Draft ETSI EN 319 122-1 V1.1.5 (2021-07)

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

Reference

REN/ESI-0019122-1v121

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 - 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/CommiteeSupportStaff.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.

Contents

Intellectual Property Rights 6
Foreword 6
Modal verbs terminology 6
Introduction 7
1 Scope 8
2 References 8
2.1 Normative references 8
2.2 Informative references 9
3 Definition of terms, symbols and abbreviations 10
3.1 Terms 10
3.2 Symbols 11
3.3 Abbreviations 11
4 General syntax 12
4.1 General requirements 12
4.2 The `data` content type 12
4.3 The `signed-data` content type 12
4.4 The `SignedData` type 12
4.5 The `EncapsulatedContentInfo` type 12
4.6 The `SignerInfo` type 13
4.7 ASN.1 Encoding 13
4.7.1 DER 13
4.7.2 BER 13
4.8 Other standard data structures 13
4.8.1 Time-stamp token format 13
4.8.2 Additional types 13
4.9 Attributes 14
5 Attribute semantics and syntax 14
5.1 CMS defined basic signed attributes 14
5.1.1 The `content-type` attribute 14
5.1.2 The `message-digest` attribute 14
5.2 Basic attributes for CAdES signatures 15
5.2.1 The `signing-time` attribute 15
5.2.2 Signing certificate reference attributes 15
5.2.2.1 General requirements 15
5.2.2.2 ESS `signing-certificate` attribute 15
5.2.2.3 ESS `signing-certificate-v2` attribute 15
5.2.3 The `commitment-type-indication` attribute 16
5.2.4 Attributes for identifying the signed data type 17
5.2.4.1 The `content-hints` attribute 17
5.2.4.2 The `mime-type` attribute 17
5.2.5 The `signer-location` attribute 18
5.2.6 Incorporating attributes of the signer 18
5.2.6.1 The `signer-attributes-v2` attribute 18
5.2.6.2 claimed-SAML-assertion 20
5.2.6.3 signed-SAML-assertion 20
5.2.7 The `countersignature` attribute 20
5.2.8 The `content-time-stamp` attribute 21
5.2.9 The `signature-policy-identifier` attribute and the `SigPolicyQualifierInfo` type 21
5.2.9.1 The `signature-policy-identifier` attribute 21
5.2.9.2 The SigPolicyQualifierInfo type 22
5.2.10 The `signature-policy-store` attribute 24
5.2.11 The `content-reference` attribute 25

5.2.12 The content-identifier attribute 25
5.2.13 The cms-algorithm-protection attribute 25
5.3 The signature-time-stamp attribute 26
5.4 Attributes for validation data values 26
5.4.1 Introduction 26
5.4.2 OCSP responses 26
5.4.2.1 OCSP response types 26
5.4.2.2 OCSP responses within RevocationInfoChoices 26
5.4.3 CRLs 27
5.5 Attributes for long term availability and integrity of validation material 27
5.5.1 Introduction 27
5.5.2 The ats-hash-index-v3 attribute 27
5.5.3 The archive-time-stamp-v3 attribute 29

6 CAdES baseline signatures 31
6.1 Signature levels 31
6.2 General requirements 32
6.2.1 Algorithm requirements 32
6.2.2 Notation for requirements 32
6.3 Requirements on components and services 34
6.4 Legacy CAdES baseline signatures 37

Annex A (normative): Additional Attributes Specification 38

A.1 Attributes for validation data 38
A.1.1 Certificates validation data 38
A.1.1.1 The complete-certificate-references attribute 38
A.1.1.2 The certificate-values attribute 39
A.1.2 Revocation validation data 39
A.1.2.1 The complete-revocation-references attribute 39
A.1.2.2 The revocation-values attribute 41
A.1.3 The attribute-certificate-references attribute 42
A.1.4 The attribute-revocation-references attribute 43
A.1.5 Time-stamps on references to validation data 44
A.1.5.1 The time-stamped-certs-crls-references attribute 44
A.1.5.2 The CAdES-C-timestamp attribute 45

A.2 Deprecated attributes 45
A.2.1 Usage of deprecated attributes 45
A.2.2 The other-signing-certificate attribute 45
A.2.3 The signer-attributes attribute 46
A.2.4 The archive-time-stamp attribute 46
A.2.5 The long-term-validation attribute 46
A.2.6 The ats-hash-index attribute 46

Annex B (normative): Alternative mechanisms for long term availability and integrity of validation data 47

Annex C: Void 48

Annex D (normative): Signature Format Definitions Using X.680 ASN.1 Syntax 49

Annex E (informative): Example Structured Contents and MIME 56

E.1 Use of MIME to Encode Data 56
E.1.1 MIME Structure 56
E.1.2 Header Information 56
E.1.3 Content Encoding 57
E.1.4 Multi-Part Content 57

E.2 S/MIME 57
E.2.1 Using S/MIME 57
E.2.2 Using application/pkcs7-mime 58

E.2.3 Using multipart/signed and application/pkcs7-signature....58
E.3 Use of MIME in the signature....59
Annex F (informative): Change History....61
History....62

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 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, augmentation and validation of CAdES digital signatures are out of scope and specified in ETSI EN 319 102-1 [i.5]. Guidance on creation, augmentation and validation of CAdES digital signatures including the usage of the different properties defined in the present document is provided in ETSI TR 119 100 [i.4].

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 IETF 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".

[19] IETF RFC 6211 (2011): "Cryptographic Message Syntax (CMS) Algorithm Identifier Protection Attribute".

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 TS 103 173 (V2.2.1): "Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile".

[i.2] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview".

[i.3] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.4] ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for signature creation and validation".

[i.5] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: 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 token 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] Void.

[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".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms 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 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

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

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 (V2.2.1) [1]

Legacy CAdES baseline signature: digital signature generated according to ETSI TS 103 173 (V2.2.1) [i.1]

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

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

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 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

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

3.2 Symbols

Void.

3.3 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 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 digital signature value produced by the signer using his/her private key, 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.

Syntax

The `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.

Syntax

The `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 clauses below shall contain one reference to the signing certificate.

The attributes specified in 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.

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.

5.2.2.3 ESS `signing-certificate-v2` attribute

Semantics

The ESS `signing-certificate-v2` attribute is a signed attribute.