

# ETSI TS 119 512 V1.1.1 (2020-01)



## Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services

iTeh STANDARD PREVIEW  
(standards.iteh.ai)  
Full standard available at  
<https://standards.iteh.ai/catalog/standards/sis/119-512-v1.1.1-2020-01>  
4278-af7a-03d088b025d/etsi-ts-119-512-v1.1.1-2020-01

---

**Reference**

DTS/ESI-0019512

---

**Keywords**electronic preservation, electronic signature,  
protocol**ETSI**650 Route des Lucioles  
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° 7803/88

---

**Important notice**The present document can be downloaded from:  
<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at [www.etsi.org/deliver](http://www.etsi.org/deliver).

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at <https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:  
<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

---

**Copyright Notification**

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2020.  
All rights reserved.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.  
**3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

**oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners.

**GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

# Contents

Intellectual Property Rights .....	9
Foreword.....	9
Modal verbs terminology.....	9
Executive summary .....	9
Introduction .....	10
1 Scope .....	11
2 References .....	11
2.1 Normative references .....	11
2.2 Informative references.....	12
3 Definition of terms, symbols and abbreviations.....	13
3.1 Terms.....	13
3.2 Symbols.....	16
3.3 Abbreviations .....	16
4 General aspects.....	17
4.1 System architecture .....	17
4.2 Preservation goals.....	18
4.3 Storage models .....	18
4.3.1 Preservation with storage.....	18
4.3.2 Preservation with temporary storage.....	18
4.3.3 Preservation without storage.....	19
4.4 Preservation schemes, profile and policies.....	19
5 Technical Specification of Protocol .....	20
5.1 Introduction and Overview.....	20
5.2 Discovery of supported preservation profiles.....	21
5.3 Operation requests and responses.....	21
5.3.1 Basic types for requests and responses.....	21
5.3.1.1 Component Request .....	21
5.3.1.1.1 Semantics.....	21
5.3.1.1.2 XML Syntax .....	21
5.3.1.1.3 JSON Syntax .....	21
5.3.1.2 Component Response .....	21
5.3.1.2.1 Semantics.....	21
5.3.1.2.2 XML Syntax .....	22
5.3.1.2.3 JSON Syntax .....	22
5.3.2 RetrieveInfo .....	22
5.3.2.1 RetrieveInfo request .....	22
5.3.2.1.1 Semantics.....	22
5.3.2.1.2 XML Syntax .....	23
5.3.2.1.3 JSON Syntax .....	23
5.3.2.2 RetrieveInfoResponse.....	23
5.3.2.2.1 Semantics.....	23
5.3.2.2.2 XML Syntax .....	24
5.3.2.2.3 JSON Syntax .....	24
5.3.3 PreservePO .....	25
5.3.3.1 PreservePO request .....	25
5.3.3.1.1 Semantics.....	25
5.3.3.1.2 XML Syntax .....	25
5.3.3.1.3 JSON Syntax .....	25
5.3.3.2 PreservePOResponse.....	26
5.3.3.2.1 Semantics.....	26
5.3.3.2.2 XML Syntax .....	27
5.3.3.2.3 JSON Syntax .....	27

5.3.4	RetrievePO (Conditional) .....	27
5.3.4.1	RetrievePO Request .....	27
5.3.4.1.1	Semantics .....	27
5.3.4.1.2	XML Syntax .....	28
5.3.4.1.3	JSON Syntax .....	29
5.3.4.2	RetrievePOResponse .....	29
5.3.4.2.1	Semantics .....	29
5.3.4.2.2	XML Syntax .....	30
5.3.4.2.3	JSON Syntax .....	30
5.3.5	DeletePO (Conditional) .....	31
5.3.5.1	DeletePO Request .....	31
5.3.5.1.1	Semantics .....	31
5.3.5.1.2	XML Syntax .....	31
5.3.5.1.3	JSON Syntax .....	32
5.3.5.2	DeletePOResponse .....	32
5.3.6	UpdatePOC (Optional) .....	33
5.3.6.1	UpdatePOC Request .....	33
5.3.6.1.1	Semantics .....	33
5.3.6.1.2	XML Syntax .....	33
5.3.6.1.3	JSON Syntax .....	34
5.3.6.2	UpdatePOCResponse .....	34
5.3.6.2.1	Semantics .....	34
5.3.6.2.2	XML Syntax .....	35
5.3.6.2.3	JSON Syntax .....	35
5.3.7	RetrieveTrace (Optional) .....	36
5.3.7.1	RetrieveTrace request .....	36
5.3.7.1.1	Semantics .....	36
5.3.7.1.2	XML Syntax .....	36
5.3.7.1.3	JSON Syntax .....	36
5.3.7.2	RetrieveTraceResponse .....	37
5.3.7.2.1	Semantics .....	37
5.3.7.2.2	XML Syntax .....	37
5.3.7.2.3	JSON Syntax .....	38
5.3.8	ValidateEvidence (Optional) .....	38
5.3.8.1	ValidateEvidence Request .....	38
5.3.8.1.1	Semantics .....	38
5.3.8.1.2	XML Syntax .....	39
5.3.8.1.3	JSON Syntax .....	39
5.3.8.2	ValidateEvidenceResponse .....	39
5.3.8.2.1	Semantics .....	39
5.3.8.2.2	XML Syntax .....	40
5.3.8.2.3	JSON Syntax .....	40
5.3.9	Search (Optional) .....	41
5.3.9.1	Search request .....	41
5.3.9.1.1	Semantics .....	41
5.3.9.1.2	XML Syntax .....	41
5.3.9.1.3	JSON Syntax .....	42
5.3.9.2	SearchResponse .....	42
5.3.9.2.1	Semantics .....	42
5.3.9.2.2	XML Syntax .....	43
5.3.9.2.3	JSON Syntax .....	43
5.4	Components for operations .....	44
5.4.1	Overview .....	44
5.4.2	Component DeletionMode .....	44
5.4.2.1	Semantics .....	44
5.4.2.2	XML Syntax .....	44
5.4.2.3	JSON Syntax .....	44
5.4.3	Component Event .....	45
5.4.3.1	Semantics .....	45
5.4.3.2	XML Syntax .....	45
5.4.3.3	JSON Syntax .....	46

5.4.4	Component Evidence.....	46
5.4.4.1	Semantics .....	46
5.4.4.2	XML Syntax.....	47
5.4.4.3	JSON Syntax .....	47
5.4.5	Component PO.....	48
5.4.5.1	Semantics .....	48
5.4.5.2	XML Syntax.....	48
5.4.5.3	JSON Syntax.....	49
5.4.6	Component PreservationStorageModel .....	50
5.4.6.1	Semantics .....	50
5.4.6.2	XML Syntax.....	50
5.4.6.3	JSON Syntax.....	50
5.4.7	Component Profile.....	50
5.4.7.1	Semantics .....	50
5.4.7.2	XML Syntax.....	52
5.4.7.3	JSON Syntax.....	53
5.4.8	Component Status .....	54
5.4.8.1	Semantics .....	54
5.4.8.2	XML Syntax.....	54
5.4.8.3	JSON Syntax.....	54
5.4.9	Component SubjectOfRetrieval.....	55
5.4.9.1	Semantics .....	55
5.4.9.2	XML Syntax.....	55
5.4.9.3	JSON Syntax .....	55
5.4.10	Component Trace.....	56
5.4.10.1	Semantics .....	56
5.4.10.2	XML Syntax.....	56
5.4.10.3	JSON Syntax.....	56
5.5	Components for ASiC extensions .....	57
5.5.1	Overview and motivation.....	57
5.5.2	Extensions for ASiCManifest .....	57
5.5.2.1	ContainerID Extension .....	57
5.5.2.1.1	Semantics.....	57
5.5.2.1.2	Syntax.....	57
5.5.2.1.3	Criticality.....	57
5.5.2.2	PreservationPeriod Extension.....	57
5.5.2.2.1	Semantics.....	57
5.5.2.2.2	Syntax.....	58
5.5.2.2.3	Criticality.....	58
5.5.2.3	PreservationSubmitter Extension.....	58
5.5.2.3.1	Semantics.....	58
5.5.2.3.2	Syntax.....	58
5.5.2.3.3	Criticality.....	58
5.5.2.4	IsUpdatedVersionOf Extension.....	58
5.5.2.4.1	Semantics.....	58
5.5.2.4.2	Syntax.....	58
5.5.2.4.3	Criticality.....	58
5.5.2.5	CanonicalizationMethod Extension .....	58
5.5.2.5.1	Semantics.....	58
5.5.2.5.2	Syntax.....	59
5.5.2.5.3	Criticality.....	59
5.5.2.6	ValidationReport Extension.....	59
5.5.2.6.1	Semantics.....	59
5.5.2.6.2	Syntax.....	59
5.5.2.6.3	Criticality.....	59
5.5.3	Extensions for DataObjectReference.....	59
5.5.3.1	IsMetaDataOf Extension .....	59
5.5.3.1.1	Semantics.....	59
5.5.3.1.2	Syntax.....	59
5.5.3.1.3	Criticality.....	59

5.6	Components for other preservation object formats .....	60
5.6.1	Component DigestList .....	60
5.6.1.1	Semantics .....	60
5.6.1.2	XML Syntax .....	60
5.6.1.3	JSON Syntax .....	60
6	Requirements for preservation object data formats .....	61
6.1	General aspects and requirements .....	61
6.2	Specific requirements for preservation object containers .....	61
7	Requirements for preservation schemes .....	62
<b>Annex A (normative): Preservation object formats .....</b>		<b>63</b>
A.1	Submission data object formats .....	63
A.1.1	CADES digital signature according to ETSI EN 319 122-1 .....	63
A.1.2	XAdES digital signature according to ETSI EN 319 132-1 .....	63
A.1.3	PAdES digital signature according to ETSI EN 319 142-1 .....	63
A.1.4	Associated Signature Container Extended (ASiC-E) .....	63
A.1.5	XML-based Archival Information Package (XAIP) .....	63
A.1.6	DigestList as submission data object format .....	63
A.2	Preservation evidence formats .....	64
A.2.1	Time-stamp Token according to IETF RFC 3161 .....	64
A.2.2	Evidence Record according to IETF RFC 4998 .....	64
A.2.3	Evidence Record according to IETF RFC 6283 .....	64
A.2.4	CADES Archive Time Stamp V3 according to ETSI EN 319 122-1 .....	64
A.2.5	XAdES Archive Time Stamp according to ETSI EN 319 132-1 .....	64
A.2.6	PAdES Document Time-Stamp according to ETSI EN 319 142-1 .....	64
A.3	Additional input and/or output data object formats .....	65
A.3.1	ASiC with Evidence Records (ASiC-ERS) .....	65
A.3.1.1	Unique Identifier .....	65
A.3.1.2	Published Specification .....	65
A.3.1.3	ASiC-ERS is a profile of ASiC-E .....	65
A.3.1.4	Fulfilment of requirements and other considerations .....	66
A.3.1.4.1	Overview and motivation .....	66
A.3.1.4.2	Data objects .....	66
A.3.1.4.3	Additional attributes .....	66
A.3.1.4.4	Preservation evidence .....	66
A.3.1.4.5	Local identifiers .....	66
A.3.1.4.6	Versioning .....	66
A.3.1.4.7	Privacy considerations .....	67
A.3.1.4.8	Validation reports .....	67
A.3.1.4.9	Security considerations .....	67
A.3.1.4.10	Interoperability considerations .....	67
A.3.2	XML-based Archival Information Package (XAIP) .....	67
A.3.2.1	Unique Identifier .....	67
A.3.2.2	Published Specification .....	68
A.3.2.3	Main component (XAIP) .....	68
A.3.2.3.1	Semantics .....	68
A.3.2.3.2	Syntax .....	68
A.3.2.4	Sub-components .....	69
A.3.2.5	Fulfilment of requirements and other considerations .....	69
A.3.2.5.1	Overview and motivation .....	69
A.3.2.5.2	Data objects .....	69
A.3.2.5.3	Additional attributes .....	69
A.3.2.5.4	Preservation evidence .....	69
A.3.2.5.5	Local identifiers .....	69
A.3.2.5.6	Versioning .....	69
A.3.2.5.7	Privacy considerations .....	70
A.3.2.5.8	Validation reports .....	70
A.3.2.5.9	Security considerations .....	70

<b>Annex B (normative):</b>	<b>WSDL Document</b> .....	<b>71</b>
<b>Annex C (normative):</b>	<b>XML Schema Document</b> .....	<b>72</b>
C.1	XML Schema file location for namespace <a href="http://uri.etsi.org/19512/v1.1.1#">http://uri.etsi.org/19512/v1.1.1#</a> .....	72
C.2	XML Schema file location for namespace <a href="http://uri.etsi.org/19512/exchange/v1.1.1#">http://uri.etsi.org/19512/exchange/v1.1.1#</a> .....	72
<b>Annex D (normative):</b>	<b>JSON Schema and OpenAPI Documents</b> .....	<b>73</b>
D.1	JSON Schema file .....	73
D.2	OpenAPI specification .....	73
<b>Annex E (informative):</b>	<b>Versioning of a Preservation Object Container</b> .....	<b>74</b>
<b>Annex F (normative):</b>	<b>Preservation schemes</b> .....	<b>77</b>
F.1	Preservation scheme with storage based on evidence records .....	77
F.1.1	Identifier .....	77
F.1.2	Preservation goal(s) .....	77
F.1.3	Preservation storage model .....	77
F.1.4	Supported operations .....	77
F.1.4.1	Mandatory operations .....	77
F.1.4.2	Optional operations .....	77
F.1.4.3	Announcement of supported operations .....	78
F.1.5	Generation and validation of preservation evidences .....	78
F.1.6	Augmentation of preservation evidences .....	78
F.1.7	Requirements and recommendations for preservation profiles .....	78
F.2	Preservation scheme with temporary storage based on evidence records .....	79
F.2.1	Identifier .....	79
F.2.2	Preservation goal(s) .....	79
F.2.3	Preservation storage model .....	80
F.2.4	Supported operations .....	80
F.2.4.1	Mandatory operations .....	80
F.2.4.2	Optional operations .....	80
F.2.4.3	Announcement of supported operations .....	80
F.2.5	Generation and validation of preservation evidences .....	80
F.2.6	Augmentation of preservation evidences .....	81
F.2.7	Requirements and recommendations for preservation profiles .....	81
F.3	Preservation scheme with signature augmentation and with storage .....	82
F.3.1	Identifier .....	82
F.3.2	Preservation goal(s) .....	82
F.3.3	Preservation storage model .....	82
F.3.4	Supported operations .....	82
F.3.4.1	Mandatory operations .....	82
F.3.4.2	Optional operations .....	82
F.3.4.3	Announcement of supported operations .....	82
F.3.5	Generation and validation of preservation evidences .....	83
F.3.6	Augmentation of preservation evidences .....	83
F.3.7	Requirements and recommendations for preservation profiles .....	83
F.4	Preservation scheme with signature augmentation and without storage .....	84
F.4.1	Identifier .....	84
F.4.2	Preservation goal(s) .....	84
F.4.3	Preservation storage model .....	84
F.4.4	Supported operations .....	84
F.4.4.1	Mandatory operations .....	84
F.4.4.2	Optional operations .....	85
F.4.4.3	Announcement of supported operations .....	85
F.4.5	Generation and Validation of Preservation Evidences .....	85
F.4.6	Augmentation of preservation evidences .....	85
F.4.7	Requirements and recommendations for preservation profiles .....	85



<b>Annex G (informative):</b>	<b>Data structure for backup or migration of preservation services with storage.....</b>	<b>87</b>
G.1	Motivation and solution outline .....	87
G.2	Data Structures for migration of preservation services .....	87
G.2.1	XML Namespace.....	87
G.2.2	Component EvidenceExchange .....	87
G.2.2.1	Semantics.....	87
G.2.2.2	Syntax .....	88
G.2.3	Component EvidenceInfo.....	88
G.2.3.1	Semantics.....	88
G.2.3.2	Syntax .....	89
G.2.4	Component HashTree .....	89
G.2.4.1	Semantics.....	89
G.2.4.2	XML Syntax .....	89
G.2.5	Component AbstractNode.....	90
G.2.5.1	Semantics.....	90
G.2.5.2	Syntax .....	90
G.2.6	Component Node.....	90
G.2.6.1	Semantics.....	90
G.2.6.2	Syntax .....	90
G.2.7	Component Leaf.....	91
G.2.7.1	Semantics.....	91
G.2.7.2	Syntax .....	91
G.2.8	Component Group .....	91
G.2.8.1	Semantics.....	91
G.2.8.2	Syntax .....	92
<b>Annex H (normative):</b>	<b>Attributes for preservation evidences .....</b>	<b>93</b>
H.1	Introduction .....	93
H.2	The preservation-service-identifier attribute .....	93
H.2.1	Semantics .....	93
H.2.2	ASN.1-Syntax .....	93
H.2.3	XML-Syntax.....	93
H.3	The preservation-evidence-policy attribute.....	94
H.3.1	Semantics .....	94
H.3.2	ASN.1-Syntax .....	94
H.3.3	XML-Syntax.....	94
H.4	The preservation-profile attribute.....	94
H.4.1	Semantics .....	94
H.4.2	ASN.1-Syntax .....	94
H.4.3	XML-Syntax.....	95
<b>Annex I (normative):</b>	<b>ASN.1 syntax for attributes for preservation evidences.....</b>	<b>96</b>
History .....		97



---

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

## Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

---

# Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

---

# Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

---

# Executive summary

The present document builds upon existing work studied in ETSI SR 019 510 [i.13] and specifies protocols for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques.

---

## Introduction

The need for long-term preservation is acknowledged amongst others in the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market [i.1], as can be seen in recital (61).

*"This Regulation should ensure the long-term preservation of information, in order to ensure the legal validity of electronic signatures and electronic seals over extended periods of time and guarantee that they can be validated irrespective of future technological changes".*

Furthermore Article 34 of the Regulation (EU) No 910/2014 [i.1] states that *"a qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period"* and that *"the Commission may, by means of implementing acts, establish reference numbers of standards for the qualified preservation service for qualified electronic signatures"*.

Against this background, the present document and its companion document ETSI TS 119 511 [i.14] have been created based on existing work related to preservation studied in ETSI SR 019 510 [i.13]. The present document complements ETSI TS 119 511 [i.14] and specifies protocols for trust service providers providing long-term data preservation services.

**iTeh STANDARD PREVIEW**  
(standards.iteh.ai)  
Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/e20a3db4-2733-4278-af7a-03d088b025d/etsi-ts-119-512-v1.1.1-2020-01>

---

# 1 Scope

Based on a scoping study and survey with respect to long-term preservation techniques for digital signatures and general data documented in ETSI SR 019 510 [i.13], the present document and its companion document ETSI TS 119 511 [i.14] have been created.

ETSI TS 119 511 [i.14] specifies policy and security requirements for trust service providers providing long-term preservation of digital signatures and of general data, i.e. unsigned data or signed data, using digital signature techniques.

The present document complements ETSI TS 119 511 [i.14] and specifies protocols for trust service providers providing long-term data preservation services of digital signatures and of general data (i.e. unsigned data or signed data).

Specifically, but not exclusively, digital signatures in the present document cover electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, and qualified electronic seals as per Regulation (EU) No 910/2014 [i.1].

The present document first addresses general aspects (see clause 4) such as a system architecture for preservation, which contains a preservation interface offered by the preservation service and used by the client (see clause 4.1). The preservation service may aim at different preservation goals (see clause 4.2), may or may not provide storage functionality (see clause 4.3), and provide different profiles of preservation schemes, which may implement different preservation evidence policies (see clause 4.4).

In a second step, the present document specifies methods and data objects constituting a protocol between a client and a long-term data preservation service for the issuance and maintenance of evidences (see clause 5). For each call at the preservation interface it first specifies the semantics in a generic fashion and then specifies the concrete syntax of the conveyed data elements based on XML and JSON together with its binding to SOAP [i.25] and REST respectively.

---

## 2 References

### 2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <https://docbox.etsi.org/Reference/>.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

- [1] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC Baseline containers".
- [2] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".
- [3] IETF RFC 4998: "Evidence Record Syntax (ERS)".
- [4] IETF RFC 6283: "Extensible Markup Language Evidence Record Syntax (XMLERS)".
- [5] OASIS: "Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0", Committee Specification 02, 11 December 2019.
- [6] OASIS: "Digital Signature Service Metadata Version 1.0", Committee Specification 02, 11 December 2019.

- [7] Recommendation ITU-T X.680 (2008): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

## 2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.8.2014, p. 73-114.

- [i.2] BSI TR-03125-F: "Preservation of Evidence of Cryptographically signed Documents, Formats (TR-ESOR-F)".

NOTE: Available at [https://www.bsi.bund.de/EN/tr-esor\\_XAIP](https://www.bsi.bund.de/EN/tr-esor_XAIP).

- [i.3] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".
- [i.4] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".
- [i.5] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAAdES digital signatures; Part 1: Building blocks and CAAdES baseline signatures".
- [i.6] ETSI TS 119 122-3: "Electronic Signatures and Infrastructures (ESI); CAAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CAAdES".
- [i.7] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".
- [i.8] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".
- [i.9] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".
- [i.10] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".
- [i.11] ETSI TS 119 441: "Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services".
- [i.12] ETSI TS 119 442: "Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services".
- [i.13] ETSI SR 019 510: "Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures".
- [i.14] ETSI TS 119 511: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques".
- [i.15] ISO 13527:2010: "Space data and information transfer systems - XML formatted data unit (XFDU) structure and construction rules".
- [i.16] ISO 14721:2012: "Space data and information transfer systems - Open archival information system (OAIS) - Reference model".

- [i.17] ISO/IEC 21320-1:2015: "Information technology - Document Container File - Part 1: Core".
- [i.18] IANA: Media Type Registry.
- NOTE: Available at <https://www.iana.org/assignments/media-types/media-types.xhtml>.
- [i.19] IETF RFC 3061: "A URN Namespace of Object Identifiers".
- [i.20] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".
- [i.21] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
- [i.22] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".
- [i.23] The National Archives: "PRONOM Unique Identifiers".
- NOTE: Available at <http://www.nationalarchives.gov.uk/aboutapps/pronom/puid.htm>.
- [i.24] W3C Recommendation 26 November 2008: "Extensible Markup Language (XML) 1.0 (Fifth Edition)".
- NOTE: Available at <https://www.w3.org/TR/xml/>.
- [i.25] W3C Recommendation 27 April 2007: "SOAP Version 1.2 Part 1: Messaging Framework (Second Edition)".
- NOTE: Available at <https://www.w3.org/TR/soap12/>.
- [i.26] W3C Recommendation 25 January 2005: "SOAP Message Transmission Optimization Mechanism".
- NOTE: Available at <https://www.w3.org/TR/soap12-ntom/>.
- [i.27] W3C Recommendation 11 April 2013: "XML Signature Syntax and Processing Version 1.1".
- NOTE: Available at <https://www.w3.org/TR/xmldsig-core1/>.

---

## 3 Definition of terms, symbols and abbreviations

### 3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 119 001 [i.3] and the following apply:

**certificate status authority:** authority providing certificate status information

EXAMPLE: The certificate status information can be provided using the Online Certificate Status Protocol (OCSP) [i.22] or in form of Certificate Revocation Lists (CRL) [i.21].

**container:** data object, which contains a set of data objects and optional additional information, which describes the contained data objects and optionally its content and its interrelationships

EXAMPLE: The format of a container can be based on, ZIP as defined in ISO/IEC 21320-1 [i.17] or XML [i.24]. ASiC [1] is an example of a container based on ZIP.

NOTE: Additional information may comprise associated digital signatures, time-stamps, evidence records, validation data (CRLs, OCSP responses) and validation reports.

**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

**delta preservation object container:** special preservation object container describing the difference to an already existing preservation object container