ETSI TS 119 142-1 V1.0.1 (2015-07)

Electronic Signatures and Infrastructures (ESI);
PAdES digital signatures;
Part 1: Building blocks and PAdES baseline signatures

Reference
RTS/ESI-0019142-1-TS

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 (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 Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 1 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".

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, and aims to meet the general requirements of the international community to provide trust and confidence in electronic transactions, including, amongst other, applicable requirements from Regulation (EU) No 910/2014 [i.2].

The present document can be used for any transaction between an individual and a company, between two 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 electronic signatures, etc.

The present document is part of a rationalized framework of standards (see ETSI TR 119 000 [i.3]).
ETSI TR 119 100 [i.4] provides guidance on how to use the present document within the aforementioned framework.

1 Scope

The present document, specifies PAdES digital signatures. PAdES signatures build on PDF signatures specified in ISO 32000-1 [1] with an alternative signature encoding to support digital signature formats equivalent to the signature format CAdES as specified in ETSI TS 119 122-1 [2], by incorporation of signed and unsigned attributes, which fulfil certain common requirements (such as the long term validity of digital signatures) in a number of use cases.

The present document specifies formats for PAdES baseline signatures, which provide the basic features necessary for a wide range of business and governmental use cases for electronic procedures and communications to be applicable to a wide range of communities when there is a clear need for interoperability of digital signatures used in electronic documents.

The present document defines four levels of PAdES baseline 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. Each level requires the presence of certain PAdES attributes, suitably profiled for reducing the optionality as much as possible.

Procedures for creation and validation of PAdES digital signatures are out of scope and specified in ETSI TS 119 102 [i.5].

The present document aim at supporting electronic signatures in different regulatory frameworks.

NOTE: Specifically but not exclusively, PAdES digital signatures specified in the present document aim at supporting electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, and qualified electronic seals as per Regulation (EU) No 910/2014 [i.2].

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 reference 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] ETSI TS 119 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

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

[4] IETF RFC 5280 (2008): "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[5] IETF RFC 6960 (2013): "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[6] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[7] W3C Recommendation (May 2008): "Canonical XML Version 1.1".

[8] 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] ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management".

[i.2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.3] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); Rationalized structure for Electronic Signature Standardization".

[i.4] ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Business Driven Guidance for Signature Creation and Validation".

[i.5] ETSI TS 119 102: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[i.6] Adobe® Supplement to ISO 32000-1. BaseVersion: 1.7 - ExtensionLevel: 5.

NOTE: Available at http://www.adobe.com/devnet/pdf/pdf_reference.html.

[i.7] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.8] Adobe® XFA: "XML Forms Architecture (XFA) Specification" version 2.5, (June 2007), Adobe Systems Incorporated".

[i.9] ETSI TS 103 172: "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile".

[i.10] IETF RFC 2315 (1998): "PKCS #7: Cryptographic Message Syntax Version 1.5".

[i.11] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.12] ETSI TS 119 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".

[i.13] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardisation of signatures; Definitions and abbreviations".3 Definitions and abbreviations.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ISO 32000-1 [1], TR 119 001 [i.13] and the following apply:

electronic time-stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time

NOTE 1: In the case of IETF RFC 3161 [6] updated by IETF RFC 5816 [8] protocol, the electronic time-stamp is referring to the `timeStampToken` field within the `TimeStampResp` element (the TSA's response returned to the requesting client).

NOTE 2: This can be the signer or the creator of a seal or any party that initially validates or further maintains the signature.

generator: any party which creates, or adds attributes to, a signature

NOTE: This can be the signer or any party that initially validates or further maintains the signature.

Legacy PAdES baseline signature: digital signature generated according to ETSI TS 103 172 [i.9]

PAdES signature: digital signature that satisfies the requirements specified within the present document and ETSI TS 119 142-2 [i.12]

proof of existence: information that can be used to prove that some data existed before a given time

signature handler: software module that implements a specific form of signing and/or authentication of digital signatures

trust service provider: body operating one or more (electronic) Trust Services

verifier: entity that validates a digital signature

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.13] and the following apply:

DSS	Document Security Store
ESS	Enhanced Security Services
TSL	Trust Status List
VRI	Validation Related Information

4 General syntax

4.1 General requirements for PAdES signatures based on PDF signatures

PAdES signatures profiled in the present document build on PDF signatures specified in ISO 32000-1 [1] with an alternative signature encoding to support digital signature formats equivalent to the signature format CAdES [2], by incorporation of signed and unsigned attributes described in clause 5.

The following requirements apply:

a) A DER-encoded SignedData object as specified in CAdES [2] shall be included as the PDF signature in the entry with the key `Contents` of the Signature Dictionary as described in ISO 32000-1 [1], clause 12.8.1. There shall only be a single signer (i.e. one single component of `SignerInfo` type within `signerInfos` element) in any PDF Signature.

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

NOTE: Given that PAdES signatures are enveloped inside a PDF document and are detached in the sense of a CMS signature, the signature placement is implied by ISO 32000-1 [1].
In ISO 32000-1 [1], section 12.8.3.3.1 reads "No data shall be encapsulated in the PKCS#7 SignedData field".

c) Some signature attributes found in CAdES [2] have the same or similar meaning as keys in the Signature Dictionary described in ISO 32000-1 [1]. For signature attributes and keys that have the same or similar meaning only one of them should be used according to the requirements set in table defined in clause 6.3 in the present document.

5 Attributes syntax and semantics

5.1 Introduction

This clause provides details on attributes specified within ISO 32000-1 [1] and CAdES [2] and defines new attributes for building PAdES signatures.

The clause distinguishes between the following types of attributes: CMS and CAdES defined attributes, ISO 32000-1 [1] defined attributes, validation data and archive validation data attributes. The first ones are the attributes that build the DER-encoded `SignedData` object included as the PDF signature in the entry with the key `Contents` of the Signature Dictionary as described in ISO 32000-1 [1], clause 12.8.1. The second ones are the attributes that build the Signature Dictionary as described in ISO 32000-1 [1]. The other ones are the attributes where to include validation data and archive validation data that can guarantee long term validity of digital signatures.

Clause 6.3 provides the requirements concerning how to use the attributes described above.

5.2 CMS and CAdES defined attributes

The attributes included in the following list may be used to generate the DER-encoded `SignedData` object included as the PDF signature in the entry with the key `Contents` of the Signature Dictionary as described in ISO 32000-1 [1], clause 12.8.1. Their syntax shall be as defined in ETSI TS 119 122-1 [2], clause 5.

- `content-type`
- `message-digest`
- `signing certificate reference attributes`
  - `ESS signing-certificate`
  - `ESS signing-certificate-v2`
- `commitment-type-indication`
- `signer-attributes-v2`
- `content-time-stamp`
- `signature-policy-identifier`
- `signature-time-stamp`

5.3 ISO 32000-1 defined attributes

The entries of the Signature Dictionary shall be as defined in ISO 32000-1 [1], clause 12.8.1 unless specified otherwise in the present document.

In particular, the entries with the following keys in the Signature Dictionary are directly addressed: `M`, `Contents`, `Filter`, `SubFilter`, `ByteRange`. Further the entries with the `Location`, `Name`, `ContactInfo` and `Reason` keys in the Signature Dictionary are inherently addressed.

5.4 Validation data and archive validation data attributes

5.4.1 Overview

Validation of a digital signature requires data to validate the signature such as CA certificates, Certificate Revocation List (CRLs) or certificate status information (OCSP) commonly provided by online services (referred to in the present document as validation data).

This clause describes an extension to ISO 32000-1 [1] called Document Security Store (**DSS**) to carry such validation data as necessary to validate a signature, optionally with Validation Related Information (**VRI**) which relates the validation data to a specific signature (see clause 5.4.2). The structure of **DSS** and **VRI** is illustrated in figure 1.

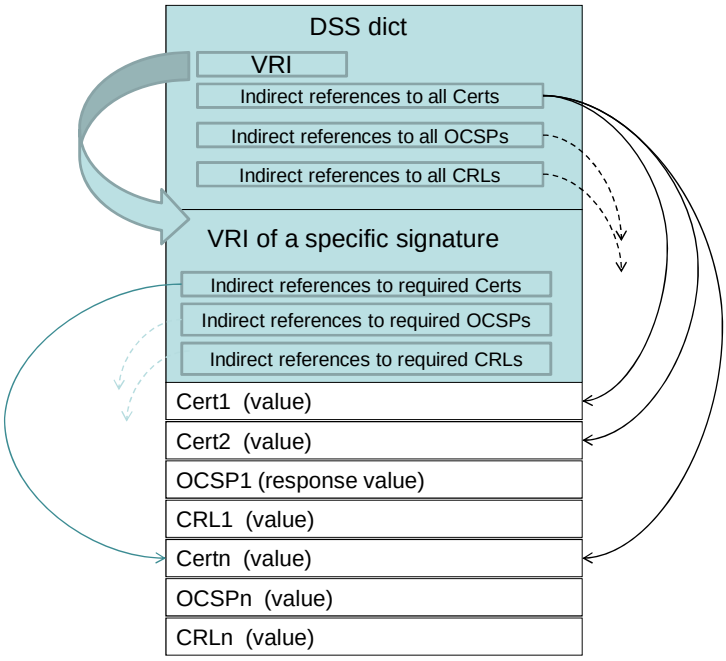

Figure 1: Illustration of DSS and VRI structures

This clause also defines another extension to ISO 32000-1 [1] called Document Time-stamp (see clause 5.4.3) to extend the life-time of protection to the document.

These extensions support Long Term Validation (LTV) of PDF Signatures. The structure of a PDF document with LTV is illustrated in figure 2.

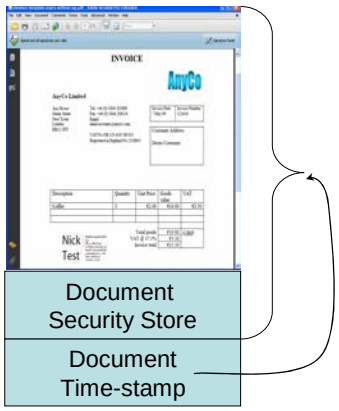

Figure 2: Illustration of PDF document with extended life-time protection

The life-time of the protection can be further extended beyond the life-time of the last document time-stamp applied by adding further DSS information to validate the previous last document time-stamp along with a new document time-stamp. This is illustrated in figure 3.

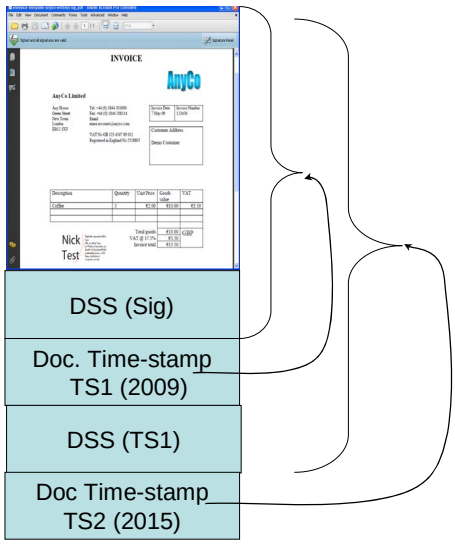

Figure 3: Illustration of PDF Document with repeated LTV

5.4.2 Document Security Store

5.4.2.1 Catalog

Added to ISO 32000-1 [1] Table 28 "Entries in catalogue dictionary"		
KEY	**TYPE**	**VALUE**
DSS	Dictionary	*(Optional)* Document-wide security-related information.

5.4.2.2 DSS Dictionary

The Document Security Store (**DSS**) shall be a dictionary that shall have the value **DSS** as key in the document catalog dictionary. This dictionary is used to provide a single place where all of the validation-related information for some or all signatures in the document should be placed.

The **DSS** dictionary, if present, shall contain validation-related information only for document signatures represented in PKCS#7 and CMS (and its derivatives) format or for XAdES signatures of forms signing dynamic XFA [i.8].

NOTE: See ETSI TS 119 142-2 [i.12] for specification of XAdES signatures of forms signing dynamic XFA.

Entries in a DSS Dictionary		
KEY	**TYPE**	**VALUE**
Type	Name	*(Optional)* It shall be **DSS** for a document security store dictionary.
VRI	Dictionary	*(Optional)* This dictionary contains Signature **VRI** dictionaries in the document. The key of each entry in this dictionary is the base-16-encoded (uppercase) SHA1 digest of the signature to which it applies and the value is the Signature **VRI** dictionary which contains the validation-related information for that signature. (See additional requirements a, b, c.).
Certs	Array	*(Optional)* An array of indirect references to streams, each containing one DER-encoded X.509 certificate (that shall be as defined in IETF RFC 5280 [4]). This array contains certificates that can be used in the validation of any signatures in the document.
OCSPs	Array	*(Optional)* An array of indirect references to streams, each containing a DER-encoded Online Certificate Status Protocol (OCSP) response (that shall be as defined in IETF RFC 6960 [5]). This array contains OCSPs that can be used in the validation of any signatures in the document.
CRLs	Array	*(Optional)* An array of indirect references to streams, each containing a DER-encoded Certificate Revocation List (CRL) (that shall be as defined in IETF RFC 5280 [4]]). This array contains CRLs that can be used in the validation of any signatures in the document.
a) For document signatures or document time-stamp signatures the bytes that are hashed shall be those of the complete hexadecimal string in the entry with the key `Contents` of the associated Signature Dictionary containing the signature's DER-encoded binary data object (e.g. PKCS#7, CMS or CAdES objects). b) For the signatures of CRLs and OCSP responses, the bytes that are hashed shall be the respective signature objects represented as a BER-encoded OCTET STRING encoded with primitive encoding. *c)* When computing the digest of a XAdES signature found in dynamic XFA [i.8], the contents of the ds:Signature shall be canonicalized using exclusive canonicalization (http://www.w3.org/2001/10/xml-exc-c14n#) as specified in [7] and then hashed.		

Any **VRI** dictionaries shall be located in document incremental update sections. If the Signature Dictionary to which a **VRI** dictionary applies is itself in an incremental update section (see clause 7.5.6 of ISO 32000-1 [1]), the **VRI** update shall be done later than the signature update.

5.4.2.3 Signature VRI Dictionary

The signature **VRI** dictionary shall contain validation-related information (**VRI**) for a specific signature in the document to which the validation information applies.

Entries in a Signature VRI Dictionary		
KEY	**TYPE**	**VALUE**
Type	Name	*(Optional)* If present, it shall be **VRI** for a validation-related information dictionary.
Cert	Array	*(Optional,* if present, it shall not be an empty array*)* An array of indirect references to streams, each containing one BER-encoded X.509 certificate (that shall be as defined in IETF RFC 5280 [4]). This array should contain all certificates that were used in the validation of this signature.
CRL	Array	(*Optional*, if present, it shall not be an empty array) An array of indirect references to streams that are all CRLs used to determine the validity of the certificates in the chains related to this signature. Each stream shall reference a CRL that is an entry in the CRLs array in the **DSS** dictionary.
OCSP	Array	(*Optional*, if present shall not be an empty array) An array of indirect references to streams that are all OCSP responses used to determine the validity of the certificates in the chains related to this signature. Each stream shall reference an OCSP response that is an entry in the OCSPs array in the **DSS** dictionary.
TU	Date	*(Optional)* The date/time at which this signature VRI dictionary was created. A signature handler may ignore this entry and use a different time for the signature validation. This entry shall be absent when the **TS** entry is present. Date shall be a date string as defined in ISO 32000-1 [1], clause 7.9.4. (See additional requirement a).
TS	Stream	*(Optional)* A stream containing the DER-encoded time-stamp token (that shall be as defined in IETF RFC 3161 [6] updated by IETF RFC 5816 [8] and which represents the secure time at which this signature VRI dictionary was created. This entry shall be absent when a **TU** entry is present. (See note 1 and additional requirement b).

Additional requirements:

a) The **TU** key should not be used.
b) The **TS** key should not be used.
c) Exactly one of the following methods to provide a **VRI** generation claimed time shall be used: the **TU** entry, the **TS** entry or a subsequent document time-stamp.

NOTE 1: For PKCS#7 signatures the datum that is hashed and included in the messageImprint field of the DER-encoded time stamp stored in **TS** entry (see IETF RFC 3161 [6] updated by IETF RFC 5816 [8]) is the `encryptedDigest` field in the signature's PKCS#7 object (as defined in IETF RFC 2315 [i.10]).

NOTE 2: The **VRI** dictionary is optional, since all necessary data to validate the signature can be available from other sources like the **DSS** dictionary itself. The **VRI** dictionary offers possibilities for optimization of the validation process, since it relates the data to one specific signature.

NOTE 3: The value of **TS** can be used as a proof of existence for the signature value itself.

Any values in the `Cert`, `CRL` and `OCSP` arrays of a Signature **VRI** dictionary shall also be present in the **DSS** dictionary applicable to the signature for which this Signature **VRI** dictionary is associated. If this signature (e.g. PKCS#7, CMS or CAdES object) does not have any associated `Certs`, `CRLs` or `OCSPs`, then the corresponding key shall not be present in the **VRI** dictionary.

A Signature **VRI** dictionary shall not be used to record the information used in an unsuccessful validation attempt.

DocMDP restrictions (see ISO 32000-1 [1] clause 12.8.2.2) shall not apply to incremental updates to a PDF document containing a **DSS** dictionary and associated `VRI`, `Certs`, `CRLs` and `OCSPs`.

NOTE: ISO 32000-1 [1], clause 12.8.2.2, addresses the DocMDP (Modification, Detection and Prevention) feature whereby a set of permissions can be associated with a PDF in conjunction with a certification signature. The permissions of DocMDP are present in the entry with the `P` key of the DocMDP transform parameters dictionary, as an integer in the range 1 through 3. Values of 2 and 3 allow for additional signatures to be included after the certification but a value of 1 does not allow any change but allows Document Time-stamps.

5.4.3 Document Time-stamp

A Document Time-stamp dictionary shall be a standard Signature Dictionary (as defined in ISO 32000-1 [1], clause 12.8.1) with the following changes.

Modifications to table 252 for a Document Time-stamp **Dictionary of ISO 32000-1 [1]**		
KEY	**TYPE**	**VALUE**
Type	Name	*(Required)* It shall be **DocTimeStamp**.
SubFilter	Name	*(Required)* The value of `SubFilter` identifies the format of the data contained in the stream. A conforming reader may use any signature handler that supports the specified format. The value of `SubFilter` should be **ETSI.RFC3161**. Other values may be defined by developers, and when used, shall be prefixed with the registered developer identification as described in ISO 32000-1 [1], annex E.
Contents	Byte string	*(Required)* When the value of `SubFilter` is **ETSI.RFC3161**, the value of `Contents` shall be the hexadecimal string (as defined in clause 7.3.4.3 in ISO 32000-1 [1]) representing the value of TimeStampToken as specified in IETF RFC 3161 [6] updated by IETF RFC 5816 [8]. The value of the `messageImprint` field within the TimeStampToken shall be a hash of the bytes of the document indicated by the `ByteRange`. The `ByteRange` shall cover the entire document, including the Document Time-stamp dictionary but excluding the TimeStampToken itself (the entry with key *Contents*).
V	Integer	(Optional) The version of the Signature Dictionary format. For Document Time-stamp dictionaries the value, if present, shall be 0. Default value: 0.
NOTE: The clause 7.3.4 in ISO 32000-1 [1] requires space for the `Contents` value to be allocated before the message digest is computed.		

In addition, the following keys shall not be present in a Document Time-stamp dictionary: `Cert`, `Reference`, `Changes`, `R`, `Prop_AuthTime`, and `Prop_AuthType`.

The following keys should not be present in a Document Time-stamp dictionary: `Name`, `M`, `Location`, `Reason`, and `ContactInfo`**.** Since this information can already be present inside of the TimeStampToken contained in `Contents`, a conforming reader should ignore these keys.

As the validation data for the last Document Time-stamp becomes at risk for obsolescence or when the encryption technology used for the Document Time-stamp signature becomes at risk for successful attack, there is the likely scenario that updates to the time stamp signature and its revocation information may need to take place. This process is done using the same LTV methodology already described.

When evaluating the DocMDP restrictions (see ISO 32000-1 [1], clause 12.8.2.2) the presence of a Document Time-stamp dictionary item shall be ignored.

NOTE: See note in clause 5.4.2.3.

5.5 Requirements on encryption

A PDF document can be encrypted to protect its contents from unauthorized access. When encryption and signatures are combined together in a single PDF document, encryption shall be applied to its content before any signature is incorporated into it.

Encryption shall apply to all strings and streams in the document's PDF file, with the following exceptions:

- The values for the ID entry in the trailer.
- Any strings in an `Encrypt` dictionary.
- Any strings that are inside streams such as content streams and compressed object streams, which themselves are encrypted.
- Any hexadecimal strings representing the value of the `Contents` key in a Signature Dictionary.

5.6 Extensions dictionary

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

an entry

```
<</ESIC
    <</BaseVersion /1.7
      /ExtensionLevel 1
     >>
  >>
```

to identify that a PDF document includes extensions as identified in clause 5.4; and

an entry

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

to identify that a PDF document includes extensions as identified in clause 6.3 requirement l.

NOTE: Use of extensions as identified in clause 5.4 and in clause 6.3 requirement l can also be identified by the following entry from Adobe® (defining equivalent extensions to the PDF document format):

```
<</ADBE
<</BaseVersion /1.7
  /ExtensionLevel 8
    >>
>>
```

6 PAdES baseline signatures

6.1 Signature levels

Clause 6 defines four levels of PAdES baseline signatures, intended to facilitate interoperability and to encompass the life cycle of PAdES signature, namely:

a) B-B level provides requirements for the incorporation of signed and some unsigned attributes when the signature is generated.

b) B-T level provides requirements for the generation and inclusion, for an existing signature, of a trusted token proving that the signature itself actually existed at a certain date and time.

c) B-LT level provides requirements for the incorporation of all the material required for validating the signature in the signature document. This level aims to tackle the long term availability of the validation material.

d) B-LTA level provides requirements for the incorporation of electronic time-stamps that allow validation of the signature long time after its generation. This level aims to tackle the long term availability and integrity of the validation material.

NOTE 1: The levels b) to d) are appropriate where the technical validity of signature needs to be preserved for a period of time after signature creation where certificate expiration, revocation and/or algorithm obsolescence is of concern. The specific level applicable depends on the context and use case as described in ETSI TR 119 100 [i.4].

NOTE 2: B-LTA level targets long term availability and integrity of the validation material of digital signatures over long term. The B-LTA level can help to validate the signature beyond any event that limits its validity. The use of B-LTA level is considered an appropriate preservation and transmission technique for signed data.

NOTE 3: Conformance to B-LT level, when combined with appropriate additional preservation techniques tackling the long term availability and integrity of the validation material is sufficient to allow validation of the signature long time after its generation. The assessment of the effectiveness of preservation techniques for signed data other than implementing the B-LTA level are out of the scope of the present document. The reader is advised to consider legal instruments in force and/or other standards (for example ETSI TS 101 533-1 [i.1]) that can indicate other preservation techniques.

e) When signed data is exchanged between parties the sender should use at least signatures conforming to a level that allows the relying parties to trust the signature at the time the exchange takes place.

6.2 General requirements for PAdES baseline signatures

6.2.1 Algorithm requirements

The algorithms and key lengths used to generate signatures should comply with ETSI TS 119 312 [i.7].

In addition MD5 algorithm shall not be used as digest algorithm.

NOTE: National legislation can define requirements regarding algorithms and key lengths.

6.2.2 Notation for requirements

The present clause describes the notation used for defining the requirements of the different PAdES signature levels.

The requirements on the attributes and certain signature fields for each PAdES signature level are expressed in table 1. A row in the table either specifies requirements for an attribute, a signature field or a service.

A service can be provided by different attributes, by certain signature fields, or by other mechanisms (service provision options hence forward). In these cases, the specification of the requirements for a service is provided by two or more rows. The first row contains the requirements of the service. The requirements for the attributes, certain signature fields, and/or mechanisms used to provide the service are stated in the following rows.

Table 1 contains 8 columns. Below follows a detailed explanation of their meanings and contents.

1) Column "Attributes/Fields/Services":

   a) In the case where the cell identifies a Service, the cell content starts with the keyword "Service:" followed by the name of the service.

   b) In the case where the attribute or signature field provides a service, this cell contains "SPO:" (for Service Provision Option), followed by the name of the attribute or signature field.

   c) Otherwise, this cell contains the name of the attribute or signature field.

2) Column "Presence in B-B level". This cell contains the specification of the presence of the attribute or signature field, or the provision of a service, for PAdES-B-B signatures.

3) Column "Presence in B-T level". This cell contains the specification of the presence of the attribute or signature field, or the provision of a service, for PAdES-B-T signatures.

4) Column "Presence in B-LT level". This cell contains the specification of the presence of the attribute or signature field, or the provision of a service, for PAdES-B-LT signatures.

5) Column "Presence in B-LTA level". This cell contains the specification of the presence of the attribute or signature field, or the provision of a service, for PAdES-B-LTA signatures.

6) Below follows the values that can appear in columns "Presence in B-B", "Presence in B-T", "Presence in B-LT", and "Presence in B-LTA":

   - "shall be present": means that the attribute or signature field shall be incorporated to the signature, and shall be as specified in the document referenced in column "References", further profiled with the additional requirements referenced in column "Requirements", and with the cardinality indicated in column "Cardinality".

- "shall not be present": means that the attribute or signature field shall not be incorporated to the signature.
- "may be present": means that the attribute or signature field may be incorporated to the signature, and shall be as specified in the document referenced in column "References", further profiled with the additional requirements referenced in column "Requirements", and with the cardinality indicated in column "Cardinality".
- "shall be provided": means that the service identified in the first column of the row shall be provided as further specified in the SPO-related rows. This value only appears in rows that contain requirements for services. It does not appear in rows that contain requirements for attributes or signature fields.
- "conditioned presence": means that the incorporation to the signature of the item identified in the first column is conditioned as per the requirement(s) specified in column "Requirements" and requirements referenced by column "References" with the cardinality indicated in column "Cardinality".
- "*": means that the attribute or signature field (service) identified in the first column should not be present (provided) in the corresponding level. Upper signature levels may specify other requirements.

7) Column "Cardinality". This cell indicates the cardinality of the attribute or signature field. If the cardinality is the same for all the levels, only the values listed below appear. Otherwise the content specifies the cardinality for each level. See the example at the end of the present clause showing this situation. Below follows the values indicating the cardinality:
   - **0**: The signature shall not incorporate any instance of the attribute or signature field.
   - **1**: The signature shall incorporate exactly one instance of the attribute or signature field.
   - **0 or 1**: The signature shall incorporate zero or one instance of the attribute or signature field.
   - ≥ **0**: The signature shall incorporate zero or more instances of the attribute or signature field.
   - ≥ **1**: The signature shall incorporate one or more instances of the attribute or signature field.
8) Column "References". This cell contains either the number of the clause specifying the attribute or signature field in the present document, or a reference to the document and clause that specifies the attribute or signature field.
9) Column "Additional notes and requirements". This cell contains numbers referencing notes and/or letters referencing additional requirements on the attribute or signature field. Both notes and additional requirements are listed below the table.

EXAMPLE: In table 1, the row corresponding to SPO: DSS signature field has a value "*" in the cells in columns "Presence in B-B level" and "Presence in B-T level", and "shall be present" in cells in columns "Presence in B-LT level" and "Presence in B-LTA level". The cell in column "Cardinality" indicates the cardinality for each level as follows: "B-B, B-T: ≥0" indicates that PAdES-B-B and PAdES-B-T signatures can incorporate zero or more instances of SPO: DSS signature field; "B-LT, B-LTA: ≥1" indicates that PAdES-B-LT and PAdES-B-LTA incorporates one or more instances of SPO: DSS signature field.

6.3 PAdES baseline signatures

This clause defines requirements on attributes, fields and services that PAdES baseline signatures have to fulfil. The attributes defined in ETSI TS 119 122-1 [2] and not listed in table 1 shall not be present.

Table 1 shows the presence and cardinality requirements on the signature fields, attributes and services indicated in the first column for the four PAdES baseline signature levels, namely: PAdES-B-B, PAdES-B-T, PAdES-B-LT, and PAdES-B-LTA). Additional requirements are detailed below the table suitably labelled with the letter indicated in the last column.

NOTE: PAdES-B-B signatures that incorporate only the signature fields/attributes that are mandatory in table 1, and that implement the mandatory requirements, contain the lowest number of signature fields/attributes, with the consequent benefits for interoperability.

Table 1: Requirements on the main attributes for PAdES baseline signatures

Attributes / Fields / Services	Presence in B-B level	Presence in B-T level	Presence in B-LT level	Presence in B-LTA level	Cardinality	References	Additional requirements and notes
SignedData.certificates	shall be present	shall be present	shall be present	shall be present	1	IETF RFC 5652 [3], clause 5.1	a, b, note 1, note 2
content-type	shall be present	shall be present	shall be present	shall be present	1	ETSI TS 119 122-1 [2], clause 5.1.1	c
message-digest	shall be present	shall be present	shall be present	shall be present	1	ETSI TS 119 122-1 [2], clause 5.1.2	-
signer-attributes-v2	may be present	may be present	may be present	may be present	0 or 1	ETSI TS 119 122-1 [2], clause 5.2.6	-
content-time-stamp	may be present	may be present	may be present	may be present	≥ 0	ETSI TS 119 122-1 [2], clause 5.2.8	-
signature-policy-identifier	may be present	may be present	may be present	may be present	0 or 1	ETSI TS 119 122-1 [2], clause 5.2.9	-
commitment-type-indication	conditioned presence	conditioned presence	conditioned presence	conditioned presence	0 or 1	ETSI TS 119 122-1 [2], clause 5.2.3	d
SERVICE: protection of signing certificate	shall be provided	shall be provided	shall be provided	shall be provided	-	-	e, f
SPO: ESS signing-certificate	conditioned presence	conditioned presence	conditioned presence	conditioned presence	0 or 1	ETSI TS 119 122-1 [2], clause 5.2.2.2	-
SPO: ESS signing-certificate-v2	conditioned presence	conditioned presence	conditioned presence	conditioned presence	0 or 1	ETSI TS 119 122-1 [2], clause 5.2.2.3	-
Service: provide claimed time of signing	shall be provided	shall be provided	shall be provided	shall be provided	-	-	-
SPO: entry with the key *M* in the Signature Dictionary	shall be present	shall be present	shall be present	shall be present	1	ISO 32000-1 [1], clause 12.8.1	g
SPO: signing-time attribute in CMS signature	shall not be present	shall not be present	shall not be present	shall not be present	0	-	-
entry with key *Contents* in the Signature Dictionary	shall be present	shall be present	shall be present	shall be present	1	ISO 32000-1 [1], clause 12.8.1	h, i
entry with key *Filter* in the Signature Dictionary	shall be present	shall be present	shall be present	shall be present	1	ISO 32000-1 [1], clause 12.8.1	j
entry with key *ByteRange* in the Signature Dictionary	shall be present	shall be present	shall be present	shall be present	1	ISO 32000-1 [1], clause 12.8.1	k
entry with key *SubFilter* in the Signature Dictionary	shall be present	shall be present	shall be present	shall be present	1	ISO 32000-1 [1], clause 12.8.1	l
entry with key *Location* in the Signature Dictionary	may be present	may be present	may be present	may be present	0 or 1	ISO 32000-1 [1], clause 12.8.1	-
entry with key *Reason* in the Signature Dictionary	may be present	may be present	may be present	may be present	0 or 1	ISO 32000-1 [1], clause 12.8.1	m
entry with key *Name* in the Signature Dictionary	may be present	may be present	may be present	may be present	0 or 1	ISO 32000-1 [1], clause 12.8.1	-
entry with key *ContactInfo* in the Signature Dictionary	may be present	may be present	may be present	may be present	0 or 1	ISO 32000-1 [1], clause 12.8.1	-

Attributes / Fields / Services	Presence in B-B level	Presence in B-T level	Presence in B-LT level	Presence in B-LTA level	Cardinality	References	Additional requirements and notes
entry with key *Cert* in the Signature Dictionary	shall not be present	shall not be present	shall not be present	shall not be present	0	ISO 32000-1 [1], clause 12.8.1	-
SERVICE: provide trusted time for existence of the signature	*	shall be provided	shall be provided	shall be provided	-	-	n
SPO: signature-time-stamp	*	conditioned presence	conditioned presence	conditioned presence	≥ 0	ETSI TS 119 122-1 [2], clause 5.3	o, p, q
SPO: document-time-stamp	*	conditioned presence	conditioned presence	conditioned presence	≥ 0	clause 5.4.3	
SERVICE: provide certificate and revocation values	*	*	shall be provided	shall be provided	-	-	-
SPO: DSS	*	*	shall be present	shall be present	B-B, -T: ≥ 0 B-LT, -LTA: ≥ 1	clause 5.4.2.2	r, s, t, u, v
SPO: DSS / VRI	*	*	conditioned presence	conditioned presence	≥ 0	clause 5.4.2.3	-
SERVICE: provide trusted time for existence of the validation data	*	*	*	shall be provided	-	-	note 3
SPO: document-time-stamp	*	*	*	shall be present	B-B, -T, -LT: ≥ 0 B-LTA: ≥ 1	clause 5.4.3	w, x, y

Additional requirements:

a) The generator shall include the signing certificate in the `SignedData.certificates` field.

b) In order to facilitate path building, generators should include in the `SignedData.certificates` field all certificates not available to verifiers that can be used during path building. When the signature is to be validated through a Trusted List as specified in ETSI TS 119 612 [i.11], the generator should include all intermediary certificates forming a chain between the signer certificate and a CA present in the Trusted List, which are not available to verifiers.

NOTE 1: A certificate is considered available to the verifier if reliable information about its location is known and allows automated retrieval of the certificate (for instance through an Authority Info Access Extension or equivalent information present in a TSL).

NOTE 2: In the general case, different verifiers can have different trust parameters and can validate the signer certificate through different chains. Therefore, generators may not know which certificates will be relevant for path building. However, in practice, generators can often clearly identify such certificates. In this case, including them in the signature is a good practice, unless verifiers can automatically retrieve them.

c) The `content-type` attribute shall have value `id-data`.

d) The `commitment-type-indication` attribute may be incorporated in the CMS signature only if the `signature-policy-identifier` attribute is present. Otherwise the `commitment-type-indication` shall not be incorporated in the CMS signature.

e) Generators shall use either the signing certificate or the signing-certificate v2 attribute, depending on the hash function, in accordance with ETSI TS 119 122-1 [2].

f) Generators should use ESS signing-certificate v2 in preference to ESS signing-certificate in line with the guidance given in ETSI TS 119 312 [i.7].

g) The generator shall include the claimed UTC time of the signature as expressed in [1], clause 7.9.4 as content of this element.

h) The Content key shall contain a DER-encoded SignedData object as specified in CMS (IETF RFC 5652 [3]) as the PDF signature. This CMS object forms a CAdES signature described in ETSI TS 119 122-1 [2].

i) Requirements specified in ISO 32000-1 [1], clauses 12.8.3.2 (PKCS#1) and 12.8.3.3 (PKCS#7) shall not be used.

j) 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.

k) The ByteRange shall cover the entire file, including the Signature Dictionary but excluding the PDF Signature itself (the entry with key *Contents*).

l) The Signature Dictionary shall contain a value of **ETSI.CAdES.detached** for the key SubFilter.

m) The entry with the key *Reason* can be used only if the `signature-policy-identifier` attribute is not present in the CMS signature.

n) The trusted time shall be provided either by a `signature-time-stamp` attribute or a `document-time-stamp`.

o) The generator shall use DER encoding for any `signature-time-stamp` attribute.

p) A PAdES-B-T signature may contain several `signature-time-stamp` or `document-time-stamp` attributes.

q) If it is anticipated to propagate PAdES-B-B signatures to a higher conformance level, they can reserve space for the signature-time-stamp attribute [2]. Alternatively a document-time-stamp, which covers the whole document including the signature value, can serve this purpose.

r) In situations different than those ones identified in the present clause requirements a) and b), applications should include certificate values within the DSS. The full set of certificates, including the trust anchor when it is available in the form of a certificate, that have been used to validate the signature and which are not already present shall be included. This set includes certificates required for validating the signing certificate, for validating any attribute certificate present in the signature, and for validating any time-stamp token's signing certificate (i.e. a TSA certificate) already incorporated to the signature.

s) Duplication of certificate values within the signature should be avoided.

t) The full set of revocation data (CRL or OCSP responses) that have been used in the validation of the signer and CA certificates used in signature shall be included. This set includes all certificate status information required for validating the signing certificate, for validating any attribute certificate present in the signature, and for validating any time-stamp token's signing certificate (i.e. a TSA certificate) already incorporated to the signature.

u) The DER encoding shall be used for the certificate-values and the revocation-values.

v) The VRI dictionary should not be used. The inclusion of VRI dictionary entries is optional. All validation material referenced in VRI entries is also referenced in DSS entries.

w) PAdES-B-LTA signatures may have more than one `document-time-stamp` applied after the `DSS` and `DSS/VRI`.

x) Before generating and incorporating a `document-time-stamp` attribute, applications shall include all the validation material, which are not already in the signature, required for validating the signature. This validation material includes all the certificates and all certificate status information (like CRLs or OCSP responses) required for:

- validating the signing certificate;
- validating any attribute certificate present in the signature; and
- validating any time-stamp token's signing certificate (i.e. a TSA certificate) already incorporated to the signature (including, of course, any previous `document-time-stamp`).

This validation material should be incorporated within `DSS.`

y) The value of `SubFilter` shall be **ETSI.RFC3161**.

NOTE 3: A PAdES-B-LTA signature helps to validate the signature beyond any event that would otherwise limit its validity.

6.4 Legacy PAdES baseline signatures

When new unsigned elements (CAdES attributes or PDF dictionary entries) are incorporated to legacy PAdES baseline signatures, these elements shall comply with the present document.

History

Document history		
V1.0.0	June 2015	EN 319 142-1 Approval Procedure AP 20151028: 2015-06-30 to 2015-10-28
V1.0.1	July 2015	Publication (same technical content as EN 319 142-1 V1.0.0)