# ETSI Standards and Electronic Archiving

eArchiving Summit Day, Salamanca

*Dr. Ignacio Alamillo-Domingo, 25th October 2023*

# Why eArchiving as trust service

- It allows for the long term preservation of electronic data and associated trust services.

- Functional requirements for the electronic archiving service & clear legal effects when a qualified electronic archiving service is used.

- Both for electronically born documents as well as paper documents that have been scanned and digitised. When required, these provisions should allow for the preserved electronic data to be ported on different media or formats for the purpose of extending their durability and legibility beyond the technological validity period, while minimising loss and alteration to the greatest extent possible.

European Commission

# Why eArchiving as trust service

- When electronic data submitted to the digital archiving service contain one or more qualified electronic signatures or qualified electronic seals, the service should use procedures and technologies capable of extending their trustworthiness for the preservation period of such data, possibly relying on the use of other qualified electronic trust services established by this Regulation.

- For creating preservation evidence where electronic signatures, electronic seals or electronic timestamps are used, qualified electronic trust services should be used.

European Commission

# "Intangibility principle"

- National archives and memory institutions, in their capacity as organizations dedicated to preserving the documentary heritage in public interest, are usually mandated to conduct their activities by national law and do not necessarily provide trust services within the meaning of this Regulation. In so far these institutions do not provide such services, this Regulation is without prejudice to their operation.

- This Regulation does not affect national or Union law related to the conclusion and validity of contracts or other legal or procedural obligations relating to form or sector-specific requirements relating to form.

# Why ETSI Standards?

## TECHNICAL COMMITTEE (TC) ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI)

Our work deals with digital signatures and related trust services.

This activity covers the format of digital signatures, as well as procedures and policies for creation and validation. TC ESI also covers policy, security and technical requirements for trust service providers (TSP) such as certification authorities, time-stamping authorities, TSP providing remote signature creation or validation functions, registered e-delivery providers, and long-term data preservation providers. We address Trusted Lists that enhance the confidence of parties relying on certificates or other services related to digital signatures by indicating whether a given TSP was operating under the approval of any recognized scheme.

Our work also aims at supporting the eIDAS Regulation as well as the general requirements of the international community to provide trust and confidence in electronic transactions.

European Commission

# Signature/Seal formats

## ETSI EN 319 122-1 V1.2.1 (2021-10)



EUROPEAN STANDARD

Electronic Signatures and Infrastructures (ESI);
CAdES digital signatures;
Part 1: Building blocks and CAdES baseline signatures

## ETSI EN 319 122-2 V1.1.1 (2016-04)



EUROPEAN STANDARD

Electronic Signatures and Infrastructures (ESI);
CAdES digital signatures;
Part 2: Extended CAdES signatures

# Signature/Seal formats

| Signature fields / Attributes / Services | Presence in B-B level | Presence in B-T level | Presence in B-LT level | Presence in B-LTA level | Cardinality | References | Additional requirements and notes |
|---|---|---|---|---|---|---|---|
| `SignedData.certificates` | shall be present | shall be present | shall be present | shall be present | 1 | Clause 4.4 | a, b, c, d, e 2, 3, 4 |
| `content-type` | shall be present | shall be present | shall be present | shall be present | 1 | Clause 5.1.1 | f |
| `message-digest` | shall be present | shall be present | shall be present | shall be present | 1 | Clause 5.1.2 | |
| Service: protection of signing certificate | shall be provided | shall be provided | shall be provided | shall be provided | 1 | Clause 5.2.2 | |
| SPO: ESS `signing-certificate` | conditioned presence | conditioned presence | conditioned presence | conditioned presence | 0 or 1 | Clause 5.2.2.2 | g, h, j |
| SPO: ESS `signing-certificate-v2` | conditioned presence | conditioned presence | conditioned presence | conditioned presence | 0 or 1 | Clause 5.2.2.3 | g, i, j |
| `signing-time` | shall be present | shall be present | shall be present | shall be present | 1 | Clause 5.2.1 | |
| `commitment-type-indication` | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.2.3 | |
| Service: identifying the signed data type | should be present | should be present | should be present | should be present | 0 or 1 | Clause 5.2.4 | t, 6,7 |
| SPO: `content-hints` | conditioned presence | conditioned presence | conditioned presence | conditioned presence | 0 or 1 | Clause 5.2.4.1 | |
| SPO: `mime-type` | conditioned presence | conditioned presence | conditioned presence | conditioned presence | 0 or 1 | Clause 5.2.4.2 | |
| `signer-location` | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.2.5 | |
| `signer-attributes-v2` | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.2.6.1 | |
| `countersignature` | may be present | may be present | may be present | may be present | ≥ 0 | Clause 5.2.7 | |
| `content-time-stamp` | may be present | may be present | may be present | may be present | ≥ 0 | Clause 5.2.8 | 5 |
| `signature-policy-identifier` | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.2.9.1 | |
| `signature-policy-store` | conditioned presence | conditioned presence | conditioned presence | conditioned presence | 0 or 1 | Clause 5.2.10 | k |
| `content-reference` | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.2.11 | |
| `content-identifier` | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.2.12 | |
| `cms-algorithm-protection` | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.2.13 | 8 |
| `signature-time-stamp` | * | shall be present | shall be present | shall be present | ≥ 1 | Clause 5.3 | l, m, 5 |

# Signature/Seal formats

| Signature fields / Attributes / Services | Presence in B-B level | Presence in B-T level | Presence in B-LT level | Presence in B-LTA level | Cardinality | References | Additional requirements and notes |
|---|---|---|---|---|---|---|---|
| certificate-values | * | * | shall not be present | shall not be present | B-B, B-T: 0 or 1<br>B-LT, B-LTA: 0 | Clause A.1.1.2 | |
| complete-certificate-references | * | * | shall not be present | shall not be present | B-B, B-T: 0 or 1<br>B-LT, B-LTA: 0 | Clause A.1.1.1 | g |
| revocation-values | * | * | shall not be present | shall not be present | B-B, B-T : 0 or 1<br>B-LT, B-LTA: 0 | Clause A.1.2.2 | |
| complete-revocation-references | * | * | shall not be present | shall not be present | B-B, B-T: 0 or 1<br>B-LT, B-LTA: 0 | Clause A.1.2.1 | |
| attribute-certificate-references | * | * | shall not be present | shall not be present | B-B, B-T : 0 or 1<br>B=LT, B=LTA: 0 | Clause A.1.3 | j, n |
| attribute-revocation-references | * | * | shall not be present | shall not be present | B-B, B-T: 0 or 1<br>B-LT, B-LTA: 0 | Clause A.1.4 | n |
| CAdES-C-timestamp | * | * | shall not be present | shall not be present | B-B, B-T: ≥ 0<br>B-LT, B-LTA: 0 | Clause A.1.5.2 | 5 |
| time-stamped-certs-crls-references | * | * | shall not be present | shall not be present | B-B, B-T: ≥ 0<br>B-LT, B-LTA: 0 | Clause A.1.5.1 | 5 |
| Service: revocation values in long-term validation | * | * | shall be provided | shall be provided | 1 | | o, p |
| SPO: SignedData.crls.crl | * | * | conditioned presence | conditioned presence | 0 or 1 | Clause 4.4 | q |
| SPO: SignedData.crls.other | * | * | conditioned presence | conditioned presence | 0 or 1 | Clause 4.4 | r |
| archive-time-stamp-v3 | * | * | * | shall be provided | ≥ 1 | Clause 5.5.3 | s |

European Commission

# Signature/Seal formats

## ETSI EN 319 132-1 V1.2.1 (2022-02)



**EUROPEAN STANDARD**

Electronic Signatures and Infrastructures (ESI);
XAdES digital signatures;
Part 1: Building blocks and XAdES baseline signatures

## ETSI EN 319 132-2 V1.1.1 (2016-04)



**EUROPEAN STANDARD**

Electronic Signatures and Infrastructures (ESI);
XAdES digital signatures;
Part 2: Extended XAdES signatures

# Signature/Seal formats

| Elements/Qualifying properties/Services | Presence in B-B level | Presence in B-T level | Presence in B-LT level | Presence in B-LTA level | Cardinality | References | Additional requirements and notes |
|---|---|---|---|---|---|---|---|
| ds:KeyInfo/X509Data | shall be present | shall be present | shall be present | shall be present | 1 | XMLDSIG [1], clause 4.5.4 | a, b, c 3, 4, 5 |
| ds:SignedInfo/ds:CanonicalizationMethod | shall be present | shall be present | shall be present | shall be present | 1 | XMLDSIG [1], clause 4.4.1 | d, e 6 |
| ds:Reference | shall be present | shall be present | shall be present | shall be present | ≥ 2 | XMLDSIG [1], clause 4.4.3 | |
| ds:Reference/ds:Transforms | may be present | may be present | may be present | may be present | 0 or 1 | XMLDSIG [1], clause 4.4.3.4 | f, g |
| SigningTime | shall be present | shall be present | shall be present | shall be present | 1 | Clause 5.2.1 | h |
| SigningCertificateV2 | shall be present | shall be present | shall be present | shall be present | 1 | Clause 5.2.2 | i, j 7 |
| SigningCertificate | shall not be present | shall not be present | shall not be present | shall not be present | 0 | - | |
| DataObjectFormat | conditioned presence | conditioned presence | conditioned presence | conditioned presence | ≥ 0 | Clause 5.2.4 | k |
| DataObjectFormat/Description | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.2.4 | l 8 |
| DataObjectFormat/ObjectIdentifier | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.2.4 | l |
| DataObjectFormat/MimeType | shall be present | shall be present | shall be present | shall be present | 1 | Clause 5.2.4 | l |
| DataObjectFormat/Encoding | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.2.4 | l |

European Commission

# Signature/Seal formats

| Elements/Qualifying properties/Services | Presence in B-B level | Presence in B-T level | Presence in B-LT level | Presence in B-LTA level | Cardinality | References | Additional requirements and notes |
|---|---|---|---|---|---|---|---|
| DataObjectFormat's ObjectReference attribute | shall be present | shall be present | shall be present | shall be present | 1 | Clause 5.2.4 | l |
| SignerRole | shall not be present | shall not be present | shall not be present | shall not be present | 0 | - | |
| SignerRoleV2 | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.2.6 | |
| CommitmentTypeIndication | may be present | may be present | may be present | may be present | ≥ 0 | Clause 5.2.3 | |
| SignatureProductionPlaceV2 | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.2.5 | |
| SignatureProductionPlace | shall not be present | shall not be present | shall not be present | shall not be present | 0 | - | |
| CounterSignature | may be present | may be present | may be present | may be present | ≥ 0 | Clause 5.2.7.2 | |
| AllDataObjectsTimeStamp | may be present | may be present | may be present | may be present | ≥ 0 | Clause 5.2.8.2 | 10 |
| IndividualDataObjectsTimeStamp | may be present | may be present | may be present | may be present | ≥ 0 | Clause 5.2.8.1 | 10 |
| SignaturePolicyIdentifier | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.2.9 | |
| SignaturePolicyStore | conditioned presence | conditioned presence | conditioned presence | conditioned presence | 0 or 1 | Clause 5.2.10 | m |
| SignatureTimeStamp | * | shall be present | shall be present | shall be present | B-B: ≥ 0 B-T, B-LT, B-LTA: ≥ 1 | Clause 5.3 | n, o 10 |
| CertificateValues | * | * | conditioned presence | conditioned presence | 0 or 1 | Clause 5.4.1 | p, q |
| CompleteCertificateRefsV2 | * | * | shall not be present | shall not be present | B-B, B-T: 0 or 1 B-LT, B-LTA: 0 | Clause A.1.1 | j |
| CompleteCertificateRefs | shall not be present | shall not be present | shall not be present | shall not be present | 0 | - | |
| AttrAuthoritiesCertValues | * | * | conditioned presence | conditioned presence | 0 or 1 | Clause 5.4.3 | q, r |
| AttributeCertificateRefsV2 | * | * | shall not be present | shall not be present | B-B, B-T: 0 or 1 B-LT, B-LTA: 0 | Clause A.1.3 | j, s |
| AttributeCertificateRefs | shall not be present | shall not be present | shall not be present | shall not be present | 0 | - | |
| RevocationValues | * | * | conditioned presence | conditioned presence | 0 or 1 | Clause 5.4.2 | t, u, v, |
| CompleteRevocationRefs | * | * | shall not be present | shall not be present | B-B, B-T: 0 or 1 B-LT, B-LTA: 0 | Clause A.1.2 | |
| AttributeRevocationValues | * | * | conditioned presence | conditioned presence | 0 or 1 | Clause 5.4.4 | v, w |
| AttributeRevocationRefs | * | * | shall not be present | shall not be present | B-B, B-T: 0 or 1 B-LT, B-LTA: 0 | Clause A.1.4 | s |

# Signature/Seal formats

| Elements/Qualifying properties/Services | Presence in B-B level | Presence in B-T level | Presence in B-LT level | Presence in B-LTA level | Cardinality | References | Additional requirements and notes |
|---|---|---|---|---|---|---|---|
| SigAndRefsTimeStampV2 | * | * | shall not be present | shall not be present | B-B, B-T: ≥ 0 <br> B-LT, B-LTA: 0 | Clause A.1.5.1 | |
| SigAndRefsTimeStamp | shall not be present | shall not be present | shall not be present | shall not be present | 0 | - | |
| RefsOnlyTimeStampV2 | * | * | shall not be present | shall not be present | B-B, B-T: ≥ 0 <br> B-LT, B-LTA: 0 | Clause A.1.5.2 | |
| RefsOnlyTimeStamp | shall not be present | shall not be present | shall not be present | shall not be present | 0 | - | |
| Service: Incorporation of validation data for electronic time-stamps | * | * | shall be provided | shall be provided | - | - | x, y 9 |
| SPO: TimeStampValidationData | * | * | conditioned presence | conditioned presence | ≥ 0 | Clause 5.5.1 | y |
| SPO: certificate and revocation values embedded in the electronic time-stamp itself | * | * | conditioned presence | conditioned presence | ≥ 0 | - | y |
| ArchiveTimeStamp (defined in namespace whose URI is "http://uri.etsi.org/01903/v1.4.1#") | * | * | * | shall be present | ≥ 1 | Clause 5.5.2 | z, aa |
| ArchiveTimeStamp (defined in namespace whose URI is "http://uri.etsi.org/01903/v1.3.2#") | shall not be present | shall not be present | shall not be present | shall not be present | 0 | - | |
| RenewedDigestsV2 | * | * | * | conditioned presence | ≥ 0 | Clause 5.5.3 | bb |

# Signature/Seal formats

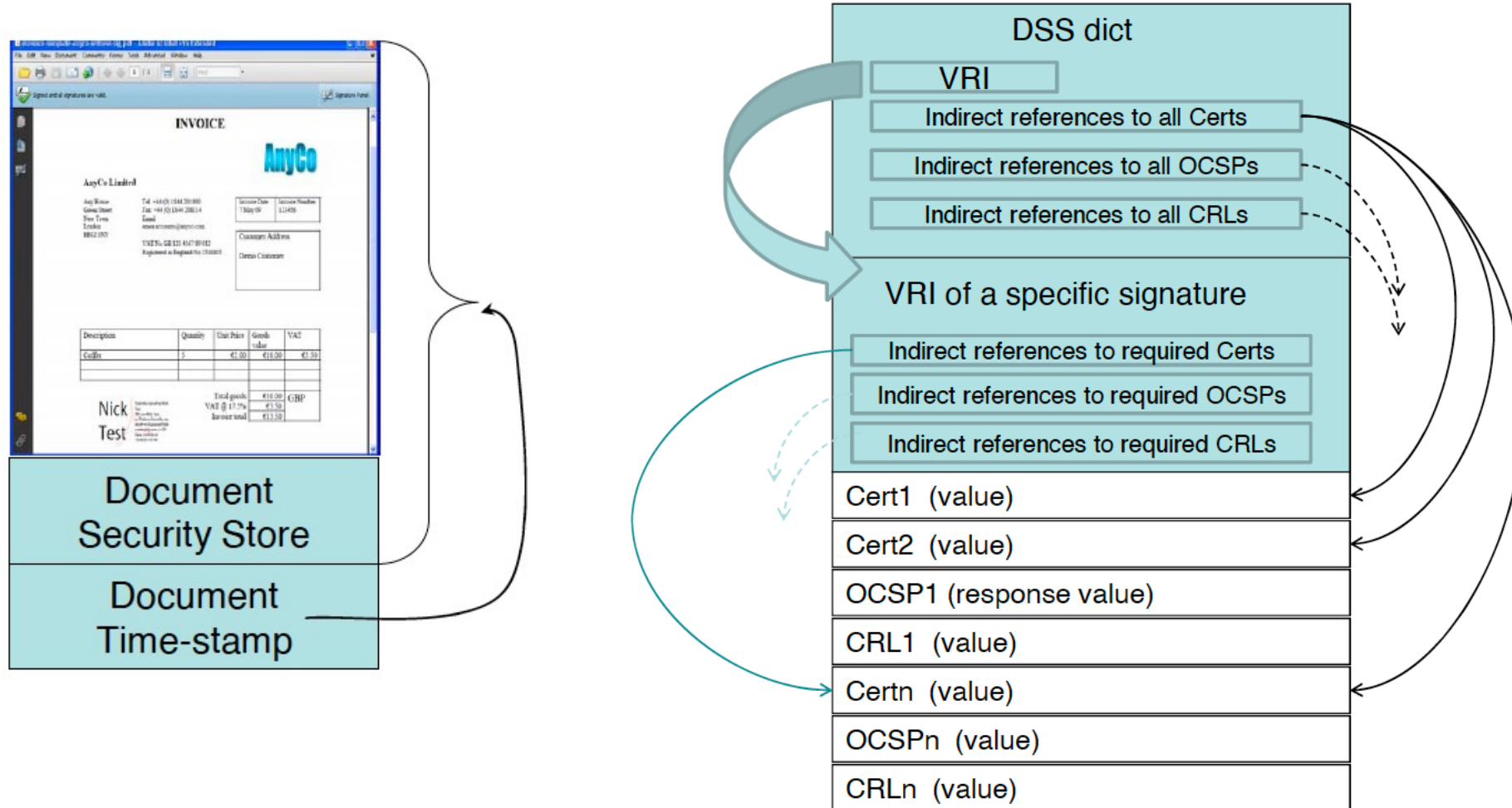## ETSI EN 319 142-1 V1.1.1 (2016-04)



**EUROPEAN STANDARD**

Electronic Signatures and Infrastructures (ESI);
PAdES digital signatures;
Part 1: Building blocks and PAdES baseline signatures

## ETSI EN 319 142-2 V1.1.1 (2016-04)



**EUROPEAN STANDARD**

Electronic Signatures and Infrastructures (ESI);
PAdES digital signatures;
Part 2: Additional PAdES signatures profiles

# Signature/Seal formats

# Signature/Seal formats

| Attributes / Fields / Services | Presence in B-B level | Presence in B-T level | Presence in B-LT level | Presence in B-LTA level | Cardinality | References | Additional requirements and notes |
|---|---|---|---|---|---|---|---|
| SignedData.certificates | shall be present | shall be present | shall be present | shall be present | 1 | IETF RFC 5652 [3], clause 5.1 | a, b, notes 1 and 2 |
| content-type | shall be present | shall be present | shall be present | shall be present | 1 | ETSI EN 319 122-1 [2], clause 5.1.1 | c |
| message-digest | shall be present | shall be present | shall be present | shall be present | 1 | ETSI EN 319 122-1 [2], clause 5.1.2 | - |
| signer-attributes-v2 | may be present | may be present | may be present | may be present | 0 or 1 | ETSI EN 319 122-1 [2], clause 5.2.6 | - |
| content-time-stamp | may be present | may be present | may be present | may be present | ≥ 0 | ETSI EN 319 122-1 [2], clause 5.2.8 | - |
| signature-policy-identifier | may be present | may be present | may be present | may be present | 0 or 1 | ETSI EN 319 122-1 [2], clause 5.2.9 | - |
| commitment-type-indication | conditioned presence | conditioned presence | conditioned presence | conditioned presence | 0 or 1 | ETSI EN 319 122-1 [2], clause 5.2.3 | d |
| SERVICE: protection of signing certificate | shall be provided | shall be provided | shall be provided | shall be provided | - | - | e, f |
| SPO: ESS signing-certificate | conditioned presence | conditioned presence | conditioned presence | conditioned presence | 0 or 1 | ETSI EN 319 122-1 [2], clause 5.2.2.2 | - |
| SPO: ESS signing-certificate-v2 | conditioned presence | conditioned presence | conditioned presence | conditioned presence | 0 or 1 | ETSI EN 319 122-1 [2], clause 5.2.2.3 | - |
| Service: provide claimed time of signing | shall be provided | shall be provided | shall be provided | shall be provided | - | - | - |
| SPO: entry with the key *M* in the Signature Dictionary | shall be present | shall be present | shall be present | shall be present | 1 | ISO 32000-1 [1], clause 12.8.1 | g |
| SPO: signing-time attribute in CMS signature | shall not be present | shall not be present | shall not be present | shall not be present | 0 | - | - |
| entry with key *Contents* in the Signature Dictionary | shall be present | shall be present | shall be present | shall be present | 1 | ISO 32000-1 [1], clause 12.8.1 | h, i |
| entry with key *Filter* in the Signature Dictionary | shall be present | shall be present | shall be present | shall be present | 1 | ISO 32000-1 [1], clause 12.8.1 | j |
| entry with key *ByteRange* in the Signature Dictionary | shall be present | shall be present | shall be present | shall be present | 1 | ISO 32000-1 [1], clause 12.8.1 | k |
| entry with key *SubFilter* in the Signature Dictionary | shall be present | shall be present | shall be present | shall be present | 1 | ISO 32000-1 [1], clause 12.8.1 | l |
| entry with key *Location* in the Signature Dictionary | may be present | may be present | may be present | may be present | 0 or 1 | ISO 32000-1 [1], clause 12.8.1 | - |
| entry with key *Reason* in the Signature Dictionary | conditioned presence | conditioned presence | conditioned presence | conditioned presence | 0 or 1 | ISO 32000-1 [1], clause 12.8.1 | m |
| entry with key *Name* in the Signature Dictionary | may be present | may be present | may be present | may be present | 0 or 1 | ISO 32000-1 [1], clause 12.8.1 | - |
| entry with key *ContactInfo* in the Signature Dictionary | may be present | may be present | may be present | may be present | 0 or 1 | ISO 32000-1 [1], clause 12.8.1 | - |

European Commission

# Signature/Seal formats

| Attributes / Fields / Services | Presence in B-B level | Presence in B-T level | Presence in B-LT level | Presence in B-LTA level | Cardinality | References | Additional requirements and notes |
|---|---|---|---|---|---|---|---|
| entry with key *Cert* in the Signature Dictionary | shall not be present | shall not be present | shall not be present | shall not be present | 0 | ISO 32000-1 [1], clause 12.8.1 | - |
| SERVICE: provide trusted time for existence of the signature | * | shall be provided | shall be provided | shall be provided | - | - | n |
| SPO: signature-time-stamp | * | conditioned presence | conditioned presence | conditioned presence | ≥ 0 | ETSI EN 319 122-1 [2], clause 5.3 | o, p, q |
| SPO: document-time-stamp | * | conditioned presence | conditioned presence | conditioned presence | ≥ 0 | clause 5.4.3 | |
| SERVICE: provide certificate and revocation values | * | * | shall be provided | shall be provided | - | - | - |
| SPO: DSS | * | * | shall be present | shall be present | B-B, -T: ≥ 0 <br> B-LT, -LTA: ≥ 1 | clause 5.4.2.2 | r, s, t, u, v |
| SPO: DSS / VRI | * | * | conditioned presence | conditioned presence | ≥ 0 | clause 5.4.2.3 | - |
| SERVICE: provide trusted time for existence of the validation data | * | * | * | shall be provided | - | - | note 3 |
| SPO: document-time-stamp | * | * | * | shall be present | B-B, -T, -LT: ≥ 0 <br> B-LTA: ≥ 1 | clause 5.4.3 | w, x, y |

European Commission

# Signature/Seal formats

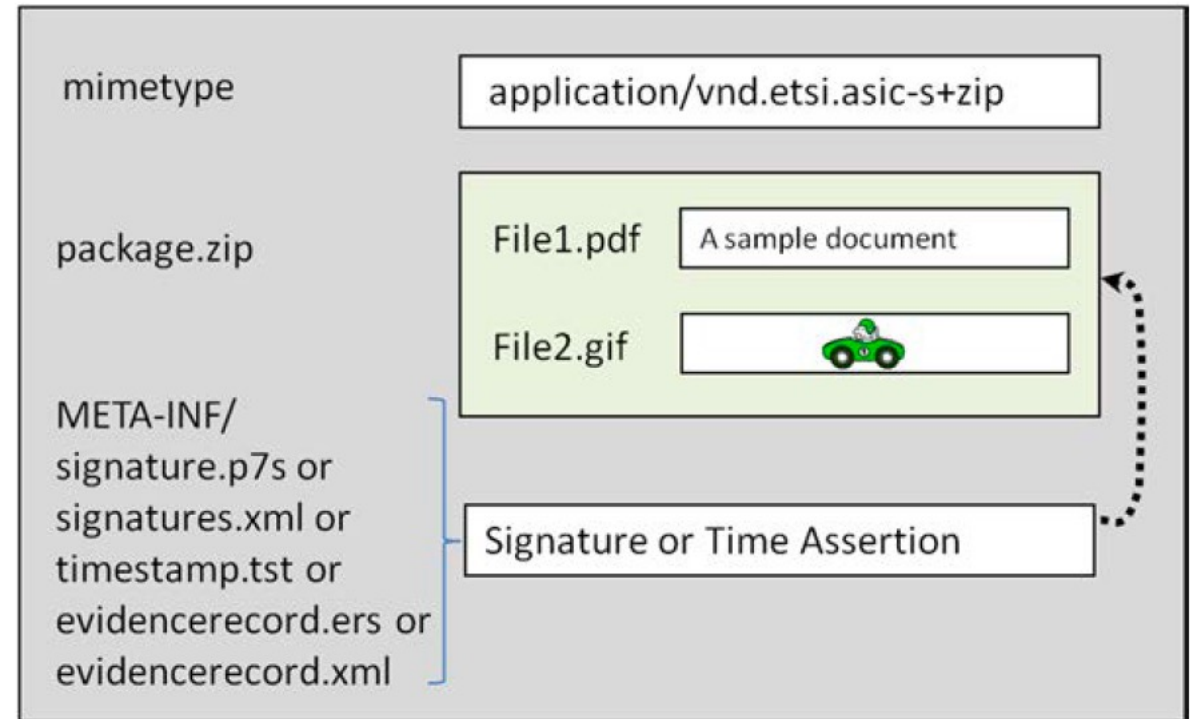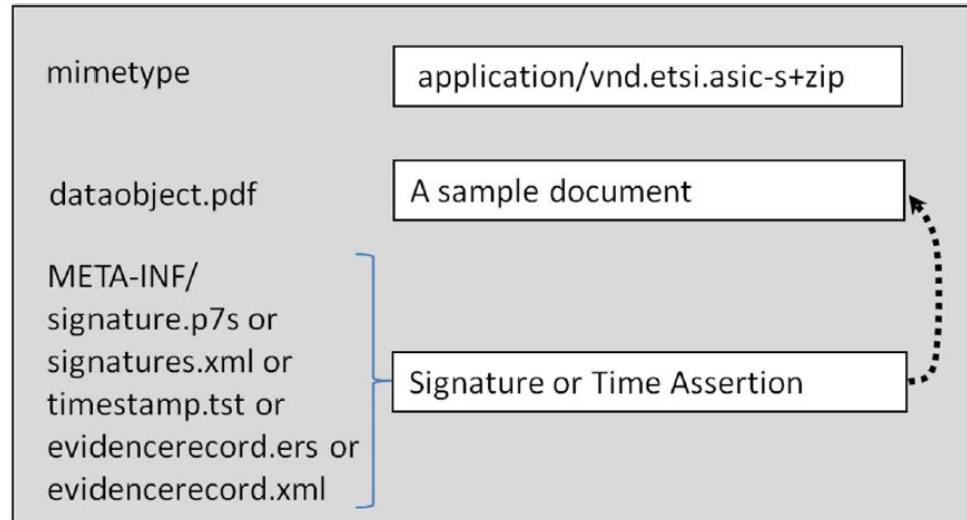## ETSI EN 319 162-1 V1.1.1 (2016-04)



**EUROPEAN STANDARD**

**Electronic Signatures and Infrastructures (ESI);
Associated Signature Containers (ASiC);
Part 1: Building blocks and ASiC baseline containers**

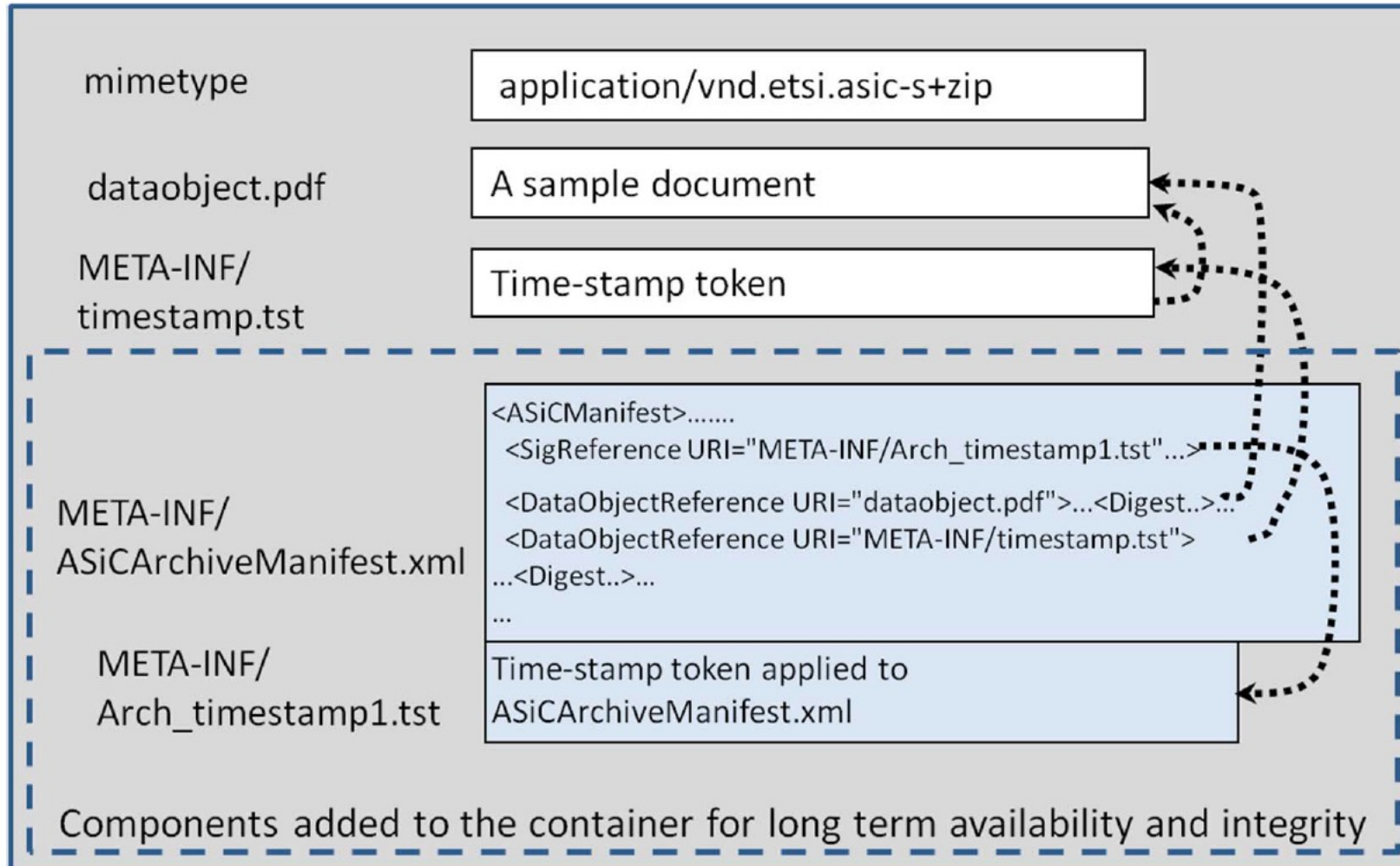## ETSI EN 319 162-2 V1.1.1 (2016-04)



**EUROPEAN STANDARD**

**Electronic Signatures and Infrastructures (ESI);
Associated Signature Containers (ASiC);
Part 2: Additional ASiC containers**

# Signature/Seal formats

# Signature/Seal formats

# Signature/Seal formats

| Header parameters/Elements in `etsiU` unsigned header parameter/Services | Presence in B-B level | Presence in B-T level | Presence in B-LT level | Presence in B-LTA level | Cardinality | References | Additional requirements and notes |
|---|---|---|---|---|---|---|---|
| `alg` | shall be present | shall be present | shall be present | shall be present | 1 | Clause 5.1.2 | |
| `cty` | conditioned presence | conditioned presence | conditioned presence | conditioned presence | 0 or 1 | Clause 5.1.3 | 2 |
| `kid` | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.1.4 | |
| `x5u` | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.1.5 | |
| `x5c` | Conditioned presence | Conditioned presence | Conditioned presence | Conditioned presence | 0 or 1 | Clause 5.1.8 | 3 |
| `crit` | Conditioned presence | Conditioned presence | Conditioned presence | Conditioned presence | | Clause 5.1.9 | 4 |
| `sigT` | shall be present | shall be present | shall be present | shall be present | 1 | Clause 5.2.1 | a |
| Service: signing a reference of the signing certificate | Conditioned presence | Conditioned presence | Conditioned presence | Conditioned presence | 1 | | 3 |
| SPO: `x5t#256` | conditioned presence | conditioned presence | conditioned presence | conditioned presence | 0 or 1 | Clause 5.1.7 | |
| SPO: `x5t#o` | conditioned presence | conditioned presence | conditioned presence | conditioned presence | 0 or 1 | Clause 5.2.2 | |
| SPO: `sigX5ts` | conditioned presence | conditioned presence | conditioned presence | conditioned presence | 0 or 1 | Clause 5.2.2 | |
| `sigD` | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.2.8 | |
| `srAts` | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.2.5 | |
| `srCms` | may be present | may be present | may be present | may be present | ≥ 0 | Clause 5.2.3 | |
| `sigPl` | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.2.4 | |
| `sigPId` | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.2.7 | |
| `cSig` | may be present | may be present | may be present | may be present | ≥ 0 | Clause 5.3.2 | |
| `adoTst` | may be present | may be present | may be present | may be present | ≥ 0 | Clause 5.3.3 | 5 |
| `sigPSt` | may be present | may be present | may be present | may be present | 0 or 1 | Clause 5.3.3 | b |
| `sigTst` | * | shall be present | shall be present | shall be present | B-B: ≥ 0 <br> B-T, B-LT, B-LTA: ≥ 1 | Clause 5.3.4 | c, d 5 |
| `xVals` | * | * | conditioned presence | conditioned presence | 0 or 1 | Clause 5.3.5.1 | e, 6 |
| `xRefs` | * | * | shall not be present | shall not be present | B-B, B-T: 0 or 1 <br> B-LT, B-LTA: 0 | Clause A.1.1 | f, g |
| `axVals` | * | * | conditioned presence | conditioned presence | 0 or 1 | Clause 5.3.5.3 | e, 7 |
| `axRefs` | * | * | shall not be present | shall not be present | B-B, B-T: 0 or 1 <br> B-LT, B-LTA: 0 | Clause A.1.3 | f, g, h |

# Signature/Seal formats

| Header parameters/Elements in `etsiU` unsigned header parameter/Services | Presence in B-B level | Presence in B-T level | Presence in B-LT level | Presence in B-LTA level | Cardinality | References | Additional requirements and notes |
|---|---|---|---|---|---|---|---|
| `rVals` | * | * | conditioned presence | conditioned presence | 0 or 1 | Clause 5.3.5.2 | i, 8 |
| `rRefs` | * | * | shall not be present | shall not be present | B-B, B-T: 0 or 1<br>B-LT, B-LTA: 0 | Clause A.1.2 | |
| `arVals` | * | * | conditioned presence | conditioned presence | 0 or 1 | Clause 5.3.5.4 | i, 9 |
| `arRefs` | * | * | shall not be present | shall not be present | B-B, B-T: 0 or 1<br>B-LT, B-LTA: 0 | Clause A.1.4 | h |
| `sigRTst` | * | * | shall not be present | shall not be present | B-B, B-T: ≥ 0<br>B-LT, B-LTA: 0 | Clause A.1.5.1 | |
| `rfsTst` | * | * | shall not be present | shall not be present | B-B, B-T: ≥ 0<br>B-LT, B-LTA: 0 | Clause A.1.5.2 | |
| Service: Incorporation of validation data for electronic time-stamps | * | * | shall be provided | shall be provided | - | - | j, k<br>10 |
| SPO: `tstVD` | * | * | conditioned presence | conditioned presence | ≥ 0 | Clause 5.3.6.1 | |
| SPO: certificate and revocation values embedded in the electronic time-stamp itself | * | * | conditioned presence | conditioned presence | ≥ 0 | - | |
| `arcTst` | * | * | * | shall be present | ≥ 1 | Clause 5.3.6.2 | l, m |

# Signature/Seal preservation service



ETSI TS 119 511 V1.1.1 (2019-06)

TECHNICAL SPECIFICATION

**Electronic Signatures and Infrastructures (ESI);
Policy and security requirements for
trust service providers providing long-term preservation
of digital signatures or general data using
digital signature techniques**
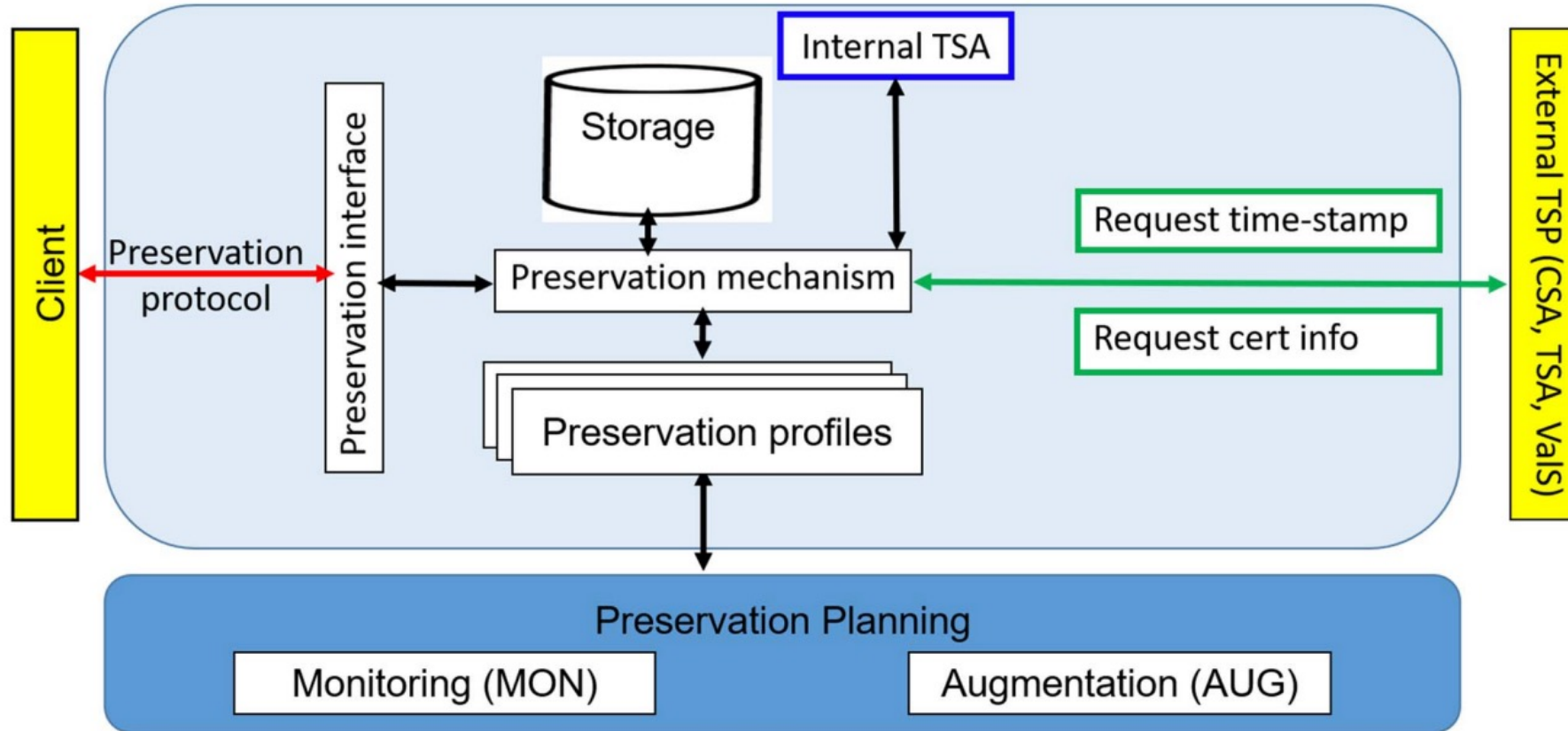
# Signature/Seal preservation service



Figure 1: Functional model of a preservation service with storage [WST]
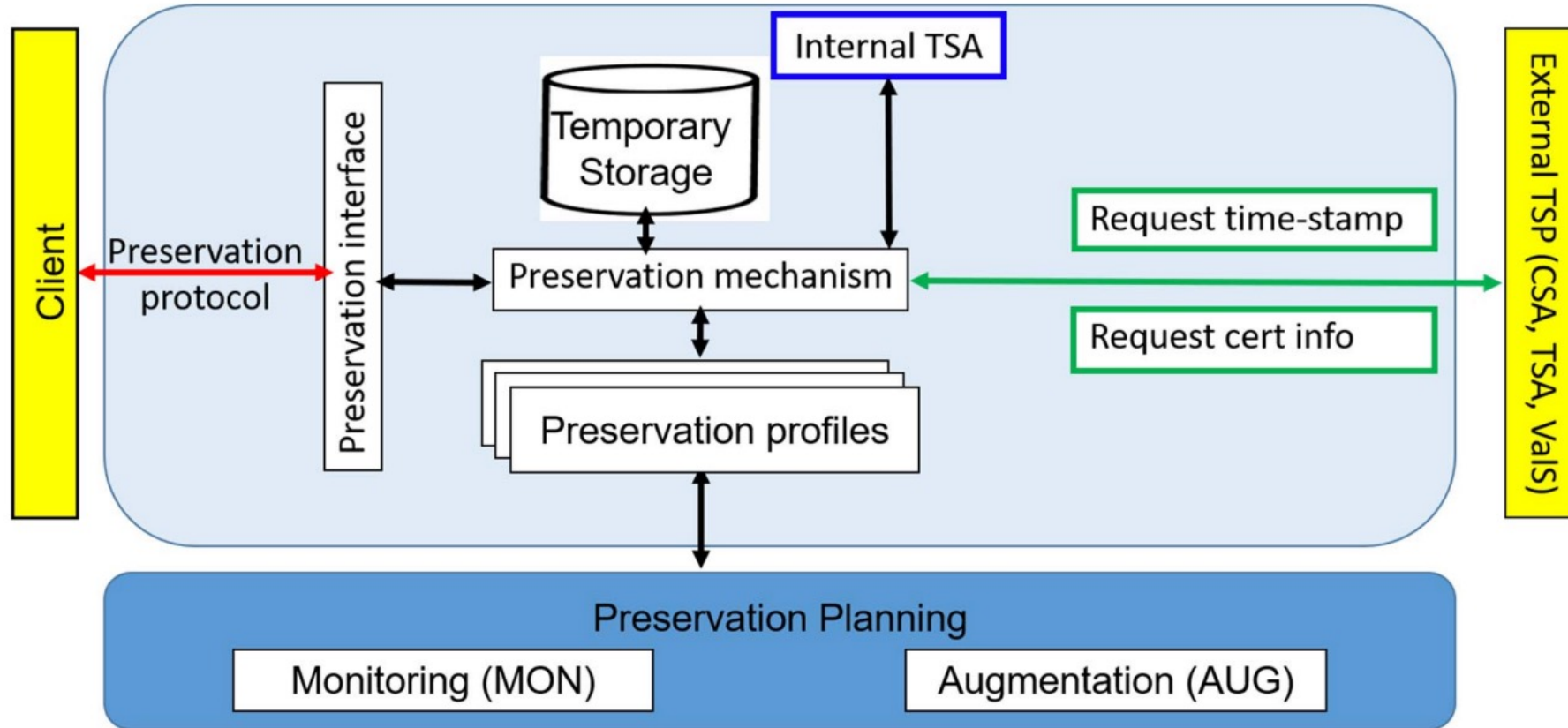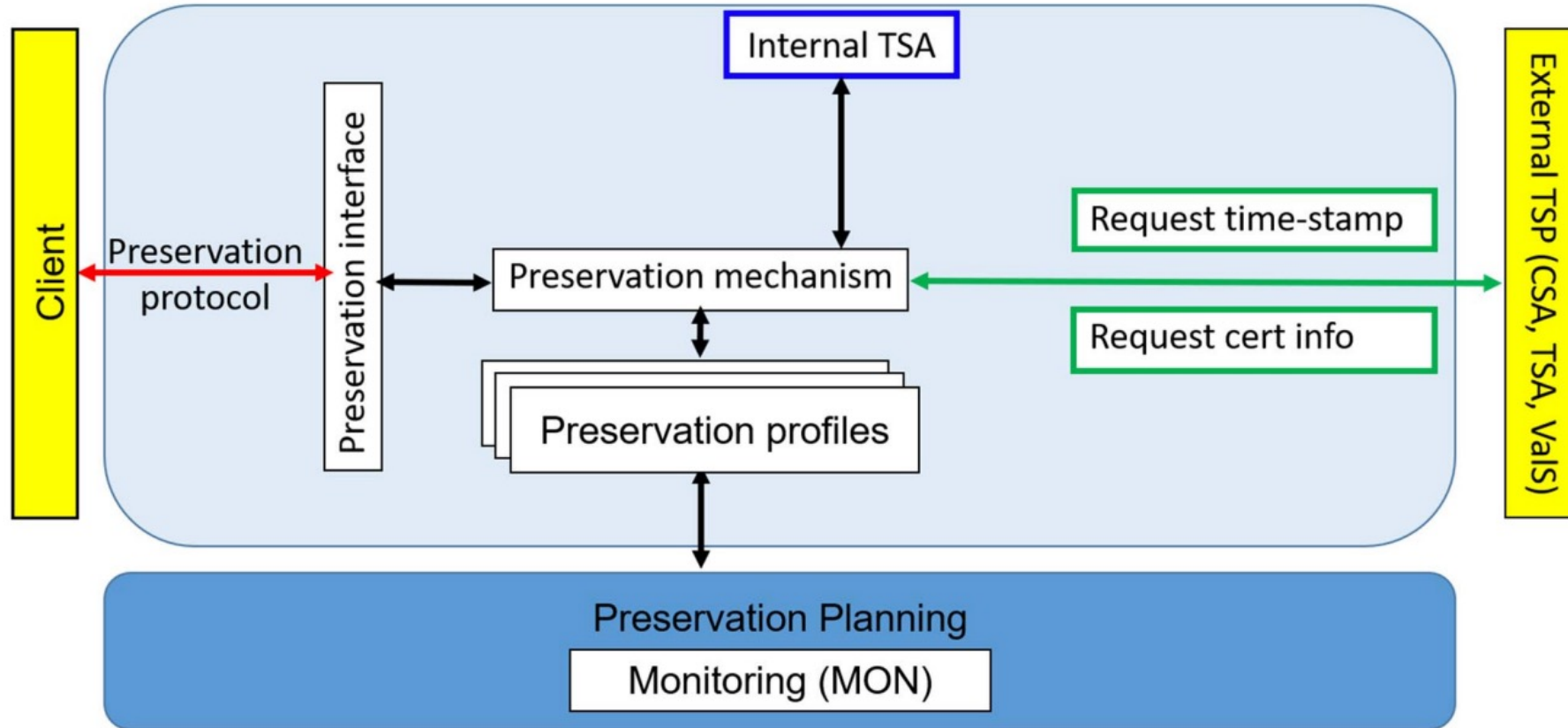
# Signature/Seal preservation service



Figure 2: Functional model of a preservation service with temporary storage [WTS]

# Signature/Seal preservation service



**Figure 3: Functional model of a preservation service without storage [WOS]**

# Signature/Seal preservation service

## C.3 Comparison of archival services with preservation services

For a digital archival service, the demonstration of a proof of existence can be based on an audit of the archival service against some criteria, e.g. ISO 14721:2012 [i.16], ISO 16363 [i.17], ISO 14641-1:2018 [i.15] or other similar norms.

For a preservation service as defined in the present document, the demonstration of a proof of existence will be based on two factors:

1) an audit of the Preservation service against some criteria, e.g. the present document; and

2) the use of digital signature techniques to demonstrate that some data has not been modified since a given date.

A digital archival service may use digital signature techniques to provide proofs of existence for some data but is not required to use them.

A preservation service can be part of an archival service.

A difference between a preservation service and an archival service is that an archival service without a preservation service does not capture nor verify any validation data associated with a digital signature.

## C.4 Relationships between archival services and preservation services

A digital archival service can use a preservation service to provide proofs of existence of data based on digital signature techniques. It needs to manage all the metadata required by an archival service.

A preservation service with storage (WST) can use an archival service for the goal of storing data.

European Commission

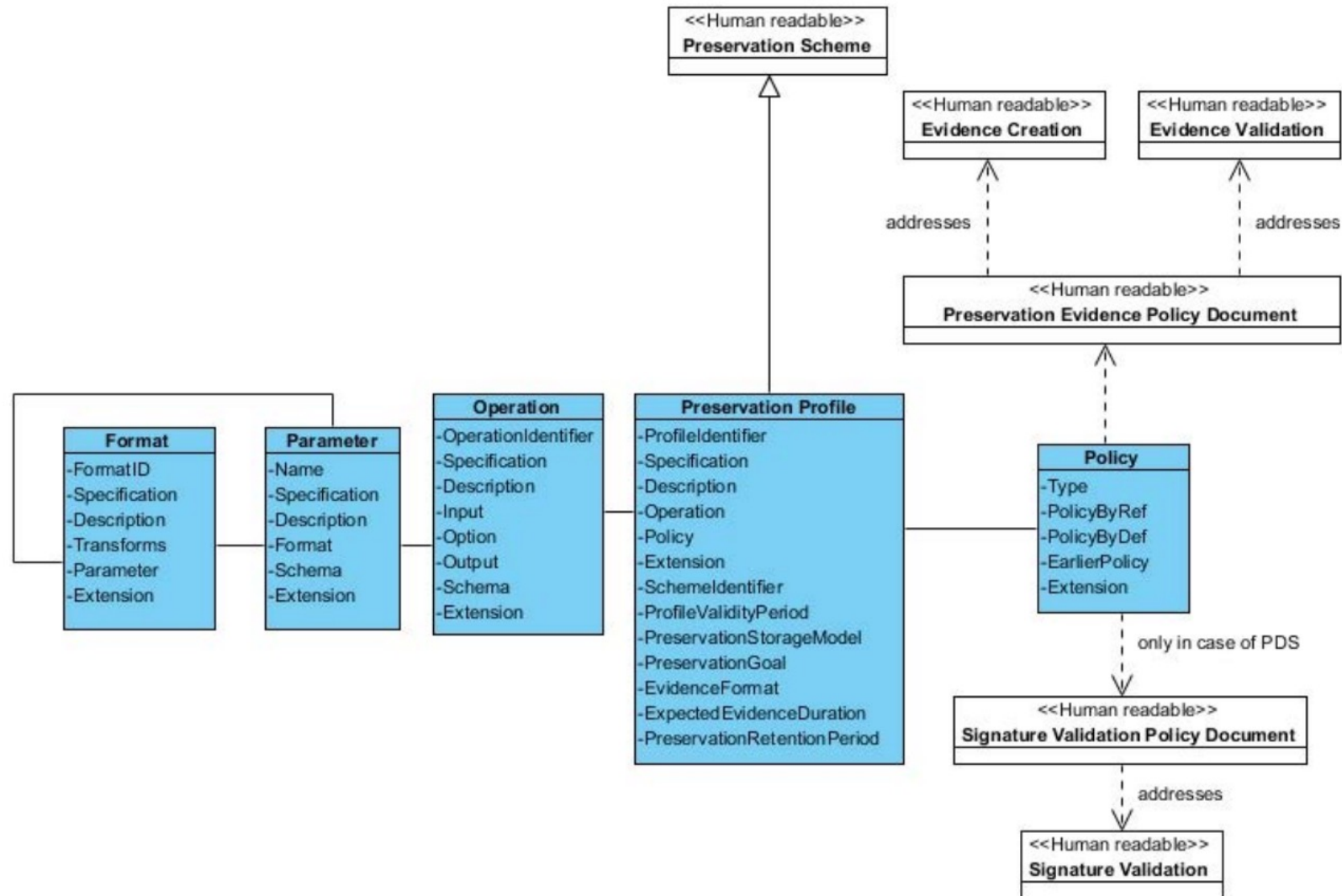# Signature/Seal preservation service



Figure 2: Relationship between preservation scheme, profile and policy

# Final remarks

- Maturity of the trust service (eIDAS Regulation) for the preservation of qualified electronic signatures or seals, with standards and products on the market.

- Emergence of national approaches aimed at regulating electronic archiving as a digital service, with a strictly technical vision.

- Reception and harmonization through regulation as a trust service in the eIDAS 2 Regulation, whose approval is expected by the end of 2023.

- New predictable offering service in the Cloud that helps, but does not displace, the function of archivists.

European Commission

# Thank you

European Commission