Draft ETSI EN 319 122-1 V1.0.0 (2015-06)

Electronic Signatures and Infrastructures (ESI);
CAdES digital signatures;
Part 1: Building blocks and CAdES baseline signatures

Reference

DEN/ESI-0019122-1

Keywords

ASN.1, CAdES, electronic signature, profile, security

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 draft European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI standards EN Approval Procedure.

The present document is part 1 of a multi-part deliverable covering CAdES digital signatures as identified below:

Part 1: "Building blocks and CAdES baseline signatures";

Part 2: "Extended CAdES signatures".

The present document partly contains an evolved specification of the ETSI TS 101 733 [1] and ETSI TS 103 173 [i.1].

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

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

Electronic commerce has emerged as a frequent way of doing business between companies across local, wide area and global networks. Trust in this way of doing business is essential for the success and continued development of electronic commerce. It is therefore important that companies using this electronic means of doing business have suitable security controls and mechanisms in place to protect their transactions and to ensure trust and confidence with their business partners. In this respect digital signatures are an important security component that can be used to protect information and provide trust in electronic business.

The present document is intended to cover digital signatures supported by PKI and public key certificates, and 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.13].

The present document can be used for any transaction between an individual and a company, between two companies, between an individual and a governmental body, etc. The present document is independent of any environment. It can be applied to any environment e.g. smart cards, GSM SIM cards, special programs for electronic signatures, etc.

The present document is part of a rationalized framework of standards (see ETSI TR 119 000 [i.2]). See ETSI TR 119 100 [i.4] for getting guidance on how to use the present document within the aforementioned framework.

1 Scope

The present document specifies CAdES digital signatures. CAdES signatures are built on CMS signatures [7], by incorporation of signed and unsigned attributes, which fulfil certain common requirements (such as the long term validity of digital signatures, for instance) in a number of use cases.

The present document specifies the ASN.1 definitions for the aforementioned attributes as well as their usage when incorporating them to CAdES signatures.

The present document specifies formats for CAdES baseline signatures, which provide the basic features necessary for a wide range of business and governmental use cases for electronic procedures and communications to be applicable to a wide range of communities when there is a clear need for interoperability of digital signatures used in electronic documents.

The present document defines four levels of CAdES baseline signatures addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it. Each level requires the presence of certain CAdES attributes, suitably profiled for reducing the optionality as much as possible.

Procedures for creation and validation of CAdES digital signatures are out of scope and specified in ETSI EN 319 102-1 [i.5].

The present document aims at supporting digital signatures in different regulatory frameworks.

NOTE: Specifically, but not exclusively, CAdES digital signatures specified in the present document aim at supporting electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, and qualified electronic seals as per Regulation (EU) No 910/2014 [i.13].

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 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 TS 101 733 (V2.2.1): "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[2] IETF RFC 2045 (1996): "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".

[3] IETF RFC 2634 (1999): "Enhanced Security Services for S/MIME".

[4] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[5] IETF RFC 5035 (2007): "Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility".

[6] IETF RFC 5280 (2008): "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

NOTE: Obsoletes IETF RFC 3280.

[7] IETF RFC 5652 (2009): "Cryptographic Message Syntax (CMS)".

NOTE: Obsoletes RFC 3852.

[8] IETF RFC 5755 (2010): "An Internet Attribute Certificate Profile for Authorization".

NOTE: Obsoletes IETF RFC 3281.

[9] IETF RFC 5816 (2010): "ESSCertIDv2 Update for RFC 3161".

[10] IETF RFC 5911 (2010): "New ASN.1 Modules for Cryptographic Message Syntax (CMS) and S/MIME".

[11] IETF RFC 5912 (2010): "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)".

NOTE: Updated by IETF RFC 6268.

[12] IETF RFC 6268 (2011): "Additional New ASN.1 Modules for the Cryptographic Message Syntax (CMS) and the Public Key Infrastructure Using X.509 (PKIX)".

[13] IETF RFC 5940 (2010): "Additional Cryptographic Message Syntax (CMS) Revocation Information Choices".

[14] IETF RFC 6960 (2013): "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

NOTE: Obsoletes IETF RFC 2560.

[15] Recommendation ITU-T X.520 (11/2008)/ISO/IEC 9594-6:2008): "Information technology - Open Systems Interconnection - The Directory: Selected attribute types".

[16] Recommendation ITU-T X.680 (2008): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[17] Recommendation ITU-T X.690 (2008): "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

[18] OASIS Standard "Security Assertion Markup Language (SAML) V2.0".

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

[i.2] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); Rationalized structure for Electronic Signature Standardization".

[i.3] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); Definitions and abbreviations".

[i.4] ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Business Driven Guidance for Signature Creation and Validation".

[i.5] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Signature Creation and Validation".

[i.6] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[i.7] 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.8] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.9] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp profiles".

[i.10] ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management".

[i.11] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.12] Commission Decision 2009/767/EC of 16 October 2009 amended by CD 2010/425/EU of 28 July 2010, 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.13] 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.

[i.14] IETF RFC 3851 (2004): "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification".

[i.15] IETF RFC 4998 (2007): "Evidence Record Syntax (ERS)".

[i.16] Recommendation ITU-T X.208 (1988): "Specification of Abstract Syntax Notation One (ASN.1)".

[i.17] Recommendation ITU-T X.501 (2008)/ISO/IEC 9594-1 (2008): "Information technology - Open Systems Interconnection - The Directory: Models".

[i.18] Recommendation ITU-T X.509 (2008)/ISO/IEC 9594-8 (2008): "Information technology - Open Systems Interconnection - The Directory: Public-key and Attribute Certificate frameworks".

[i.19] Recommendation ITU-T X.683 (2008): "Information technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications".

[i.20] ETSI TS 101 733 (V2.1.1): "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TR 119 001 [i.3] and the following apply:

CAdES signature: digital signature that satisfies the requirements specified within ETSI EN 319 122 part 1 or part 2 [i.6]

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

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

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

NOTE: In the case of IETF RFC 3161 [4] protocol, the electronic time-stamp is referring to the `timeStampToken` field within the `TimeStampResp` element (the TSA's response returned to the requesting client).

Legacy CAdES 101 733 signature: digital signature generated according to ETSI TS 101 733 [1]

Legacy CAdES baseline signature: digital signature generated according to ETSI TS 103 173 [i.1]

Legacy CAdES signature: legacy CAdES 101 733 signature or a legacy CAdES baseline signature

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.3] and the following apply:

ATSv2 archive-time-stamp attribute

NOTE: As defined in clause A.2.4.

ATSv3 archive-time-stamp-v3 attribute

NOTE: As defined in clause 5.5.3.

4 General syntax

4.1 General requirements

CAdES signatures shall build on Cryptographic Message Syntax (CMS), as defined in IETF RFC 5652 [7], by incorporation of signed and unsigned attributes as defined in clause 5.1.

CAdES signatures shall comply with clauses 2, 3, 4 and 5 of IETF RFC 5652 [7].

The following clauses list the types that are used in the attributes described in clause 5.1.

4.2 The `data` content type

The `data` content type shall be as defined in CMS (IETF RFC 5652 [7], clause 4). It is used to refer to arbitrary octet strings.

NOTE: The `data` content type is identified by the object identifier `id-data OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 1 }`.

4.3 The `signed-data` content type

The `signed-data` content type shall be as defined in CMS (IETF RFC 5652 [7], clause 5). It represents the content to sign and one or more signature values.

4.4 The `SignedData` type

The `SignedData` type shall be as defined in CMS (IETF RFC 5652 [7], clause 5.1). The `CMSVersion` shall be set to either 1 or 3 as specified in clause 5.1 of IETF RFC 5652 [7].

`SignedData.xxx` refers to the element `xxx` within the `SignedData` type, like for example `SignedData.certificates`, or `SignedData.crls`. In the same way, if `xxx` is of type `XXX`, `SignedData.xxx.yyy` is used to refer to the element `yyy` of type `XXX`, like for example `SignedData.crls.crl` or `SignedData.crls.other`.

NOTE: Clause 5.1 of IETF RFC 5652 [7] requires that the CMS `SignedData` version be set to 3 if certificates from `SignedData` is present AND (any version 1 attribute certificates are present OR any `SignerInfo` structures are version 3 OR `eContentType` from `encapContentInfo` is other than `id-data`). Otherwise, the CMS `SignedData` version is required to be set to 1.

4.5 The `EncapsulatedContentInfo` type

The `EncapsulatedContentInfo` type shall be as defined in CMS (IETF RFC 5652 [7], clause 5.2).

For the purpose of long-term validation, either the `eContent` should be present, or the data that is signed should be archived in such a way as to preserve any data encoding.

NOTE 1: It is important that the OCTET STRING used to generate the signature remains the same every time either the verifier or an arbitrator validates the signature.

NOTE 2: The `eContent` is optional in CMS:

- When it is present, this allows the signed data to be encapsulated in the `SignedData` structure which then contains both the signed data and the signature. However, the signed data can only be accessed by a verifier able to decode the ASN.1 encoded `SignedData` structure.
- When it is missing, this allows the signed data to be sent or stored separately from the signature, and the `SignedData` structure only contains the signature. Under these circumstances, the data object that is signed needs to be stored and distributed in such a way as to preserve any data encoding.

4.6 The `SignerInfo` type

The `SignerInfo` type of the digital signature shall be as defined in CMS (IETF RFC 5652 [7], clause 5.3).

The per-signer information is represented in the type `SignerInfo`. In the case of multiple parallel signatures, there is one instance of this field for each signer.

The degenerate case where there are no signers shall not be used.

4.7 ASN.1 Encoding

4.7.1 DER

Distinguished Encoding Rules (DER) for ASN.1 types shall be as defined in Recommendation ITU-T X.690 [17].

4.7.2 BER

If Basic Encoding Rules (BER) are used for some ASN.1 types, it shall be as defined in Recommendation ITU-T X.690 [17].

4.8 Other standard data structures

4.8.1 Time-stamp token format

The `TimeStampToken` type shall be as defined in IETF RFC 3161 [4] and updated by IETF RFC 5816 [9].

NOTE: Time-stamp tokens are profiled in ETSI EN 319 422 [i.9].

4.8.2 Additional types

The `VisibleString`, `BMPString`, `IA5String`, `GeneralizedTime` and `UTCTime` types shall be as defined in Recommendation ITU-T X.680 [16].

The `DirectoryString` type shall be as defined in Recommendation ITU-T X.520 [15].

The AttributeCertificate type shall be as defined in IETF RFC 5755 [8] which is compatible with the definition in Recommendation ITU-T X.509 [i.18].

The ResponderID, OCSPResponse and BasicOCSPResponse types shall be as defined in IETF RFC 6960 [14].

The Name, Certificate and AlgorithmIdentifier types shall be as defined in IETF RFC 5280 [6].

The Attribute type shall be as defined in IETF RFC 5280 [6] which is compatible with the definition in Recommendation ITU-T X.501 [i.17].

The CertificateList type shall be as defined in IETF RFC 5280 [6] which is compatible with the X.509 v2 CRL syntax in Recommendation ITU-T X.509 [i.18].

The RevocationInfoChoices type shall be as defined in IETF RFC 5652 [7].

4.9 Attributes

Clause 5 provides details on attributes specified within CMS (IETF RFC 5652 [7]), ESS (IETF RFC 2634 [3] and IETF RFC 5035 [5]), and defines new attributes for building CAdES signatures.

The clause distinguishes between two main types of attributes: signed attributes and unsigned attributes. The first ones are attributes that are covered by the signature produced by the signer, which implies that the signer has processed these attributes before creating the signature. The unsigned attributes are added by the signer, by the verifier or by other parties after the production of the signature. They are not secured by the signature in the SignerInfo element (the one computed by the signer); however they can be actually covered by subsequent times-stamp attributes.

Signed and unsigned attributes are stored, respectively, in the signedAttrs and unsignedAttrs fields of SignerInfo (see clause 4.6).

5 Attribute semantics and syntax

5.1 CMS defined basic signed attributes

5.1.1 The content-type attribute

Semantics

The content-type attribute is a signed attribute.

The content-type attribute indicates the type of the signed content.

SyntaxThe content-type attribute shall be as defined in CMS (IETF RFC 5652 [7], clause 11.1).

NOTE: As stated in IETF RFC 5652 [7], the content of ContentType (the value of the attribute content-type) is the same as the eContentType of the EncapsulatedContentInfo value being signed.

5.1.2 The message-digest attribute

Semantics

The message-digest attribute is a signed attribute.

The message-digest attribute specifies the message digest of the content being signed.

SyntaxThe message-digest attribute shall be as defined in CMS (IETF RFC 5652 [7], clause 11.2).

The message digest calculation process shall be as defined in CMS (IETF RFC 5652 [7], clause 5.4).

5.2 Basic attributes for CAdES signatures

5.2.1 The `signing-time` attribute

Semantics

The `signing-time` attribute is a signed attribute.

The `signing-time` attribute shall specify the time at which the signer claims to having performed the signing process.

Syntax

The `signing-time` attribute shall be as defined in CMS (IETF RFC 5652 [7], clause 11.3).

5.2.2 Signing certificate reference attributes

5.2.2.1 General requirements

Semantics

The attributes specified in sub-clauses below shall contain one reference to the signing certificate.

The attributes specified in sub-clauses below may contain references to some of or all the certificates within the signing certificate path, including one reference to the trust anchor when this is a certificate.

For each certificate, these attributes shall contain a digest value.

NOTE 1: For instance, the signature validation policy can mandate other certificates to be present which can include all the certificates up to the trust anchor.

NOTE 2: IETF RFC 2634 [3] and IETF RFC 5035 [5] state that the first certificate in the sequence is the certificate used to verify the signature and that other certificates in the sequence can be attribute certificates or other certificate types.

5.2.2.2 ESS `signing-certificate` attribute

Semantics

The ESS `signing-certificate` attribute is a signed attribute.

The ESS `signing-certificate` attribute is a signing certificate attribute using the SHA-1 hash algorithm.

Syntax

The `signing-certificate` attribute shall be as defined in Enhanced Security Services (ESS), IETF RFC 2634 [3], clause 5.4, and further specified in the present document.

NOTE 1: The `certHash` from `ESSCertID` is computed using SHA-1 over the entire DER encoded certificate (IETF RFC 2634 [3]).

The `policies` field shall not be used.

If the `issuerAndSerialNumber` field in `SignerIdentifier` field of the `SignerInfo` and the `issuerSerial` field in `ESSCertID` are present, they shall match.

NOTE 2: The information in the `IssuerSerial` element is only a hint that can help to identify the certificate whose digest matches the value present in the reference. But the binding information is the digest of the certificate.