ETSI TS 119 172-1 V1.1.1 (2015-07)

Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents

Reference

DTS/ESI-0019172-1

Keywords

electronic signature, e-commerce,
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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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
http://portal.etsi.org/tb/status/status.asp

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

IPRs essential or potentially essential to the present document 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 (http://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.

Foreword

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

The present document is part 1 of a multi-part deliverable specifying Signature Policies as identified below:

Part 1: "Building blocks and table of contents for human readable signature policy documents";

Part 2: "XML Format for signature policies";

Part 3: "ASN.1 Format for signature policies";

Part 4: "Signature validation policy for European qualified electronic signatures/seals using trusted lists".

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.

Introduction

A digital signature is always used in a context, either implicit or explicit, e.g. as part of a business process.

That context can impose various types of requirements such as requirements related to the application and/or the business process for which implementation of a digital signature is required (e.g. which document(s)/data, in which steps of the business process one would need to sign and how):

- requirements influenced by legal provisions associated to the application and/or business context in which the business process takes place (e.g. the level of assurance on evidences and the longevity of such evidences);
- requirements on the actors involved in the creation/validation of signatures; and/or
- requirements linked to the technological environment in which the process takes place.

NOTE 1: Regulation (EU) No 910/2014 [i.1] defines the terms electronic signature, advanced electronic signature, qualified electronic signature, electronic seal, advanced electronic seal and qualified electronic seal. These electronic signatures and seals can be created using digital signature technology.

NOTE 2: When not stated otherwise in the present document, "signature" denotes "digital signature".

Implementing digital signatures into a business process very often implies considering more than one signature to make a transaction effective or to give legal validity to one or several documents. Those signatures can be parallel and independent over the content (e.g. such as those of a buyer and seller on a contract); or enveloping countersignatures where each countersignature covers both content and all previous signature(s); or not-enveloping countersignatures where each countersignature covers previous signature(s) but not the previously signed content; or a mix of such signatures. Since very complex situations can arise when considering multiple signatures, specific requirements on their sequencing and respective scope in terms of data to be signed needs to be considered to ensure their correct implementation into the concerned work-flow.

There needs to be some way of expressing all applicable requirements into rules for creating, augmenting, and validating a single signature or a set of signatures in the context in which that(these) signature(s) have been applied so that the concerned parties, signers and relying parties, can abide by the applicable rules.

The purpose of a signature policy is to describe the requirements imposed on or committing the involved actors (signers, verifiers, relying parties and/or potentially one or more trust service providers) with respect to the application of signatures to documents and data that will be signed in a particular context, transaction, process, business or application domain, in order for these signatures to be considered as valid or conformant signatures under this signature policy.

The establishment of such rules into a signature policy results from the need:

- to document the decisions resulting from an analysis driven by a business or application context on how the concerned signature(s) needs to be implemented to meet the needs of the specific business application or electronic process it(they) support; and

- to specify the means for the creation, augmentation or long term management and verification of ***all*** the features of the concerned signature(s).

1 Scope

The present document defines the building blocks of signature policy and specifies a table of contents for human readable signature policy documents.

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 reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://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 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[2] ISO 19005-2:2011: "Document management - Electronic document file format for long-term preservation - Part 2: Use of ISO 32000-1 (PDF/A-2)".

[3] ETSI TS 103 172: "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile".

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 reference 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 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.2] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardisation of signatures; Definitions and abbreviations".

[i.3] ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Business Driven Guidance for Signature Creation and Validation".

[i.4] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Signature Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[i.5] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.6] ISO/IEC 27001: "Information technology -- Security techniques -- Information security management systems -- Requirements".

[i.7] ISO/IEC 27002: "Information technology -- Security techniques -- Code of practice for information security management".

[i.8] ETSI TS 103 173: "Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile".

[i.9] ETSI TS 103 171: "Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile".

[i.10] Unified Modelling Language.

NOTE: Available at http://www.uml.org/#UML2.0.

[i.11] ETSI TS 102 231: "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information".

[i.12] ETSI TS 119 612 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.13] IETF RFC 5280: "internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[i.14] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[i.15] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.16] Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market.

[i.17] Commission Decision 2013/662/EU 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.

[i.18] Commission Decision 2011/130/EU of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market.

[i.19] Business Process Modelling Notation: "A standard for modelling business processes and web service processes, as put forth by the Business Process Management Initiative".

NOTE: Available at www.bpmi.org.

[i.20] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[i.21] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[i.22] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[i.23] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

[i.24] IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

[i.25] ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".

[i.26] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC Baseline containers".

[i.27] ETSI EN 319 162-2: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Extended Containers".

[i.28] ETSI TS 102 918: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)".

[i.29] Commission Implementing Decision 2014/148/EU of 17 March 2014 amending Decision 2011/130/EU establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market.

[i.30] ETSI TS 119 172-2: "Electronic Signature Infrastructure; Signature Policies; Part 2: XML format for signature policies".

[i.31] ETSI TS 119 172-3: "Electronic Signature Infrastructure; Signature Policies; Part 3: ASN.1 format for signature policies".

[i.32] Commission Decision 2010/425/EU of 28 July 2010 amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States.

[i.33] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[i.34] ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[i.35] ETSI TS 102 778: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; CMS Profile based on ISO 32000-1".

[i.36] Recommendation CCITT X.800 (1991): "Security Architecture for Open Systems Interconnection for CCITT applications. ISO 7498-2:1989, Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".

[i.37] Recommendation ITU-T X.1252 (2010): "Cyberspace security - Identity management - Baseline identity management terms and definitions".

[i.38] Recommendation ITU-T X.509 | ISO/IEC 9594-8: "Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

CA-certificate: public-key certificate for one CA issued by another CA or by the same CA

NOTE: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

certification authority (CA)**:** authority trusted by one or more users to create and assign public-key certificates. Optionally the certification authority may create the subjects' keys

NOTE: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

certification path: ordered list of one or more public-key certificates, starting with a public-key certificate signed by the trust anchor, and ending with the public key certificate to be validated

NOTE 1: All intermediate public-key certificates, if any, are CA-certificates in which the subject of the preceding certificate is the issuer of the following certificate.

NOTE 2: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

certificate validation: process of verifying and confirming that a certificate is valid

cryptographic system: collection of transformations, normally defined by a mathematical algorithm, from plain text into cipher text and vice versa, the particular transformation(s) to be used being selected by (private or public) keys

NOTE: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

data integrity: property that data has not been altered or destroyed in an unauthorized manner

NOTE: As defined in ITU-TRecommendation X.800 | ISO 7498-2 [i.36].

data origin authentication: corroboration that the source of data received is as claimed

NOTE: As defined in ITU-TRecommendation X.800 | ISO 7498-2 [i.36].

digital signature: data appended to, or a cryptographic transformation (see cryptography) 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 e.g. by the recipient.

NOTE: As defined in ITU-TRecommendation X.800 | ISO 7498-2 [i.36].

private key: in a public key cryptographic system, that key of an entity's key pair which is known only by that entity

NOTE: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

public key: in a public key cryptographic system, that key of an entity's key pair which is publicly known.

NOTE: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

public key certificate: public key of an entity, together with some other information, rendered unforgeable by digital signature with the private key of the certification authority which issued it

NOTE: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

public key infrastructure: infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services

NOTE: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

repudiation: denial by one of the entities involved in a communication of having participated in all or part of the communication

NOTE: As defined in ITU-TRecommendation X.800 | ISO 7498-2 [i.36].

signature augmentation: process of incorporating to a digital signature information aiming to maintain the validity of that signature over the long term

NOTE: Augmenting signatures is a co-lateral process to the validation of signatures, namely the process by which certain material (e.g. time stamps, validation data and even archival-related material) is incorporated to the signatures for making them more resilient to change or for enlarging their longevity.

signature augmentation policy: set of rules, applicable to one or more digital signatures, that defines the technical and procedural requirements for their augmentation, in order to meet a particular business need, and under which the digital signature(s) can be determined to be conformant

NOTE: This covers collection of information and creation of new structures that allows performing, on the long term, validations of a signature.

signature creation device: configured software or hardware used to create a digital signature

signature creation policy: set of rules, applicable to one or more digital signatures, that defines the technical and procedural requirements for their creation, in order to meet a particular business need, and under which the digital signature(s) can be determined to be conformant

signature policy: signature creation policy, signature augmentation policy, signature validation policy or any combination thereof, applicable to the same signature or set of signatures

signature policy authority: entity responsible for the drafting, registering, maintaining, issuing and updating of a signature policy

signature policy document: document expressing one or more signature policies in a human readable form

signature validation: process of verifying and confirming that a digital signature is valid

signature validation policy: set of rules, applicable to one or more digital signatures, that defines the technical and procedural requirements for their validation, in order to meet a particular business need, and under which the digital signature(s) can be determined to be valid

trust: firm belief in the reliability and truth of information or in the ability and disposition of an entity to act appropriately, within a specified context

NOTE: As defined in Recommendation ITU-T X.1252 [i.37].

Trust Anchor (TA): entity that is trusted by a relying party and used for validating certificates in certification paths

NOTE: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

Trust Anchor information: at least the: distinguished name of the Trust Anchor, associated public key, algorithm identifier, public key parameters (if applicable), and any constrains on its use including a validity period

NOTE: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

validation data: data that is used to validate a digital signature

3.2 Abbreviations

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

ASiC	Associated Signature Container
ASN	Abstract Syntax Notation
B2B	Business to Business
B2C	Business to Consumer
BPMN	Business Process Modelling Notation
BSP	Business Scoping Parameter
CA	Certification Authority
CD	Commission Decision
CRL	Certificate Revocation List
DA	Driving Application
DTBS	Data To Be Signed
EC	European Commission
EN	European Standard
EU	European Union
IP	Internet Protocol
Gov2B	Government to Business
Gov2C	Government to Consumer
LoA	Level of Assurance
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
PKI	Public Key Infrastructure
SCA	Signature Creation Application
SVA	Signature Validation Application
TA	Trust Anchor
ToC	Table of Content
TR	Technical Report
TS	Technical Specification
TSP	Trust Service provider
TST_A	Time-Stamp Token applied in an archive level of CAdES signature or XAdES signature
$TST_{T\text{-}Level}$	Time-Stamp Token applied in a T-Level of CAdES signature or XAdES signature
UML	Unified Modelling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UK	United Kingdom
XML	eXtensible Markup Language
WYSIWYS	What You See IS What You Sign

4 Signature policies and signature policy document

A signature policy should be derived from the analysis of the requirements applicable to the implementation of digital signatures into a specific business electronic process or application domain.

That requirement analysis should be done according to the process described in ETSI TR 119 100 [i.3].

The resulting rules related to the creation, augmentation and/or validation of one or more signatures to which the same set of rules apply shall be documented in a signature policy.

A signature policy shall cover at least one of the three following aspects related to the management of the signatures to which it applies:

1) a signature creation policy;

2) a signature augmentation policy; or

3) a signature validation policy.

When there is a need for expressing a signature policy in a human readable form, the table of content (ToC) specified in annex A shall be followed to establish the corresponding signature policy document, or the signature policy shall be expressed under the form of a signature policy statement summary established on the basis of table A.1 from annex A.

The numbering of the clauses of the table of content is provided in annex A as it shall appear in the signature policy document by removing the starting "A.". Each clause shall appear. If the clause does not apply, "not applicable" shall be written after the clause title. The text provided in each clause of annex A specifies the expected content of each clause. This text shall not be copied in the signature policy document.

Where applicable, the sub-clauses of the signature policy document may identify separate provisions for each signature policy addressed by the signature policy document and for each of them may identify separate provisions for the creation, augmentation and validation by using the following labels to start dedicated clauses on creation, augmentation, or validation aspects, respectively:

- [CREATION]
- [AUGMENTATION]
- [VALIDATION]

The provisions expressed in each clause may be texted explicitly or incorporated by reference to other sources of provisions, in particular to abide by, endorse, inherit or enforce requirements from other signature policies.

Clause A.3 covers the rules or requirements set by a signature policy organized against business scoping parameters (BSPs) which are:

- parameters mainly related to the application and/or business process for which implementation of signature(s) is required;
- parameters mainly influenced by legal provisions associated to the application and/or business context in which the business process takes place;
- parameters related to the actors involved in the creation/validation of signatures; and
- other signature parameters.

The sub-clauses of clause A.3 shall each include the description of the applicable BSP provisions in terms of business language and shall indicate separately the corresponding requirements on signers, entities augmenting signatures and/or relying parties validating signatures covered by each signature policy addressed by the signature policy document.

When a specific business or application process involves several groups of signatures addressed by different signature policies, a single signature policy document may be used to express those signature policies.

EXAMPLE: Multiple signatures applied to the same data or to different (sets of) data being signed by the same or different entities at different moments alongside the workflow of events with a need for evidences covered by the considered workflow.