SLOVENSKI STANDARD
SIST EN 319 102-1 V1.4.1:2024

01-september-2024

Elektronski podpisi in infrastrukture zaupanja (ESI) - Postopki za oblikovanje in validacijo digitalnih podpisov AdES - 1. del: Oblikovanje in validacija

Electronic Signatures and Trust Infrastructures (ESI) - Procedures for Creation and Validation of AdES Digital Signatures - Part 1: Creation and Validation

Ta slovenski standard je istoveten z: **ETSI EN 319 102-1 V1.4.1 (2024-06)**

ICS:

35.040.01	Kodiranje informacij na splošno	Information coding in general

SIST EN 319 102-1 V1.4.1:2024 **en**

ETSI EN 319 102-1 V1.4.1 (2024-06)

Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

Reference
REN/ESI-0019102-1v1.4.1

Keywords
electronic signature, security, 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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://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

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights 7
Foreword 7
Modal verbs terminology 7
Introduction 8
1 Scope 9
2 References 9
2.1 Normative references 9
2.2 Informative references 10
3 Definition of terms, symbols and abbreviations 11
3.1 Terms 11
3.2 Symbols 14
3.3 Abbreviations 14
4 Signature creation 15
4.1 Signature creation model 15
4.2 Signature creation information model 17
4.2.1 Introduction 17
4.2.2 Signature Creation Constraints 18
4.2.3 Signer's Document (SD) 18
4.2.4 Signer's Document Representation (SDR) 18
4.2.5 Signature attributes 19
4.2.5.1 General requirements 19
4.2.5.2 Signing certificate identifier 19
4.2.5.3 Signature policy identifier 19
4.2.5.4 Signature policy store 19
4.2.5.5 Data content type 20
4.2.5.6 Commitment type indication 20
4.2.5.7 Counter signatures 20
4.2.5.8 Claimed signing time 20
4.2.5.9 Claimed signer location 20
4.2.5.10 Signer's attributes 21
4.2.6 Data To Be Signed (DTBS) 21
4.2.7 Data To Be Signed (Formatted) (DTBSF) 21
4.2.8 Data To Be Signed Representation (DTBSR) 21
4.2.9 Signature 21
4.2.10 Signed Data Object (SDO) 22
4.2.11 Validation data 22
4.3 Signature Classes and Creation Processes 22
4.3.1 Introduction 22
4.3.2 Creation of Basic Signatures 23
4.3.2.1 Description 23
4.3.2.2 Inputs 24
4.3.2.3 Outputs 24
4.3.2.4 Processing 24
4.3.2.4.1 Selection of documents to sign 24
4.3.2.4.2 Signature attribute and parameters selection 25
4.3.2.4.3 Pre-signature presentation 25
4.3.2.4.4 Signature invocation 25
4.3.2.4.5 Signing 26
4.3.2.4.6 Signer authentication 26
4.3.2.4.7 SDO composition 26
4.3.3 Creation of a Signature with Time 26
4.3.3.1 Description 26
4.3.3.2 Inputs 27
4.3.3.3 Outputs 27

4.3.3.4 Process 27
4.3.4 Creation of Signatures with Long-Term Validation Material 28
4.3.4.1 Description 28
4.3.4.2 Inputs 28
4.3.4.3 Outputs 28
4.3.4.4 Process 28
4.3.5 Creation of Signatures providing Long Term Availability and Integrity of Validation Material 29
4.3.5.1 Description 29
4.3.5.2 Inputs 29
4.3.5.3 Outputs 30
4.3.5.4 Process 30

5 Signature validation 30
5.1 Signature validation model 30
5.1.1 General requirements 30
5.1.2 Selecting validation processes 33
5.1.3 Status indication of the signature validation process and signature validation report 34
5.1.4 Validation constraints 42
5.1.4.1 General requirements 42
5.1.4.2 X.509 Validation Constraints 43
5.1.4.3 Cryptographic Constraints 43
5.1.4.4 Signature Elements Constraints 43
5.2 Basic building blocks 43
5.2.1 Description 43
5.2.2 Format Checking 44
5.2.2.1 Description 44
5.2.2.2 Inputs 44
5.2.2.3 Outputs 44
5.2.3 Identification of the signing certificate 45
5.2.3.1 Description 45
5.2.3.2 Inputs 45
5.2.3.3 Outputs 45
5.2.3.4 Processing 45
5.2.4 Validation context initialization 46
5.2.4.1 Description 46
5.2.4.2 Inputs 46
5.2.4.3 Outputs 46
5.2.4.4 Processing 46
5.2.5 Revocation freshness checker 47
5.2.5.1 Description 47
5.2.5.2 Inputs 47
5.2.5.3 Output 47
5.2.5.4 Processing 48
5.2.6 X.509 certificate validation 48
5.2.6.1 Description 48
5.2.6.2 Inputs 49
5.2.6.3 Outputs 49
5.2.6.4 Processing 49
5.2.7 Cryptographic verification 52
5.2.7.1 Description 52
5.2.7.2 Inputs 52
5.2.7.3 Outputs 53
5.2.7.4 Processing 53
5.2.8 Signature Acceptance Validation (SAV) 53
5.2.8.1 Description 53
5.2.8.2 Inputs 54
5.2.8.3 Outputs 54
5.2.8.4 Processing 54
5.2.8.4.1 General requirements 54
5.2.8.4.2 Processing AdES attributes 55
5.2.9 Signature validation presentation building block 56
5.3 Validation process for Basic Signatures 57

5.3.1 Description 57
5.3.2 Inputs 57
5.3.3 Outputs 57
5.3.4 Processing 57
5.4 Time-stamp validation building block 59
5.4.1 Description 59
5.4.2 Inputs 60
5.4.3 Outputs 60
5.4.4 Processing 60
5.5 Validation process for Signatures with Time and Signatures with Long-Term Validation Material 60
5.5.1 Description 60
5.5.2 Inputs 61
5.5.3 Outputs 61
5.5.4 Processing 61
5.6 Validation process for Signatures providing Long Term Availability and Integrity of Validation Material 64
5.6.1 Introduction 64
5.6.2 Additional building blocks 65
5.6.2.1 Past certificate validation 65
5.6.2.1.1 Description 65
5.6.2.1.2 Input 65
5.6.2.1.3 Output 65
5.6.2.1.4 Processing 66
5.6.2.2 Validation time sliding process 66
5.6.2.2.1 Description 66
5.6.2.2.2 Input 66
5.6.2.2.3 Output 67
5.6.2.2.4 Processing 67
5.6.2.3 POE extraction 68
5.6.2.3.1 Description 68
5.6.2.3.2 Input 69
5.6.2.3.3 Output 69
5.6.2.3.4 Processing 69
5.6.2.4 Past signature validation building block 69
5.6.2.4.1 Description 69
5.6.2.4.2 Input 69
5.6.2.4.3 Output 70
5.6.2.4.4 Processing 70
5.6.3 Validation Process for Signatures providing Long Term Availability and Integrity of Validation Material 71
5.6.3.1 Description 71
5.6.3.2 Input 72
5.6.3.3 Output 72
5.6.3.4 Processing 72

Annex A (informative): Validation examples 76

A.1 General remarks and assumptions 76

A.2 Symbols 76

A.3 Example 1: Revoked certificate 77
A.3.1 Introduction 77
A.3.2 Basic signature validation 77
A.3.3 Validating a Signature with Time 78
A.3.4 Example 2: Revoked CA certificate 78
A.3.5 Basic signature validation 79
A.3.6 Validation of a Signature with Time 79
A.3.7 Long-Term Validation 80

Annex B (informative): Signature Classes and AdES Signatures 83

Annex C (informative): Applicability rules checking and format conformance check 84

C.1 Applicability checking 84
C.2 Format conformance.....84
Annex D (informative): Change history 86
History 88

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

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.

Foreword

This European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 1 of a multi-part deliverable covering Procedures for Creation and Validation of AdES Digital Signatures, as identified below:

ETSI EN 319 102-1: "Creation and Validation";

ETSI TS 119 102-2: "Signature Validation Report".

National transposition dates	
Date of adoption of this EN:	17 June 2024
Date of latest announcement of this EN (doa):	30 September 2024
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 March 2025
Date of withdrawal of any conflicting National Standard (dow):	31 March 2025

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

The present document aims to meet the general requirements of the international community to provide trust and confidence in electronic transactions, including, amongst other, applicable requirements from Regulation (EU) No 910/2014 [i.15].

1 Scope

The present document specifies procedures for:

- the creation of AdES digital signatures (specified in ETSI EN 319 122-1 [i.2], ETSI EN 319 132-1 [i.4], ETSI EN 319 142-1 [i.6] respectively);
- establishing whether an AdES digital signature is technically valid;

whenever the AdES digital signature is based on public key cryptography and supported by Public Key Certificates (PKCs). To improve readability of the present document, *AdES digital signatures* are meant when the term *signature* is being used.

NOTE 1: Regulation (EU) No 910/2014 [i.15] defines the terms electronic signature, advanced electronic signature, electronic seals and advanced electronic seal. These signatures and seals are usually created using digital signature technology. The present document aims at supporting the Regulation (EU) No 910/2014 [i.15] for creation and validation of advanced electronic signatures and seals when they are implemented as AdES digital signatures.

The present document introduces general principles, objects and functions relevant when creating or validating signatures based on signature creation and validation constraints and defines general classes of signatures that allow for verifiability over long periods.

The following aspects are considered to be out of scope:

- generation and distribution of Signature Creation Data (keys, etc.), and the selection and use of cryptographic algorithms;
- format, syntax or encoding of data objects involved, specifically format or encoding for documents to be signed or signatures created; and
- the legal interpretation of any signature, especially the legal validity of a signature.

NOTE 2: The signature creation and validation procedures specified in the present document provide several options and possibilities. The selection of these options is driven by a signature creation policy, a signature augmentation policy or a signature validation policy respectively. Note that legal requirements can be provided through specific policies, e.g. in the context of qualified electronic signatures as defined in the Regulation (EU) 910/2014 [i.15].

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

[2] ISO/IEC 9594-8:2020: "Information technology -- Open Systems Interconnection -- Part 8: The Directory: Public-key and attribute certificate frameworks".

[3] IETF RFC 3161: "Internet X.509 Public Key Infrastructure; Time Stamp Protocol (TSP)".

[4] 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".

[5] T7 & TeleTrusT: "Common PKI Specifications for Interoperable Applications", Specification Part 9 SigG-Profile, Version 2.0, 20 January 2009.

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] IETF RFC 4158: "Internet X.509 Public Key Infrastructure: Certification Path Building".

[i.2] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[i.3] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

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

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

[i.6] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[i.7] ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".

[i.8] IETF RFC 5652: "Cryptographic Message Syntax (CMS)".

[i.9] IETF RFC 4998: "Evidence Record Syntax (ERS)".

[i.10] IETF RFC 6283: "Extensible Markup Language Evidence Record Syntax (XMLERS)".

[i.11] Void.

[i.12] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[i.13] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

[i.14] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.15] 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.16] IETF RFC 3852: "Cryptographic Message Syntax (CMS)".

[i.17] ETSI TS 119 442: "Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services".

[i.18] ETSI TS 119 102-2: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report".

[i.19] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[i.20] ISO/IEC 14533-4:2019: "Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 4: Attributes pointing to (external) proof of existence objects used in long term signature formats (PoEAttributes)".

[i.21] ETSI EN 319 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

attribute authority: authority which assigns privileges by issuing attribute certificates

attribute certificate: data structure, digitally signed by an attribute authority, that binds some attribute values with identification information about its holder

certificate: See Public Key Certificate (PKC).

certificate identifier: unambiguous identifier of a certificate

certificate path (chain) validation: process of verifying and confirming that a certificate path (chain) is valid

Certificate Revocation List (CRL): signed list indicating a set of certificates that are no longer considered valid by the certificate issuer

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

certification authority: authority trusted by one or more users to create and assign public-key certificates

chain model: model for validation of X.509 certificate chains where all CA certificates have to be valid at the time they were used for issuing a certificate and the end-entity certificate was valid when creating the signature

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

(signature) commitment type: signer-selected indication of the exact implication of a digital signature

(signature) creation constraint: criteria used when creating a digital signature

cryptographic suite: combination of a signature scheme with a padding method and a cryptographic hash function

detached (digital) signature: digital signature that, with respect to the Signed Data Object, is neither enveloping nor enveloped

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

Driving Application (DA): application that uses a Signature Creation System (SCS) to create a signature or a Signature Validation Application (SVA) in order to validate digital signatures or a signature augmentation application to augment digital signatures

electronic document: any content stored in electronic form, in particular text or sound, visual or audiovisual recording

enveloped (digital) signature: digital signature embedded within the Signed Data Object

enveloping (digital) signature: digital signature embedding the Signed Data Object

evidence: information that can be used to resolve a dispute about various aspects of authenticity of archived data objects

Evidence Record (ER): 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.9] and IETF RFC 6283 [i.10].

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

prospective certificate chain: sequence of n certificates which satisfies the conditions (a) to (c) in IETF RFC 5280 [1] clause 6.1, and the trust anchor is trusted according to the signature validation policy in use

Public Key Certificate (PKC): 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

revocation data: data issued by a revocation status service, including the signature of the issuing authority, for the purpose of providing revocation status information about one or more certificates

EXAMPLE: Certificate Revocation List, OCSP response.

NOTE: ETSI EN 319 411-1 [i.19] defines the revocation status service as a component service of the certification services.

shell model: model for validation of X.509 certificate chains where all certificates have to be valid at a given time

NOTE: The given time is an input parameter to the validation.

signature acceptance: technical verification to be performed on the signature itself or on the attributes of the signature (i.e. the "signature elements constraints")

signature attribute: signature property

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

NOTE 1: Augmenting signatures is 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.

NOTE 2: This covers collection of information and creation of new structures that allows performing, on the long term, validations of a signature.

signature augmentation constraint: technical criteria used when augmenting a signature to a specific signature class

signature augmentation policy: set of signature augmentation constraints

NOTE 1: An augmentation policy can be uniquely identified by an OID/URI.

NOTE 2: The present document does not further specify the content of such a policy.

signature augmentation report: information about the augmentation provided by the Signature Augmentation Application to the Driving Application

NOTE: The present document does not further specify the content of such a report.

signature augmentation result: either the augmented signature or an error message that augmentation did not succeed, and optionally a **signature augmentation report**

NOTE: ETSI TS 119 442 [i.17] specifies how to convey such signature augmentation result.