ÖVE/ÖNORM
EN 319 142-2 V1.1.1

Ausgabe: 2016-06-01

Electronic Signatures and Infrastructures (ESI); PAdES digital signatures;
Part 2: Additional PAdES signatures profiles
(ETSI EN 319 142-2 V1.1.1 (2016-04))

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/webshop
Tel.: +43 1 587 63 73
Fax: +43 1 587 63 73 - 99

ICS 35.040

Ident (IDT) mit ETSI EN 319 142-2 V1.1.1 (2016-04)

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

Nationales Vorwort

Diese Europäische Norm EN 319 142-2 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 319 142-2 V1.1.1 (2016-04)

Electronic Signatures and Infrastructures (ESI);
PAdES digital signatures;
Part 2: Additional PAdES signatures profiles

Reference
DEN/ESI-0019142-2

Keywords
electronic signature, PAdES, 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

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 (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 2 of a multi-part deliverable covering the PDF digital signatures (PAdES). Full details of the entire series can be found in part 1 [4].

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. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (i.e. repudiates; see ISO/IEC 10181-4 [i.1]) the validity of the signature.

Thus, the present document can be used for any document encoded in a portable document format (PDF) produced by an individual and a company, and exchanged between 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, SIM cards, special programs for digital signatures, etc.

The present document is part of a rationalized framework of standards (see ETSI TR 119 000 [i.8]). See ETSI TR 119 100 [i.9] for getting guidance on how to use the present document within the aforementioned framework.

1 Scope

The present document defines multiple profiles for PAdES digital signatures which are digital signatures embedded within a PDF file.

The present document contains a profile for the use of PDF signatures, as described in ISO 32000-1 [1] and based on CMS digital signatures [i.6], that enables greater interoperability for PDF signatures by providing additional restrictions beyond those of ISO 32000-1 [1]. This first profile is not related to ETSI EN 319 142-1 [4].

The present document also contains a second set of profiles that extend the scope of the profile in PAdES part 1 [5], while keeping some features that enhance interoperability of PAdES signatures. These profiles define three levels of PAdES extended 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. These PAdES extended signatures offer a higher degree of optionality than the PAdES baseline signatures specified in ETSI EN 319 142-1 [4].

The present document also defines a third profile for usage of an arbitrary XML document signed with XAdES signatures that is embedded within a PDF file.

The profiles defined in the present document provide equivalent requirements to profiles found in ETSI TS 102 778 [i.10].

Procedures for creation, augmentation, and validation of PAdES digital signatures are out of scope and specified in ETSI EN 319 102-1 [i.11]. Guidance on creation, augmentation and validation of PAdES digital signatures including the usage of the different attributes is provided in ETSI TR 119 100 [i.9].

The present document does not repeat the base requirements of the referenced standards, but instead aims to maximize interoperability of digital signatures in various business areas.

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] ISO 32000-1: "Document management - Portable document format - Part 1: PDF 1.7".

NOTE: Available at http://www.adobe.com/devnet/acrobat/pdfs/PDF32000_2008.pdf.

[2] IETF RFC 2315: "PKCS #7: Cryptographic Message Syntax Version 1.5".

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

[4] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[5] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[6] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".