Draft EN 319 142-3 V0.0.2 (2013-11)

Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles

STABLE DRAFT FOR PUBLIC REVIEW UNTIL 15 JANUARY 2014

Download the template for comments:

http://docbox.etsi.org/ESI/Open/Latest_Drafts/Template-for-comments.doc

Send comments to E-SIGNATURES_COMMENTS@LIST.ETSI.ORG

Reference
DEN/ESI-0019142-3

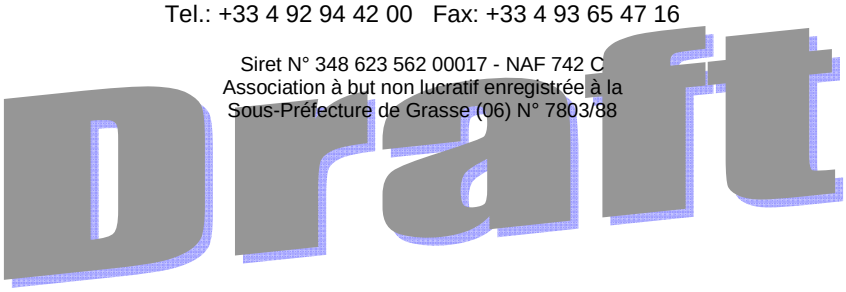
Keywords
e-commerce, electronic signature, security,
PAdES

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

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

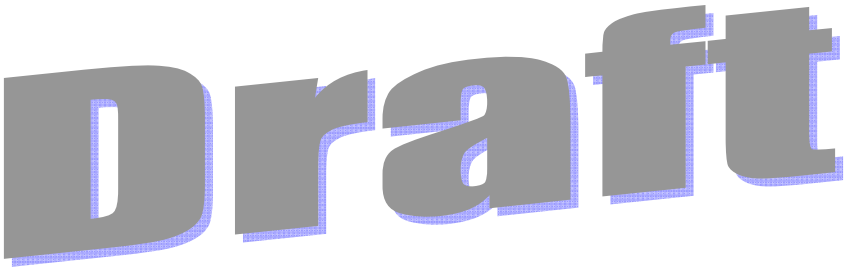
Copyright Notification

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 3 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 102 778-3 [i.2].

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, but with some restrictions as specified in the present document (e.g. parallel signatures not supported).

The present document specifies digital signatures in PDF to provide Advanced Electronic Signature equivalent to the CAdES-BES, CAdES-EPES and CAdES-T forms.

1 Scope

The present document profiles the use of PDF Signatures specified in ISO 32000-1 [1] with an alternative signature encoding to support signature formats equivalent to the signature forms CAdES-BES, CAdES-EPES and CAdES-T as specified in EN 319 122 [2].

The PAdES-BES profile supports basic CMS (RFC 5652 [4]) signature features as specified in EN 319 142-2 [8] with the additional protection against signing certificate substitution.

The PAdES-EPES profile extends the PAdES-BES profile to include signature policies.

Both profiles, PAdES-BES and PAdES-EPES allow the inclusion of a signature time stamp creating a signature similar to the CAdES-T form.

The present document does not repeat the base requirements of the referenced standards, but instead aims to disambiguate between the techniques used in the different referenced standards. These profiles are intended to be used by a signer.

The present document is part of a series of standards for advanced electronic signature formats applied to PDF documents. General information the series of profiles is specified in EN 319 142-1 [3].

The requirements specified in the present document take precedence over those specified in ISO 32000-1 [1] and EN 319 122 [2].

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

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

[2] EN 319 122: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

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

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

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

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

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

[8] EN 319 142-2: “Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1”.

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

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

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

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

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

[14] EN 319 102: “Electronic Signature and Infrastructures (ESI); Procedures for Signature Creation and Validation”.

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

NOTE: The ENs mentioned in [2], [3], [8], [9], [10], [11], [12], [13], [14] are published in the context of the work in Mandate M460. They might not yet be published.

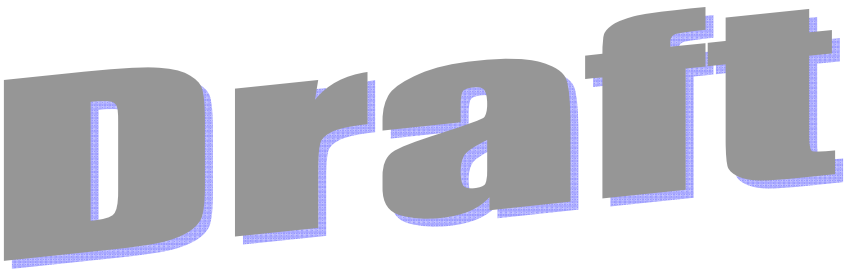
2.2 Informative references

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 102 778-3: “Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles”

[i.3] ETSI Directives.



3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in [1], [2] and the following apply:

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

PDF signature: DER-encoded binary data object based on the PKCS #7 [15] or the CMS (RFC5652 [2]) 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

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 information about the Digital Signature

signer: entity that creates an electronic signature

verifier: entity that validates an electronic signature

The present document makes use of certain keywords defined in ETSI Drafting Rules [i.3] to signify requirements.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ISO 32000-1 [1], EN 319 122 [2] and the following apply:

CAdES	CMS Advanced Electronic Signature
CMS	Cryptographic Message Syntax

NOTE: As specified in RFC 5652 [4].

CRL	Certificate Revocation List
EPES	Explicit Policy-based Electronic Signature
GSM	Global System for Mobile Communications
LTV	Long Term Validation
OCSP	Online Certificate Status Protocol
PAdES	PDF Advanced Electronic Signature
PAdES-BES	PAdES Basic Electronic Signature
PAdES-EPES	PAdES Explicit Policy Electronic Signature
PDF	Portable Document Format
PKCS	Public Key Cryptography Standard
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module

4 PAdES-BES and PAdES-EPES Profiles

4.1 Introduction

This set of profiles describes the creation and verification of signatures in PDF documents that have similar features as described in CAdES (EN 319 122 [2]) by the signature forms CAdES-BES, CAdES-EPES and CAdES-T.

Rather than having a separate "-T" form, as in CAdES, this set of profiles can incorporate the signature time-stamp attribute for both PAdES-BES and PAdES-EPES profiles which allows making the signature effectively a CAdES-T form.

Some signature attributes found in CAdES have the same or similar meaning as keys in the signature dictionary described in ISO 32000-1 [1]. The signature dictionary items should be used in preference to CAdES attributes unless specified otherwise in the present document.

4.2 General Requirements

For all profiles covered in the present document:

a) Requirements for handling PDF Signatures specified in ISO 32000-1 [1], clause 12.8 apply except where overridden by the present document.

b) A DER-encoded SignedData object as specified in CMS (RFC 5652 [4]) shall be included as the PDF signature in the entry with the key **Content** of the signature dictionary as described in ISO 32000-1 [1], clause 12.8.1. This CMS object forms a CAdES signature described in EN 319 122 [2] as it may contain several attributes required by the rules given in the following clauses.

c) The ByteRange shall cover the entire file, including the signature dictionary but excluding the PDF Signature itself.

d) Requirements specified in ISO 32000-1 [1], clauses 12.8.3.2 (PKCS#1) and 12.8.3.3 (PKCS#7) signatures as used in ISO 32000-1 [1] do not apply.

e) The signature dictionary shall contain a value of **ETSI.CAdES.detached** for the key **SubFilter**.

f) A verifier may substitute a different signature handler, other than that specified in Filter, when verifying the signature, as long as it supports the specified SubFilter format.

g) The signature dictionary shall not contain a **`Cert`** entry.

h) Unsigned signature attributes not described in this profile may be ignored unless used in conjunction with other profiles which place requirements on the use of such attributes. The handling of unsupported signed attributes is a matter for the verifier.

NOTE 1: A signature attribute cannot be supported by an implementation of a verifier if that verifier has no specification on how to process the attribute.

i) A timestamp from a trusted timestamp server should be applied on the digital signature immediately after the signature is created so the timestamp specifies a time as close as possible to the time at which the document was signed.

4.3 SignerInfo

For all profiles covered in the present document only a single signer (e.g. one single component of “SignerInfo” type within “signerInfos” element) shall be present in any PDF signature.

4.4 Mandatory Attributes

As in CAdES (EN 319 122 [2]) the following attributes are mandatory for all profiles covered in the present document.

4.4.1 content-type Attribute

The `content-type` for this profile shall always have the value "`id-data`".

NOTE: Although it can be thought as implicit, it is a mandatory attribute in order to provide maximum compatibility with existing implementation of CAdES.

4.4.2 message-digest Attribute

The syntax of the `message-digest` attribute type of the ES shall be used as defined in CMS (see RFC 5652 [4]).

4.4.3 Signing Certificate Reference Attribute

The ESS `signing-certificate` attribute or the ESS `signing-certificate-v2` attribute as defined in clause 6.2.2 of CAdES (EN 319 122 [2]) shall be used as a signed attribute. The entry with the key **`Cert`** in the signature dictionary shall not be used.

NOTE: As specified in ETSI TR 119 312 [7], when the SHA-1 hash function is used, the `signing-certificate` attribute is required to be used. The `signing-certificate-v2` attribute is required to be used if any algorithm other than SHA-1 is used. The use of SHA-1 is being phased out and hence the use of other hashing algorithms is recommended.

4.5 Attributes Optional in CAdES

The following attributes may be present with the signed-data depending on the profile employed. The use of these attributes shall be as defined in CAdES (see EN 319 122 [2]) qualified by the present document which takes precedence.

4.5.1 signature-policy-identifier Attribute

For the PAdES-EPES profile: a `signature-policy-identifier` attribute shall be present as a signed attribute. The rules from clause 6.2.9 in CAdES (EN 319 122 [2]) shall apply.

It is important not to confuse this EPES attribute with the "seed values" defined in ISO 32000-1 [1], clause 12.7.4.5. 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.

Conforming signature handlers shall enforce seed values constraints at signing time and should enforce signature policies constraints at signing time when possible. During validation conforming signature handlers should not enforce seed values constraints, if present, but shall enforce signature policy constraints.

Since "seed values" define rules to be enforced by conforming signature handler during signature creation, it would be desirable to have the ability to indicate which signature policy to use for a given signature.

To enable this, the present document defines four new elements that can be inserted in the "signature field seed value dictionary" defined in ISO 32000-1 [1].

Table 1

Key	Type	Value
SignaturePolicyOID	ASCII string	*(Optional)* The string representation of the OID of the signature policy to use when signing.
SignaturePolicyHashValue	Byte String	*(Optional)* The value of the hash of the signature policy, computed the same way as in clause 6.2.9 of CAdES (EN 319 122 [2])
SignaturePolicyHashAlgorithm	ASCII String	*(Optional)* The hash function used to compute the value of the SignaturePolicyHashValue entry. Entries shall be represented the same way as SubFilter values specified in table 257 of ISO 32000-1 [1].
SignaturePolicyCommitmentType	Array of ASCII strings	*(Optional)* If the SignaturePolicyOID is present, this array defines the commitment types that can be used within the signature policy. An empty string can be used to indicate that all commitments defined by the signature policy may be used.

If the SignaturePolicyOID is absent, the three other fields defined above shall be ignored.

NOTE: The above entries allow the creation of a signature-policy-identifier attribute as in CAdES (EN 319 122 [2]). All rules defined in CAdES apply. In particular, CAdES allows the creation of a EPES signature when the signature policy hash is not available, therefore, the absence of the SignaturePolicyHashValue does not preclude the creation of a PAdES-EPES signature.

4.5.2 signature-time-stamp Attribute

For all profiles covered in the present document a `signature-time-stamp` attribute should be present as an unsigned attribute in a signature. The rules from clause 6.3 in CAdES (EN 319 122 [2]) shall apply.

NOTE: These rules for this attribute are the same as described in clause 12.8.3.3.1 of ISO 32000-1 [1] except that specific requirements for treatment of time-stamps may be specified in the signature policy in the case of EPES being used. By providing a signature`-time-stamp` attribute a signature format functional equivalent to the form CAdES-T can be created.

4.5.3 signing-time Attribute

For all profiles covered in the present document the `signing-time` attribute shall not be used.

NOTE: The time of signing can be indicated by the value of the **M** entry in the signature dictionary.

4.5.4 counter-signature Attribute

For all profiles covered in the present document the `counter-signature` attribute shall not be used.

4.5.5 content-reference Attribute

For all profiles covered in the present document the `content-reference` attribute shall not be used.

NOTE: The PDF format provides its own means to refer between different signature objects that can be used instead.

4.5.6 content-identifier Attribute

For all profiles covered in the present document the `content-identifier` attribute shall not be used.

NOTE: The PDF format provides its own means to refer between different signature objects that can be used instead.

4.5.7 content-hints Attribute

For all profiles covered in the present document the `content-hints` attribute shall not be used.

4.5.8 commitment-type-indication Attribute

For the PAdES-EPES profile: The `commitment-type-indication` attribute may be present. Seed values may indicate restrictions in the values of this attribute (see clause 4.5.1).

For the PAdES-BES profile the `commitment-type-indication` attribute shall not be present.

NOTE: `commitment-type-indication` can be used to select different sub-options with the signature policy in the case of EPES. The signature dictionary item **`Reason`** field can be used for different purposes to provide general information on the reason that the signature is applied.

4.5.9 signer-location Attribute

For all profiles covered in the present document the `signer-location` attribute shall not be present.

NOTE: The location can be indicated by the value of the **`Location`** entry in the signature dictionary.

4.5.10 signer-attributes Attribute

For all profiles covered in the present document the `signer-attributes` attribute may be present. If present this shall be used as defined in CAdES clause 6.2.6 of EN 319 122 [2].

Attribute certificates shall not be included in the CMS [4] SignedData object.

NOTE: This avoids redundant information being included in the signature.

4.5.11 content-time-stamp Attribute

For all profiles covered in the present document the `content-time-stamp` attribute may be present. If the `content-time-stamp` attribute is present it shall be used in the same way as defined in CAdES, clause 6.2.8 of EN 319 122 [2] and it shall protect all the data being signed as identified by the ByteRange.

4.6 Signature Validation

For all profiles covered in the present document when the user opens a signed document or requests verification of the signature(s) present in the PDF, a conforming signature handler shall perform the steps described in EN 319 102 [10], clause 5.3 to verify them.

NOTE 1: The verifier shall check that the document digest matches that in the signature as specified in ISO 32000-1 [1], clause 12.8.1.

NOTE 2: This profile on its own is intended to be used for validation in the short-term, that is before used certificates are likely to expire or being revoked. To achieve long-term validation this profile is to be used in conjunction with the LTV profile specified in EN 319 142-4 [9]. If this profile is used in conjunction with the LTV profile then requirements specified in EN 319 142-4 [9] take precedence.

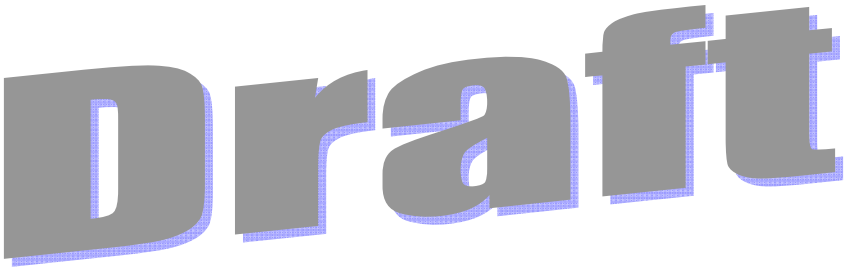
4.7 Extensions Dictionary

The extensions dictionary (see ISO 32000-1 [1] clause 7.12) should include an entry:

```
<</ESIC
   <</BaseVersion /1.7 /
      ExtensionLevel 2
```

>>
>>

to identify that a PDF document includes extensions as identified in the present document.



Annex A (informative): Change History

date	Version	Information about changes
July 2009	v1.1.1	Publication as TS 102 778
December 2009	v1.1.2	Publication as TS 102 778
July 2010	V1.2.1	Publication as TS 102 778
April 2013	v1.2.1	Draft forwarded by ***editHelp!*** for revision purposes
May 2013	v0.0.0	Draft version of EN inside ETSI STF458
September 2013	V0.0.1	Incomplete Draft for Review in ESI#40
November 2013	V0.0.2	Draft for public Review

Latest changes made on 2013-11-07