ETSI TS 119 102-2 V1.1.1 (2018-08)

Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report

Reference
DTS/ESI-0019102-2

Keywords
electronic signature, trust services, validation

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
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 2 of a multi-part deliverable covering Procedures for Creation and Validation of AdES Digital Signatures, as identified below:

Part 1: "Creation and Validation";

Part 2: "Signature Validation Report".

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 specifies a general structure and an XML format for reporting the validation of AdES digital signatures (specified in ETSI EN 319 122-1 [i.1], ETSI EN 319 132-1 [4], ETSI EN 319 142-1 [i.3] respectively). The present document is aligned with the requirements specified in ETSI TS 119 102-1 [1].

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 119 102-1 (V1.2.1): "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[2] W3C Recommendation: "XML-Signature Syntax and Processing Version 1.1", D. Eastlake et al., April 2013.

NOTE: Available at http://www.w3.org/TR/xmldsig-core/.

[3] ETSI TS 101 903 (V1.3.2): "XML Advanced Electronic Signatures (XAdES)".

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

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

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

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

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

[9] ISO 32000-1:2008: "Document management - Portable document format - Part 1: PDF 1.7".

[10] W3C Recommendation: "XML Schema Definition Language (XSD) 1.1 Part 1: Structures".

NOTE: Available at https://www.w3.org/TR/xmlschema11-1/.

[11] 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".

[12] IETF RFC 5035: "Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility".

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

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

[i.3] ETSI EN 319 142-1: "ETSI EN 319 142 1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[i.4] ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".

[i.6] IETF RFC 4998: "Evidence Record Syntax (ERS)".

[i.7] IETF RFC 6283: "Extensible Markup Language Evidence Record Syntax (XMLERS)".

[i.8] 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.

[i.9] Recommendation ITU-R TF.460-6: "Standard-frequency and time-signal emissions".

3 Definitions and abbreviations

3.1 Definitions

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

AdES (digital) signature: digital signature that is either a CAdES signature, or a PAdES signature or a XAdES signature

advanced electronic signature: As defined in Regulation (EU) No 910/2014 [i.8].

CAdES signature: digital signature that satisfies the requirements specified within ETSI EN 319 122-1 [i.1] or ETSI EN 319 122-2 [i.2]

certificate: See public key certificate.

certificate revocation list: signed list indicating a set of certificates that are no longer considered valid by the certificate issuer

claimed signing time: time of signing claimed by the signer which on its own does not provide independent evidence of the actual signing time

Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-R TF.460-6 [i.9]

data object: actual binary/octet data being operated on (transformed, digested, or signed) by an application

data to be signed formatted: data created from the data to be signed objects by formatting them and placing them in the correct sequence for the computation of the data to be signed representation

data to be signed representation: hash of the data to be signed formatted, which is used to compute the digital signature value

digital signature: data appended to, or a cryptographic transformation 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

digital signature value: result of the cryptographic transformation 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

evidence record: unit of data, which can be used to prove the existence of an archived data object or an archived data object group at a certain time

NOTE: See IETF RFC 4998 [i.6] and IETF RFC 6283 [i.7].

PAdES signature: digital signature that satisfies the requirements specified within ETSI EN 319 142-1 [i.3] or ETSI EN 319 142-2 [i.4]

proof of existence: evidence that proves that an object existed at a specific date/time

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

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

qualified electronic signature: As defined in Regulation (EU) No 910/2014 [i.8].

signature attribute: signature property

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

NOTE: The signature validation application (SVA) is specified in ETSI TS 119 102-1 [1].

signature validation constraint: technical criteria against which a digital signature can be validated, e.g. as specified in ETSI TS 119 102-1 [1].

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

signature validation report: comprehensive report of the validation provided by the signature validation application to the driving application and allowing the driving application, and any party beyond the driving application, to inspect details of the decisions made during validation and investigate the detailed causes for the status indication provided by the signature validation application

NOTE: Clause 5.1.3 of ETSI TS 119 102-1 [1] specifies minimum requirements for the content of such a report.

signature validation status: One of the following indications: TOTAL-PASSED, TOTAL-FAILED or INDETERMINATE.

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

signer: entity being the creator of a digital signature

(electronic) time-stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time

trust anchor: entity that is trusted by a relying party and used for validating certificates in certification paths

trusted list: list that provides information about the status and the status history of the trust services from trust service providers regarding compliance with the applicable requirements and the relevant provisions of the applicable legislation

NOTE: In the context of European Union Member States, as specified in Regulation (EU) No 910/2014 [i.8], it refers to an EU Member State list including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.

In the context of non-EU countries or international organizations, it refers to a list meeting the requirements of ETSI TS 119 612 [6] and providing assessment scheme based approval status information about trust services from trust service providers, for compliance with the relevant provisions of the applicable approval scheme and the relevant legislation.

XAdES signature: digital signature that satisfies the requirements specified within ETSI EN 319 132-1 [4] or ETSI EN 319 132-2 [5]

3.2 Abbreviations

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

AdES	Advanced Electronic Signature
CRL	Certificate Revocation List
DA	Driving Application
DSS	Digital Signature Service
DTBSF	Data To Be Signed Formatted
DTBSR	Data To Be Signed Representation
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
POE	Proof Of Existence
SD	Signer's Document
SDR	Signer's Document Representation
SVA	Signature Validation Application
TSP	Trust Service Provider
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UTC	Coordinated Universal Time
VRI	Validation Related Information
W3C	World Wide Web Consortium
XML	eXtensible Markup Language

4 Signature Validation Report Structure

4.1 General provisions

4.1.1 Report Structure

4.1.1.1 General

The present document defines the structure of reporting the result of the validation of an AdES digital signature (specified in ETSI EN 319 122-1 [i.1], ETSI EN 319 132-1 [4], ETSI EN 319 142-1 [i.3] respectively). The signature validation application (SVA) is assumed to follow the signature validation model specified in ETSI TS 119 102-1 [1] and illustrated by Figure 1.