Draft ETSI EN 319 142-2 V1.0.0 (2015-06)

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
http://portal.etsi.org/tb/status/status.asp

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

Copyright Notification

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 (http://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 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 2 of a multi-part deliverable covering the PDF digital signatures (PAdES), as identified below.

Part 1: "Building blocks and PAdES baseline signatures";

Part 2: "Additional PAdES signatures profiles".

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. 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 part 1 of ETSI EN 319 142 [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 part 1 of ETSI EN 319 142 [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 ETSI TS 102 778 [i.10].

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 reference 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); Rationalized structure for Electronic Signature Standardization".

[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".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ISO 32000-1 [1] and the following apply:

certificate: public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it

certificate policy (CP): named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

Certificate Revocation List (CRL): signed list indicating a set of public key certificates that are no longer considered valid by the certificate issuer

Certification Authority (CA): authority trusted by one or more users to create and assign public key certificates; optionally, the certification authority may create the users' keys

certification signature: digital signature that is used in conjunction with Modification Detection Permissions (MDP) as defined by ISO 32000-1 [1], clause 12.8.2.2

electronic time-stamp: data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed at that time

NOTE: In the case of IETF RFC 3161 [11] updated by IETF RFC 5816 [12] protocol, the electronic time-stamp is referring to the `timeStampToken` field within the `TimeStampResp` element (the TSA's response returned to the requesting client).

PAdES signature: digital signature that satisfies the requirements specified within the present document

PDF serial signature: specific digital signature where the second (and subsequent) signers of a PDF not only sign the document but also the signature of the previous signer and any modification that can also have taken place (e.g. form fill-in)

PDF signature: DER-encoded binary data object based on the PKCS #7 [2] or the CMS (IETF RFC 5652 [i.6]) or related syntax containing a digital signature and other information necessary to validate the electronic signature such as the signer's certificate along with any supplied revocation information placed within a PDF document structure as specified in ISO 32000-1 [1], clause 12.8

relying party: natural or legal person that relies upon electronic identification or trust service

seed value dictionary: PDF data structure, of type dictionary, as described in ISO 32000-1 [1], clause 12.7.4.5, table 234, that contains information that constrains the properties of a digital signature that is applied to a specific Signature field

signature dictionary: PDF data structure, of type dictionary, as described in ISO 32000-1 [1], clause 12.8.1, table 252 that contains all information about the digital signature

signature handler: software application, or part of a software application, that knows how to perform digital signature operations (e.g. signing and/or validating) in conformance with ISO 32000-1 [1] and the requirements of the appropriate profile

signer: natural or legal person who creates a digital signature

Time-Stamping Authority (TSA): trusted third party that creates electronic time-stamps in order to indicate that a datum existed at a particular point in time

validation data: data that can be used by a verifier of digital signatures to determine that a digital signature is valid (e.g. certificates, CRLs, OCSP responses)

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CA	Certification Authority
CAdES	CMS Advanced Electronic Signatures

NOTE: As per ETSI EN 319 122-1 [5].

CMS	Cryptographic Message Syntax

NOTE: As specified in IETF RFC 5652 [i.6].

CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
OCSP	Online Certificate Status Protocol
PDF	Portable Document Format
TSA	Time-Stamping Authority

4 Profile for CMS digital signatures in PDF

4.1 Features

The present profile specifies digital signatures that:

- Are encoded in CMS as defined by PKCS #7 1.5 (see IETF RFC 2315 [2]).
- Support serial signatures.
- Optionally include signature time-stamps.
- Optionally include revocation information.
- Protect integrity of the document and authenticates the signer identity information included in the signing certificate.
- Can optionally include the "reasons" for the signature.
- Can optionally include a description of the location of signing.
- Can optionally include contact info of the signer.

A "legal content attestation" can be used to indicate to the relying party the PDF capabilities which may affect the signed document (e.g. JavaScript).

4.2 Requirements of Profile for CMS Signatures in PDF

4.2.1 Requirements on PDF signatures

While ISO 32000-1 [1], clause 12.8 clearly states the majority of the requirements necessary for conformance with this profile, this clause specifies additional requirements for conformance.

a) PDF Signatures shall be as specified in ISO 32000-1 [1], clause 12.8.

b) The signature information shall be embedded into the document itself and the ByteRange shall be the entire file, including the signature dictionary but excluding the PDF Signature itself.

c) The PDF Signature (a DER-encoded PKCS#7 binary data object) shall be placed into the **Contents** entry of the signature dictionary.

d) The PKCS#7 object shall conform to the PKCS#7 specification in IETF RFC 2315 [2]. At minimum, it shall include the signer's X.509 signing certificate.

NOTE 1: Although ISO 32000-1 [1] also allows the value of the Contents entry of signature dictionary to be a DER-encoded PKCS#1 binary data object, that format is not supported by this profile.

e) Timestamping and revocation information should be included in the PDF Signature. This revocation information and as much of the complete chain of certificates as is available should be captured and validated before completing the creation of the PDF Signature.

f) If present, any revocation information shall be a signed attribute of the PDF Signature.

g) IETF RFC 5755 [i.3] attribute certificates associated with the signer certificate should not be used.

NOTE 2: ISO 32000-1 [1] allows the inclusion of one or more IETF RFC 5755 [i.3] attribute certificates associated with the signer certificate. However, attribute certificates are not widely supported and hence use of this attribute will reduce interoperability.

h) There shall only be a single signer (i.e. one single component of "SignerInfo" type within "signerInfos" element) in any PDF Signature.

4.2.2 Requirements on PDF signature handlers

a) A PDF reader may substitute a different signature handler, other than that specified in **Filter**, when validating the signature, as long as it supports the specified **SubFilter** format.

b) Only the two values for **SubFilter** listed in ISO 32000-1 [1], clause 12.8.3.3.1 (i.e. **adbe.pkcs7.detached** and **adbe.pkcs7.sha1**) shall be used.

NOTE: While the names of the SubFilters can imply specific algorithms, the actual list of supported algorithms can be found in ISO 32000-1 [1], clause 12.8.3.3.2, table 257. Consult ETSI TS 119 312 [i.2] for guidance on algorithm choices.

The use of SHA-1 is being phased out and hence other hashing algorithms should be used.

4.2.3 Requirements on signature validation

When the user opens a signed document and requests validation of the signature(s) present in the PDF, a reader shall invoke the appropriate signature handler that shall perform the following steps to validate them.

a) Validate that the document digest matches that in the signature as specified in ISO 32000-1 [1], clause 12.8.1.

b) Validate the path of certificates used to validate the binding between the subject distinguished name and subject public key as specified in IETF RFC 5280 [3]. The validity checks shall be carried out at the time indicated either by electronic time-stamp applied as per clause 4.2.4 or some other trusted indication of the signing time. The revocation status shall be checked as specified in clause 4.2.5.

c) To achieve consistent validation results with existing signatures and existing implementations of signature handlers, that did not know this attribute, the signing certificate reference attribute itself should be ignored during validation if present.

NOTE: Unlike any other Profile in the present document inclusion of the certificate hash (see CAdES [5], clause 5.2.2) is not required by this profile. Applications requiring the existence of certificate hash can use signatures based on PAdES baseline profiles [4] or the profile defined in clause 5.3 or the profile defined in clause 5.4.

4.2.4 Requirements on Time Stamping

4.2.4.1 Requirements on electronic time-stamp creation

a) An electronic time-stamp from a trusted TSA should be applied to the digital signature as soon as possible after the signature is created so the electronic time-stamp reflects the time after the document was signed.

b) If a signature handler chooses to embed an electronic time-stamp into the PDF Signature, then it shall be embedded as described in ISO 32000-1 [1], clause 12.8.3.3.1.