatures standard [EN 319 132-1], or detached CAdES signature conformant to Building blocks and CAdES baseline signatures standard [EN 319 122-1]	One file presented within ASiC container	B-B, B-T, B-LT, B-LTA levels
PDF with PAdES signature according ETSI TS 103 172 [TS 103 172]	Enveloped PAdES signatures conformant to PAdES baseline profile standard [TS 103 172]	One whole PDF file	B-B, B-T, B-LT, B-LTA levels

PDF with PAdES signature according ETSI EN 319 142-1 [EN 319 142-1]	Enveloped PAdES signatures conformant to Building blocks and PAdES baseline signatures standard [EN 319 142-1]	One whole PDF file	B-B, B-T, B-LT, B-LTA levels
PDF document with CMS signatures	Enveloped PAdES signatures conformant to Profile for CMS Signatures in PDF, which is defined in PAdES standards [TS 102 778-2], [TS 102 778-4]	One whole PDF file	PAdES-BASIC, PAdES-LTV

Note: column "Signature formats or levels" defines signatures formats or levels, those are supported by the MitSoft Qualified Long-term Preservation Service for the newly received documents for preservation. MitSoft Qualified Long-term Preservation Service should augment every valid digital signature to be preserved to reach B-LTA level or XAdES-A, PAdES-LTV format accordingly. For the non-baseline XAdES signatures (presented within ADOC-V1.0, EGAS-V1.0, MDOC-V1.0 electronic documents) reaching XAdES-A format ensures the same long-term availability as B-LTA level for baseline signatures. For the non-baseline PAdES signatures (presented within PDF documents with CMS signatures) reaching PAdES-LTV format by adding validation data and necessary document time stamps ensures the same long-term availability as B-LTA level for baseline signatures.

3.1.4. BSP (d): Targeted community

The target community is the MitSoft Qualified Long-term Preservation Service and its subscribers. MitSoft Qualified Long-term Preservation Service is used to preserve validity of the electronic documents and containers provided by the subscribers.

The present signature policy does not define any constraint regards to the creator/signer of the electronic document or container. Electronic document or container may be created and signed by the subscriber itself or by any relying entity.

3.1.5. BSP (e): Allocation of responsibility for signature validation and augmentation

Subscribers of the MitSoft Qualified Long-term Preservation Service are responsible to provide signed electronic documents and containers for the service.

MitSoft Qualified Long-term Preservation Service is responsible to validate digital signatures presented in the provided electronic documents or containers against this signature policy and return validation report.

If provided electronic documents or containers contains digital signature, those do not ensure long term validity due to missing validation data or electronic time stamps, MitSoft Qualified Long-term Preservation Service is responsible to augment such a digital signature to reach B-LTA level for baseline signatures and corresponding signature format for non-baseline signatures.

During whole preservation period, MitSoft Qualified Long-term Preservation Service is also responsible for periodical upgrade of the digital signatures contained in the preserved electronic documents and containers to ensure their validity and protection against possible future weakness of cryptographic algorithms. This covers maintenance of the used cryptographic algorithms and digital signatures augmentation

by timely inclusion of archive time stamps (for XAdES, CAdES signatures) and document time stamps (for PAdES signatures) into preserved digital signatures.

3.2. BSPs mainly influenced by the legal/regulatory provisions

3.2.1. BSP (f): Legal type of the signatures

MitSoft Qualified Long-term Preservation Service ensures preservation only for qualified electronic signatures, qualified electronic seals, advanced electronic signatures and advanced electronic seals according eIDAS Regulation (EU) No 910/2014 [eIDAS]. Therefore, every digital signature augmented or validated using the present signature document should be qualified electronic signature, qualified electronic seal, advanced electronic signature or advanced electronic seal.

Qualified electronic signatures created before eIDAS Regulation entered into force (i.e., 1 July 2016) should meet requirements for the qualified electronic signatures laid down in the European Commission Implementing Decision CID 2013/662/EU [CID 2013/662].

Augmentation and validation processes should use EU List of eIDAS Trusted Lists (LOTL) as the source of the trusted anchors.

3.2.2. BSP (g): Commitment assumed by the signer

MitSoft Qualified Long-term Preservation Service preserves electronic documents and containers compliant to some electronic document specification or European standard. Electronic document specifications define their own requirements for commitment types and signature purpose metadata usage. In the case of validation of digital signature, which is contained in the electronic document conformant to some electronic document specification, requirements for the commitment type and signature purpose metadata shall be used as defined in the corresponding electronic document specification.

In all other cases, commitment types, their meanings and usage are regulated by the business requirements of the MitSoft Qualified Long-term Preservation Service subscribers and are out of the scope of the present signature policy document. Therefore, MitSoft Qualified Long-term Preservation Service validation process applies no constraints on the used commitment types.

Commitments and signature purpose metadata constraints, those are applied during validation process are listed in the Table 7.

Table 7. Commitments and signature purpose metadata constraints to be applied in the validation process

Electronic document, or container specification	Commitment constraints	Signature purpose metadata constraints
ADOC-V1.0 electronic documents [ADOC-V1.0]	As defined in [ADOC-V1.0]	As defined in [ADOC-V1.0]
ADOC-V2.0 electronic documents [ADOC-V2.0]	As defined in [ADOC-V2.0]	As defined in [ADOC-V2.0]
EGAS-V1.0 electronic document [EGAS-V1.0]	As defined in [EGAS-V1.0]	As defined in [EGAS-V1.0]
MDOC-V1.0 electronic document [MDOC-V1.0]	As defined in [MDOC-V1.0]	As defined in [MDOC-V1.0]
PDF-LT-V1.0 electronic document [PDF-LT-V1.0]	As defined in [PDF-LT-V1.0]	As defined in [PDF-LT-V1.0]

PDF-RC-V1.0 electronic document [PDF-RC-V1.0]	As defined in [PDF-RC-V1.0]	As defined in [PDF-RC-V1.0]
ASiC-E container according to ETSI TS 103 174 [TS 103 174]	No constraints	Not applicable
ASiC-E container according to ETSI EN 319 162-1 [EN 319 162-1]	No constraints	Not applicable
ASiC-S container according to ETSI TS 103 174 [TS 103 174]	No constraints	Not applicable
ASiC-S container according to ETSI EN 319 162-1 [EN 319 162-1]	No constraints	Not applicable
PDF with PAdES signature according ETSI TS 103 172 [TS 103 172]	No constraints	Not applicable
PDF with PAdES signature according ETSI EN 319 142-1 [EN 319 142-1]	No constraints	Not applicable
PDF document with CMS signatures	No constraints	Not applicable

3.2.3. BSP (h): Level of assurance on timing evidences

Electronic time stamps are used for augmentation and validation of the preserved electronic signatures or electronic seals. Only electronic time stamps are used as timing evidences. Time marks, evidence records or other types of timing evidences shall not be used.

Every used electronic time stamp shall be qualified electronic time stamp issued by the qualified trust service provider.

Electronic time stamps shall be aligned with the following standards:

- RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) [RFC 3161].
- RFC 5816 (2010) 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].

Electronic document specifications define their own requirements for used electronic time stamp attributes. In the case of augmentation or preservation of digital signature, which is contained in the electronic document conformant to some electronic document specification, requirements for electronic time stamp attributes shall be used as defined in the corresponding electronic document specification.

In all other cases, only time stamp attributes permitted by the corresponding signature, baseline signature or baseline container standards shall be used.

Permitted time stamp attributes to be used during signature augmentation and preservation are listed in the Table 8.

Table 8. Time stamp attributes to be used for augmentation and preservation

Electronic document, or container specification	Permitted time stamp types for augmentation	Permitted time stamp types for preservation
ADOC-V1.0 electronic documents [ADOC-V1.0]	As defined in [ADOC-V1.0]	As defined in [ADOC-V1.0]
ADOC-V2.0 electronic documents [ADOC-V2.0]	As defined in [ADOC-V2.0]	As defined in [ADOC-V2.0]
EGAS-V1.0 electronic document [EGAS-V1.0]	As defined in [EGAS-V1.0]	As defined in [EGAS-V1.0]

MDOC-V1.0 electronic document [MDOC-V1.0]	As defined in [MDOC-V1.0]	As defined in [MDOC-V1.0]
PDF-LT-V1.0 electronic document [PDF-LT-V1.0]	As defined in [PDF-LT-V1.0]	As defined in [PDF-LT-V1.0]
PDF-RC-V1.0 electronic document [PDF-RC-V1.0]	As defined in [PDF-RC-V1.0]	As defined in [PDF-RC-V1.0]
ASiC-E container according to ETSI TS 103 174 [TS 103 174]	XAdES SignatureTimeStamp and ArchiveTimeStamp	XAdES ArchiveTimeStamp
ASiC-E container according to ETSI EN 319 162-1 [EN 319 162-1]	XAdES SignatureTimeStamp and ArchiveTimeStamp	XAdES ArchiveTimeStamp
ASiC-S container according to ETSI TS 103 174 [TS 103 174]	XAdES SignatureTimeStamp and ArchiveTimeStamp, or CAdES SignatureTimeStamp and ArchiveTimeStampV3	XAdES ArchiveTimeStamp, or CAdES ArchiveTimeStampV3
ASiC-S container according to ETSI EN 319 162-1 [EN 319 162-1]	XAdES SignatureTimeStamp and ArchiveTimeStamp, or CAdES SignatureTimeStamp and ArchiveTimeStampV3	XAdES ArchiveTimeStamp, or CAdES ArchiveTimeStampV3
PDF with PAdES signature according ETSI TS 103 172 [TS 103 172]	PAdES DocumentTimeStamp	PAdES DocumentTimeStamp
PDF with PAdES signature according ETSI EN 319 142-1 [EN 319 142-1]	PAdES DocumentTimeStamp	PAdES DocumentTimeStamp
PDF document with CMS signatures	PAdES DocumentTimeStamp	PAdES DocumentTimeStamp

3.2.4. BSP (i): Formalities of signing

Not applicable.

3.2.5. BSP (j): Longevity and resilience to change

The present signature policy is applied for the augmentation and validation of the digital signatures, those should be preserved for a very long time. The very long-term longevity is ensured by augmenting digital signatures to reach B-LTA level (or corresponding archival signature format for non-baseline signatures) and periodical signature upgrade – new archive time stamps (or DocumentTimeStamps for PAdES signatures) inclusion.

3.2.6. BSP (k): Archival

Electronic document or container archiving by writing them into read-only storages are not applied. Periodical signatures upgrade is used to ensure digital signature preservation over the whole preservation period.

The exact period of preservation should be defined in the Subscriber agreements between MitSoft Qualified Long-term Preservation Service provider and its subscribers. By default, preservation period is unlimited.

3.3. BSPs mainly related to the actors involved in creating/augmenting/validating signatures

3.3.1. BSP (l): Identity (and roles/attributes) of the signers

In all the cases, signer is identified according signer's certificate, which shall be included into the signature. Signer type may be only one of the following:

- Natural person,
- Natural person, which represents some legal person, or
- Legal person.

Electronic document specifications define their own requirements for allowed signer types (i.e., natural person, legal person, or legal person representative) and required signer identity data (signer roles, attributes or specific signer metadata). In the case of validation of the digital signature, which is contained in the electronic document conformant to some electronic document specification, requirements for signer types and signer identity data shall be used as defined in the corresponding electronic document specification.

In all other cases, no requirements for the signer identity data are applied. Therefore, any signer type (listed above in this section) is permitted, and no constraints are applied for the signer roles or attributes.

Constraints for the signer types and signer identity data are listed in the Table 9.

Table 9. Constraints for the signer types and signer identity data

Electronic document, or container specification	Constraints for the signer types	Constraints for signer identity data
ADOC-V1.0 electronic documents [ADOC-V1.0]	As defined in [ADOC-V1.0]	As defined in [ADOC-V1.0]
ADOC-V2.0 electronic documents [ADOC-V2.0]	As defined in [ADOC-V2.0]	As defined in [ADOC-V2.0]
EGAS-V1.0 electronic document [EGAS-V1.0]	As defined in [EGAS-V1.0]	As defined in [EGAS-V1.0]
MDOC-V1.0 electronic document [MDOC-V1.0]	As defined in [MDOC-V1.0]	As defined in [MDOC-V1.0]
PDF-LT-V1.0 electronic document [PDF-LT-V1.0]	As defined in [PDF-LT-V1.0]	As defined in [PDF-LT-V1.0]
PDF-RC-V1.0 electronic document [PDF-RC-V1.0]	As defined in [PDF-RC-V1.0]	As defined in [PDF-RC-V1.0]
ASiC-E container according to ETSI TS 103 174 [TS 103 174]	As listed above in this section	No constraints
ASiC-E container according to ETSI EN 319 162-1 [EN 319 162-1]	As listed above in this section	No constraints
ASiC-S container according to ETSI TS 103 174 [TS 103 174]	As listed above in this section	No constraints
ASiC-S container according to ETSI EN 319 162-1 [EN 319 162-1]	As listed above in this section	No constraints
PDF with PAdES signature according ETSI TS 103 172 [TS 103 172]	As listed above in this section	No constraints

PDF with PAdES signature according ETSI EN 319 142-1 [EN 319 142-1]	As listed above in this section	No constraints
PDF document with CMS signatures	As listed above in this section	No constraints

3.3.2. BSP (m): Level of assurance required for the authentication of the signer

In all the cases, signer certificate shall be a certificate for electronic signature or certificate for electronic seal, issued by the qualified trust service provider according Regulation (EU) No 910/2014 [eIDAS].

3.3.3. BSP (n): Signature creation devices

In the case of qualified electronic signature or qualified electronic seal, signer shall use qualified signature creation device according Regulation (EU) No 910/2014 [eIDAS].

If signature or seal is created after eIDAS Regulation entered into force (i.e., 1 July 2016), signer certificate (for qualified electronic signature or qualified electronic seal) shall contain an extension claiming QSCD usage as it is defined in the standard ETSI EN 319 412-5 "Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements" [EN 319 412-5].

3.4. Other BSPs

3.4.1. BSP (o): Other information to be associated with the signature

Electronic document specifications ADOC-V1.0 [ADOC-V1.0], ADOC-V2.0 [ADOC-V2.0], EGAS-V1.0 [EGAS-V1.0], MDOC-V1.0 [MDOC-V1.0] requires, that electronic signatures or electronic seals to be created according some signature policy. Therefore, explicit or implicit signature policy attribute shall be used in electronic signatures or electronic seals presented within the electronic documents conformant to these specifications.

No other constraints defined for other electronic document specifications and containers.

3.4.2. BSP (p): Cryptographic suites

Cryptographic suites are bases on the recommendations listed in the standard 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].

MitSoft Qualified Long-term Preservation Service may ensure reliable preservation of the electronic signatures and electronic seals only if they are verifiable at the time of submission. It also includes cryptographic algorithm reliability. Therefore, cryptographic algorithms used in the electronic signatures or electronic seals shall be reliable at least at a time of submission to preservation service. Preservation service takes all needed actions to protect preserved signatures from the possible obsolescence of the used cryptographic algorithms. This is achieved by augmenting digital signature to reach B-LTA level (or corresponding signature format for non-baseline signatures) and further timely inclusion of new archive time stamps (or DocumentTimeStamps for PAdES signatures).

Requirements for the cryptographic algorithms used in the submitted electronic signatures or electronic seals at a time of the submission to preservation service are described in the Section 3.4.2.1.

Requirements for the cryptographic algorithms used by the preservation service during electronic signatures or electronic seals augmentation at a time of augmentation are described in the Section 3.4.2.2. Cryptographic algorithms requirements for the preservation are the same as for augmentation, since preservation is obtained by the means of augmentation.

Electronic document specifications define additional constraints for allowed cryptographic algorithms. In the case of validation or augmentation of the digital signature, which is contained in the electronic document conformant to some electronic document specification, additional requirements defined in the electronic document specification shall also be applied.

3.4.2.1 Requirements for the Cryptographic algorithms used in the submitted signatures

This section describes requirements for the cryptographic algorithms, those are used in the electronic signatures or electronic seals submitted to MitSoft Qualified Long-term Preservation Service for further preservation.

Cryptographic algorithms (their parameters and key sizes) shall satisfy one of the listed requirements:

- Cryptographic algorithms (their parameters and key sizes) should be listed as recommended or legacy in [TS 119 312] and in [ENISA] at a time of validation performed during submission, or
- There shall be a proof of existence (i.e., electronic time stamp) inside electronic signature or electronic seal, which proves, what algorithm was applied to the data, and affected data itself were existed at a time the algorithm was still reliable.

3.4.2.2 Requirements for the Cryptographic algorithms used for augmentation

This section describes requirements for the cryptographic algorithms, those are used during electronic signatures and electronic seals augmentation (and preservation).

In the case, signature validation data (certificates, OCSP, CRL) is included during augmentation, algorithms (their parameters and key sizes) used for validation data generation should be listed as recommended or legacy in [TS 119 312] and [ENISA] at a time of augmentation.

Augmentation process is based on new electronic time stamps creation and inclusion into the digital signatures. These electronic time stamps should ensure digital signatures verifiability till the next augmentation event. Therefore, used cryptographic algorithms should be expected to be reliable till the next augmentation event. The requirements for the hash functions and algorithms used for electronic time stamp generation are as follows:

- For electronic time stamp digest calculation, augmentation process shall use hash functions, those expected resistance period according to ETSI TS 119 312 "Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites" [TS 119 312] is 3 years or more at a time of augmentation and those are recommended by [ENISA].
- The expected resistance period according to ETSI TS 119 312 "Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites" [TS 119 312] of the cryptographic algorithms (their parameters and key

sizes) used in newly created electronic time stamps should be 3 years or more at a time of augmentation and should be recommended by [ENISA].

3.4.3. BSP (q): Technological environment

Not applicable.

4. Requirements / statements on technical mechanisms and standards implementation

4.1. Technical counterparts of BSPs - Statement summary

4.1.1. Statement summary for ADOC-V1.0 electronic documents

Statement summary for ADOC-V1.0 [ADOC-V1.0] electronic documents are presented in the Table 10.

Table 10. Statement summary for ADOC-V1.0 electronic documents

Name and identifier of the signature policy authority: joint stock company "MIT-SOFT", registration number 120792080 **Name and identifier of the signature policy:** MitSoft Qualified Long-term Preservation Service signature policy, OID 1.3.6.1.4.1.57890.1.6.1.1 **Identifier of the concerned signature(s) in the concerned signature workflow**: qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals contained in the ADOC-V1.0 electronic document			
BSP	**BSP title**	**Business statement summary**	**Technical statement counterpart**
(a)	Workflow (sequencing & timing) of signatures	Countersignatures are allowed only if they are detached counter signatures.	XAdES CounterSignature attribute is forbidden.
(b)	Data to be signed (DTBS)	One or more files of the formats allowed by appropriate electronic document specifications and parts of the XML metadata files.	Specified in ADOC-1.0.
(c)	Relationship between DTBS & signature(s)	Detached XAdES signatures associated within electronic document.	Specified in ADOC-1.0.
(d)	Targeted community	MitSoft Qualified Long-term Preservation Service and its subscribers.	-
(e)	Allocation of responsibility for signature validation and augmentation	Preservation client is responsible to provide signed electronic document or container. Preservation Service is responsible to validate and augment digital signatures to reach B-LTA level.	-
(f)	Legal type of signature	Qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals.	-

(g)	Commitment assumed by the signer	Commitment type is optional, if used, only commitment type values defined in ADOC-V1.0 are allowed. Signature purpose is required in the metadata. Allowed signature purposes are defined in ADOC-1.0.	Specified in ADOC-1.0.
(h)	Level of assurance on timing evidences	Only qualified electronic time stamps shall be used.	[RFC 3161], [RFC 5816], [EN 319 422]
(i)	Formalities of signing	Not applicable.	-
(j)	Longevity & resilience to change	Very long term.	XAdES-A format should be reached.
(k)	Archival	Ensures digital signatures verifiability for the whole preservation period.	Digital signature augmentation by incorporating archive time stamps.
(l)	Identity of signers	Signer shall be natural person, natural person, which represents some legal person, or legal person. Constraints for the signer role attributes as defined in the electronic document specification.	Specified in ADOC-1.0.
(m)	Level of assurance required for the authentication of the signer	Electronic signature or electronic seal certificate, issued by the qualified trust service provider.	-
(n)	Signature creation devices	QSCD shall be used for qualified electronic signature or qualified electronic seal.	Signer certificate shall contain QCStatement `esi4-qcStatement-4` ([EN 319 412-5]).
(o)	Other information to be associated with the signature	Explicit or implicit signature policy attribute shall be used.	XAdES SignaturePolicy-Identifier attribute is required.
(p)	Cryptographic suites	According [TS 119 312] and [ENISA], and suppressed by electronic document specification.	ETSI TS 119 312, [ENISA] and ADOC-V1.0.
(q)	Technological environment	Not applicable.	-
Signature creation/validation application practices statements		MitSoft Qualified Long-term Preservation Service Practice Statement, OID: 1.3.6.1.4.1.57890.1.4.1.	[MitSoft PS]
Summary: Electronic signature/seal shall be detached XAdES signature according ETSI TS 101 903 within electronic document ADOC-V1.0 package; signed data – files (formats are listed in the electronic document specification) or parts of the XML metadata files presented within the same package; expected signature level is B-LTA (other levels are also allowed).			

4.1.2. Statement summary for ADOC-V2.0 electronic documents

Statement summary for ADOC-V2.0 [ADOC-V2.0] electronic documents are presented in the Table 11.

Table 11. Statement summary for ADOC-V2.0 electronic documents

Name and identifier of the signature policy authority: joint stock company "MIT-SOFT", registration number 120792080 **Name and identifier of the signature policy:** MitSoft Qualified Long-term Preservation Service signature policy, OID 1.3.6.1.4.1.57890.1.6.1.1 **Identifier of the concerned signature(s) in the concerned signature workflow**: qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals contained in the ADOC-V2.0 electronic document			
BSP	**BSP title**	**Business statement summary**	**Technical statement counterpart**
(a)	Workflow (sequencing & timing) of signatures	Declared signing time attribute shall be included. Countersignatures are allowed only if they are detached counter signatures.	XAdES SigningTime attribute is required, CounterSignature attribute is forbidden.
(b)	Data to be signed (DTBS)	One or more files of the formats allowed by appropriate electronic document specifications and parts of the XML metadata files. The mime type of the signed data files shall be indicated in the signature.	Specified in ADOC-2.0.
(c)	Relationship between DTBS & signature(s)	Detached XAdES baseline signatures associated within electronic document.	Specified in ADOC-2.0.
(d)	Targeted community	MitSoft Qualified Long-term Preservation Service and its subscribers	-
(e)	Allocation of responsibility for signature validation and augmentation	Preservation client is responsible to provide signed electronic document or container. Preservation Service is responsible to validate and augment digital signatures to reach LTA level.	-
(f)	Legal type of signature	Qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals.	-
(g)	Commitment assumed by the signer	Commitment type is required. Allowed commitment type values are defined in ADOC-V2.0.	Specified in ADOC-2.0.
(h)	Level of assurance on timing evidences	Only qualified electronic time stamps shall be used.	[RFC 3161], [RFC 5816], [EN 319 422]
(i)	Formalities of signing	Not applicable.	-

(j)	Longevity & resilience to change	Very long term.	B-LTA level should be reached.
(k)	Archival	Ensures digital signatures verifiability for the whole preservation period.	Digital signature augmentation by incorporating archive time stamps.
(l)	Identity of signers	Signer shall be natural person, natural person, which represents some legal person, or legal person. Constraints for the signer role attributes as defined in the electronic document specification.	Specified in ADOC-2.0.
(m)	Level of assurance required for the authentication of the signer	Electronic signature or electronic seal certificate, issued by the qualified trust service provider.	-
(n)	Signature creation devices	QSCD shall be used for qualified electronic signature or qualified electronic seal.	Signer certificate shall contain QCStatement `esi4-qcStatement-4` ([EN 319 412-5]).
(o)	Other information to be associated with the signature	Explicit or implicit signature policy attribute shall be used.	XAdES SignaturePolicy-Identifier attribute is required.
(p)	Cryptographic suites	According [TS 119 312] and [ENISA], and suppressed by electronic document specification.	ETSI TS 119 312, [ENISA] and ADOC-V2.0.
(q)	Technological environment	Not applicable.	-
Signature creation/validation application practices statements		MitSoft Qualified Long-term Preservation Service Practice Statement, OID: 1.3.6.1.4.1.57890.1.4.1.	[MitSoft PS]
Summary: Electronic signature/seal shall be detached XAdES baseline signature according ETSI TS 103 171 within electronic document ADOC-V2.0 package; signed data – files (formats are listed in the electronic document specification) or parts of the XML metadata files presented within the same package; expected signature level is B-LTA (other levels are also allowed).			

4.1.3. Statement summary for EGAS-V1.0 electronic documents

Statement summary for EGAS-V1.0 [EGAS-V1.0] electronic documents are presented in the Table 12.

Table 12. Statement summary for EGAS-V1.0 electronic documents

Name and identifier of the signature policy authority: joint stock company "MIT-SOFT", registration number 120792080 **Name and identifier of the signature policy:** MitSoft Qualified Long-term Preservation Service signature policy, OID 1.3.6.1.4.1.57890.1.6.1.1 **Identifier of the concerned signature(s) in the concerned signature workflow**: qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals contained in the EGAS-V1.0 electronic document			
BSP	**BSP title**	**Business statement summary**	**Technical statement counterpart**
(a)	Workflow (sequencing & timing) of signatures	Countersignatures are allowed only if they are detached counter signatures.	XAdES CounterSignature attribute is forbidden.
(b)	Data to be signed (DTBS)	One or more files of the formats allowed by appropriate electronic document specifications and parts of the XML metadata files.	Specified in EGAS-1.0.
(c)	Relationship between DTBS & signature(s)	Detached XAdES signatures associated within electronic document.	Specified in EGAS-1.0.
(d)	Targeted community	MitSoft Qualified Long-term Preservation Service and its subscribers	-
(e)	Allocation of responsibility for signature validation and augmentation	Preservation client is responsible to provide signed electronic document or container. Preservation Service is responsible to validate and augment digital signatures to reach LTA level.	-
(f)	Legal type of signature	Qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals.	-
(g)	Commitment assumed by the signer	Commitment type is optional, if used, only commitment type values defined in EGAS-1.0 are allowed. Signature purpose is required in the metadata. Allowed signature purposes are defined in EGAS-1.0.	Specified in EGAS-1.0.
(h)	Level of assurance on timing evidences	Only qualified electronic time stamps shall be used.	[RFC 3161], [RFC 5816], [EN 319 422]
(i)	Formalities of signing	Not applicable.	-

(j)	Longevity & resilience to change	Very long term.	XAdES-A format should be reached.
(k)	Archival	Ensures digital signatures verifiability for the whole preservation period.	Digital signature augmentation by incorporating archive time stamps.
(l)	Identity of signers	Signer shall be natural person, natural person, which represents some legal person, or legal person. Constraints for the signer role attributes as defined in the electronic document specification.	Specified in EGAS-1.0.
(m)	Level of assurance required for the authentication of the signer	Electronic signature or electronic seal certificate, issued by the qualified trust service provider.	-
(n)	Signature creation devices	QSCD shall be used for qualified electronic signature or qualified electronic seal.	Signer certificate shall contain QCStatement `esi4-qcStatement-4` ([EN 319 412-5]).
(o)	Other information to be associated with the signature	Explicit or implicit signature policy attribute shall be used.	XAdES SignaturePolicy-Identifier attribute is required.
(p)	Cryptographic suites	According [TS 119 312] and [ENISA], and suppressed by electronic document specification.	ETSI TS 119 312, [ENISA] and EGAS-V1.0.
(q)	Technological environment	Not applicable.	-
Signature creation/validation application practices statements		MitSoft Qualified Long-term Preservation Service Practice Statement, OID: 1.3.6.1.4.1.57890.1.4.1.	[MitSoft PS]
Summary: Electronic signature/seal shall be detached XAdES signature according ETSI TS 101 903 within electronic document EGAS-V1.0 package; signed data – files (formats are listed in the electronic document specification) or parts of the XML metadata files presented within the same package; expected signature level is B-LTA (other levels are also allowed).			

4.1.4. Statement summary for MDOC-V1.0 electronic documents

Statement summary for MDOC-V1.0 [MDOC-V1.0] electronic documents are presented in the Table 13.

Table 13. Statement summary for MDOC-V1.0 electronic documents

Name and identifier of the signature policy authority: joint stock company "MIT-SOFT", registration number 120792080 **Name and identifier of the signature policy:** MitSoft Qualified Long-term Preservation Service signature policy, OID 1.3.6.1.4.1.57890.1.6.1.1 **Identifier of the concerned signature(s) in the concerned signature workflow**: qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals contained in the MDOC-V1.0 electronic document			
BSP	**BSP title**	**Business statement summary**	**Technical statement counterpart**
(a)	Workflow (sequencing & timing) of signatures	Countersignatures are allowed only if they are detached counter signatures.	XAdES CounterSignature attribute is forbidden.
(b)	Data to be signed (DTBS)	One or more files of the formats allowed by appropriate electronic document specifications and parts of the XML metadata files.	Specified in MDOC-1.0.
(c)	Relationship between DTBS & signature(s)	Detached XAdES signatures associated within electronic document.	Specified in MDOC-1.0.
(d)	Targeted community	MitSoft Qualified Long-term Preservation Service and its subscribers	-
(e)	Allocation of responsibility for signature validation and augmentation	Preservation client is responsible to provide signed electronic document or container. Preservation Service is responsible to validate and augment digital signatures to reach LTA level.	-
(f)	Legal type of signature	Qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals.	-
(g)	Commitment assumed by the signer	Commitment type is optional, if used, only commitment type values defined in MDOC-V1.0 are allowed. Signature purpose is required in the metadata. Allowed signature purposes are defined in MDOC-V1.0.	Specified in MDOC-1.0.
(h)	Level of assurance on timing evidences	Only qualified electronic time stamps shall be used.	[RFC 3161], [RFC 5816], [EN 319 422]
(i)	Formalities of signing	Not applicable.	-

(j)	Longevity & resilience to change	Very long term.	XAdES-A format should be reached.
(k)	Archival	Ensures digital signatures verifiability for the whole preservation period.	Digital signature augmentation by incorporating archive time stamps.
(l)	Identity of signers	Signer shall be natural person, natural person, which represents some legal person, or legal person. Constraints for the signer role attributes as defined in the electronic document specification	Specified in MDOC-1.0.
(m)	Level of assurance required for the authentication of the signer	Electronic signature or electronic seal certificate, issued by the qualified trust service provider	-
(n)	Signature creation devices	QSCD shall be used for qualified electronic signature or qualified electronic seal.	Signer certificate shall contain QCStatement `esi4-qcStatement-4` ([EN 319 412-5]).
(o)	Other information to be associated with the signature	Explicit or implicit signature policy attribute shall be used.	XAdES SignaturePolicy-Identifier attribute is required.
(p)	Cryptographic suites	According [TS 119 312] and [ENISA], and suppressed by electronic document specification.	ETSI TS 119 312, [ENISA] and MDOC-V1.0.
(q)	Technological environment	Not applicable.	-
Signature creation/validation application practices statements		MitSoft Qualified Long-term Preservation Service Practice Statement, OID: 1.3.6.1.4.1.57890.1.4.1.	[MitSoft PS]
Summary: Electronic signature/seal shall be detached XAdES signature according ETSI TS 101 903 within electronic document MDOC-V1.0 package; signed data – files (formats are listed in the electronic document specification) or parts of the XML metadata files presented within the same package; expected signature level is B-LTA (other levels are also allowed).			

4.1.5. Statement summary for PDF-LT-V1.0 electronic documents

Statement summary for PDF-LT-V1.0 [PDF-LT-V1.0] electronic documents are presented in the Table 14.

Table 14. Statement summary for PDF-LT-V1.0 electronic documents

Name and identifier of the signature policy authority: joint stock company "MIT-SOFT", registration number 120792080 **Name and identifier of the signature policy:** MitSoft Qualified Long-term Preservation Service signature policy, OID 1.3.6.1.4.1.57890.1.6.1.1 **Identifier of the concerned signature(s) in the concerned signature workflow**: qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals contained in the PDF-LT-V1.0 electronic document			
BSP	**BSP title**	**Business statement summary**	**Technical statement counterpart**
(a)	Workflow (sequencing & timing) of signatures	Declared signing time attribute shall be included.	PAdES signature field M is required.
(b)	Data to be signed (DTBS)	Whole PDF/A-2 file.	Specified in PDF-LT-V1.0.
(c)	Relationship between DTBS & signature(s)	Enveloped PAdES baseline signatures.	Specified in PDF-LT-V1.0.
(d)	Targeted community	MitSoft Qualified Long-term Preservation Service and its subscribers	-
(e)	Allocation of responsibility for signature validation and augmentation	Preservation client is responsible to provide signed electronic document or container. Preservation Service is responsible to validate and augment digital signatures to reach LTA level.	-
(f)	Legal type of signature	Qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals.	-
(g)	Commitment assumed by the signer	Commitment type is optional. Values for PDF signature dictionary field Reason are defined in PDF-LT-V1.0.	Specified in PDF-LT-V1.0.
(h)	Level of assurance on timing evidences	Only qualified electronic time stamps shall be used.	[RFC 3161], [RFC 5816], [EN 319 422]
(i)	Formalities of signing	Not applicable.	-
(j)	Longevity & resilience to change	Very long term.	B-LTA level should be reached.
(k)	Archival	Ensures digital signatures verifiability for the whole preservation period.	Digital signature augmentation by incorporating PAdES document time stamps.

(l)	Identity of signers	Signer shall be natural person, natural person, which represents some legal person, or legal person. Constraints for the signer role attributes as defined in the electronic document specification.	Specified in PDF-LT-V1.0.
(m)	Level of assurance required for the authentication of the signer	Electronic signature or electronic seal certificate, issued by the qualified trust service provider.	-
(n)	Signature creation devices	QSCD shall be used for qualified electronic signature or qualified electronic seal.	Signer certificate shall contain QCStatement `esi4-qcStatement-4` ([EN 319 412-5]).
(o)	Other information to be associated with the signature	Not applicable.	-
(p)	Cryptographic suites	According [TS 119 312] and [ENISA], and suppressed by electronic document specification.	ETSI TS 119 312, [ENISA] and PDF-LTC-V1.0.
(q)	Technological environment	Not applicable.	-
Signature creation/validation application practices statements		MitSoft Qualified Long-term Preservation Service Practice Statement, OID: 1.3.6.1.4.1.57890.1.4.1.	[MitSoft PS]
Summary: Electronic signature/seal shall be enveloped PAdES baseline signature according ETSI TS 103 172 [TS 103 172] within PDF/A-2 document and conformant to electronic document specification PDF-LT-V1.0; signed data – whole PDF file; expected signature level is B-LTA (other levels are also allowed).			

4.1.6. Statement summary for PDF-RC-V1.0 electronic documents

Statement summary for PDF-RC-V1.0 [PDF-RC-V1.0] electronic documents are presented in the Table 15.

Table 15. Statement summary for PDF-RC-V1.0 electronic documents

Name and identifier of the signature policy authority: joint stock company "MIT-SOFT", registration number 120792080 **Name and identifier of the signature policy:** MitSoft Qualified Long-term Preservation Service signature policy, OID 1.3.6.1.4.1.57890.1.6.1.1 **Identifier of the concerned signature(s) in the concerned signature workflow**: qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals contained in the PDF-RC-V1.0 electronic document			
BSP	**BSP title**	**Business statement summary**	**Technical statement counterpart**
(a)	Workflow (sequencing & timing) of signatures	Declared signing time attribute shall be included.	PAdES signature field M is required.
(b)	Data to be signed (DTBS)	Whole PDF/A-3 file together with embedded files.	Specified in PDF-RC-V1.0.
(c)	Relationship between DTBS & signature(s)	Enveloped PAdES baseline signatures.	Specified in PDF-RC-V1.0.
(d)	Targeted community	MitSoft Qualified Long-term Preservation Service and its subscribers	-
(e)	Allocation of responsibility for signature validation and augmentation	Preservation client is responsible to provide signed electronic document or container. Preservation Service is responsible to validate and augment digital signatures to reach LTA level.	-
(f)	Legal type of signature	Qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals.	-
(g)	Commitment assumed by the signer	Commitment type is optional and values are restricted by PDF-RC-V1.0. Values for PDF signature dictionary field Reason are defined in PDF-RC-V1.0.	Specified in PDF-RC-V1.0.
(h)	Level of assurance on timing evidences	Only qualified electronic time stamps shall be used.	[RFC 3161], [RFC 5816], [EN 319 422]
(i)	Formalities of signing	Not applicable.	-
(j)	Longevity & resilience to change	Very long term.	B-LTA level should be reached.

(k)	Archival	Ensures digital signatures verifiability for the whole preservation period.	Digital signature augmentation by incorporating PAdES document time stamps.
(l)	Identity of signers	Signer shall be natural person, natural person, which represents some legal person, or legal person. Constraints for the signer role attributes as defined in the electronic document specification	Specified in PDF-RC-V1.0.
(m)	Level of assurance required for the authentication of the signer	Electronic signature or electronic seal certificate, issued by the qualified trust service provider.	-
(n)	Signature creation devices	QSCD shall be used for qualified electronic signature or qualified electronic seal.	Signer certificate shall contain QCStatement `esi4-qcStatement-4` ([EN 319 412-5]).
(o)	Other information to be associated with the signature	Not applicable.	-
(p)	Cryptographic suites	According [TS 119 312] and [ENISA], and suppressed by electronic document specification.	ETSI TS 119 312, [ENISA] and PDF-RC-V1.0.
(q)	Technological environment	Not applicable.	-
Signature creation/validation application practices statements		MitSoft Qualified Long-term Preservation Service Practice Statement, OID: 1.3.6.1.4.1.57890.1.4.1.	[MitSoft PS]
Summary: Electronic signature/seal shall be enveloped PAdES baseline signature according ETSI EN 319 142-1 [EN 319 142-1] within PDF/A-3 document, which is conformant to electronic document specification PDF-RC-V1.0; signed data – whole PDF file (with embedded files); expected signature level is B-LTA (other levels are also allowed).			

4.1.7. Statement summary for ASiC baseline containers

Statement summary for the baseline ASiC-E and ASiC-S containers according ETSI TS 103 174 [TS 103 174] or ETSI EN 319 162-1 [EN 319 162-1] standards are presented in the Table 16.

Table 16. Statement summary for ASiC baseline containers

Name and identifier of the signature policy authority: joint stock company "MIT-SOFT", registration number 120792080 **Name and identifier of the signature policy:** MitSoft Qualified Long-term Preservation Service signature policy, OID 1.3.6.1.4.1.57890.1.6.1.1 **Identifier of the concerned signature(s) in the concerned signature workflow**: qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals contained in the baseline ASiC-E and ASiC-S container			
BSP	**BSP title**	**Business statement summary**	**Technical statement counterpart**
(a)	Workflow (sequencing & timing) of signatures	Declared signing time attribute shall be included.	XAdES or CAdES SigningTime attribute is required.
(b)	Data to be signed (DTBS)	One or more file of the format defined in the ASiC-E container manifest file. One file of the format defined in the ASiC-S container.	Specified in ETSI TS 103 174 or ETSI EN 319 162-1.
(c)	Relationship between DTBS & signature(s)	Detached XAdES or CAdES baseline signature associated within ASiC container.	Specified in ETSI TS 103 174 or ETSI EN 319 162-1.
(d)	Targeted community	MitSoft Qualified Long-term Preservation Service and its subscribers	-
(e)	Allocation of responsibility for signature validation and augmentation	Preservation client is responsible to provide signed electronic document or container. Preservation Service is responsible to validate and augment digital signatures to reach LTA level.	-
(f)	Legal type of signature	Qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals.	-
(g)	Commitment assumed by the signer	No constraints.	-
(h)	Level of assurance on timing evidences	Only qualified electronic time stamps shall be used.	[RFC 3161], [RFC 5816], [EN 319 422]
(i)	Formalities of signing	Not applicable.	-
(j)	Longevity & resilience to change	Very long term.	B-LTA level should be reached.

(k)	Archival	Ensures digital signatures verifiability for the whole preservation period.	Digital signature augmentation by incorporating archive time stamps.
(l)	Identity of signers	Signer shall be natural person, natural person, which represents some legal person, or legal person. No constraints for the signer role attributes.	-
(m)	Level of assurance required for the authentication of the signer	Electronic signature or electronic seal certificate, issued by the qualified trust service provider.	-
(n)	Signature creation devices	QSCD shall be used for qualified electronic signature or qualified electronic seal.	Signer certificate shall contain QCStatement `esi4-qcStatement-4` ([EN 319 412-5]).
(o)	Other information to be associated with the signature	Not applicable.	-
(p)	Cryptographic suites	According [TS 119 312] and [ENISA].	ETSI TS 119 312, [ENISA].
(q)	Technological environment	Not applicable.	-
Signature creation/validation application practices statements		MitSoft Qualified Long-term Preservation Service Practice Statement, OID: 1.3.6.1.4.1.57890.1.4.1.	[MitSoft PS]
Summary: Electronic signature/seal shall be detached XAdES baseline signature according ETSI TS 103 171 [TS 103 171], ETSI EN 319 132-1 [EN 319 132-1], or detached CAdES baseline signature according ETSI TS 103 172 [TS 103 172], ETSI EN 319 122-1 [EN 319 122-1] within ASiC-E or ASiC-S baseline container specified in ETSI TS 103 174 or in ETSI EN 319 162-1; signed data – files presented within the same ASiC container; expected signature level is B-LTA (other levels are also allowed).			

4.1.8. Statement summary for PAdES baseline signatures

Statement summary for PAdES baseline signatures according ETSI TS 103 172 [TS 103 172] or ETSI EN 319 142-1 [EN 319 142-1] are presented in the Table 17.

Table 17. Statement summary for PAdES baseline signatures

Name and identifier of the signature policy authority: joint stock company "MIT-SOFT", registration number 120792080 **Name and identifier of the signature policy:** MitSoft Qualified Long-term Preservation Service signature policy, OID 1.3.6.1.4.1.57890.1.6.1.1 **Identifier of the concerned signature(s) in the concerned signature workflow**: qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals contained in the PDF file			
BSP	**BSP title**	**Business statement summary**	**Technical statement counterpart**
(a)	Workflow (sequencing & timing) of signatures	Declared signing time attribute shall be included.	PAdES signature field M is required.
(b)	Data to be signed (DTBS)	Whole PDF file.	Specified in ETSI TS 103 172 or ETSI EN 319 142-1.
(c)	Relationship between DTBS & signature(s)	Enveloped PAdES baseline signatures.	Specified in ETSI TS 103 172 or ETSI EN 319 142-1.
(d)	Targeted community	MitSoft Qualified Long-term Preservation Service and its subscribers	-
(e)	Allocation of responsibility for signature validation and augmentation	Preservation client is responsible to provide signed electronic document or container. Preservation Service is responsible to validate and augment digital signatures to reach LTA level.	-
(f)	Legal type of signature	Qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals.	-
(g)	Commitment assumed by the signer	No constraints.	-
(h)	Level of assurance on timing evidences	Only qualified electronic time stamps shall be used.	[RFC 3161], [RFC 5816], [EN 319 422]
(i)	Formalities of signing	Not applicable.	-
(j)	Longevity & resilience to change	Very long term.	B-LTA level should be reached.
(k)	Archival	Ensures digital signatures verifiability for the whole preservation period.	Digital signature augmentation by incorporating PAdES document time stamps

(l)	Identity of signers	Signer shall be natural person, natural person, which represents some legal person, or legal person. No constraints for the signer role attributes.	-
(m)	Level of assurance required for the authentication of the signer	Electronic signature or electronic seal certificate, issued by the qualified trust service provider.	-
(n)	Signature creation devices	QSCD shall be used for qualified electronic signature or qualified electronic seal.	Signer certificate shall contain QCStatement `esi4-qcStatement-4` ([EN 319 412-5]).
(o)	Other information to be associated with the signature	Not applicable.	-
(p)	Cryptographic suites	According [TS 119 312] and [ENISA].	ETSI TS 119 312, [ENISA].
(q)	Technological environment	Not applicable.	-
Signature creation/validation application practices statements		MitSoft Qualified Long-term Preservation Service Practice Statement, OID: 1.3.6.1.4.1.57890.1.4.1.	[MitSoft PS]
Summary: Electronic signature/seal shall be enveloped PAdES baseline signature according ETSI TS 103 172 or ETSI EN 319 142-1 within PDF (PDF-1.7, PDF/A-1, PDF/A-2, PDF/A-3) document; signed data – whole PDF file; expected signature level is B-LTA (other levels are also allowed).			

4.1.9. Statement summary for CMS signatures in PDF (PAdES-Basic)

Statement summary for CMS signatures in PDF (PAdES-Basic) according ETSI TS 102 778-2 [TS 102 778-2] and ETSI TS 102 778-4 [TS 102 778-4] are presented in the Table 18.

Table 18. Statement summary for CMS signatures in PDF (PAdES-Basic)

Name and identifier of the signature policy authority: joint stock company "MIT-SOFT", registration number 120792080 **Name and identifier of the signature policy:** MitSoft Qualified Long-term Preservation Service signature policy, OID 1.3.6.1.4.1.57890.1.6.1.1 **Identifier of the concerned signature(s) in the concerned signature workflow**: qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals contained in the PDF file			
BSP	**BSP title**	**Business statement summary**	**Technical statement counterpart**
(a)	Workflow (sequencing & timing) of signatures	Not applicable.	-
(b)	Data to be signed (DTBS)	Whole PDF file.	Specified in ETSI TS 102 778-2.
(c)	Relationship between DTBS & signature(s)	Enveloped PAdES signatures.	Specified in ETSI TS 102 778-2.
(d)	Targeted community	MitSoft Qualified Long-term Preservation Service and its subscribers	-
(e)	Allocation of responsibility for signature validation and augmentation	Preservation client is responsible to provide signed electronic document or container. Preservation Service is responsible to validate and augment digital signatures to reach LTA level.	-
(f)	Legal type of signature	Qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals.	-
(g)	Commitment assumed by the signer	No constraints.	-
(h)	Level of assurance on timing evidences	Only qualified electronic time stamps shall be used.	[RFC 3161], [RFC 5816], [EN 319 422]
(i)	Formalities of signing	Not applicable.	-
(j)	Longevity & resilience to change	Very long term.	PAdES-LTV format (LTA level) should be reached.
(k)	Archival	Ensures digital signatures verifiability for the whole preservation period.	Digital signature augmentation by incorporating PAdES document time stamps

(l)	Identity of signers	Signer shall be natural person, natural person, which represents some legal person, or legal person. No constraints for the signer role attributes.	-
(m)	Level of assurance required for the authentication of the signer	Electronic signature or electronic seal certificate, issued by the qualified trust service provider.	-
(n)	Signature creation devices	QSCD shall be used for qualified electronic signature or qualified electronic seal.	Signer certificate shall contain QCStatement `esi4-qcStatement-4` ([EN 319 412-5]).
(o)	Other information to be associated with the signature	Not applicable.	-
(p)	Cryptographic suites	According [TS 119 312] and [ENISA].	ETSI TS 119 312, [ENISA].
(q)	Technological environment	Not applicable.	-
Signature creation/validation application practices statements		MitSoft Qualified Long-term Preservation Service Practice Statement, OID: 1.3.6.1.4.1.57890.1.4.1.	[MitSoft PS]
Summary: Electronic signature/seal shall be enveloped PAdES signature conformant to Profile for CMS Signatures in PDF defined in the standard ETSI TS 102 778-2 [TS 102 778-2]. Long-term form for this profile is defined in the standard ETSI TS 102 778-4 [TS 102 778-4]. Electronic signature/seal shall reside in PDF (PDF-1.7, PDF/A-1, PDF/A-2, PDF/A-3) document. Signed data – whole PDF file; expected signature level is B-LTA (other levels are also allowed).			

4.2. Input and output constraints for signature creation, augmentation and validation procedures

4.2.1. Input constraints to be used when generating, augmenting and/or validating signatures in the context of the identified signature policy

4.2.1.1 Input constraints for ADOC-V1.0 electronic documents

Input constraints to be used when augmenting or validating electronic signatures/seals presented within ADOC-V1.0 [ADOC-V1.0] electronic documents are presented in the Table 19.

Table 19. Input constraints for ADOC-V1.0 electronic documents

Name and identifier of the signature policy authority: joint stock company "MIT-SOFT", registration number 120792080 **Name and identifier of the signature policy:** MitSoft Qualified Long-term Preservation Service signature policy, OID 1.3.6.1.4.1.57890.1.6.1.1 **Identifier of the concerned signature(s) in the concerned signature workflow**: qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals contained in the ADOC-V1.0 electronic document						
BSP	**BSP title**	**Business statement summary**	**Technical counterpart statement**	**Constraint(s)**	**Constraint value at signature augment-ation (SCA, SVA or DA)**	**Constraint value at signature validation (SVA or DA)**
(a)	Workflow (sequencing & timing)	Counter-signatures are allowed only if they are detached counter signatures.	XAdES CounterSignature attribute is forbidden.	-	SVA	SVA
(b)	DTBS	One or more content files of the formats	Specified in ADOC-1.0.	(b)1. ConstraintOnDTBS: Allowed formats of the signed files are defined in the ADOC-1.0 specification.	SVA	SVA

		allowed by appropriate electronic document specifications and parts of the XML metadata files.		(b)3. DOTBSAsAWholeOrInParts: parts: whole content files and parts of the XML metadata files may be signed as it is defined in the ADOC-1.0 specification.	SVA	SVA
(c)	Relationship between DTBS and Signature	Detached XAdES signatures associated within electronic document.	Specified in ADOC-1.0.	(c)2. ConstraintsOnTheNumberOfDOTBS: 2 ≤ x	SVA	SVA
				(c)3. SignatureRelativePosition: associated	SVA	SVA
				(c)4. MandatedSignatureFormat: XAdES	SVA	SVA
(d)	Targeted community	MitSoft Qualified Long-term Preservation Service and its subscribers.	-	d)1. TargetedCommunityConstraints: MitSoft Qualified Long-term Preservation Service and its subscribers.		
(e)	Allocation of responsibility for validation & augmentation	Preservation client is responsible to provide signed electronic document or container. Preservation Service is responsible to validate and augment digital signatures to reach LTA level.	-	(e)1. ValidationRequiredBeforeAugmenting: True	SVA	-
				(e)2. AugmentToLevel: LTA	SVA	-

(f)	Legal type	Qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals.	-	(f)1. ConstraintsOnCertificateMetadata: (f)1.1. LegalPersonSignerRequired: False (f)1.2. LegalPersonSignerAllowed: True (f)1.3. EUAdESigRequired: True (if it is a signature) (f)1.4. EUAdESealRequired: True (if it is a seal) (f)1.5. EUQSigCDRequired: True (if it is a qualified electronic signature) (f)1.6. EUQSealCDRequired: True (if it is a qualified electronic seal)	SVA	SVA
(g)	Commitment type	Commitment type is optional, if used, only commitment type values defined in ADOC-V1.0 are allowed. Signature purpose is required in the metadata. Allowed signature purposes are defined in ADOC-V1.0.	Specified in ADOC-1.0.	(g)1. CommitmentTypesRequired: (g)1.1. MandatedSignedQProperties-commitment-type-indication: False. (g)1.2. MandatedCommitmentTypeValues: MatchingValuesIndicator: atLeastOne CommitmentTypeValues: Commitment type values defined in Annex B of ETSI TS 119 172-1 [TS 119 172-1]: • http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin, • http://uri.etsi.org/01903/v1.2.2#ProofOfApproval.	SVA	SVA
(h)	LoA on timing evidences	Only qualified electronic time stamps shall be used.	[RFC 3161], [RFC 5816], [EN 319 422]	h)1. LoAOnTimingEvidences: (h)1.3. LoA-on-signature-time-stamp: Qualified electronic time stamps only (h)1.4. LoA-on-archival-time-stamp: Qualified electronic time stamps only.	SVA	SVA
(i)	Formalities of signing	Not applicable.	-	-		
(j)	Longevity & resilience	Very long term.	XAdES-A format should be reached.	(j)1. LoAOnLongevityAndResilience: Very long term	SVA	-

(k)	Archival	Ensures digital signatures verifiability for the whole preservation period.	Digital signature augmentation by incorporating archive time stamps.	(k)1. ArchivalConstraints: Digital signatures verifiability shall be ensured for the whole preservation period	SVA	-
(l)	Identity and role attributes of the signer	Signer shall be natural person, natural person, which represents some legal person, or legal person. Constraints for the signer role attributes as defined in the electronic document specification.	Specified in ADOC-1.0.	(l)1. ConstraintsOnCertificateMetadata-LegalPersonSignerRequired: False	SVA	SVA
				(l)2. ConstraintsOnCertificateMetadata-LegalPersonSignerAllowed: True	SVA	SVA
(m)	LoA on signer authentication	Electronic signature or electronic seal certificate, issued by the qualified trust service provider	-	(m)1. X509CertificateValidationConstraints: (m)1.1. SetOfTrustAnchors: • For certificates issued to signer or to CAs: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml); • For certificates issued to OCSP responders or to CRL issuers: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml) and sets of trusted certificates stored in the environment; • For certificates issued to Time-Stamping Units: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml).	SVA	SVA

				(m)2. RevocationConstraints[1]: (m)2.1. RevocationCheckingConstraints: eitherCheck. (m)2.2. RevocationFreshnessConstraints: The maximum accepted difference between the issuance date of the revocation status information (thisUpdate) of a certificate and the time of validation for the signing certificate is set to 1 minute for validation and 0 minutes for augmentation[2].	SVA	SVA
(n)	Signature Creation Devices	QSCD shall be used for qualified el. signature or qualified el. seal.	Signer certificate shall contain QCStatement esi4-qcStatement-4 ([EN 319 412-5]).	(n)1. LoAOnSCD: QSCD shall be used for signer certificate.	SVA	SVA
(o)	Other information to be associated with signatures	Explicit or implicit signature policy attribute shall be used.	XAdES SignaturePolicy-Identifier attribute is required.	(o)2. MandatedUnsignedQProperties-signature-policy-extension: True.	SVA	SVA
(p)	Cryptographic suites	According [TS 119 312] and [ENISA], and suppressed by electronic document specification.	ETSI TS 119 312, [ENISA] and ADOC-V1.0.	(p)1. CryptographicSuitesConstraints: According ETSI TS 119 312 and [ENISA], and suppressed by electronic document specification.	SVA	SVA
(q)	Technological environment	Not applicable.	-	-		
Summary: Electronic signature/seal shall be detached XAdES signature according ETSI TS 101 903 within electronic document ADOC-V1.0 package; signed data – files (formats are listed in the electronic document specification) or parts of the XML metadata files presented within the same package; expected signature level is B-LTA (other levels are also allowed).						

[1] Constraints are not used if certificate does represent a trust anchor.
[2] New validation data to be inserted into the signature only if it has been issued after the best signature time.

4.2.1.2 Input constraints for ADOC-V2.0 electronic documents

Input constraints to be used when augmenting or validating electronic signatures/seals presented within ADOC-V2.0 [ADOC-V2.0] electronic documents are presented in the Table 20.

Table 20. Input constraints for ADOC-V2.0 electronic documents

Name and identifier of the signature policy authority: joint stock company "MIT-SOFT", registration number 120792080 **Name and identifier of the signature policy:** MitSoft Qualified Long-term Preservation Service signature policy, OID 1.3.6.1.4.1.57890.1.6.1.1 **Identifier of the concerned signature(s) in the concerned signature workflow**: qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals contained in the ADOC-V2.0 electronic document						
BSP	**BSP title**	**Business statement summary**	**Technical counterpart statement**	**Constraint(s)**	**Constraint value at signature augment-ation (SCA, SVA or DA)**	**Constraint value at signature validation (SVA or DA)**
(a)	Workflow (sequencing & timing)	Declared signing time attribute shall be included. Countersignatures are allowed only if they are detached counter signatures.	XAdES SigningTime attribute is required, CounterSignature attribute is forbidden.	(a)3. TimingRelevance: (a)3.2 TimingRelevanceOnEvidence: (a)3.2.1 MandatedSignedQProperties-signing-time	SVA	SVA
(b)	DTBS	One or more content files of the formats	Specified in ADOC-2.0.	(b)1. ConstraintOnDTBS: Allowed formats of the signed files are defined in the ADOC-2.0 specification.	SVA	SVA

		allowed by appropriate electronic document specifications and parts of the XML metadata files.		(b)3. DOTBSAsAWholeOrInParts: parts: whole content files and parts of the XML metadata files may be signed as it is defined in the ADOC-2.0 specification.	SVA	SVA
		The mime type of the signed data files shall be indicated in the signature.	XAdES DataObjectFormat is required.	(b)2. ContentRelatedConstraintsAsPartOfSignatureElements: (b)2.1 MandatedSignedQProperties-DataObjetFormat.	SVA	SVA
(c)	Relationship between DTBS and Signature	Detached XAdES baseline signatures associated within electronic document.	Specified in ADOC-2.0.	(c)2. ConstraintsOnTheNumberOfDOTBS: 1 ≤ x	SVA	SVA
				(c)3. SignatureRelativePosition: associated	SVA	SVA
				(c)4. MandatedSignatureFormat: XAdES baseline	SVA	SVA
(d)	Targeted community	MitSoft Qualified Long-term Preservation Service and its subscribers.	-	d)1. TargetedCommunityConstraints: MitSoft Qualified Long-term Preservation Service and its subscribers.		
(e)	Allocation of responsibility for validation & augmentation	Preservation client is responsible to provide signed electronic document or container. Preservation Service is responsible to validate and augment digital signatures to reach LTA level.	-	(e)1. ValidationRequiredBeforeAugmenting: True	SVA	-
				(e)2. AugmentToLevel: LTA	SVA	-

(f)	Legal type	Qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals.	-	(f)1. ConstraintsOnCertificateMetadata: (f)1.1. LegalPersonSignerRequired: False (f)1.2. LegalPersonSignerAllowed: True (f)1.3. EUAdESigRequired: True (if it is a signature) (f)1.4. EUAdESealRequired: True (if it is a seal) (f)1.5. EUQSigCDRequired: True (if it is a qualified electronic signature) (f)1.6. EUQSealCDRequired: True (if it is a qualified electronic seal)	SVA	SVA

(g)	Commitment type	Commitment type is required. Allowed commitment type values are defined in ADOC-V2.0.	Specified in ADOC-2.0.	(g)1. CommitmentTypesRequired: (g)1.1. MandatedSignedQProperties-commitment-type-indication: True. (g)1.2. MandatedCommitmentTypeValues: MatchingValuesIndicator: atLeastOne CommitmentTypeValues: Commitment type values defined in Annex B of ETSI TS 119 172-1 [TS 119 172-1]: • http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin, • http://uri.etsi.org/01903/v1.2.2#ProofOfApproval; Commitment type values defined in ADOC-V2.0: • <SigPurposeURN>/signature • <SigPurposeURN>/confirmation • <SigPurposeURN>/visa • <SigPurposeURN>/conciliation • <SigPurposeURN>/registration • <SigPurposeURN>/registrationOfIncommingDocuments • <SigPurposeURN>/acknowledgement • <SigPurposeURN>/resolution • <SigPurposeURN>/endOfExecution • <SigPurposeURN>/notarisation • <SigPurposeURN>/copyCertification • <SigPurposeURN>/authenticity. Here <SigPurposeURN> stands for http://www.archyvai.lt/adoc/2014/signaturePurpose	SVA	SVA
(h)	LoA on timing evidences	Only qualified electronic time stamps shall be used.	[RFC 3161], [RFC 5816], [EN 319 422]	h)1. LoAOnTimingEvidences: (h)1.3. LoA-on-signature-time-stamp: Qualified electronic time stamps only (h)1.4. LoA-on-archival-time-stamp: Qualified electronic time stamps only.	SVA	SVA
(i)	Formalities of signing	Not applicable.	-	-		
(j)	Longevity & resilience	Very long term.	B-LTA level should be reached.	(j)1. LoAOnLongevityAndResilience: Very long term	SVA	-

(k)	Archival	Ensures digital signatures verifiability for the whole preservation period.	Digital signature augmentation by incorporating archive time stamps.	(k)1. ArchivalConstraints: Digital signatures verifiability shall be ensured for the whole preservation period	SVA	-
(l)	Identity and role attributes of the signer	Signer shall be natural person, natural person, which represents some legal person, or legal person. Constraints for the signer role attributes as defined in the electronic document specification.	Specified in ADOC-2.0.	(l)1. ConstraintsOnCertificateMetadata-LegalPersonSignerRequired: False	SVA	SVA
				(l)2. ConstraintsOnCertificateMetadata-LegalPersonSignerAllowed: True	SVA	SVA
(m)	LoA on signer authentication	Electronic signature or electronic seal certificate, issued by the qualified trust service provider	-	(m)1. X509CertificateValidationConstraints: (m)1.1. SetOfTrustAnchors: • For certificates issued to signer or to CAs: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml); • For certificates issued to OCSP responders or to CRL issuers: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml) and sets of trusted certificates stored in the environment; • For certificates issued to Time-Stamping Units: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml).	SVA	SVA

				(m)2. RevocationConstraints[1]: (m)2.1. RevocationCheckingConstraints: eitherCheck. (m)2.2. RevocationFreshnessConstraints: The maximum accepted difference between the issuance date of the revocation status information (thisUpdate) of a certificate and the time of validation for the signing certificate is set to 1 minute for validation and 0 minutes for augmentation[2].	SVA	SVA
(n)	Signature Creation Devices	QSCD shall be used for qualified el. signature or qualified el. seal.	Signer certificate shall contain QCStatement esi4-qcStatement-4 ([EN 319 412-5]).	(n)1. LoAOnSCD: QSCD shall be used for signer certificate.	SVA	SVA
(o)	Other information to be associated with signatures	Explicit or implicit signature policy attribute shall be used.	XAdES SignaturePolicy-Identifier attribute is required.	(o)2. MandatedUnsignedQProperties-signature-policy-extension: True.	SVA	SVA
(p)	Cryptographic suites	According [TS 119 312] and [ENISA], and suppressed by electronic document specification.	ETSI TS 119 312, [ENISA] and ADOC-V2.0.	(p)1. CryptographicSuitesConstraints: According ETSI TS 119 312 and [ENISA], and suppressed by electronic document specification.	SVA	SVA
(q)	Technological environment	Not applicable.	-	-		
Summary: Electronic signature/seal shall be detached XAdES baseline signature according ETSI TS 103 171 within electronic document ADOC-V2.0 package; signed data – files (formats are listed in the electronic document specification) or parts of the XML metadata files presented within the same package; expected signature level is B-LTA (other levels are also allowed).						

[1] Constraints are not used if certificate does represent a trust anchor.
[2] New validation data to be inserted into the signature only if it has been issued after the best signature time.

4.2.1.3 Input constraints for EGAS-V1.0 electronic documents

Input constraints to be used when augmenting or validating electronic signatures/seals presented within EGAS-V1.0 [EGAS-V1.0] electronic documents are presented in the Table 21.

Table 21. Input constraints for EGAS-V1.0 electronic documents

Name and identifier of the signature policy authority: joint stock company "MIT-SOFT", registration number 120792080 **Name and identifier of the signature policy:** MitSoft Qualified Long-term Preservation Service signature policy, OID 1.3.6.1.4.1.57890.1.6.1.1 **Identifier of the concerned signature(s) in the concerned signature workflow**: qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals contained in the EGAS-V1.0 electronic document						
BSP	**BSP title**	**Business statement summary**	**Technical counterpart statement**	**Constraint(s)**	**Constraint value at signature augment-ation (SCA, SVA or DA)**	**Constraint value at signature validation (SVA or DA)**
(a)	Workflow (sequencing & timing)	Countersignatures are allowed only if they are detached counter signatures.	XAdES CounterSignature attribute is forbidden.	-	SVA	SVA
(b)	DTBS	One or more content files of the formats allowed by appropriate electronic document specifications and parts of the XML metadata files.	Specified in EGAS-1.0.	(b)1. ConstraintOnDTBS: Allowed formats of the signed files are defined in the EGAS-1.0 specification.	SVA	SVA
				(b)3. DOTBSAsAWholeOrInParts: parts: whole content files and parts of the XML metadata files may be signed as it is defined in the EGAS-1.0 specification.	SVA	SVA
(c)	Relationship between	Detached XAdES signatures	Specified in EGAS-1.0.	(c)2. ConstraintsOnTheNumberOfDOTBS: $2 \leq x$	SVA	SVA

	DTBS and Signature	associated within electronic document.		(c)3. SignatureRelativePosition: associated	SVA	SVA
				(c)4. MandatedSignatureFormat: XAdES	SVA	SVA
(d)	Targeted community	MitSoft Qualified Long-term Preservation Service and its subscribers.	-	d)1. TargetedCommunityConstraints: MitSoft Qualified Long-term Preservation Service and its subscribers.		
(e)	Allocation of responsibility for validation & augmentation	Preservation client is responsible to provide signed electronic document or container. Preservation Service is responsible to validate and augment digital signatures to reach LTA level.	-	(e)1. ValidationRequiredBeforeAugmenting: True	SVA	-
				(e)2. AugmentToLevel: LTA	SVA	-
(f)	Legal type	Qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals.	-	(f)1. ConstraintsOnCertificateMetadata: (f)1.1. LegalPersonSignerRequired: False (f)1.2. LegalPersonSignerAllowed: True (f)1.3. EUAdESigRequired: True (if it is a signature) (f)1.4. EUAdESealRequired: True (if it is a seal) (f)1.5. EUQSigCDRequired: True (if it is a qualified electronic signature) (f)1.6. EUQSealCDRequired: True (if it is a qualified electronic seal)	SVA	SVA

(g)	Commitment type	Commitment type is optional, if used, only commitment type values defined in EGAS-V1.0 are allowed. Signature purpose is required in the metadata. Allowed signature purposes are defined in EGAS-V1.0.	Specified in EGAS-1.0.	(g)1. CommitmentTypesRequired: (g)1.1. MandatedSignedQProperties-commitment-type-indication: False. (g)1.2. MandatedCommitmentTypeValues: MatchingValuesIndicator: atLeastOne CommitmentTypeValues: Commitment type values defined in Annex B of ETSI TS 119 172-1 [TS 119 172-1]: • http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin, • http://uri.etsi.org/01903/v1.2.2#ProofOfApproval.	SVA	SVA
(h)	LoA on timing evidences	Only qualified electronic time stamps shall be used.	[RFC 3161], [RFC 5816], [EN 319 422]	h)1. LoAOnTimingEvidences: (h)1.3. LoA-on-signature-time-stamp: Qualified electronic time stamps only (h)1.4. LoA-on-archival-time-stamp: Qualified electronic time stamps only.	SVA	SVA
(i)	Formalities of signing	Not applicable.	-	-		
(j)	Longevity & resilience	Very long term.	XAdES-A format should be reached.	(j)1. LoAOnLongevityAndResilience: Very long term	SVA	-
(k)	Archival	Ensures digital signatures verifiability for the whole preservation period.	Digital signature augmentation by incorporating archive time stamps.	(k)1. ArchivalConstraints: Digital signatures verifiability shall be ensured for the whole preservation period	SVA	-
(l)	Identity and role attributes of the signer	Signer shall be natural person, natural person,	Specified in EGAS-1.0.	(l)1. ConstraintsOnCertificateMetadata-LegalPersonSignerRequired: False	SVA	SVA

		which represents some legal person, or legal person. Constraints for the signer role attributes as defined in the electronic document specification.		(l)2. ConstraintsOnCertificateMetadata-LegalPersonSignerAllowed: True	SVA	SVA
(m)	LoA on signer authentication	Electronic signature or electronic seal certificate, issued by the qualified trust service provider	-	(m)1. X509CertificateValidationConstraints: (m)1.1. SetOfTrustAnchors: • For certificates issued to signer or to CAs: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml); • For certificates issued to OCSP responders or to CRL issuers: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml) and sets of trusted certificates stored in the environment; • For certificates issued to Time-Stamping Units: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml).	SVA	SVA
				(m)2. RevocationConstraints[1]: (m)2.1. RevocationCheckingConstraints: eitherCheck. (m)2.2. RevocationFreshnessConstraints: The maximum accepted difference between the issuance date of the revocation status information (thisUpdate) of a certificate and the time of validation for the signing certificate is set to 1 minute for validation and 0 minutes for augmentation[2].	SVA	SVA

[1] Constraints are not used if certificate does represent a trust anchor.
[2] New validation data to be inserted into the signature only if it has been issued after the best signature time.

(n)	Signature Creation Devices	QSCD shall be used for qualified el. signature or qualified el. seal.	Signer certificate shall contain QCStatement esi4-qcStatement-4 ([EN 319 412-5]).	(n)1. LoAOnSCD: QSCD shall be used for signer certificate.	SVA	SVA
(o)	Other information to be associated with signatures	Explicit or implicit signature policy attribute shall be used.	XAdES SignaturePolicy-Identifier attribute is required.	(o)2. MandatedUnsignedQProperties-signature-policy-extension: True.	SVA	SVA
(p)	Cryptographic suites	According [TS 119 312] and [ENISA], and suppressed by electronic document specification.	ETSI TS 119 312, [ENISA] and EGAS-V1.0.	(p)1. CryptographicSuitesConstraints: According ETSI TS 119 312 and [ENISA], and suppressed by electronic document specification.	SVA	SVA
(q)	Technological environment	Not applicable.	-	-		
Summary: Electronic signature/seal shall be detached XAdES signature according ETSI TS 101 903 within electronic document EGAS-V1.0 package; signed data – files (formats are listed in the electronic document specification) or parts of the XML metadata files presented within the same package; expected signature level is B-LTA (other levels are also allowed).						

4.2.1.4 Input constraints for MDOC-V1.0 electronic documents

Input constraints to be used when augmenting or validating electronic signatures/seals presented within MDOC-V1.0 [MDOC-V1.0] electronic documents are presented in the Table 22.

Table 22. Input constraints for MDOC-V1.0 electronic documents

Name and identifier of the signature policy authority: joint stock company "MIT-SOFT", registration number 120792080 **Name and identifier of the signature policy:** MitSoft Qualified Long-term Preservation Service signature policy, OID 1.3.6.1.4.1.57890.1.6.1.1 **Identifier of the concerned signature(s) in the concerned signature workflow**: qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals contained in the MDOC-V1.0 electronic document						
BSP	**BSP title**	**Business statement summary**	**Technical counterpart statement**	**Constraint(s)**	**Constraint value at signature augment-ation (SCA, SVA or DA)**	**Constraint value at signature validation (SVA or DA)**
(a)	Workflow (sequencing & timing)	Countersignatures are allowed only if they are detached counter signatures.	XAdES CounterSignature attribute is forbidden.	-	SVA	SVA
(b)	DTBS	One or more content files of the formats allowed by appropriate electronic document specifications and parts of the XML metadata files.	Specified in MDOC-1.0.	(b)1. ConstraintOnDTBS: Allowed formats of the signed files are defined in the MDOC-1.0 specification.	SVA	SVA
				(b)3. DOTBSAsAWholeOrInParts: parts: whole content files and parts of the XML metadata files may be signed as it is defined in the MDOC-1.0 specification.	SVA	SVA
(c)	Relationship between	Detached XAdES signatures	Specified in MDOC-1.0.	(c)2. ConstraintsOnTheNumberOfDOTBS: $2 \leq x$	SVA	SVA

	DTBS and Signature	associated within electronic document.		(c)3. SignatureRelativePosition: associated	SVA	SVA
				(c)4. MandatedSignatureFormat: XAdES	SVA	SVA
(d)	Targeted community	MitSoft Qualified Long-term Preservation Service and its subscribers.	-	d)1. TargetedCommunityConstraints: MitSoft Qualified Long-term Preservation Service and its subscribers.		
(e)	Allocation of responsibility for validation & augmentation	Preservation client is responsible to provide signed electronic document or container. Preservation Service is responsible to validate and augment digital signatures to reach LTA level.	-	(e)1. ValidationRequiredBeforeAugmenting: True	SVA	-
				(e)2. AugmentToLevel: LTA	SVA	-
(f)	Legal type	Qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals.	-	(f)1. ConstraintsOnCertificateMetadata: (f)1.1. LegalPersonSignerRequired: False (f)1.2. LegalPersonSignerAllowed: True (f)1.3. EUAdESigRequired: True (if it is a signature) (f)1.4. EUAdESealRequired: True (if it is a seal) (f)1.5. EUQSigCDRequired: True (if it is a qualified electronic signature) (f)1.6. EUQSealCDRequired: True (if it is a qualified electronic seal)	SVA	SVA

(g)	Commitment type	Commitment type is optional, if used, only commitment type values defined in MDOC-V1.0 are allowed. Signature purpose is required in the metadata. Allowed signature purposes are defined in MDOC-V1.0.	Specified in MDOC-1.0.	(g)1. CommitmentTypesRequired: (g)1.1. MandatedSignedQProperties-commitment-type-indication: False. (g)1.2. MandatedCommitmentTypeValues: MatchingValuesIndicator: atLeastOne CommitmentTypeValues: Commitment type values defined in Annex B of ETSI TS 119 172-1 [TS 119 172-1]: • http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin, • http://uri.etsi.org/01903/v1.2.2#ProofOfApproval.	SVA	SVA
(h)	LoA on timing evidences	Only qualified electronic time stamps shall be used.	[RFC 3161], [RFC 5816], [EN 319 422]	h)1. LoAOnTimingEvidences: (h)1.3. LoA-on-signature-time-stamp: Qualified electronic time stamps only (h)1.4. LoA-on-archival-time-stamp: Qualified electronic time stamps only.	SVA	SVA
(i)	Formalities of signing	Not applicable.	-	-		
(j)	Longevity & resilience	Very long term.	XAdES-A format should be reached.	(j)1. LoAOnLongevityAndResilience: Very long term	SVA	-
(k)	Archival	Ensures digital signatures verifiability for the whole preservation period.	Digital signature augmentation by incorporating archive time stamps.	(k)1. ArchivalConstraints: Digital signatures verifiability shall be ensured for the whole preservation period	SVA	-
(l)	Identity and role attributes of the signer	Signer shall be natural person, natural person,	Specified in MDOC-1.0.	(l)1. ConstraintsOnCertificateMetadata-LegalPersonSignerRequired: False	SVA	SVA

		which represents some legal person, or legal person. Constraints for the signer role attributes as defined in the electronic document specification.		(l)2. ConstraintsOnCertificateMetadata-LegalPersonSignerAllowed: True	SVA	SVA
(m)	LoA on signer authentication	Electronic signature or electronic seal certificate, issued by the qualified trust service provider	-	(m)1. X509CertificateValidationConstraints: (m)1.1. SetOfTrustAnchors: • For certificates issued to signer or to CAs: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml); • For certificates issued to OCSP responders or to CRL issuers: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml) and sets of trusted certificates stored in the environment; • For certificates issued to Time-Stamping Units: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml).	SVA	SVA
				(m)2. RevocationConstraints[1]: (m)2.1. RevocationCheckingConstraints: eitherCheck. (m)2.2. RevocationFreshnessConstraints: The maximum accepted difference between the issuance date of the revocation status information (thisUpdate) of a certificate and the time of validation for the signing certificate is set to 1 minute for validation and 0 minutes for augmentation[2].	SVA	SVA

[1] Constraints are not used if certificate does represent a trust anchor.
[2] New validation data to be inserted into the signature only if it has been issued after the best signature time.

(n)	Signature Creation Devices	QSCD shall be used for qualified el. signature or qualified el. seal.	Signer certificate shall contain QCStatement esi4-qcStatement-4 ([EN 319 412-5]).	(n)1. LoAOnSCD: QSCD shall be used for signer certificate.	SVA	SVA
(o)	Other information to be associated with signatures	Explicit or implicit signature policy attribute shall be used.	XAdES SignaturePolicy-Identifier attribute is required.	(o)2. MandatedUnsignedQProperties-signature-policy-extension: True.	SVA	SVA
(p)	Cryptographic suites	According [TS 119 312] and [ENISA], and suppressed by electronic document specification.	ETSI TS 119 312, [ENISA] and MDOC-V1.0.	(p)1. CryptographicSuitesConstraints: According ETSI TS 119 312 and [ENISA], and suppressed by electronic document specification.	SVA	SVA
(q)	Technological environment	Not applicable.	-	-		
Summary: Electronic signature/seal shall be detached XAdES signature according ETSI TS 101 903 within electronic document MDOC-V1.0 package; signed data – files (formats are listed in the electronic document specification) or parts of the XML metadata files presented within the same package; expected signature level is B-LTA (other levels are also allowed).						

4.2.1.5 Input constraints for PDF-LT-V1.0 electronic documents

Input constraints to be used when augmenting or validating electronic signatures/seals presented within PDF-LT-V1.0 [PDF-LT -V1.0] electronic documents are presented in the Table 23.

Table 23. Input constraints for PDF-LT-V1.0 electronic documents

Name and identifier of the signature policy authority: joint stock company "MIT-SOFT", registration number 120792080 **Name and identifier of the signature policy:** MitSoft Qualified Long-term Preservation Service signature policy, OID 1.3.6.1.4.1.57890.1.6.1.1 **Identifier of the concerned signature(s) in the concerned signature workflow**: qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals contained in the PDF-LT-V1.0 electronic document						
BSP	**BSP title**	**Business statement summary**	**Technical counterpart statement**	**Constraint(s)**	**Constraint value at signature augment-ation (SCA, SVA or DA)**	**Constraint value at signature validation (SVA or DA)**
(a)	Workflow (sequencing & timing)	Declared signing time attribute shall be included.	PAdES signature field M is required.	(a)3. TimingRelevance: (a)3.2 TimingRelevanceOnEvidence: (a)3.2.1 MandatedSignedQProperties-signing-time	SVA	SVA
(b)	DTBS	Whole PDF/A-2 file.	Specified in PDF-LT-V1.0.	(b)1. ConstraintOnDTBS: Data to be signed is a PDF/A-2 file.	SVA	SVA
				(b)3. DOTBSAsAWholeOrInParts: whole	SVA	SVA
(c)	Relationship between DTBS and Signature	Enveloped PAdES baseline signatures.	Specified in PDF-LT-V1.0.	(c)2. ConstraintsOnTheNumberOfDOTBS: x =1	SVA	SVA
				(c)3. SignatureRelativePosition: enveloped	SVA	SVA
				(c)4. MandatedSignatureFormat: PAdES baseline	SVA	SVA
(d)	Targeted community	MitSoft Qualified Long-term Preservation Service and its subscribers.	-	d)1. TargetedCommunityConstraints: MitSoft Qualified Long-term Preservation Service and its subscribers.		

(e)	Allocation of responsibility for validation & augmentation	Preservation client is responsible to provide signed electronic document or container. Preservation Service is responsible to validate and augment digital signatures to reach LTA level.	-	(e)1. ValidationRequiredBeforeAugmenting: True	SVA	-
				(e)2. AugmentToLevel: LTA	SVA	-
(f)	Legal type	Qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals.	-	(f)1. ConstraintsOnCertificateMetadata: (f)1.1. LegalPersonSignerRequired: False (f)1.2. LegalPersonSignerAllowed: True (f)1.3. EUAdESigRequired: True (if it is a signature) (f)1.4. EUAdESealRequired: True (if it is a seal) (f)1.5. EUQSigCDRequired: True (if it is a qualified electronic signature) (f)1.6. EUQSealCDRequired: True (if it is a qualified electronic seal)	SVA	SVA
(g)	Commitment type	Commitment type is optional. Values for PDF signature dictionary field Reason are defined in PDF-LT-V1.0.	Specified in PDF-LT-V1.0.	(g)1. CommitmentTypesRequired: (g)1.1. MandatedSignedQProperties-commitment-type-indication: False.	SVA	SVA

(h)	LoA on timing evidences	Only qualified electronic time stamps shall be used.	[RFC 3161], [RFC 5816], [EN 319 422]	h)1. LoAOnTimingEvidences: (h)1.3. LoA-on-signature-time-stamp: Qualified electronic time stamps only (h)1.4. LoA-on-archival-time-stamp: Qualified electronic time stamps only.	SVA	SVA
(i)	Formalities of signing	Not applicable.	-	-		
(j)	Longevity & resilience	Very long term.	B-LTA level should be reached.	(j)1. LoAOnLongevityAndResilience: Very long term	SVA	-
(k)	Archival	Ensures digital signatures verifiability for the whole preservation period.	Digital signature augmentation by incorporating PAdES document time stamps.	(k)1. ArchivalConstraints: Digital signatures verifiability shall be ensured for the whole preservation period	SVA	-
(l)	Identity and role attributes of the signer	Signer shall be natural person, natural person, which represents some legal person, or legal person. Constraints for the signer role attributes as defined in the electronic document specification.	Specified in PDF-LT-1.0.	(l)1. ConstraintsOnCertificateMetadata-LegalPersonSignerRequired: False	SVA	SVA
				(l)2. ConstraintsOnCertificateMetadata-LegalPersonSignerAllowed: True	SVA	SVA

(m)	LoA on signer authentication	Electronic signature or electronic seal certificate, issued by the qualified trust service provider	-	(m)1. X509CertificateValidationConstraints: (m)1.1. SetOfTrustAnchors: • For certificates issued to signer or to CAs: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml); • For certificates issued to OCSP responders or to CRL issuers: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml) and sets of trusted certificates stored in the environment; • For certificates issued to Time-Stamping Units: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml).	SVA	SVA
				(m)2. RevocationConstraints[1]: (m)2.1. RevocationCheckingConstraints: eitherCheck. (m)2.2. RevocationFreshnessConstraints: The maximum accepted difference between the issuance date of the revocation status information (thisUpdate) of a certificate and the time of validation for the signing certificate is set to 1 minute for validation and 0 minutes for augmentation[2].	SVA	SVA
(n)	Signature Creation Devices	QSCD shall be used for qualified el. signature or qualified el. seal.	Signer certificate shall contain QCStatement esi4-qcStatement-4 ([EN 319 412-5]).	(n)1. LoAOnSCD: QSCD shall be used for signer certificate.	SVA	SVA
(o)	Other information to be associated with signatures	Not applicable.	-	-		

[1] Constraints are not used if certificate does represent a trust anchor.
[2] New validation data to be inserted into the signature only if it has been issued after the best signature time.

(p)	Cryptographic suites	According [TS 119 312] and [ENISA], and suppressed by electronic document specification.	ETSI TS 119 312, [ENISA] and PDF-LT-V1.0.	(p)1. CryptographicSuitesConstraints: According ETSI TS 119 312 and [ENISA], and suppressed by electronic document specification.	SVA	SVA
(q)	Technological environment	Not applicable.	-	-		
Summary: Electronic signature/seal shall be enveloped PAdES baseline signature according ETSI TS 103 172 [TS 103 172] within PDF/A-2 document and conformant to electronic document specification PDF-LT-V1.0; signed data – whole PDF file; expected signature level is B-LTA (other levels are also allowed).						

4.2.1.6 Input constraints for PDF-RC-V1.0 electronic documents

Input constraints to be used when augmenting or validating electronic signatures/seals presented within PDF-RC-V1.0 [PDF-RC-V1.0] electronic documents are presented in the Table 24.

Table 24. Input constraints for PDF-RC-V1.0 electronic documents

Name and identifier of the signature policy authority: joint stock company "MIT-SOFT", registration number 120792080 **Name and identifier of the signature policy:** MitSoft Qualified Long-term Preservation Service signature policy, OID 1.3.6.1.4.1.57890.1.6.1.1 **Identifier of the concerned signature(s) in the concerned signature workflow**: qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals contained in the PDF-RC-V1.0 electronic document						
BSP	**BSP title**	**Business statement summary**	**Technical counterpart statement**	**Constraint(s)**	**Constraint value at signature augment-ation (SCA, SVA or DA)**	**Constraint value at signature validation (SVA or DA)**
(a)	Workflow (sequencing & timing)	Declared signing time attribute shall be included.	PAdES signature field M is required.	(a)3. TimingRelevance: (a)3.2 TimingRelevanceOnEvidence: (a)3.2.1 MandatedSignedQProperties-signing-time	SVA	SVA
(b)	DTBS	Whole PDF/A-3 file together with embedded files.	Specified in PDF-RC-V1.0.	(b)1. ConstraintOnDTBS: Data to be signed is a PDF/A-3 file, which contains embedded files of the file formats defined in PDF-RC-V1.0.	SVA	SVA
				(b)3. DOTBSAsAWholeOrInParts: whole	SVA	SVA
(c)	Relationship between DTBS and Signature	Enveloped PAdES baseline signatures.	Specified in PDF-RC-V1.0.	(c)2. ConstraintsOnTheNumberOfDOTBS: x =1	SVA	SVA
				(c)3. SignatureRelativePosition: enveloped	SVA	SVA
				(c)4. MandatedSignatureFormat: PAdES baseline	SVA	SVA

(d)	Targeted community	MitSoft Qualified Long-term Preservation Service and its subscribers.	-	d)1. TargetedCommunityConstraints: MitSoft Qualified Long-term Preservation Service and its subscribers.		
(e)	Allocation of responsibility for validation & augmentation	Preservation client is responsible to provide signed electronic document or container. Preservation Service is responsible to validate and augment digital signatures to reach LTA level.	-	(e)1. ValidationRequiredBeforeAugmenting: True	SVA	-
				(e)2. AugmentToLevel: LTA	SVA	-
(f)	Legal type	Qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals.	-	(f)1. ConstraintsOnCertificateMetadata: (f)1.1. LegalPersonSignerRequired: False (f)1.2. LegalPersonSignerAllowed: True (f)1.3. EUAdESigRequired: True (if it is a signature) (f)1.4. EUAdESealRequired: True (if it is a seal) (f)1.5. EUQSigCDRequired: True (if it is a qualified electronic signature) (f)1.6. EUQSealCDRequired: True (if it is a qualified electronic seal)	SVA	SVA

(g)	Commitment type	Commitment type is optional and values are restricted by PDF-RC-V1.0. Values for PDF signature dictionary field Reason are defined in PDF-RC-V1.0.	Specified in PDF-RC-V1.0.	(g)1. CommitmentTypesRequired: (g)1.1. MandatedSignedQProperties-commitment-type-indication: False. (g)1.2. MandatedCommitmentTypeValues: MatchingValuesIndicator: atLeastOne CommitmentTypeValues: Commitment type values defined in Annex B of ETSI TS 119 172-1 [TS 119 172-1]: • http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin, • http://uri.etsi.org/01903/v1.2.2#ProofOfApproval.	SVA	SVA
(h)	LoA on timing evidences	Only qualified electronic time stamps shall be used.	[RFC 3161], [RFC 5816], [EN 319 422]	h)1. LoAOnTimingEvidences: (h)1.3. LoA-on-signature-time-stamp: Qualified electronic time stamps only (h)1.4. LoA-on-archival-time-stamp: Qualified electronic time stamps only.	SVA	SVA
(i)	Formalities of signing	Not applicable.	-	-		
(j)	Longevity & resilience	Very long term.	B-LTA level should be reached.	(j)1. LoAOnLongevityAndResilience: Very long term	SVA	-
(k)	Archival	Ensures digital signatures verifiability for the whole preservation period.	Digital signature augmentation by incorporating PAdES document time stamps.	(k)1. ArchivalConstraints: Digital signatures verifiability shall be ensured for the whole preservation period	SVA	-
(l)	Identity and role attributes of the signer	Signer shall be natural person, natural person,	Specified in PDF-RC-1.0.	(l)1. ConstraintsOnCertificateMetadata-LegalPersonSignerRequired: False	SVA	SVA

		which represents some legal person, or legal person. Constraints for the signer role attributes as defined in the electronic document specification.		(l)2. ConstraintsOnCertificateMetadata-LegalPersonSignerAllowed: True	SVA	SVA
(m)	LoA on signer authentication	Electronic signature or electronic seal certificate, issued by the qualified trust service provider	-	(m)1. X509CertificateValidationConstraints: (m)1.1. SetOfTrustAnchors: • For certificates issued to signer or to CAs: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml); • For certificates issued to OCSP responders or to CRL issuers: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml) and sets of trusted certificates stored in the environment; • For certificates issued to Time-Stamping Units: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml).	SVA	SVA
				(m)2. RevocationConstraints[1]: (m)2.1. RevocationCheckingConstraints: eitherCheck. (m)2.2. RevocationFreshnessConstraints: The maximum accepted difference between the issuance date of the revocation status information (thisUpdate) of a certificate and the time of validation for the signing certificate is set to 1 minute for validation and 0 minutes for augmentation[2].	SVA	SVA

[1] Constraints are not used if certificate does represent a trust anchor.
[2] New validation data to be inserted into the signature only if it has been issued after the best signature time.

(n)	Signature Creation Devices	QSCD shall be used for qualified el. signature or qualified el. seal.	Signer certificate shall contain QCStatement esi4-qcStatement-4 ([EN 319 412-5]).	(n)1. LoAOnSCD: QSCD shall be used for signer certificate.	SVA	SVA
(o)	Other information to be associated with signatures	Not applicable.	-	-		
(p)	Cryptographic suites	According [TS 119 312] and [ENISA], and suppressed by electronic document specification.	ETSI TS 119 312, [ENISA] and PDF-RC-V1.0.	(p)1. CryptographicSuitesConstraints: According ETSI TS 119 312 and [ENISA], and suppressed by electronic document specification.	SVA	SVA
(q)	Technological environment	Not applicable.	-	-		
Summary: Electronic signature/seal shall be enveloped PAdES baseline signature according ETSI EN 319 142-1 [EN 319 142-1] within PDF/A-3 document, which is conformant to electronic document specification PDF-RC-V1.0; signed data – whole PDF file (with embedded files); expected signature level is B-LTA (other levels are also allowed).						

4.2.1.7 Input constraints for ASiC baseline containers

Input constraints to be used when augmenting or validating electronic signatures/seals presented within baseline ASiC-E and ASiC-S containers according ETSI TS 103 174 [TS 103 174] or ETSI EN 319 162-1 [EN 319 162-1] are presented in the Table 25.

Table 25. Input constraints for ASiC baseline containers

Name and identifier of the signature policy authority: joint stock company "MIT-SOFT", registration number 120792080 **Name and identifier of the signature policy:** MitSoft Qualified Long-term Preservation Service signature policy, OID 1.3.6.1.4.1.57890.1.6.1.1 **Identifier of the concerned signature(s) in the concerned signature workflow**: qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals contained in the baseline ASiC-E and ASiC-S container						
BSP	**BSP title**	**Business statement summary**	**Technical counterpart statement**	**Constraint(s)**	**Constraint value at signature augment-ation (SCA, SVA or DA)**	**Constraint value at signature validation (SVA or DA)**
(a)	Workflow (sequencing & timing)	Declared signing time attribute shall be included.	XAdES or CAdES SigningTime attribute is required.	(a)3. TimingRelevance: (a)3.2 TimingRelevanceOnEvidence: (a)3.2.1 MandatedSignedQProperties-signing-time	SVA	SVA
(b)	DTBS	One or more file of the format defined in the ASiC E container manifest file. One file of the format defined in the ASiC S container.	Specified in ETSI TS 103 174 or ETSI EN 319 162-1.	(b)1. ConstraintOnDTBS: Any file in the ASiC-E container or single file in the ASIC-S container.	SVA	SVA
				(b)3. DOTBSAsAWholeOrInParts: whole or parts	SVA	SVA
		The mime type of the signed data files shall be indicated in the signature.	XAdES DataObjectFormat is required.	(b)2. ContentRelatedConstraintsAsPartOfSignatureElements: (b)2.1 MandatedSignedQProperties-DataObjetFormat.	SVA	SVA
(c)	Relationship between	Detached XAdES or CAdES		(c)2. ConstraintsOnTheNumberOfDOTBS: 1 ≤ x	SVA	SVA

	DTBS and Signature	baseline signature associated within ASiC container.	Specified in ETSI TS 103 174 or ETSI EN 319 162-1.	(c)3. SignatureRelativePosition: associated	SVA	SVA
				(c)4. MandatedSignatureFormat: XAdES baseline or CAdES baseline	SVA	SVA
(d)	Targeted community	MitSoft Qualified Long-term Preservation Service and its subscribers.	-	d)1. TargetedCommunityConstraints: MitSoft Qualified Long-term Preservation Service and its subscribers.		
(e)	Allocation of responsibility for validation & augmentation	Preservation client is responsible to provide signed electronic document or container. Preservation Service is responsible to validate and augment digital signatures to reach LTA level.	-	(e)1. ValidationRequiredBeforeAugmenting: True	SVA	-
				(e)2. AugmentToLevel: LTA	SVA	-
(f)	Legal type	Qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals.	-	(f)1. ConstraintsOnCertificateMetadata: (f)1.1. LegalPersonSignerRequired: False (f)1.2. LegalPersonSignerAllowed: True (f)1.3. EUAdESigRequired: True (if it is a signature) (f)1.4. EUAdESealRequired: True (if it is a seal) (f)1.5. EUQSigCDRequired: True (if it is a qualified electronic signature) (f)1.6. EUQSealCDRequired: True (if it is a qualified electronic seal)	SVA	SVA
(g)	Commitment type	No constraints.	-	-		

(h)	LoA on timing evidences	Only qualified electronic time stamps shall be used.	[RFC 3161], [RFC 5816], [EN 319 422]	h)1. LoAOnTimingEvidences: (h)1.3. LoA-on-signature-time-stamp: Qualified electronic time stamps only (h)1.4. LoA-on-archival-time-stamp: Qualified electronic time stamps only.	SVA	SVA
(i)	Formalities of signing	Not applicable.	-	-		
(j)	Longevity & resilience	Very long term.	B-LTA level should be reached.	(j)1. LoAOnLongevityAndResilience: Very long term	SVA	-
(k)	Archival	Ensures digital signatures verifiability for the whole preservation period.	Digital signature augmentation by incorporating archive time stamps.	(k)1. ArchivalConstraints: Digital signatures verifiability shall be ensured for the whole preservation period	SVA	-
(l)	Identity and role attributes of the signer	Signer shall be natural person, natural person, which represents some legal person, or legal person. No constraints for the signer role attributes.	-	(l)1. ConstraintsOnCertificateMetadata-LegalPersonSignerRequired: False	SVA	SVA
				(l)2. ConstraintsOnCertificateMetadata-LegalPersonSignerAllowed: True	SVA	SVA
(m)	LoA on signer authentication	Electronic signature or electronic seal certificate, issued by the qualified trust service provider	-	(m)1. X509CertificateValidationConstraints: (m)1.1. SetOfTrustAnchors: • For certificates issued to signer or to CAs: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml); • For certificates issued to OCSP responders or to CRL issuers: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml) and sets of trusted certificates stored in the environment; • For certificates issued to Time-Stamping Units: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml).	SVA	SVA

				(m)2. RevocationConstraints[1]: (m)2.1. RevocationCheckingConstraints: eitherCheck. (m)2.2. RevocationFreshnessConstraints: The maximum accepted difference between the issuance date of the revocation status information (thisUpdate) of a certificate and the time of validation for the signing certificate is set to 1 minute for validation and 0 minutes for augmentation[2].	SVA	SVA
(n)	Signature Creation Devices	QSCD shall be used for qualified el. signature or qualified el. seal.	Signer certificate shall contain QCStatement esi4-qcStatement-4 ([EN 319 412-5]).	(n)1. LoAOnSCD: QSCD shall be used for signer certificate.	SVA	SVA
(o)	Other information to be associated with signatures	Not applicable.	-	-		
(p)	Cryptographic suites	According [TS 119 312] and [ENISA].	ETSI TS 119 312, [ENISA].	(p)1. CryptographicSuitesConstraints: According ETSI TS 119 312 and [ENISA].	SVA	SVA
(q)	Technological environment	Not applicable.	-	-		
Summary: Electronic signature/seal shall be detached XAdES baseline signature according ETSI TS 103 171 [TS 103 171], ETSI EN 319 132-1 [EN 319 132-1], or detached CAdES baseline signature according ETSI TS 103 172 [TS 103 172], ETSI EN 319 122-1 [EN 319 122-1] within ASiC-E or ASiC-S baseline container specified in ETSI TS 103 174 or in ETSI EN 319 162-1; signed data – files presented within the same ASiC container; expected signature level is B-LTA (other levels are also allowed).						

[1] Constraints are not used if certificate does represent a trust anchor.
[2] New validation data to be inserted into the signature only if it has been issued after the best signature time.

4.2.1.8 Input constraints for PAdES baseline signatures

Input constraints to be used when augmenting or validating PAdES baseline electronic signatures/seals according ETSI TS 103 172 [TS 103 172] or ETSI EN 319 142-1 [EN 319 142-1] presented within PDF file are presented in the Table 26.

Table 26. Input constraints for PAdES baseline signatures

Name and identifier of the signature policy authority: joint stock company "MIT-SOFT", registration number 120792080 **Name and identifier of the signature policy:** MitSoft Qualified Long-term Preservation Service signature policy, OID 1.3.6.1.4.1.57890.1.6.1.1 **Identifier of the concerned signature(s) in the concerned signature workflow**: qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals contained in the PDF file						
BSP	**BSP title**	**Business statement summary**	**Technical counterpart statement**	**Constraint(s)**	**Constraint value at signature augment-ation (SCA, SVA or DA)**	**Constraint value at signature validation (SVA or DA)**
(a)	Workflow (sequencing & timing)	Declared signing time attribute shall be included.	PAdES signature field M is required.	(a)3. TimingRelevance: (a)3.2 TimingRelevanceOnEvidence: (a)3.2.1 MandatedSignedQProperties-signing-time	SVA	SVA
(b)	DTBS	Whole PDF file.	Specified in ETSI TS 103 172 or ETSI EN 319 142-1.	(b)1. ConstraintOnDTBS: Data to be signed is a PDF file.	SVA	SVA
				(b)3. DOTBSAsAWholeOrInParts: whole	SVA	SVA
(c)	Relationship between DTBS and Signature	Enveloped PAdES baseline signatures.	Specified in ETSI TS 103 172 or ETSI EN 319 142-1.	(c)2. ConstraintsOnTheNumberOfDOTBS: x =1	SVA	SVA
				(c)3. SignatureRelativePosition: enveloped	SVA	SVA
				(c)4. MandatedSignatureFormat: PAdES baseline	SVA	SVA
(d)	Targeted community	MitSoft Qualified Long-term Preservation Service and its subscribers.	-	d)1. TargetedCommunityConstraints: MitSoft Qualified Long-term Preservation Service and its subscribers.		

(e)	Allocation of responsibility for validation & augmentation	Preservation client is responsible to provide signed electronic document or container. Preservation Service is responsible to validate and augment digital signatures to reach LTA level.	-	(e)1. ValidationRequiredBeforeAugmenting: True	SVA	-
				(e)2. AugmentToLevel: LTA	SVA	-
(f)	Legal type	Qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals.	-	(f)1. ConstraintsOnCertificateMetadata: (f)1.1. LegalPersonSignerRequired: False (f)1.2. LegalPersonSignerAllowed: True (f)1.3. EUAdESigRequired: True (if it is a signature) (f)1.4. EUAdESealRequired: True (if it is a seal) (f)1.5. EUQSigCDRequired: True (if it is a qualified electronic signature) (f)1.6. EUQSealCDRequired: True (if it is a qualified electronic seal)	SVA	SVA
(g)	Commitment type	No constraints.	-	-		
(h)	LoA on timing evidences	Only qualified electronic time stamps shall be used.	[RFC 3161], [RFC 5816], [EN 319 422]	h)1. LoAOnTimingEvidences: (h)1.3. LoA-on-signature-time-stamp: Qualified electronic time stamps only (h)1.4. LoA-on-archival-time-stamp: Qualified electronic time stamps only.	SVA	SVA
(i)	Formalities of signing	Not applicable.	-	-		
(j)	Longevity & resilience	Very long term.	B-LTA level should be reached.	(j)1. LoAOnLongevityAndResilience: Very long term	SVA	-

(k)	Archival	Ensures digital signatures verifiability for the whole preservation period.	Digital signature augmentation by incorporating PAdES document time stamps.	(k)1. ArchivalConstraints: Digital signatures verifiability shall be ensured for the whole preservation period	SVA	-
(l)	Identity and role attributes of the signer	Signer shall be natural person, natural person, which represents some legal person, or legal person. No constraints for the signer role attributes.	-	(l)1. ConstraintsOnCertificateMetadata-LegalPersonSignerRequired: False	SVA	SVA
				(l)2. ConstraintsOnCertificateMetadata-LegalPersonSignerAllowed: True	SVA	SVA
(m)	LoA on signer authentication	Electronic signature or electronic seal certificate, issued by the qualified trust service provider	-	(m)1. X509CertificateValidationConstraints: (m)1.1. SetOfTrustAnchors: • For certificates issued to signer or to CAs: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml); • For certificates issued to OCSP responders or to CRL issuers: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml) and sets of trusted certificates stored in the environment; • For certificates issued to Time-Stamping Units: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml).	SVA	SVA

				(m)2. RevocationConstraints[1]: (m)2.1. RevocationCheckingConstraints: eitherCheck. (m)2.2. RevocationFreshnessConstraints: The maximum accepted difference between the issuance date of the revocation status information (thisUpdate) of a certificate and the time of validation for the signing certificate is set to 1 minute for validation and 0 minutes for augmentation[2].	SVA	SVA
(n)	Signature Creation Devices	QSCD shall be used for qualified el. signature or qualified el. seal.	Signer certificate shall contain QCStatement esi4-qcStatement-4 ([EN 319 412-5]).	(n)1. LoAOnSCD: QSCD shall be used for signer certificate.	SVA	SVA
(o)	Other information to be associated with signatures	Not applicable.	-	-		
(p)	Cryptographic suites	According [TS 119 312] and [ENISA].	ETSI TS 119 312, [ENISA].	(p)1. CryptographicSuitesConstraints: According ETSI TS 119 312 and [ENISA].	SVA	SVA
(q)	Technological environment	Not applicable.	-	-		
Summary: Electronic signature/seal shall be enveloped PAdES baseline signature according ETSI TS 103 172 or ETSI EN 319 142-1 within PDF (PDF-1.7, PDF/A-1, PDF/A-2, PDF/A-3) document; signed data – whole PDF file; expected signature level is B-LTA (other levels are also allowed).						

[1] Constraints are not used if certificate does represent a trust anchor.
[2] New validation data to be inserted into the signature only if it has been issued after the best signature time.

4.2.1.9 Input constraints for CMS signatures in PDF (PAdES-Basic)

Input constraints to be used when augmenting or validating CMS signatures in PDF (PAdES-Basic) according ETSI TS 102 778-2 [TS 102 778-2] and ETSI TS 102 778-4 [TS 102 778-4] are presented within PDF file are presented in the Table 26.

Table 26. Input constraints for CMS signatures in PDF (PAdES-Basic)

Name and identifier of the signature policy authority: joint stock company "MIT-SOFT", registration number 120792080 **Name and identifier of the signature policy:** MitSoft Qualified Long-term Preservation Service signature policy, OID 1.3.6.1.4.1.57890.1.6.1.1 **Identifier of the concerned signature(s) in the concerned signature workflow**: qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals contained in the PDF file						
BSP	**BSP title**	**Business statement summary**	**Technical counterpart statement**	**Constraint(s)**	**Constraint value at signature augment-ation (SCA, SVA or DA)**	**Constraint value at signature validation (SVA or DA)**
(a)	Workflow (sequencing & timing)	Not applicable.	-	-		
(b)	DTBS	Whole PDF file.	Specified in ETSI TS 102 778-2.	(b)1. ConstraintOnDTBS: Data to be signed is a PDF file.	SVA	SVA
				(b)3. DOTBSAsAWholeOrInParts: whole	SVA	SVA
(c)	Relationship between DTBS and Signature	Enveloped PAdES signatures.	Specified in ETSI TS 102 778-2.	(c)2. ConstraintsOnTheNumberOfDOTBS: x =1	SVA	SVA
				(c)3. SignatureRelativePosition: enveloped	SVA	SVA
				(c)4. MandatedSignatureFormat: CMS signature in PDF (PAdES-Basic)	SVA	SVA
(d)	Targeted community	MitSoft Qualified Long-term Preservation Service and its subscribers.	-	d)1. TargetedCommunityConstraints: MitSoft Qualified Long-term Preservation Service and its subscribers.		
(e)	Allocation of responsibility	Preservation client is	-	(e)1. ValidationRequiredBeforeAugmenting: True	SVA	-

	for validation & augmentation	responsible to provide signed electronic document or container. Preservation Service is responsible to validate and augment digital signatures to reach LTA level.		(e)2. AugmentToLevel: LTA	SVA	-
(f)	Legal type	Qualified electronic signatures, qualified electronic seals, advanced electronic signatures or advanced electronic seals.	-	(f)1. ConstraintsOnCertificateMetadata: (f)1.1. LegalPersonSignerRequired: False (f)1.2. LegalPersonSignerAllowed: True (f)1.3. EUAdESigRequired: True (if it is a signature) (f)1.4. EUAdESealRequired: True (if it is a seal) (f)1.5. EUQSigCDRequired: True (if it is a qualified electronic signature) (f)1.6. EUQSealCDRequired: True (if it is a qualified electronic seal)	SVA	SVA
(g)	Commitment type	No constraints.	-	-		
(h)	LoA on timing evidences	Only qualified electronic time stamps shall be used.	[RFC 3161], [RFC 5816], [EN 319 422]	h)1. LoAOnTimingEvidences: (h)1.3. LoA-on-signature-time-stamp: Qualified electronic time stamps only (h)1.4. LoA-on-archival-time-stamp: Qualified electronic time stamps only.	SVA	SVA
(i)	Formalities of signing	Not applicable.	-	-		
(j)	Longevity & resilience	Very long term.	B-LTA level should be reached.	(j)1. LoAOnLongevityAndResilience: Very long term	SVA	-

(k)	Archival	Ensures digital signatures verifiability for the whole preservation period.	Digital signature augmentation by incorporating PAdES document time stamps.	(k)1. ArchivalConstraints: Digital signatures verifiability shall be ensured for the whole preservation period	SVA	-
(l)	Identity and role attributes of the signer	Signer shall be natural person, natural person, which represents some legal person, or legal person. No constraints for the signer role attributes.	-	(l)1. ConstraintsOnCertificateMetadata-LegalPersonSignerRequired: False	SVA	SVA
				(l)2. ConstraintsOnCertificateMetadata-LegalPersonSignerAllowed: True	SVA	SVA
(m)	LoA on signer authentication	Electronic signature or electronic seal certificate, issued by the qualified trust service provider	-	(m)1. X509CertificateValidationConstraints: (m)1.1. SetOfTrustAnchors: • For certificates issued to signer or to CAs: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml); • For certificates issued to OCSP responders or to CRL issuers: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml) and sets of trusted certificates stored in the environment; • For certificates issued to Time-Stamping Units: EU Trusted List (https://ec.europa.eu/tools/lotl/eu-lotl.xml).	SVA	SVA

				(m)2. RevocationConstraints[1]: (m)2.1. RevocationCheckingConstraints: eitherCheck. (m)2.2. RevocationFreshnessConstraints: The maximum accepted difference between the issuance date of the revocation status information (thisUpdate) of a certificate and the time of validation for the signing certificate is set to 1 minute for validation and 0 minutes for augmentation[2].	SVA	SVA
(n)	Signature Creation Devices	QSCD shall be used for qualified el. signature or qualified el. seal.	Signer certificate shall contain QCStatement esi4-qcStatement-4 ([EN 319 412-5]).	(n)1. LoAOnSCD: QSCD shall be used for signer certificate.	SVA	SVA
(o)	Other information to be associated with signatures	Not applicable.	-	-		
(p)	Cryptographic suites	According [TS 119 312] and [ENISA].	ETSI TS 119 312, [ENISA].	(p)1. CryptographicSuitesConstraints: According ETSI TS 119 312 and [ENISA].	SVA	SVA
(q)	Technological environment	Not applicable.	-	-		
Summary: Electronic signature/seal shall be enveloped PAdES signature conformant to Profile for CMS Signatures in PDF defined in the standard ETSI TS 102 778-2 [TS 102 778-2]. Long-term form for this profile is defined in the standard ETSI TS 102 778-4 [TS 102 778-4]. Electronic signature/seal shall reside in PDF (PDF-1.7, PDF/A-1, PDF/A-2, PDF/A-3) document. Signed data – whole PDF file; expected signature level is B-LTA (other levels are also allowed).						

[1] Constraints are not used if certificate does represent a trust anchor.
[2] New validation data to be inserted into the signature only if it has been issued after the best signature time.

4.2.2. Output constraints to be used when validating signatures in the context of the identified signature policy

Not applicable.

4.2.3. Output constraints to be used for generating/augmenting signatures in the context of the identified signature policy

Not applicable.

5. Other business and legal matters

Not applicable.

6. Other business and legal matters Compliance audit and other assessments

Not applicable.