ÖVE/ÖNORM
EN 319 122-1 V1.2.1

Ausgabe: 2022-01-01

Electronic Signatures and Infrastructures (ESI); CAdES digital signatures;
Part 1: Building blocks and CAdES baseline signatures
(ETSI EN 319 122-1 V1.2.1 (2021-10))

Medieninhaber und Hersteller:
OVE Österreichischer Verband für Elektrotechnik
Austrian Standards Institute

Verkauf von in- und ausländischen Normen und technischen Regelwerken durch
Austrian Standards Institute
Heinestraße 38, 1020 Wien
E-Mail: sales@austrian-standards.at
Internet: www.austrian-standards.at
Webshop: 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
Internet: www.ove.at
Webshop: www.ove.at/shop
Tel.: +43 1 587 63 73

ICS 35.040

Ident (IDT) mit ETSI EN 319 122-1 V1.2.1 (2021-10)

Ersatz für siehe nationales Vorwort

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

Nationales Vorwort

Diese Europäische Norm EN 319 122-1 V1.2.1:2022 hat sowohl den Status einer nationalen elektrotechnischen Norm gemäß ETG 1992 als auch den einer nationalen Norm gemäß NormG 2016. 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 nationalen (elektrotechnischen) Norm ist den jeweils geltenden Verordnungen zum Elektrotechnikgesetz zu entnehmen.

Bei mittels Verordnungen zum Elektrotechnikgesetz verbindlich erklärten nationalen (elektrotechnischen) Normen ist zu beachten:

- Hinweise auf Veröffentlichungen beziehen sich, sofern nicht anders angegeben, auf den Stand zum Zeitpunkt der Herausgabe dieser nationalen (elektrotechnischen) Norm. Zum Zeitpunkt der Anwendung dieser nationalen (elektrotechnischen) Norm 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) von ETSI werden gemäß den „Gemeinsamen Regeln“ von CEN/CENELEC durch Veröffentlichung eines identen Titels und Textes in das Gesamtwerk der nationalen (elektrotechnischen) Normen übernommen, wobei der Nummerierung der Zusatz ÖVE/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.

Erläuterung zum Ersatzvermerk

Gemäß Vorwort zur EN wird das späteste Datum, zu dem nationale (elektrotechnische) Normen, die der vorliegenden Norm entgegenstehen, zurückgezogen werden müssen, mit dow (date of withdrawal) festgelegt. Bis zum Zurückziehungsdatum (dow) 2022-07-31 ist somit die Anwendung folgender Norm(en) noch erlaubt:

ÖVE/ÖNORM EN 319 122-1 V1.1.1:2016-06-01.

ETSI EN 319 122-1 V1.2.1 (2021-10)

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

Contents

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 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].

National transposition dates	
Date of adoption of this EN:	18 October 2021
Date of latest announcement of this EN (doa):	31 January 2022
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 July 2022
Date of withdrawal of any conflicting National Standard (dow):	31 July 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

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 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] 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".