Draft EN 319 142-2 V0.0.3 (2013-11)

EUROPEAN STANDARD

Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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:
http://portal.etsi.org/chaircor/ETSI_support.asp

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 European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

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

The present document is part 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 [11].

The present document was previously published as ETSI TS 102 778-2 [i.4].

Introduction

Electronic documents are a major part of a modern companies business. Trust in this way of doing business is essential for the success and continued development of electronic business. It is, therefore, important that companies using electronic documents have suitable security controls and mechanisms in place to protect their documents and to ensure trust and confidence with their business practices. In this respect the electronic signature is an important security component that can be used to protect information and provide trust in electronic business.

The present document is intended to cover electronic signatures for electronic documents. 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, GSM SIM cards, special programs for electronic signatures, etc.

The European Directive on a community framework for Electronic Signatures defines an electronic signature as: "Data in electronic form which is attached to or logically associated with other electronic data and which serves as a method of authentication".

The formats defined in the present document, are able to support advanced electronic signatures as defined in the Directive.

ISO 32000-1 [1] specifies a digital form for representing documents called the Portable Document Format (PDF) that enables users to exchange and view electronic documents easily and reliably, independent of the environment in which they were created or the environment in which they are viewed or printed.

Clause 12.8 of ISO 32000-1 [1] identifies the ways in which an electronic signature may be used to authenticate the identity of a user and the accuracy of the document's content. These electronic signatures are based on the same CMS [10] technology and techniques on which EN 319 122 [3] (CAdES) is based too, without the extended signature capabilities of CAdES itself, i. e.for the purposes of long term validation.

Therefore the following provisions represent a general consensus of the use of these standards and hence provide a reliable basis for maximizing interoperability. Nevertheless, in particular business areas and niches there may be specific needs and/or regulations that may require variations to these profiles.

1 Scope

The present document profiles the use of PDF signatures, as described in ISO 32000-1 and based on CMS [10], for its use in any application areas where PDF is the appropriate technology for exchange of digital documents including interactive forms.

This profile does not repeat the base requirements of the referenced standards, but instead aims to maximize interoperability of CMS-based electronic signatures in various business areas. Clause 4 provides a general informative description of the profile, while clause 5 specifies the normative conformance requirements of this profile.

2   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.

2.1   Normative references

The following referenced documents are necessary for the application of the present document.

[1]   ISO 32000-1 (2008): "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]   EN 319 122: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

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

[5]   IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[6]   IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[7]   ETSI TR 119 312: " Cryptographic Suites ".

[8]   ISO 19005-1:2005, Document management - Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1).

[9]   EN 319 102: "Electronic Signature and Infrastructures (ESI); Procedures for Signature Creation and Validation".

[10]   IETF RFC 5652 (2009): "Cryptographic Message Syntax (CMS)".

[11]   EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES ".

[12]   EN 319 142-3: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles".

[13]   EN 319 142-4: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES LTV Profile".

[14]   EN 319 142-5: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures".

[15]   EN 319 142-6: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 6: Visual Representations of Electronic Signatures".

[16]   EN 319 142-7: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 7: PAdES Baseline Profile".

[17]   EN 319 172: " Electronic Signatures and Infrastructures (ESI); Signature Policies".

2.2   Informative references

Clause 2.2 only shall contain informative references which are cited in the document itself.

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]   ITU-T Recommendation X.509 / ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.3]   IETF RFC 5755: "An Internet Attribute Certificate Profile for Authorization".

[i.4]   ETSI TS 102 778-2: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1".

[i.5]   ETSI Directives

3   Definitions, symbols 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:

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

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

PDF serial signature: specific signature workflow 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 may 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 (RFC5652 [10]) or related syntax containing a electronic signature and other information necessary to verify 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

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 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 the of information about the Electronic Signature

The present document makes use of certain keywords defined in ETSI Drafting Rules [i.5] to signify requirements.

3.2   Abbreviations

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

    CAdES   CMS Advanced Electronic Signatures

    NOTE: As per EN 319 122 [3].

    CMS   Cryptographic Message Syntax
    CRL   Certificate Revocation List
    OCSP   Online Certificate Status Protocol
    PDF   Portable Document Format

4 Description of Profile for CMS Signatures in PDF

4.1 Introduction

This profile specifies a PDF signature as specified in ISO 32000-1:2008 [1] that enables greater interoperability for PDF Signatures by providing additional restrictions beyond those of ISO 32000-1 [1].

4.2 Features

- Signature encoded in CMS as defined by PKCS #7 1.5 (see RFC 2315 [2]).

- Supports serial signatures.

- Optionally includes signature time-stamp.

- Optionally includes revocation information.

- Signature protects integrity of the document and authenticates the signatory.

- Signature can optionally include the "reasons" for the signature.

- Signature can optionally include a description of the location of signing.

- Signature can optionally include contact info of the signatory.

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).

4.3 Time Stamping

When a electronic signature is applied to a document, a conforming signature handler may choose to stamp it with the signer's local machine time, and that is what may appear in the signature appearance. Because a user can set that time forward or back on their computer, that time is usually not trusted. Therefore a time-stamp from a trusted time-stamping server should instead be applied on the electronic signature as soon as possible after the signature is created so the timestamp reflects the time at which the document was signed. A conforming signature handler that is signing a document should be sure that no other user actions take place between the creation of the signature and obtaining the timestamp. Timestamps fulfil a critical need in the validation process: if a conforming signature handler validates and timestamps the signature using a trusted timestamp server then the signer cannot later claim that it was signed by someone else, that the document was altered after they signed it, or that it was signed at another time.

The process for timestamping a electronic signature is described in RFC 3161 [6]. If a conforming signature handler chooses to embed a timestamp into the PDF Signature, then it shall be embedded as described in ISO 32000-1 [1], clause 12.8.3.3.1.

4.4 Revocation Checking

A conforming signature handler should embed the revocation information with the signature to save time when the signature is validated by the recipient. In addition, the inclusion of the revocation information protects against some threats relating to the use of previously revoked certificates which affect the non-repudiation properties of the signature. If the revocation information is to be included in the PDF Signature, then it should be captured and validated before completing the creation of the PDF Signature.

NOTE ISO 32000-1 [1], clause 12.8.3.3.2 describes the adbe-revocationInfoArchival attribute that should be used, as a signed attribute, to include this information into the PDF Signature.

When validating the PDF Signature, a conforming signature handler may ignore any embedded revocation information in favour of alternative storage or referenced data as per its own policies.

To incorporate the revocation status into an electronic signature, a conforming signature handler may use either (or both) of the following methods:

- Certificate Revocation List (CRL) [4] is one common method that public key infrastructures use. With CRL, the certificate is checked against a list of revoked certificates. In addition to the certificate issue date and the issuing entities, the list specifies revoked certificates as well as the reasons for revocation.

- Online Certificate Status Protocol (OCSP) [5] defines a protocol for obtaining the revocation status of a given certificate from a server.

4.5 Seed Values and Signature Policies

When preparing a document or form to be signed in the future, the author of the form may add to the signature field some additional entries (ISO 32000-1 [1], clause 12.7.4.5, table 232) including one called a *seed value dictionary*.

A *seed value dictionary* (ISO 32000-1 [1], clause 12.7.4.5, table 234) contains information that conveys a set of rules (or policies) that the form's author wishes the conforming signature handler to enforce at the time the signature is applied. These wishes can be specified either as requirements or recommendations. It is important not to confuse this "seed values" attribute with signature policies EPES attribute whose usage is specified in EN 319 122 [3]. While both bear similarities, seed values are workflow constraints for a given document, whereas signature policies represent general endorsement rules agreed upon by the signer and the verifier.

Common uses for seed values are to specify digest methods, revocation information, timestamping authorities and certificate attributes. Seed values that would require a conforming signature handler to violate this profile shall not be used.

NOTE   For example, use of a seed value that specifies the use of PKCS#1 instead of PKCS#7 should not be permitted by this profile.

Because the seed values are part of the PDF data structures, they are covered by the signatures.

5 Requirements of Profile for CMS Signatures in PDF

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.

5.1 Requirements on PDF Signatures

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 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 shall 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)   Use of RFC 5755 [i.3] attribute certificates associated with the signer certificate is not recommended.

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

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

5.2   Requirements on PDF Conforming signature handlers

a)   A PDF reader may substitute a different conforming signature handler, other than that specified in **Filter**, when verifying 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 in order to comply with this profile.

NOTE 1:   While the names of the SubFilters may imply specific algorithms, the actual list of supported algorithms that can be used can be found in ISO 32000-1 [1], clause 12.8.3.3.2, table 257. Consult TS 102 176-1 [7] for guidance on algorithm choices.

NOTE 2:   The use of SHA-1 is being phased out and hence the use of other hashing algorithms is recommended.

5.3   Requirements on Signature Validation

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

a) Verify 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 verify the binding between the subject distinguished name and subject public key as specified in RFC 5280 [4]. The validity checks shall be carried out at the time indicated either by time-stamp applied as per clause 4.3 or some other trusted indication of the signing time. The revocation status shall be checked as specified in clause 4.4.

NOTE: Unlike Part 3, PAdES-Enhanced [12] inclusion of the certificate hash (see CAdES [5], Clause 6.2.2) is not required by this profile. 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. Applications requiring the existence of certificate hash should use only signatures based on Part 3, PAdES-Enhanced [12].

5.4   Requirements on Time Stamping

a)   A timestamp from a trusted timestamp server should be applied to the electronic signature immediately after the signature is created so the timestamp reflects the time at which the document was signed.

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

5.4.1   Requirements on Time Stamping Validation

a) A conforming signature handler shall take the signature field of the PKCS#7 signature, encode it and compute the digest of the resulting byte stream using the algorithm indicated in the time stamp token.

b) A conforming signature handler shall check if the value obtained in the first step is the same as the digest present in the time-stamp token.

5.5   Requirements on Revocation Checking

a)   When validating the PDF Signature, a conforming signature handler may ignore any embedded revocation information in favour of alternative storage or referenced data as per its own policies (as described in EN 319 102 [9]).

5.6   Requirements on Seed Values

a)   Seed values that would require a conforming signature handler to violate this profile shall not be used.

Annex A (informative):
Change History

Document history		
V1.1.1	April 2009	Publication as TS 102 778
V1.2.1	July 2009	Publication
V1.2.1	April 2013	Draft forwarded by *editHelp!* for revision purposes
V0.0.0	May 2013	Draft version of EN inside ETSI STF458
V0.0.1	September 2013	Incomplete Draft for Review by ESI#40
V0.0.2	November 2013	Draft for Review by ESI#41
V0.0.3	November 2013	Stable draft for public comment

Latest changes made on 2013-11-28