

STN	Elektronické podpisy a infraštruktúry (ESI). Digitálne podpisy vo formáte PAdES. Časť 2: Doplňujúce podpisy profilov vo formáte PAdES.	STN EN 319 142-2 V1.1.1 87 9142
------------	---	---

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

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 01/17

Obsahuje: EN 319 142-2 V1.1.1:2016

124092

Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, 2017
Podľa zákona č. 264/1999 Z. z. v znení neskorších predpisov sa môžu slovenské technické normy
rozmnžovať a rozširovať iba so súhlasom Úradu pre normalizáciu, metrológiu a skúšobníctvo SR.

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

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	9
4 Profile for CMS digital signatures in PDF	9
4.1 Features	9
4.2 Requirements of Profile for CMS Signatures in PDF	10
4.2.1 Requirements on PDF signatures.....	10
4.2.2 Requirements on PDF signature handlers.....	10
4.2.3 Requirements on signature validation.....	10
4.2.4 Requirements on Time Stamping.....	11
4.2.4.1 Requirements on electronic time-stamp creation	11
4.2.4.2 Requirements on electronic time-stamp validation	11
4.2.5 Requirements on revocation checking.....	11
4.2.6 Requirements on Seed Values	11
4.2.7 Requirements on encryption	11
5 Extended PAdES signature profiles	11
5.1 Features	11
5.2 General Requirements	11
5.2.1 Requirements from Part 1	11
5.2.2 Notation of Requirements.....	12
5.3 PAdES-E-BES Level.....	12
5.4 PAdES-E-EPES Level.....	14
5.5 PAdES-E-LTV Level	14
6 Profiles for XAdES Signatures signing XML content in PDF	14
6.1 Features	14
6.2 Profiles for XAdES signatures of signed XML documents embedded in PDF containers.....	15
6.2.1 Overview	15
6.2.2 Profile for Basic XAdES signatures of XML documents embedded in PDF containers	17
6.2.2.1 Features	17
6.2.2.2 General syntax and requirements	17
6.2.2.3 Requirements for applications generating signed XML document to be embedded	17
6.2.2.4 Mandatory operations.....	18
6.2.2.4.1 Protecting the signing certificate	18
6.2.2.5 Requirements on XAdES optional properties	18
6.2.2.6 Serial Signatures	19
6.2.2.7 Parallel Signatures.....	19
6.2.2.8 PAdES Signatures	19
6.2.3 Profile for long-term XAdES signatures of signed XML documents embedded in PDF containers	19
6.2.3.1 Features	19
6.2.3.2 Augmentation mechanism.....	19
6.2.3.3 Optional properties.....	19
6.2.3.4 Validation Process.....	19
6.3 Profiles for XAdES signatures on XFA Forms	20
6.3.1 Overview	20
6.3.2 Profile for Basic XAdES signatures on XFA forms	22

6.3.2.1	Features	22
6.3.2.2	General syntax and requirements	22
6.3.2.3	Mandatory operations.....	23
6.3.2.3.1	Protecting the signing certificate	23
6.3.2.4	Requirements on XAdES optional properties	23
6.3.2.5	Serial Signatures	24
6.3.2.6	Parallel Signatures.....	25
6.3.3	Profile for long-term validation XAdES signatures on XFA forms.....	25
6.3.3.1	Overview	25
6.3.3.2	Features	25
6.3.3.3	General Requirements.....	25
6.3.4	Extensions Dictionary	25
Annex A (informative):	General Features.....	26
A.1	PDF signatures	26
A.2	PDF Signature types.....	27
A.3	PDF Signature Handlers.....	27
A.4	PDF serial signatures.....	27
A.5	PDF signature Validation and Time-stamping	28
A.6	ISO 19005-1: 2005 (PDF/A-1).....	28
A.7	ISO 19005-2:2011 (PDF/A-2).....	29
A.8	Seed Values and Signature Policies	29
History		30

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".

- [7] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".
- [8] Adobe ® XFA: "XML Forms Architecture (XFA) Specification" version 2.5, (June 2007), Adobe Systems Incorporated".
- [9] W3C Recommendation: "XML-Signature Syntax and Processing, Version 1.1".
- [10] IETF RFC 5035 (2007): "Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility".
- [11] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".
- [12] IETF RFC 5816 (2010): "ESSCertIDv2 Update for RFC 3161".

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] ISO/IEC 10181-4: "Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework".
- [i.2] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".
- [i.3] IETF RFC 5755: "An Internet Attribute Certificate Profile for Authorization".
- [i.4] W3C® Working Group Note, XML Signature Best Practices, 11 April 2013.
- [i.5] ISO 19005-1:2005: "Document management - Electronic document file format for long-term preservation - Part 1: Use of PDF 1.4 (PDF/A-1)".
- [i.6] IETF RFC 5652 (2009): "Cryptographic Message Syntax (CMS)".
- [i.7] ISO 19005-2 (2011): "Document management - Electronic document file format for long-term preservation - Part 2: Use of ISO 32000-1 (PDF/A-2)".
- [i.8] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview".
- [i.9] ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Business Driven Guidance for Signature Creation and Validation".
- [i.10] ETSI TS 102 778: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; CMS Profile based on ISO 32000-1".
- [i.11] 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.12] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

koniec náhľadu – text ďalej pokračuje v platenej verzii STN