

**Electronic Signatures and Infrastructures (ESI);  
CAAdES digital signatures;  
Part 1: Building blocks and CAAdES baseline signatures**  
(ETSI EN 319 122-1 V1.1.1 (2016-04))

Copyright ÖVE

---

**Medieninhaber und Hersteller:**

OVE Österreichischer Verband für Elektrotechnik  
Austrian Standards Institute

**ICS** 35.040

**Copyright © OVE/Austrian Standards Institute – 2016.**

**Alle Rechte vorbehalten!** Nachdruck oder  
Vervielfältigung, Aufnahme auf oder in sonstige Medien  
oder Datenträger nur mit Zustimmung gestattet!

**Ident (IDT) mit** ETSI EN 319 122-1 V1.1.1 (2016-04)

**zuständig** OVE/Komitee  
TK IT-EG  
Informationstechnologie, Telekommunikation und  
Elektronik

**Verkauf von in- und ausländischen Normen und  
technischen Regelwerken durch**

Austrian Standards Institute  
Heinestraße 38, 1020 Wien  
E-Mail: [sales@austrian-standards.at](mailto:sales@austrian-standards.at)  
Internet: [www.austrian-standards.at](http://www.austrian-standards.at)  
Webshop: [www.austrian-standards.at/webshop](http://www.austrian-standards.at/webshop)  
Tel.: +43 1 213 00-300  
Fax: +43 1 213 00-818

Alle Regelwerke für die Elektrotechnik auch erhältlich bei

OVE Österreichischer Verband für Elektrotechnik

Eschenbachgasse 9, 1010 Wien

E-Mail: [verkauf@ove.at](mailto:verkauf@ove.at)

Internet: [www.ove.at](http://www.ove.at)

Webshop: [www.ove.at/webshop](http://www.ove.at/webshop)

Tel.: +43 1 587 63 73

Fax: +43 1 587 63 73 - 99

## Nationales Vorwort

Diese Europäische Norm EN 319 122-1 V1.1.1:2016 hat sowohl den Status von ÖSTERREICHISCHEN BESTIMMUNGEN FÜR DIE ELEKTROTECHNIK gemäß ETG 1992 als auch den einer ÖNORM gemäß NG 1971. Bei ihrer Anwendung ist dieses Nationale Vorwort zu berücksichtigen.

Für den Fall einer undatierten normativen Verweisung (Verweisung auf einen Standard ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste Ausgabe dieses Standards.

Für den Fall einer datierten normativen Verweisung bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Standards.

Der Rechtsstatus dieser ÖSTERREICHISCHEN BESTIMMUNGEN FÜR DIE ELEKTROTECHNIK/ÖNORM ist den jeweils geltenden Verordnungen zum Elektrotechnikgesetz zu entnehmen.

Bei mittels Verordnungen zum Elektrotechnikgesetz verbindlich erklärten ÖSTERREICHISCHEN BESTIMMUNGEN FÜR DIE ELEKTROTECHNIK/ÖNORMEN ist zu beachten:

- Hinweise auf Veröffentlichungen beziehen sich, sofern nicht anders angegeben, auf den Stand zum Zeitpunkt der Herausgabe dieser ÖSTERREICHISCHEN BESTIMMUNGEN FÜR DIE ELEKTROTECHNIK/ÖNORM. Zum Zeitpunkt der Anwendung dieser ÖSTERREICHISCHEN BESTIMMUNGEN FÜR DIE ELEKTROTECHNIK/ÖNORM ist der durch die Verordnungen zum Elektrotechnikgesetz oder gegebenenfalls auf andere Weise festgelegte aktuelle Stand zu berücksichtigen.
- Informative Anhänge und Fußnoten sowie normative Verweise und Hinweise auf Fundstellen in anderen, nicht verbindlichen Texten werden von der Verbindlicherklärung nicht erfasst.

Europäische Normen (EN) werden durch Veröffentlichung eines identen Titels und Textes in das Gesamtwerk der ÖSTERREICHISCHEN BESTIMMUNGEN FÜR DIE ELEKTROTECHNIK/ÖNORMEN übernommen, wobei der Nummerierung der Zusatz ÖVE/ÖNORM bzw. ÖNORM vorangestellt wird.

Der von ETSI übermittelte Normentext wird in englischer Sprache veröffentlicht, da davon ausgegangen werden kann, dass die Anwender der Norm über ausreichende englische Sprachkenntnisse verfügen.

ETSI EN 319 122-1 V1.1.1 (2016-04)



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

Copyright OVER

---

**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  
<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>

---

**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.

© European Telecommunications Standards Institute 2016.  
All rights reserved.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.  
**3GPP™** and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.  
**GSM®** and the GSM logo are Trade Marks registered and owned by the GSM Association.

# Contents

Intellectual Property Rights .....	5
Foreword.....	5
Modal verbs terminology.....	5
Introduction .....	5
1 Scope .....	7
2 References .....	7
2.1 Normative references .....	7
2.2 Informative references.....	8
3 Definitions and abbreviations.....	9
3.1 Definitions.....	9
3.2 Abbreviations .....	10
4 General syntax.....	10
4.1 General requirements .....	10
4.2 The data content type.....	10
4.3 The signed-data content type.....	11
4.4 The SignedData type.....	11
4.5 The EncapsulatedContentInfo type.....	11
4.6 The SignerInfo type.....	11
4.7 ASN.1 Encoding.....	11
4.7.1 DER .....	11
4.7.2 BER .....	11
4.8 Other standard data structures .....	12
4.8.1 Time-stamp token format.....	12
4.8.2 Additional types.....	12
4.9 Attributes.....	12
5 Attribute semantics and syntax.....	12
5.1 CMS defined basic signed attributes .....	12
5.1.1 The content-type attribute.....	12
5.1.2 The message-digest attribute .....	13
5.2 Basic attributes for CADES signatures .....	13
5.2.1 The signing-time attribute.....	13
5.2.2 Signing certificate reference attributes .....	13
5.2.2.1 General requirements .....	13
5.2.2.2 ESS signing-certificate attribute .....	13
5.2.2.3 ESS signing-certificate-v2 attribute.....	14
5.2.3 The commitment-type-indication attribute.....	14
5.2.4 Attributes for identifying the signed data type.....	15
5.2.4.1 The content-hints attribute .....	15
5.2.4.2 The mime-type attribute.....	16
5.2.5 The signer-location attribute .....	16
5.2.6 Incorporating attributes of the signer .....	17
5.2.6.1 The signer-attributes-v2 attribute .....	17
5.2.6.2 claimed-SAML-assertion .....	18
5.2.7 The countersignature attribute.....	19
5.2.8 The content-time-stamp attribute.....	19
5.2.9 The signature-policy-identifier attribute and the SigPolicyQualifierInfo type.....	19
5.2.9.1 The signature-policy-identifier attribute.....	19
5.2.9.2 The SigPolicyQualifierInfo type .....	20
5.2.10 The signature-policy-store attribute .....	22
5.2.11 The content-reference attribute .....	23
5.2.12 The content-identifier attribute.....	23
5.3 The signature-time-stamp attribute.....	23
5.4 Attributes for validation data values.....	24

5.4.1	Introduction.....	24
5.4.2	OCSP responses.....	24
5.4.2.1	OCSP response types.....	24
5.4.2.2	OCSP responses within RevocationInfoChoices.....	24
5.4.3	CRLs.....	24
5.5	Attributes for long term availability and integrity of validation material.....	24
5.5.1	Introduction.....	24
5.5.2	The ats-hash-index-v3 attribute.....	25
5.5.3	The archive-time-stamp-v3 attribute.....	26
6	CADES baseline signatures.....	29
6.1	Signature levels.....	29
6.2	General requirements.....	29
6.2.1	Algorithm requirements.....	29
6.2.2	Notation for requirements.....	29
6.3	Requirements on components and services.....	32
6.4	Legacy CADES baseline signatures.....	35
<b>Annex A (normative): Additional Attributes Specification.....</b>		<b>36</b>
A.1	Attributes for validation data.....	36
A.1.1	Certificates validation data.....	36
A.1.1.1	The complete-certificate-references attribute.....	36
A.1.1.2	The certificate-values attribute.....	37
A.1.2	Revocation validation data.....	37
A.1.2.1	The complete-revocation-references attribute.....	37
A.1.2.2	The revocation-values attribute.....	39
A.1.3	The attribute-certificate-references attribute.....	40
A.1.4	The attribute-revocation-references attribute.....	41
A.1.5	Time-stamps on references to validation data.....	42
A.1.5.1	The time-stamped-certs-crls-references attribute.....	42
A.1.5.2	The CADES-C-timestamp attribute.....	43
A.2	Deprecated attributes.....	43
A.2.1	Usage of deprecated attributes.....	43
A.2.2	The other-signing-certificate attribute.....	43
A.2.3	The signer-attributes attribute.....	44
A.2.4	The archive-time-stamp attribute.....	44
A.2.5	The long-term-validation attribute.....	44
A.2.6	The ats-hash-index attribute.....	44
<b>Annex B (normative): Alternative mechanisms for long term availability and integrity of validation data.....</b>		<b>45</b>
<b>Annex C (informative): Signature Format Definitions Using X.208 ASN.1 Syntax.....</b>		<b>46</b>
<b>Annex D (normative): Signature Format Definitions Using X.680 ASN.1 Syntax.....</b>		<b>52</b>
<b>Annex E (informative): Example Structured Contents and MIME.....</b>		<b>59</b>
E.1	Use of MIME to Encode Data.....	59
E.1.1	MIME Structure.....	59
E.1.2	Header Information.....	59
E.1.3	Content Encoding.....	60
E.1.4	Multi-Part Content.....	60
E.2	S/MIME.....	60
E.2.1	Using S/MIME.....	60
E.2.2	Using application/pkcs7-mime.....	61
E.2.3	Using multipart/signed and application/pkcs7-signature.....	61
E.3	Use of MIME in the signature.....	62
History.....		64

---

## 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 (<https://ipr.etsi.org/>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

---

## 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 CAAdES digital signatures, as identified below:

**Part 1: "Building blocks and CAAdES baseline signatures";**

Part 2: "Extended CAAdES signatures".

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

National transposition dates	
Date of adoption of this EN:	1 April 2016
Date of latest announcement of this EN (doa):	31 July 2016
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 January 2017
Date of withdrawal of any conflicting National Standard (dow):	31 January 2017

---

## 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.

Copyright OVER

---

# 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.