

STN	Elektronické podpisy a infraštruktúry (ESI) Postupy na tvorbu a overenie digitálnych podpisov AdES Časť 1: Tvorba a overenie	STN EN 319 102-1 V1.3.1 87 9102
------------	---	---

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

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 05/22

Obsahuje: EN 319 102-1 V1.3.1:2021

134783



ETSI EN 319 102-1 V1.3.1 (2021-11)



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

Reference

REN/ESI-0019102-1v121

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:

<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/CommitteeSupportStaff.aspx>

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

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2021.
All rights reserved.

Contents

Intellectual Property Rights	7
Foreword.....	7
Modal verbs terminology.....	8
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.....	16
4.2.1 Introduction.....	16
4.2.2 Signature Creation Constraints	17
4.2.3 Signer's Document (SD)	17
4.2.4 Signer's Document Representation (SDR).....	18
4.2.5 Signature attributes	18
4.2.5.1 General requirements	18
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	19
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.....	20
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)	21
4.2.11 Validation data.....	21
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.....	23
4.3.2.3 Outputs	23
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	24
4.3.2.4.3 Pre-signature presentation	24
4.3.2.4.4 Signature invocation.....	25
4.3.2.4.5 Signing.....	25
4.3.2.4.6 Signer authentication.....	25
4.3.2.4.7 SDO composition	25
4.3.3 Creation of a Signature with Time.....	26
4.3.3.1 Description	26
4.3.3.2 Inputs.....	26
4.3.3.3 Outputs.....	26

4.3.3.4	Process	27
4.3.4	Creation of Signatures with Long-Term Validation Material	27
4.3.4.1	Description	27
4.3.4.2	Inputs.....	27
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	28
4.3.5.1	Description	28
4.3.5.2	Inputs.....	29
4.3.5.3	Outputs	29
4.3.5.4	Process	29
5	Signature validation.....	30
5.1	Signature validation model.....	30
5.1.1	General requirements.....	30
5.1.2	Selecting validation processes	32
5.1.3	Status indication of the signature validation process and signature validation report.....	33
5.1.4	Validation constraints	41
5.1.4.1	General requirements	41
5.1.4.2	X.509 Validation Constraints	42
5.1.4.3	Cryptographic Constraints	42
5.1.4.4	Signature Elements Constraints	42
5.2	Basic building blocks	42
5.2.1	Description.....	42
5.2.2	Format Checking	43
5.2.2.1	Description	43
5.2.2.2	Inputs.....	43
5.2.2.3	Outputs	43
5.2.3	Identification of the signing certificate	44
5.2.3.1	Description	44
5.2.3.2	Inputs.....	44
5.2.3.3	Outputs	44
5.2.3.4	Processing	44
5.2.4	Validation context initialization.....	45
5.2.4.1	Description	45
5.2.4.2	Inputs.....	45
5.2.4.3	Outputs	45
5.2.4.4	Processing	45
5.2.5	Revocation freshness checker	46
5.2.5.1	Description	46
5.2.5.2	Inputs.....	46
5.2.5.3	Output	46
5.2.5.4	Processing	46
5.2.6	X.509 certificate validation.....	47
5.2.6.1	Description	47
5.2.6.2	Inputs.....	47
5.2.6.3	Outputs	47
5.2.6.4	Processing	48
5.2.7	Cryptographic verification.....	50
5.2.7.1	Description	50
5.2.7.2	Inputs.....	50
5.2.7.3	Outputs	50
5.2.7.4	Processing	51
5.2.8	Signature Acceptance Validation (SAV).....	51
5.2.8.1	Description	51
5.2.8.2	Inputs.....	51
5.2.8.3	Outputs	52
5.2.8.4	Processing	52
5.2.8.4.1	General requirements.....	52
5.2.8.4.2	Processing AdES attributes	53
5.2.9	Signature validation presentation building block.....	54
5.3	Validation process for Basic Signatures.....	55

5.3.1	Description.....	55
5.3.2	Inputs	55
5.3.3	Outputs.....	55
5.3.4	Processing.....	55
5.4	Time-stamp validation building block.....	57
5.4.1	Description.....	57
5.4.2	Inputs	58
5.4.3	Outputs.....	58
5.4.4	Processing.....	58
5.5	Validation process for Signatures with Time and Signatures with Long-Term Validation Material	58
5.5.1	Description.....	58
5.5.2	Inputs	59
5.5.3	Outputs.....	59
5.5.4	Processing.....	59
5.6	Validation process for Signatures providing Long Term Availability and Integrity of Validation Material	62
5.6.1	Introduction.....	62
5.6.2	Additional building blocks.....	62
5.6.2.1	Past certificate validation	62
5.6.2.1.1	Description	62
5.6.2.1.2	Input	63
5.6.2.1.3	Output.....	63
5.6.2.1.4	Processing.....	63
5.6.2.2	Validation time sliding process.....	64
5.6.2.2.1	Description	64
5.6.2.2.2	Input	64
5.6.2.2.3	Output.....	64
5.6.2.2.4	Processing.....	64
5.6.2.3	POE extraction	65
5.6.2.3.1	Description	65
5.6.2.3.2	Input	66
5.6.2.3.3	Output.....	66
5.6.2.3.4	Processing.....	66
5.6.2.4	Past signature validation building block	66
5.6.2.4.1	Description	66
5.6.2.4.2	Input	67
5.6.2.4.3	Output.....	67
5.6.2.4.4	Processing.....	67
5.6.3	Validation Process for Signatures providing Long Term Availability and Integrity of Validation Material.....	68
5.6.3.1	Description	68
5.6.3.2	Input	68
5.6.3.3	Output	68
5.6.3.4	Processing	69
Annex A (informative): Validation examples.....		72
A.1	General remarks and assumptions.....	72
A.2	Symbols.....	72
A.3	Example 1: Revoked certificate	73
A.3.1	Introduction	73
A.3.2	Basic signature validation	73
A.3.3	Validating a Signature with Time.....	74
A.3.4	Example 2: Revoked CA certificate	74
A.3.5	Basic signature validation	75
A.3.6	Validation of a Signature with Time	75
A.3.7	Long-Term Validation.....	76
Annex B (informative): Signature Classes and AdES Signatures.....		79
Annex C (informative): Applicability rules checking and format conformance check.....		80

C.1	Applicability checking	80
C.2	Format conformance.....	80
Annex D (informative):	Change History	82
History		83

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:	1 November 2021
Date of latest announcement of this EN (doa):	28 February 2022
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 August 2022
Date of withdrawal of any conflicting National Standard (dow):	31 August 2022

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".

NOTE: Available at [ISO - 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); CAAdES digital signatures; Part 1: Building blocks and CAAdES baseline signatures".
- [i.3] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAAdES digital signatures; Part 2: Extended CAAdES 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".

koniec náhľadu – text ďalej pokračuje v platenej verzii STN