ETSI TS 119 172-3 V1.1.1 (2019-12)

TECHNICAL SPECIFICATION

Electronic Signatures and Infrastructures (ESI);
Signature Policies;
Part 3: ASN.1 format for signature policies

Reference

DTS/ESI-0019172-3

Keywords

ASN.1, e-commerce, electronic signature,
policies, trust services

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.

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

Contents

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).

The present document is part 3 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.2].

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.

1 Scope

The present document defines an ASN.1 format of machine readable signature policies based on the building blocks that define technical constraints on digital signatures and are specified in ETSI TS 119 172-1 [i.2].

Pure signature applicability rules, directly related to procedural constraints imposed by business processes, are out of the scope of the present document which does not define ASN.1 elements for the building blocks specified in ETSI TS 119 172-1 [i.2] defining only applicability rules.

For each element of the machine readable signature policy, the present document references to the semantics described in ETSI TS 119 172-2 [3] and defines the corresponding ASN.1 syntax.

The present document defines elements which can be used to describe technical constraints on signature creation, signature validation, and signature augmentation. These elements are designed in a way that it is possible to generate ASN.1 documents that include components of a signature generation policy, or/and signature validation policy, and/or signature augmentation policy.

An ASN.1 document conformant to the present specification, defines constraints (on generation, augmentation, validation, any combination of two of them, or the three of them) that one signature has to meet.

NOTE: Complex business processes, where several digital signatures need to be managed, having to meet different set of technical constraints, will require several ASN.1 documents conformant to the present document, each one defining one of these sets of technical constraints.

It is out of the scope to specify mechanisms for protecting the integrity of the machine-readable signature policy documents specified in the present document.

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 319 122-1:"Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

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

[3] ETSI TS 119 172-2:"Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 2: XML format for signature policies".

[4] Recommendation ITU-T X.680 (2015): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[5] Recommendation ITU-T X.690 (2015): "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

[6] IETF RFC 5646: "Tags for Identifying Languages".

[7] IETF RFC 5912 (2010): "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)".

[8] W3C Recommendation: "XML Schema Part 2: Datatypes Second Edition". October 2004.

NOTE: See https://www.w3.org/TR/xmlschema-2/.

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] ETSI TS 119 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[i.2] 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".

[i.3] ETSI TS 119 192: "Electronic Signatures and Infrastructures (ESI); AdES related Uniform Resource Identifier".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 119 172-1 [i.2] and the following apply:

signature applicability rules: set of rules, applicable to one or more digital signatures, that defines the requirements for determination of whether a signature is fit for a particular business or legal purpose

signature augmentation constraint: criteria used when augmenting a digital signature

signature augmentation policy: set of signature augmentation constraints

signature creation application: application within the signature creation system that creates the AdES digital signature and relies on the signature creation device to create a digital signature value

signature creation constraint: criteria used when creating a digital signature

signature creation policy: set of signature creation constraints processed or to be processed by the signature creation application

signature validation application: application that validates a signature against a signature validation policy, and that outputs a status indication (i.e. the signature validation status) and a signature validation report

signature validation constraint: technical criteria against which a digital signature can be validated

EXAMPLE: As specified in ETSI TS 119 102-1 [i.1].

signature validation policy: set of signature validation constraints processed or to be processed by the signature validation application

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ASN.1	Abstract Syntax Notation One
BER	Basic Encoding Rules
DER	Distinguished Encoding Rules
OID	Object IDentifier
URI	Uniform Resource Identifier
XML	eXtensible Markup Language

4 ASN.1 syntax for machine processable signature policy document

4.1 Introduction

4.1.1 Technical approach

The present document takes as starting point the contents of ETSI TS 119 172-1 [i.2], which defines the building blocks of a human readable signature policy document. These building blocks are of two types:

- Building blocks defining applicability rules, which are the procedural constraints enforced by the business processes where the digital signatures are used. These procedural constraints, if not satisfied, could prevent further processing (in other words, accepting for the purpose of the business) a certain signed document even if the digital signature is technically valid.

- Building blocks defining technical constraints, related with technical aspects of the digital signature and its technical validation (signature format, signature attributes, constraints on certificates, time-stamp tokens, revocation material data, etc.).

The present document specifies an ASN.1 format for the building blocks specified in ETSI TS 119 172-1 [i.2], which define technical constraints, and allows building documents which define technical constraints in a machine-readable format.

The ASN.1 elements defined within the present contain information that clearly signal whether the constraints that they define apply to the generation of a signature, the validation of a signature, the augmentation of a signature, any combination of two of the former, or to the three of them. Therefore, the ASN.1 documents built using the present document may contain components of signature generation policy, or/and signature validation policy, and/or signature augmentation policy.

4.1.2 ASN.1 module

Annex A defines the ASN.1 module which describes the elements defined in the present document.

4.1.3 ASN.1 encoding

4.1.3.1 DER

Distinguished Encoding Rules (DER) for ASN.1 types shall be as specified in Recommendation ITU-T X.690 [5].

4.1.3.2 BER

If Basic Encoding Rules (BER) are used for some ASN.1 types, it shall be as specified in Recommendation ITU-T X.690 [5].

4.1.4 ASN.1 type to allow extensions: the `Other` type

Semantics

The `Other` type shall contain an element of a type as defined by the `OTHER.&id`.

The `Other` type shall be parametized by a set of allowed `OTHER.&id` types, the `MyOtherSet`.

The `MyOtherSet` may be extensible, i.e. contains the "…".

NOTE: The `Other` type allows to extends specific types later with specific elements.

Syntax

The `OTHER` class and the `Other` type shall be as defined in annex A and is copied below for information.

```
OTHER ::= CLASS {
    &id OBJECT IDENTIFIER UNIQUE,
    &Value OPTIONAL }
WITH SYNTAX {
    OTHER-ID &id
    [OTHER-TYPE &Value] }

Other{OTHER:MyOtherSet} ::= SEQUENCE {
  otherId OTHER.&id({MyOtherSet}),
  otherValue OTHER.&Value({MyOtherSet}{@otherId}) OPTIONAL }
```

4.2 The `SignaturePolicy` type

4.2.1 Semantics

The semantics shall be as in clause 4.2.1 of ETSI TS 119 172-2 [3].

4.2.2 Syntax

The `SignaturePolicy` type shall be as defined in annex A and is copied below for information.

```
SignaturePolicy ::= SEQUENCE {
    digest Digest,
    policyComponents PolicyComponents}
```

The element of type `Digest` shall be as specified in clause 4.3.2.

The element of type `PolicyComponents` shall be as specified in clause 4.4.2.

4.3 The `Digest` type

4.3.1 Semantics

The semantics shall be as in clause 4.3.1 of ETSI TS 119 172-2 [3].

4.3.2 Syntax

The `Digest` type shall be as defined in annex A and is copied below for information.