*For BIS use only* **Doc No.: SSD 10 (27043)**

**January 2025**

**Last date to comment: 20 February 2025**

*Draft Indian Standard*

*(Draft for comments only)*

# *इलेक्ट्रॉनिक हस्ताक्षर और इन्फ्रास्ट्रक्चर (ईएसआई) — पीएडीईएस डिजिटल हस्ताक्षर भाग* 1: *बिल्डिंग ब्लॉक्स और पीएडीईएस आधारभूत हस्ताक्षर*

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

ICS 35.020

Information Technology and Information Technology enabled Services Sectional Committee, SSD 10

## FOREWORD

(*Formal Clauses will be added later*)

This draft Indian Standard will be adopted by the Bureau of Indian Standards after the draft is finalized by the Information Technology and Information Technology enabled Services Sectional Committee, had been approved by the Service Sector Division Council.

This Indian Standard is developed for PAdES digital signatures and will be published in two parts. Other parts in the series are:

Part 2 : Additional PAdES Signature Profiles

The draft Indian Standard is the technical adoption of the European Standard ETSI EN 319 142-1 v 1.1.1 ‘Electronic Signatures and Infrastructures (ESI) — PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures’ developed by ETSI. Modifications have been made to adapt it to India and are limited to referencing the relevant regulatory context (*Information Technology Act*, 2000). The technical coverage is otherwise identical.

*For BIS use only* **Doc No.: SSD 10 (27043)**

**January 2025**

**Last date to comment: 20 February 2025**

*Draft Indian Standard*

# ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI) — PAdES DIGITAL SIGNATURES PART 1: BUILDING BLOCKS AND PAdES BASELINE SIGNATURES

## 1 SCOPE

This draft standard specifies PAdES digital signatures. PAdES signatures build on PDF signatures with an alternative signature encoding to support digital signature formats equivalent to the signature format CAdES, 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 standard 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 standard 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.

## 2 REFERENCES

The standards listed in Annex A contain provisions, which through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent edition of these standards.

## 3 TERMINOLOGY AND ABBREVIATIONS

### 3.1 Terminology

For the purposes of the present document, the terms given in IS 16276-1:2017, ETSI TR 119 001 and the following shall apply:

**3.1.1** *Digital Signature* — Data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, for example by the recipient.

**3.1.2** *Digital Signature Value* — Result of the cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, for example by the recipient.

**3.1.3** *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.

**3.1.4** *Generator* — Any party which creates, or augments a digital signature

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

**3.1.5** Void

**3.1.6** *PAdES Signature* — Digital signature that satisfies the requirements specified within the present document.

**3.1.7** *Proof of Existence* — Evidence that proves that an object existed at a specific date/time.

**3.1.8** *Signature Augmentation Policy* — Set of rules, applicable to one or more digital signatures, that defines the technical and procedural requirements for their augmentation, in order to meet a particular business need, and under which the digital signature(s) can be determined to be conformant.

**3.1.9** *Signature Creation Policy* — Set of rules, applicable to one or more digital signatures, that defines the technical and procedural requirements for their creation, in order to meet a particular business need, and under which the digital signature(s) can be determined to be conformant.

**3.1.10** *Signature Handler* — Software application, or part of a software application, that knows how to perform digital signature operations (for example, signing and/or validating) in conformance with IS 16276-1:2017 and the requirements of the appropriate profile.

**3.1.11** *Signature Policy* — Signature creation policy, signature augmentation policy, signature validation policy or any combination thereof, applicable to the same signature or set of signatures.

**3.1.12** *Signature Validation Policy* — Set of rules, applicable to one or more digital signatures, that defines the technical and procedural requirements for their validation, in order to meet a particular business need, and under which the digital signature(s) can be determined to be valid.

**3.1.13** *Trust Service Provider* — Natural or legal person who provides one or more trust services.

**3.1.14** *Validation Data* — Data that is used to validate a digital signature.

**3.1.15** *Verifier* — Entity that wants to validate or verify a digital signature.

### 3.2 Symbols

Void

### 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 and the following shall apply:

| Abbreviation | Description |
|---|---|
| DSS | Document Security Store |
| ESS | Enhanced Security Services |
| 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 IS 16276-1:2017 with an alternative signature encoding to support digital signature formats equivalent to the signature format CAdES as specified in ETSI EN 319 122-1, by incorporation of signed and unsigned attributes as described in **5**.

The following requirements apply:

a) DER-encoded SignedData object as specified in ETSI EN 319 122-1 shall be included as the PDF signature in the entry with the key Contents of the Signature Dictionary as described in **12.8.1** of IS 16276-1:2017. There shall only be a single signer (for example, one single component of SignerInfo type within signerInfos element) in any PDF Signature;

b) Requirements for handling PDF Signatures specified in **12.8** of IS 16276-1:2017shall apply except where overridden by the present document; and

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 IS 16276-1:2017. In **12.8.3.3.1** of IS 16276-1:2017 reads "No data shall be encapsulated in the PKCS#7 SignedData field".

c) Some signature attributes found in ETSI EN 319 122-1 have the same or similar meaning as keys in the Signature Dictionary described in IS 16276-1:2017. 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 1 defined in **6.3** in the present document.

## 5 ATTRIBUTES SYNTAX AND SEMANTICS

### 5.1 Introduction

This clause provides details on attributes specified within IS 16276-1:2017 and ETSI EN 319 122-1 and defines new attributes for building PAdES signatures.

The clause distinguishes between the following types of attributes: CMS and CAdES defined attributes, IS 16276-1:2017 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 **12.8.1** of IS 16276-1:2017. The second ones are the attributes that build the Signature Dictionary as described in IS 16276-1:2017. The other ones are the attributes where to include validation data and archive validation data that can guarantee long term validity of digital signatures.

*See* **6.3** for 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 **12.8.1** of IS 16276-1:2017. Their syntax shall be as defined in **5** of ETSI EN 319 122-1.

a) Content-type.
b) Message-digest.
c) Signing certificate reference attributes:
   1) ESS signing-certificate;
   2) ESS signing-certificate-v2;
d) Commitment-type-indication.
e) Signer-attributes-v2.
f) Content-time-stamp.
g) Signature-policy-identifier.
h) Signature-time-stamp.

## 5.3 IS 16276-1:2017 Defined Attributes

The entries of the Signature Dictionary shall be as defined in **12.8.1** of IS 16276-1:2017unless 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, Contact Info 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 (CRL) or Online Certificate Status Protocol (OCSP) commonly provided by online services (referred to in the present document as validation data).

This clause describes an extension to IS 16276-1:2017 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* **5.4.2**). The structure of DSS and VRI is illustrated in Fig. 1.

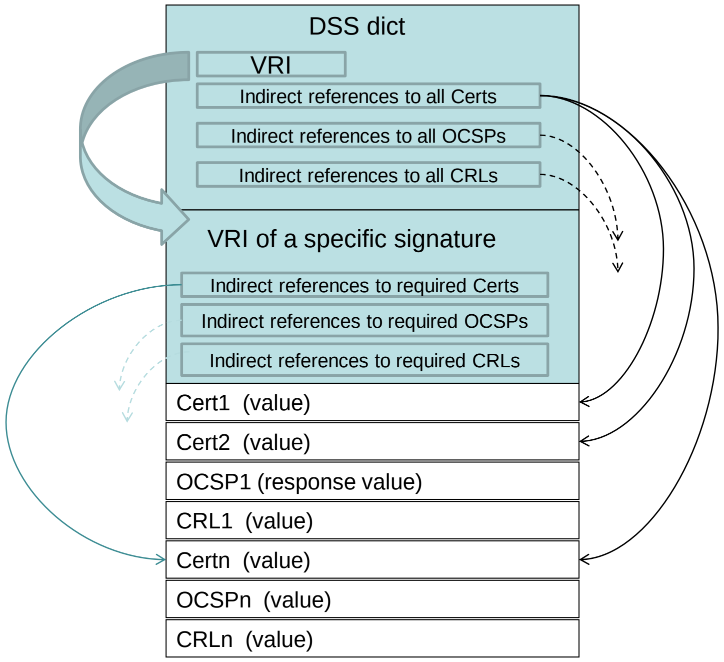
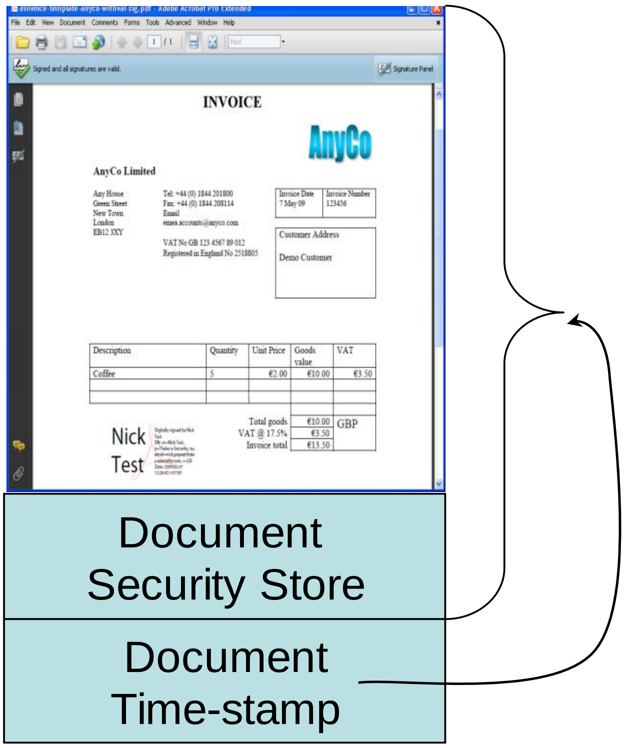

DSS dict
VRI
Indirect references to all Certs
Indirect references to all OCSPs
Indirect references to all CRLs
VRI of a specific signature
Indirect references to required Certs
Indirect references to required OCSPs
Indirect references to required CRLs
Cert1 (value)
Cert2 (value)
OCSP1 (response value)
CRL1 (value)
Certn (value)
OCSPn (value)
CRLn (value)

FIG. **1** ILLUSTRATION OF DSS AND VRI STRUCTURES

This clause also defines another extension to IS 16276-1:2017 called Document Time-stamp (*see* **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 Fig. 2.



eInvoice-template-anyco-withval-sig.pdf - Adobe Acrobat Pro Extended
File Edit View Document Comments Forms Tools Advanced Window Help
1 / 1
Find
Signature Panel
AnyCo
Nick Test
Document Security Store
Document Time-stamp

Signed and all signatures are valid.

INVOICE

AnyCo Limited

Any House
Green Street
New Town
London
EB12 3XY

Tel: +44 (0) 1844 201800
Fax: +44 (0) 1844 208114
Email
emea.accounts@anyco.com

VAT No GB 123 4567 89 012
Registered in England No 2518805

| Invoice Date | Invoice Number |
|---|---|
| 7 May 09 | 123456 |

Customer Address

Demo Customer

| Description | Quantity | Unit Price | Goods value | VAT |
|---|---|---|---|---|
| Coffee | 5 | €2.00 | €10.00 | €3.50 |
| | | | | |
| | | | | |
| | | | | |
| | | Total goods | €10.00 | GBP |
| | | VAT @ 17.5% | €3.50 | |
| | | Invoice total | €13.50 | |

FIG. 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. Every time a DSS Dictionary is updated during incremental update, it should contain the values from the previous DSS Dictionary.

NOTE — In general the DSS Dictionary will contain validation data from previous revisions plus validation data added for the current revision. If entries are removed from a DSS Dictionary during an incremental update the set of validation data might not be complete for validation of the signatures, but replacement of validation data (for example, more up-to-date certificate status information - might be performed for optimization reasons).

This is illustrated in Fig. 3.

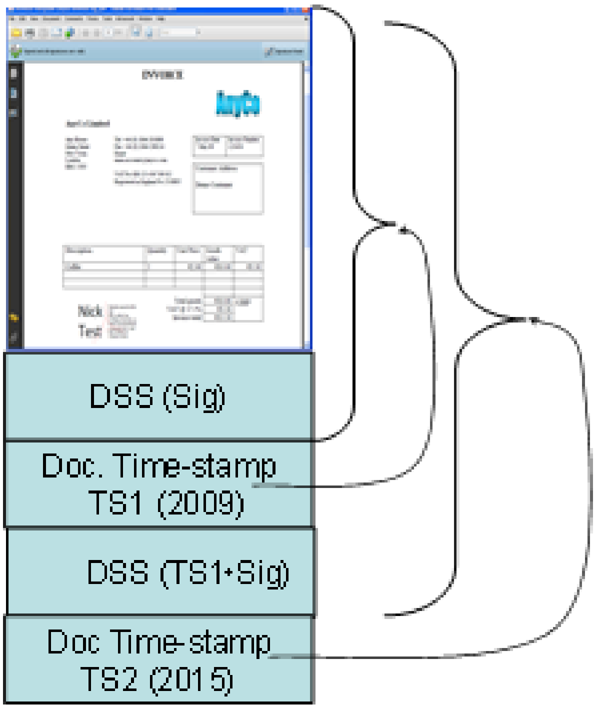


FIG. 3 ILLUSTRATION OF PDF DOCUMENT WITH REPEATED LTV

## 5.4.2 *Document Security Store*

### 5.4.2.1 *Catalog*

| Added to IS 16276-1:2017 "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 and time-stamps signatures represented in PKCS#7 and CMS (and its derivatives) format or for XAdES signatures of forms signing dynamic XFA.

NOTE — *See* ETSI EN 319 142-2 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.<br>(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). 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, which can be used in the validation of any signature in the document. The OCSP response shall be encoded by using the encoding of the OCSPResponse type as defined in IETF RFC 6960. |
| 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). 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 (for example, 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, the contents of the ds:Signature shall be canonicalized using exclusive canonicalization (as specified in http://www.w3.org/2001/10/xml-exc-c14n#) 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* **7.5.6** of IS 16276-1:2017), the VRI update shall be done later than the signature update.

NOTE — To facilitate the verification of signatures created according to previous versions of the signature format specifications, a verifier can also accept OCSP responses encoded by using the encoding of the BasicOCSPResponse type as defined in IETF RFC 6960.

**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 DER-encoded X.509 certificate (that shall be as defined in IETF RFC 5280). 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 **7.9.4** of IS 16276-1:2017,. (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 updated by IETF RFC 5816 and which represents the |

| **Entries in a Signature VRI Dictionary** | | |
|---|---|---|
| **Key** | **Type** | **Value** |
| | | 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:<br>a) The TU key should not be used.<br>b) The TS key should not be used.<br>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.<br>NOTES<br>**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 updated by IETF RFC 5816) is the encryptedDigest field in the signature's PKCS#7 object (as defined in IETF RFC 2315).<br>**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.<br>**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 (for example, 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* **12.8.2.2** of IS 16276-1:2017) shall not apply to incremental updates to a PDF document containing a DSS dictionary and associated VRI, Certs, CRLs and OCSPs.

NOTE — **12.8.2.2** of IS 16276-1:2017, 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 **12.8.1** of IS 16276-1:2017) with the following changes.

| Modifications for a Document Time-stamp Dictionary of IS 16276-1:2017 | | |
|---|---|---|
| **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.<br>The value of SubFilter should be ETSI.RFC3161.<br>Other values may be defined by developers, and when used, shall be prefixed with the registered developer identification as described in Annex E of IS 16276-1:2017.. |
| Contents | Byte string | *(Required)* When the value of SubFilter is ETSI.RFC3161, the value of Contents shall be the hexadecimal string (as defined in **7.3.4.3** of IS 16276-1:2017) representing the value of TimeStampToken as specified in IETF RFC 3161 updated by IETF RFC 5816. The value of the message Imprint 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.<br>Default value: 0. |
| NOTE — **7.3.4** in IS 16276-1:2017 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* **12.8.2.2** of IS 16276-1:2017) the presence of a Document Time-stamp dictionary item shall be ignored.

NOTE — *See* note **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:

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

### 5.6 Extensions Dictionary

The extensions dictionary (*see* **7.12** of IS 16276-1:2017,) should include:

an entry

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

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

an entry

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

to identify that a PDF document includes extensions as identified in **6.3**, requirement l).

Both the above entries should be included in the extensions dictionary when a PDF document includes both the extensions identified in **5.4** and in **6.3**, requirement l).

NOTE — As an alternative to the above entries, use of extensions as identified in **5.4** and in **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

This clause 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.

NOTES

**1** ETSI TR 119 100 provides a description on the life-cycle of a signature and the rationales on which level is suitable in which situation.
**2** The levels c) 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.
**3** 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 many events that limit its validity (for instance, the weakness of used cryptographic algorithms, or expiration of validation data). The use of B-LTA level is considered an appropriate preservation and transmission technique for signed data.
**4** 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) 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 and augment digital signatures should be as specified in IS 19156 : 2025.

NOTE — Cryptographic suites recommendations defined in IS 19156 : 2025 can be superseded by national recommendations.

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

### 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 hereinafter). 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.

a) Column "Attributes/Fields/Services":
   1) In the case where the cell identifies a Service, the cell content starts with the keyword "Service:" followed by the name of the service.
   2) 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.
   3) Otherwise, this cell contains the name of the attribute or signature field.

b) 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.

c) 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.

d) 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.

e) 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.

f) 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":
   1) "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".
   2) "shall not be present": means that the attribute or signature field shall not be incorporated to the signature.

   3) "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".
   4) "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.

5) "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".
6) "*": 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.

g) 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:

1) 0: The signature shall not incorporate any instance of the attribute or signature field.
2) 1: The signature shall incorporate exactly one instance of the attribute or signature field.
3) 0 or 1: The signature shall incorporate zero or one instance of the attribute or signature field.
4) ≥ 0: The signature shall incorporate zero or more instances of the attribute or signature field.
5) ≥ 1: The signature shall incorporate one or more instances of the attribute or signature field.

h) 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.

j) 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 1.

*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 EN 319 122-1 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 1 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.

**Last date to comment: 20 February 2025**

**Table 1 Requirements on the Main Attributes for PAdES Baseline Signatures**

*(Clause* 6.3*)*

| **Sl No.** | **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** |
|---|---|---|---|---|---|---|---|---|
| **(1)** | **(2)** | **(3)** | **(4)** | **(5)** | **(6)** | **(7)** | **(8)** | **(9)** |
| i) | SignedData.certificates | shall be present | shall be present | shall be present | shall be present | 1 | See 5.1 of IETF RFC 5652 | a), b)<br>Notes 1 and 2 |
| ii) | content-type | shall be present | shall be present | shall be present | shall be present | 1 | See 5.1.1 of ETSI EN 319 122-1 | c) |
| iii) | message-digest | shall be present | shall be present | shall be present | shall be present | 1 | See 5.1.2 of ETSI EN 319 122-1 | - |
| iv) | signer-attributes-v2 | may be present | may be present | may be present | may be present | 0 or 1 | See 5.2.6 of ETSI EN 319 122-1 | - |
| v) | content-time-stamp | may be present | may be present | may be present | may be present | ≥ 0 | See 5.2.8 of ETSI EN 319 122-1 | - |
| vi) | signature-policy-identifier | may be present | may be present | may be present | may be present | 0 or 1 | See 5.2.9 of ETSI EN 319 122-1 | - |
| vii) | commitment-type-indication | conditioned presence | conditioned presence | conditioned presence | conditioned presence | 0 or 1 | See 5.2.3 of ETSI EN 319 122-1 | d) |
| viii) | SERVICE: protection of signing certificate | shall be provided | shall be provided | shall be provided | shall be provided | - | - | e), f) |
| ix) | SPO: ESS signing-certificate | conditioned presence | conditioned presence | conditioned presence | conditioned presence | 0 or 1 | See 5.2.2.2 of ETSI EN 319 122-1 | - |

**Table 1** (*Continued*)

| **Sl No.**<br>**(1)** | **Attributes/Fields/Services**<br>**(2)** | **Presence in B-B level**<br>**(3)** | **Presence in B-T level**<br>**(4)** | **Presence in B-LT level**<br>**(5)** | **Presence in B-LTA level**<br>**(6)** | **Cardinality**<br>**(7)** | **References**<br>**(8)** | **Additional requirements and notes**<br>**(9)** |
|---|---|---|---|---|---|---|---|---|
| x) | SPO: ESS signing-certificate-v2 | conditioned presence | conditioned presence | conditioned presence | conditioned presence | 0 or 1 | See 5.2.2.3 of ETSI EN 319 122-1 | - |
| xi) | Service: provide claimed time of signing | shall be provided | shall be provided | shall be provided | shall be provided | - | - | - |
| xii) | SPO: entry with the key *M* in the Signature Dictionary | shall be present | shall be present | shall be present | shall be present | 1 | See 12.8.1 of IS 16276-1:2017 | g) |
| xiii) | SPO: signing-time attribute in CMS signature | shall not be present | shall not be present | shall not be present | shall not be present | 0 | - | - |
| xiv) | entry with key *Contents* in the Signature Dictionary | shall be present | shall be present | shall be present | shall be present | 1 | See 12.8.1 of IS 16276-1:2017 | h), j) |
| xv) | entry with key *Filter* in the Signature Dictionary | shall be present | shall be present | shall be present | shall be present | 1 | See 12.8.1 of IS 16276-1:2017 | k) |
| xvi) | entry with key *ByteRange* in the Signature Dictionary | shall be present | shall be present | shall be present | shall be present | 1 | See 12.8.1 of IS 16276-1:2017 | m) |
| xvii) | entry with key *SubFilter* in the Signature Dictionary | shall be present | shall be present | shall be present | shall be present | 1 | See 12.8.1 of IS 16276-1:2017 | n) |
| xviii) | entry with key *Location* in the Signature Dictionary | may be present | may be present | may be present | may be present | 0 or 1 | See 12.8.1 of IS 16276-1:2017 | - |
| xix) | entry with key *Reason* in the Signature Dictionary | conditioned presence | conditioned presence | conditioned presence | conditioned presence | 0 or 1 | See 12.8.1 of IS 16276-1:2017 | p) |
| xx) | entry with key *Name* in the Signature Dictionary | may be present | may be present | may be present | may be present | 0 or 1 | See 12.8.1 of IS 16276-1:2017 | - |
| xxi) | entry with key *ContactInfo* in the Signature Dictionary | may be present | may be present | may be present | may be present | 0 or 1 | See 12.8.1 of IS 16276-1:2017 | - |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| xxii) | 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 | See 12.8.1 of IS 16276-1:2017 | - |

**Table 1** (*Continued*)

| **Sl No.** | **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** |
|---|---|---|---|---|---|---|---|---|
| **(1)** | **(2)** | **(3)** | **(4)** | **(5)** | **(6)** | **(7)** | **(8)** | **(9)** |
| xxiii) | SERVICE: provide trusted time for existence of the signature | * | shall be provided | shall be provided | shall be provided | - | - | q) |
| xxiv) | SPO: signature-time-stamp | * | conditioned presence | conditioned presence | conditioned presence | ≥ 0 | See 5.3 of ETSI EN 319 122-1 | r), s), t) |
| xxv) | SPO: document-time-stamp | * | conditioned presence | conditioned presence | conditioned presence | ≥ 0 | See **5.4.3** | |
| xxvi) | SERVICE: provide certificate and revocation values | * | * | shall be provided | shall be provided | - | - | - |
| xxvii | SPO: DSS | * | * | shall be present | shall be present | B-B, -T: ≥ 0<br>B-LT, -LTA: ≥ 1 | See **5.4.2.2** | u), v), w), y), z) |
| xxvii | SPO: DSS/VRI | * | * | conditioned presence | conditioned presence | ≥ 0 | See **5.4.2.3** | - |
| xxix) | SERVICE: provide trusted time for existence of the validation data | * | * | * | shall be provided | - | - | Note 3 |
| xxx) | SPO: document-time-stamp | * | * | * | shall be present | B-B, -T, -LT: ≥ 0<br>B-LTA: ≥ 1 | See **5.4.3** | aa), ab), ac) |

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 for trust hierarchy, the generator should include all intermediary certificates forming a chain between the signer certificate and a Trusted CA, which are not available to verifiers.

NOTES

**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).

**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 entry with the key *Reason* is not used. 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 EN 319 122-1.

f) Generators should use ESS signing-certificate v2 in preference to ESS signing-certificate in line with the guidance given in IS 19156 : 2025.

g) The generator shall include the claimed UTC time of the signature as expressed in **7.9.4** of IS 16276-1:2017as content of this element.

h) The Content key shall contain a DER-encoded SignedData object as specified in CMS (IETF RFC 5652) as the PDF signature. This CMS object forms a CAdES signature described in ETSI EN 319 122-1.

j) Requirements specified in **12.8.3.2** (PKCS#1) and **12.8.3.3** (PKCS#7) of IS 16276-1:2017, shall not be used.

k) 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.

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

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

p) The entry with the key *Reason* shall not be used when the commitment-type-indication attribute is present in the CMS signature. The entry with the key *Reason* shall not be used if the signature-policy-identifier attribute is present in the CMS signature.

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

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

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

t) 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 that will be added to the DER-encoded SignedData object as specified in ETSI EN 319 122-1. Alternatively a document-time-stamp, which covers the whole document including the signature value, can serve this purpose.

u) 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 (for example, a TSA certificate) already incorporated to the signature.

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

w) 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 (for example, a TSA certificate) already incorporated to the signature.

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

z) 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.

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

ab) 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:

1) validating the signing certificate;

2) validating any attribute certificate present in the signature; and

3) validating any time-stamp token's signing certificate (for example, a TSA certificate) already incorporated to the signature (including, of course, any previous document-time-stamp).

This validation material should be incorporated within DSS.

ac) The value of SubFilter shall be ETSI RFC 3161.

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

## ANNEX A
(*Clause* 2)

## LIST OF REFERRED STANDARDS

| *IS No.* | *Title* |
|---|---|
| IS 16276-1:2017 | Document management - Portable document format - Part 1: PDF 1.7 |
| ETSI EN 319 122-1 | Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures |
| IETF RFC 5652 (2009) | Cryptographic Message Syntax (CMS) |
| IETF RFC 5816 (2010) | ESSCertIDv2 Update for RFC 3161 |
| IETF RFC 5280 (2008) | Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile |
| IETF RFC 3161 (2001) | Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) |
| IETF RFC 6960 (2013) | X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP |
| W3C® Recommendation (May 2008) | Canonical XML Version 1.1 |

## ANNEX B
(*Foreword*)

## BIBLIOGRAPHY

[1] IS 19156 : 2025: “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”

[2] ETSI EN 319 102-1: “Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation”

[3] ETSI TR 119 001: “Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations”

[4] ETSI TR 119 100: “Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for signature creation and validation”

[5] ETSI TR 119 000: “Electronic Signatures and Infrastructures (ESI); The framework for standardization of digital signatures and trust services; Overview”

[6] ETSI EN 319 142-2 : “Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles”

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

[8] ETSI TS 103 172: “Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile”

[9] ETSI TS 119 612: “Electronic Signatures and Infrastructures (ESI); Trusted Lists”

[10] Adobe® XFA: “XML Forms Architecture (XFA) Specification" version 2.5, (June 2007), Adobe Systems Incorporated”