ETSI TS 119 172-2 V1.1.1 (2019-12)

Electronic Signatures and Infrastructures (ESI);
Signature Policies;
Part 2: XML format for signature policies

Reference

DTS/ESI-0019172-2

Keywords

e-commerce, electronic signature, policies, trust services, XML

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

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 2 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 XML 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 XML elements for the building blocks specified in ETSI TS 119 172-1 [i.2] that define only applicability rules.

For each element of the machine readable signature policy, the present document specifies the semantics and the how to implement it in XML 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 XML documents that include components of a signature generation policy, or/and signature validation policy, and/or signature augmentation policy.

An XML 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 XML 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 TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[2] IETF RFC 3061: "A URN Namespace of Object Identifiers".

[3] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[4] IETF RFC 6960: "X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP".

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 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.4] ETSI TS 119 192: "Electronic Signatures and Infrastructures (ESI); AdES related Uniform Resource Identifier".

[i.5] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. OJ L 13, 19.1.2000, p. 12-20.

[i.6] 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.

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:

EU qualified certificate: qualified certificate as specified in Directive 1999/93/EC [i.5] or in Regulation (EU) No 910/2014 [i.6] whichever is in force at the time of issuance

EU qualified trust service provider: trust service provider that meets the requirements for qualified trust service providers laid down in Regulation (EU) 910/2014 [i.6]

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:

BSP	Business Scoping Parameter
CA	Certification Authority
CRL	Certificate Revocation List
EUMS	European Union Member State
IETF	Internet Engineering Task Force
LOTL	List Of Trusted Lists
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
RFC	Request For Comments
TL	Trusted List
TSP	Trusted Service Provider
URI	Universal Resource Identifier
URN	Universal Resource Name
XML	eXtensible Markup Language

4 XML 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 a XML 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 XML 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 XML 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 XML namespaces

The present document uses the URI namespaces listed below:

- http://uri.etsi.org/19172/v1.1.1
- http://www.w3.org/2000/09/xmldsig#
- http://uri.etsi.org/02231/v2#
- http://www.w3.org/2001/XMLSchema

The present document defines one XML Schema file, namely: "19172xmlSchema.xsd". See Annex B for details on their locations.

Table 1 shows the URIs of the namespaces used in the XML Schema definitions, mapped to their corresponding prefixes.

Table 1: Namespaces with constant prefixes

XML Namespace URI	Prefix
http://www.w3.org/2000/09/xmldsig#	ds
http://www.w3.org/2001/XMLSchema	xs
http://uri.etsi.org/02231/v2#"	tsl

Below follows a copy of the `xs:schema` element of the XML Schema file "19172xmlSchema.xsd", whose location is detailed in clause B.1, and that defines the namespace whose URI is http://uri.etsi.org/19172/v1.1.1.

```
<xs:schema targetNamespace="http://uri.etsi.org/19172/v1.1.1#"
xmlns:tsl="http://uri.etsi.org/02231/v2#" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns="http://uri.etsi.org/19172/v1.1.1#"
elementFormDefault="qualified" attributeFormDefault="unqualified">

    <xs:import namespace="http://uri.etsi.org/02231/v2#"
schemaLocation="https://uri.etsi.org/02231/v3.1.2/ts_102231v030102_xsd.xsd"/>
    <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
schemaLocation="http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/xmldsig-core-schema.xsd"/>
```

4.1.3 XML type to allow extensions: the `AnyType` type

Semantics

The `AnyType` type shall have a content model allowing a sequence of arbitrary XML elements that (mixed with text) is of unrestricted length.

The `AnyType` type shall have a content model allowing for text content only.

The `AnyType` type shall have a content model allowing an element of this data type to bear an unrestricted number of arbitrary attributes.

NOTE: The `AnyType` data type is used throughout the remaining parts of the present document wherever the content of an XML element has been left open.

Syntax

The `AnyType` element shall be as defined in XML Schema file "19172xmlSchema.xsd", whose location is detailed in clause B.1, and is copied below for information.

```
<xs:complexType name="AnyType" mixed="true">
    <xs:sequence minOccurs="0" maxOccurs="unbounded">
        <xs:any namespace="##any" processContents="lax"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##any"/>
</xs:complexType>
```

4.2 The `SignaturePolicy` element

4.2.1 Semantics

This element shall contain:

1) A digest for securing the contents of the signature policy document, and an identifier of the digest algorithm used for computing it, as specified in clause 4.3.

2) An element that contains all the machine-processable components of the signature policy, as specified in clause 4.4.

4.2.2 Syntax

The `SignaturePolicy` element shall be as defined in XML Schema file "19172xmlSchema.xsd", whose location is detailed in clause B.1, and is copied below for information.

```
<xs:element name="SignaturePolicy" type="SignaturePolicyType" />

    <xs:complexType name="SignaturePolicyType">
        <xs:sequence>
            <xs:element ref="Digest" />
            <xs:element ref="PolicyComponents" />
        </xs:sequence>
    </xs:complexType>
```

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

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

4.3 The `Digest` element

4.3.1 Semantics

This element shall contain:

1) One identifier of a digest algorithm.

2) One digest value.

In the case that the structured document is an XML document, this element shall also contain:

1) A canonicalization algorithm.

4.3.2 Syntax

The `Digest` element shall be as defined in XML Schema file "19172xmlSchema.xsd", whose location is detailed in clause B.1, and is copied below for information.

```
<xs:element name="Digest" type="DigestDetailsType"/>
<xs:complexType name="DigestDetailsType">
    <xs:sequence>
        <xs:element ref="ds:DigestMethod" />
        <xs:element ref="ds:DigestValue" />
        <xs:element ref="ds:CanonicalizationMethod" />
    </xs:sequence>
</xs:complexType>
```

The digest value shall be computed on the output of applying the canonicalization algorithm identified in this component, to the `PolicyComponents` element specified in clause 4.4.

4.4 The `PolicyComponents` element

4.4.1 Semantics

This element shall contain an element containing all the rules defined by the signature policy itself, as specified in clause 4.14.

This element should also contain an element including general details, as specified in clause 4.5.

4.4.2 Syntax

The `PolicyComponents` element shall be as defined in XML Schema file "19172xmlSchema.xsd", whose location is detailed in clause B.1, and is copied below for information.

```
<xs:element name="PolicyComponents" type="PolicyComponentsType"/>
<xs:complexType name="PolicyComponentsType">
    <xs:sequence>
        <xs:element ref="GeneralDetails"/>
        <xs:element ref="PolicyRules"/>
    </xs:sequence>
</xs:complexType>
```

The element `GeneralDetails` shall be as specified in clause 4.5.2.

The element `PolicyRules` shall be as specified in clause 4.14.2.

4.5 The `GeneralDetails` element

4.5.1 Semantics

This element shall contain an element containing details on the signature policy itself, as specified in clause 4.6.

This element may also contain:

1) An element containing details of the responsible authority of the signature policy, as specified in clause 4.7.

2) An element containing other details not defined within the present document, as specified in clause 4.13.

4.5.2 Syntax

The `GeneralDetails` element shall be as defined in XML Schema file "19172xmlSchema.xsd", whose location is detailed in clause B.1, and is copied below for information.

```
<xs:element name="GeneralDetails" type="GeneralDetailsType"/>
<xs:complexType name="GeneralDetailsType">
    <xs:sequence>
        <xs:element ref="SigPolicyDetails"/>
        <xs:element ref="AuthorityDetails" minOccurs="0"/>
        <xs:element ref="OtherDetails" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
```

The element `SigPolicyDetails` shall be as specified in clause 4.6.2.

The element `AuthorityDetails` shall be as specified in clause 4.7.2.

The element `OtherDetails` shall be as specified in clause 4.13.2.