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


**Electronic Signatures and Infrastructures (ESI);**
**PAdES digital signatures;**
**Part 2: Additional PAdES signatures profiles**

Reference
DEN/ESI-0019142-2

Keywords
electronic signature, PAdES, profile, security

***ETSI***

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

# Contents

# Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

# Foreword

This draft European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI standards EN Approval Procedure.

The present document is part 2 of a multi-part deliverable covering the PDF digital signatures (PAdES), as identified below.

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

**Part 2: "Additional PAdES signatures profiles".**

| **Proposed national transposition dates** | |
|---|---|
| Date of latest announcement of this EN (doa): | 3 months after ETSI publication |
| Date of latest publication of new National Standard or endorsement of this EN (dop/e): | 6 months after doa |
| Date of withdrawal of any conflicting National Standard (dow): | 6 months after doa |

# Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

# Introduction

Electronic commerce has emerged as a frequent way of doing business between companies across local, wide area and global networks. Trust in this way of doing business is essential for the success and continued development of electronic commerce. It is therefore important that companies using this electronic means of doing business have suitable security controls and mechanisms in place to protect their transactions and to ensure trust and confidence with their business partners. In this respect digital signatures are an important security component that can be used to protect information and provide trust in electronic business.

The present document is intended to cover digital signatures supported by PKI and public key certificates. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (i.e. repudiates; see ISO/IEC 10181-4 [i.1]) the validity of the signature.

Thus, the present document can be used for any document encoded in a portable document format (PDF) produced by an individual and a company, and exchanged between companies, between an individual and a governmental body, etc. The present document is independent of any environment; it can be applied to any environment, e.g. smart cards, SIM cards, special programs for digital signatures, etc.

The present document is part of a rationalized framework of standards (see ETSI TR 119 000 [i.8]). See ETSI TR 119 100 [i.9] for getting guidance on how to use the present document within the aforementioned framework.

# 1 Scope

The present document defines multiple profiles for PAdES digital signatures which are digital signatures embedded within a PDF file.

The present document contains a profile for the use of PDF signatures, as described in ISO 32000-1 [1] and based on CMS digital signatures [i.6], that enables greater interoperability for PDF signatures by providing additional restrictions beyond those of ISO 32000-1 [1]. This first profile is not related to part 1 of ETSI EN 319 142 [4].

The present document also contains a second set of profiles that extend the scope of the profile in PAdES part 1 [5], while keeping some features that enhance interoperability of PAdES signatures. These profiles define three levels of PAdES extended signatures addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it. These PAdES extended signatures offer a higher degree of optionality than the PAdES baseline signatures specified in part 1 of ETSI EN 319 142 [4].

The present document also defines a third profile for usage of an arbitrary XML document signed with XAdES signatures that is embedded within a PDF file.

The profiles defined in the present document provide equivalent requirements to profiles found in ETSI ETSI TS 102 778 [i.10].

The present document does not repeat the base requirements of the referenced standards, but instead aims to maximize interoperability of digital signatures in various business areas.

# 2 References

## 2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

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

[1] ISO 32000-1: "Document management - Portable document format - Part 1: PDF 1.7".

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

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

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

[4] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[5] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[6] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[7] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

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

[9] W3C Recommendation: "XML-Signature Syntax and Processing. Version 1.1".

[10] IETF RFC 5035 (2007): "Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility".

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

[12] IETF RFC 5816 (2010): "ESSCertIDv2 Update for RFC 3161".

## 2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ISO/IEC 10181-4: "Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework".

[i.2] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

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

[i.4] W3C® Working Group Note, XML Signature Best Practices, 11 April 2013.

[i.5] ISO 19005-1:2005: "Document management - Electronic document file format for long-term preservation - Part 1: Use of PDF 1.4 (PDF/A-1)".

[i.6] IETF RFC 5652 (2009): "Cryptographic Message Syntax (CMS)".

[i.7] ISO 19005-2 (2011): "Document management - Electronic document file format for long-term preservation - Part 2: Use of ISO 32000-1 (PDF/A-2)".

[i.8] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); Rationalized structure for Electronic Signature Standardization".

[i.9] ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Business Driven Guidance for Signature Creation and Validation".

[i.10] ETSI TS 102 778: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; CMS Profile based on ISO 32000-1".

# 3 Definitions and abbreviations

## 3.1 Definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**signer:** natural or legal person who creates a digital signature

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

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

## 3.2 Abbreviations

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

| | |
|---|---|
| CA | Certification Authority |
| CAdES | CMS Advanced Electronic Signatures |

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

| | |
|---|---|
| CMS | Cryptographic Message Syntax |

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

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

# 4 Profile for CMS digital signatures in PDF

## 4.1 Features

The present profile specifies digital signatures that:

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

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

## 4.2 Requirements of Profile for CMS Signatures in PDF

### 4.2.1 Requirements on PDF signatures

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

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

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

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

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

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

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

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

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

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

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

### 4.2.2 Requirements on PDF signature handlers

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

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

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

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

### 4.2.3 Requirements on signature validation

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

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

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

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

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

### 4.2.4 Requirements on Time Stamping

#### 4.2.4.1 Requirements on electronic time-stamp creation

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

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

#### 4.2.4.2 Requirements on electronic time-stamp validation

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

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

### 4.2.5 Requirements on revocation checking

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

### 4.2.6 Requirements on Seed Values

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

EXAMPLE: Seed values that specify the use of PKCS#1 are not permitted as the present document requires use of PKCS#7.

### 4.2.7 Requirements on encryption

The Requirements in PAdES Part 1 [4], clause 5.5 shall apply.

# 5 Extended PAdES signature profiles

## 5.1 Features

The profiles in this clause define PAdES signatures based on the building blocks defined in PAdES Part 1 [4]. These profiles define three levels of PAdES extended signatures that offer a higher degree of optionality than the PAdES baseline signatures specified in part 1 [4].

PAdES-E-BES Level allows basic digital signatures embedded within a PDF file. There is a unambiguous connection from the signature to the identity of a certificate intended to identify the signer.

PAdES-E-EPES Level is built on top of the PAdES-E-BES Level and allows inclusion of signature policies.

PAdES-E-LTV can build on either PAdES-E-BES Level or PAdES-E-EPES Level addressing incremental requirements to maintain the validity of the signatures over the long term.

## 5.2 General Requirements

### 5.2.1 Requirements from Part 1

The requirements given in clause 4.1 of [4] (PAdES Part 1) shall apply to all profiles in this clause.

### 5.2.2 Notation of Requirements

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

The requirements on the attributes and certain signature fields are expressed in tables. A row in the table either specifies requirements for an attribute or a service.

These tables contain five columns.

1) Column "Attribute/Field/Service":

   - this cell contains the name of the attribute or signature field.

2) Colum "Presence": This cell contains the specification of the presence of the attribute or signature as follows:

   - "shall be present": means that the attributes or signature fields shall be present, 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 attributes or signature fields shall not be present.
   - "may be present": means that the attributes or signature fields may be present, 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".
   - "conditioned presence": means that the presence 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".

3) Column "Cardinality". This cell indicates the cardinality of the attribute or signature field as follows:

   - **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.

4) 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.

5) Column "Reference": This cell contains either the number of the clause specifying the attribute in the present document, or a reference to the document and clause that specifies the signature field.

## 5.3 PAdES-E-BES Level

The requirements and the attributes within signature dictionary and `SignerInfo` are as defined in table 1.

For any optional unsigned attribute incorporated in the signature, DER encoding shall be used for this attribute, whilst preserving the encoding of any other attribute field.

**Table 1: Requirements for the main attributes in PAdES-BES signature**

| Attribute/Field/Service | Presence | Cardinality | Additional notes and requirements | Reference |
|---|---|---|---|---|
| `content-type` | shall be present | 1 | a | ETSI EN 319 122-1 [5], clause 5.1.1 |
| `message-digest` | shall be present | 1 | | ETSI EN 319 122-1 [5], clause 5.1.2 |
| `signing-certificate reference` | shall be present | 1 | b, c, d | |
| `signer-attributes-v2` | may be present | 0 or 1 | | ETSI EN 319 122-1 [5], clause 5.2.6.1 |
| `content-time-stamp` | may be present | ≥ 0 | | ETSI EN 319 122-1 [5], clause 5.2.8 |
| `signature-time-stamp` | may be present | ≥ 0 | | ETSI EN 319 122-1 [5], clause 5.3 |
| entry with key *`M`* in the `Signature Dictionary` | may be present | 0 or 1 | e | ISO 32000-1 [1], clause 12.8.1 |
| entry with key *`Location`* in the `Signature Dictionary` | 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 | 0 or 1 | | ISO 32000-1 [1], clause 12.8.1 |
| entry with key *`Filter`* in the `Signature Dictionary` | shall be present | 1 | f | ISO 32000-1 [1], clause 12.8.1 |
| entry with key *`ByteRange`* in the `Signature Dictionary` | shall be present | 1 | g | ISO 32000-1 [1], clause 12.8.1 |
| entry with key *`SubFilter`* in the `Signature Dictionary` | shall be present | 1 | h | ISO 32000-1 [1], clause 12.8.1 |
| entry with key *`Contents`* in the `Signature Dictionary` | shall be present | 1 | i | ISO 32000-1 [1], clause 12.8.1 |
| entry with key *`Name`* in the `Signature Dictionary` | 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 | 0 or 1 | | ISO 32000-1 [1], clause 12.8.1 |
| entry with key *`Cert`* in the `Signature Dictionary` | shall not be present | 0 | | ISO 32000-1 [1], clause 12.8.1 |

Additional requirements:

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

b) As specified in IETF RFC 5035 [10], the ESS `signing-certificate` attribute shall be used if the SHA-1 hash algorithm is used.

c) As specified in IETF RFC 5035 [10], the ESS `signing-certificate-v2` attribute shall be used when another hash algorithms than SHA-1 is used.

d) The generator should migrate to the use of ESS `signing-certificate-v2` in preference to ESS `signing-certificate` in line with the guidance regarding limited lifetime for the use of SHA-1 given in ETSI TS 119 312 [i.2].

e) The generator should include the claimed UTC time of the signature in a format defined in ISO 32000-1 [1], clause 7.9.4 as content of this element.

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

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

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

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.

## 5.4 PAdES-E-EPES Level

The requirements and the attributes within `SignerInfo` are as defined in table 1 to which those ones defined in table 2 shall be added/replaced.

For any optional unsigned attribute incorporated in the signature, DER encoding shall be used for this attribute, whilst preserving the encoding of any other attribute field.

**Table 2: Requirements for the main CAdES attributes in PAdES-E-EPES level**

| Attribute/Field/Service | Presence | Cardinality | Additional notes and requirements | Reference |
|---|---|---|---|---|
| `signature-policy-identifier` | shall be present | 1 | | ETSI EN 319 122-1 [5], clause 5.2.9 |
| `commitment-type-indication` | may be present | 0 or 1 | | ETSI EN 319 122-1 [5], clause 5.2.3 |
| entry with key *Reason* in the Signature Dictionary | shall not be present | 0 | | ISO 32000-1 [1], clause 12.8.1 |

## 5.5 PAdES-E-LTV Level

Signature handlers creating and/or validating PDF documents with PAdES-LTV shall support PDF documents with:

a) Document security store information as specified in clause 5.4.2 in ETSI EN 319 142-1 [4].

b) Document time-stamps as specified in clause 5.4.3 in ETSI EN 319 142-1 [4].

Signed PDF documents should contain DSS followed by a document time-stamp.

Validation data shall be carried by values within the DSS.

NOTE 1: Use of validation data in DSS referencing external sources is not supported by the current profile.

Systems shall support creation and/or validation of signatures with one or more DSS entries and document time-stamps.

NOTE 2: Object IDs should not be reused when adding new validation data, because of the possibility to "hide" already existing validation data. A signature handler may check the existence of older validation data having the same Object IDs to be explicitly aware of the fact that the latest objects could contain invalid or unusable validation data.

# 6 Profiles for XAdES Signatures signing XML content in PDF

## 6.1 Features

The profiles in this clause allow the signing of XML Data that is embedded in a PDF file. The first two profiles allow inclusion of XAdES signatures in PDF and the augmentation of these signatures to achieve long-term validation. The second two profiles allow signatures on XFA-forms and the augmentation of these signatures to achieve long-term validation.

## 6.2 Profiles for XAdES signatures of signed XML documents embedded in PDF containers

### 6.2.1 Overview

This clause defines a profile for usage of an arbitrary XML document signed with XAdES signatures that is embedded within a PDF file, for providing integrity, authentication and non-repudiation services on the data objects that are signed with the XAdES signature. This XML document can be aligned with any XML language, i.e. a signed UBL e-Invoice.

NOTE 1: The term "data object" applies to any resource that is referenced by the XMLDSig mechanisms. It does apply to the XML document when it is signed as a whole, and also to a collection of elements of the XML document if only these elements are signed.

This clause defines two profiles, namely: a basic profile for XAdES-E-BES, XAdES-E-EPES, and XAdES-E-T signature levels, and a long-term profile for signature levels from XAdES-E-C to XAdES-E-A.

The scenario for usage of the first profile, specified in clause 6.2.2, is described below and shown in figure 1:

1) An XML document is created and signed with XAdES (levels XAdES-E-BES, XAdES-E-EPES, XAdES-E-T) out of the PDF framework.

2) The aforementioned signed XML document is embedded within the PDF container and is transported within it.

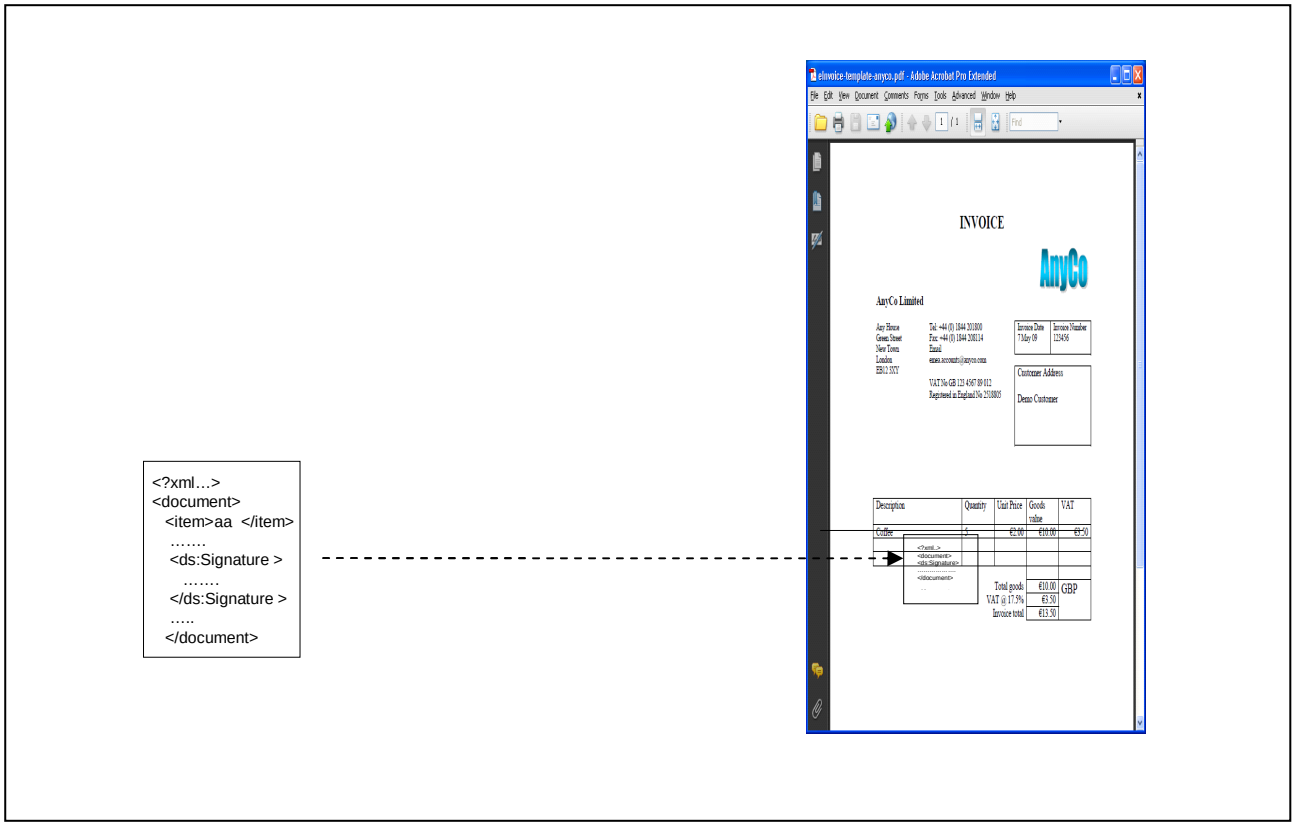


**Figure 1: Scenario for profile for basic XAdES signatures of XML documents embedded in PDF containers**

The scenario for usage of the second profile, specified in clause 6.2.3, is described below and shown in figure 2:

1) The PDF container with the signed XML document is received by the verifier. The verifier extracts the embedded file and validates the XAdES signature.

2) The verifier can augment the XAdES signature to upper levels as specified in ETSI EN 319 132-2 [7]. As the XAdES signature is part of an embedded file, the Document Secure Store specified in ETSI EN 319 142-1 [4] is not able to contain the validation material added during the augmentation. This augmentation will, in consequence, be done outside the PDF container and within the XAdES signature itself.

NOTE 2: It is understood that augmenting the XAdES signature or augmenting the document by a Document Secure Store could provide the verifier with the same information to validate the document in the long run. It is important to augment the XAdES signature in order to enhance interoperability between verifiers.

3) The signed XML document with the augmented XAdES signature is embedded again within the PDF container.

NOTE 3: Augmenting the XAdES signature can be done by extracting the stream object containing the XAdES signature from the containing document, augmenting the XAdES signature in that XML document and including the augmented XML document in a new stream with the same pdf object number by an incremental update.

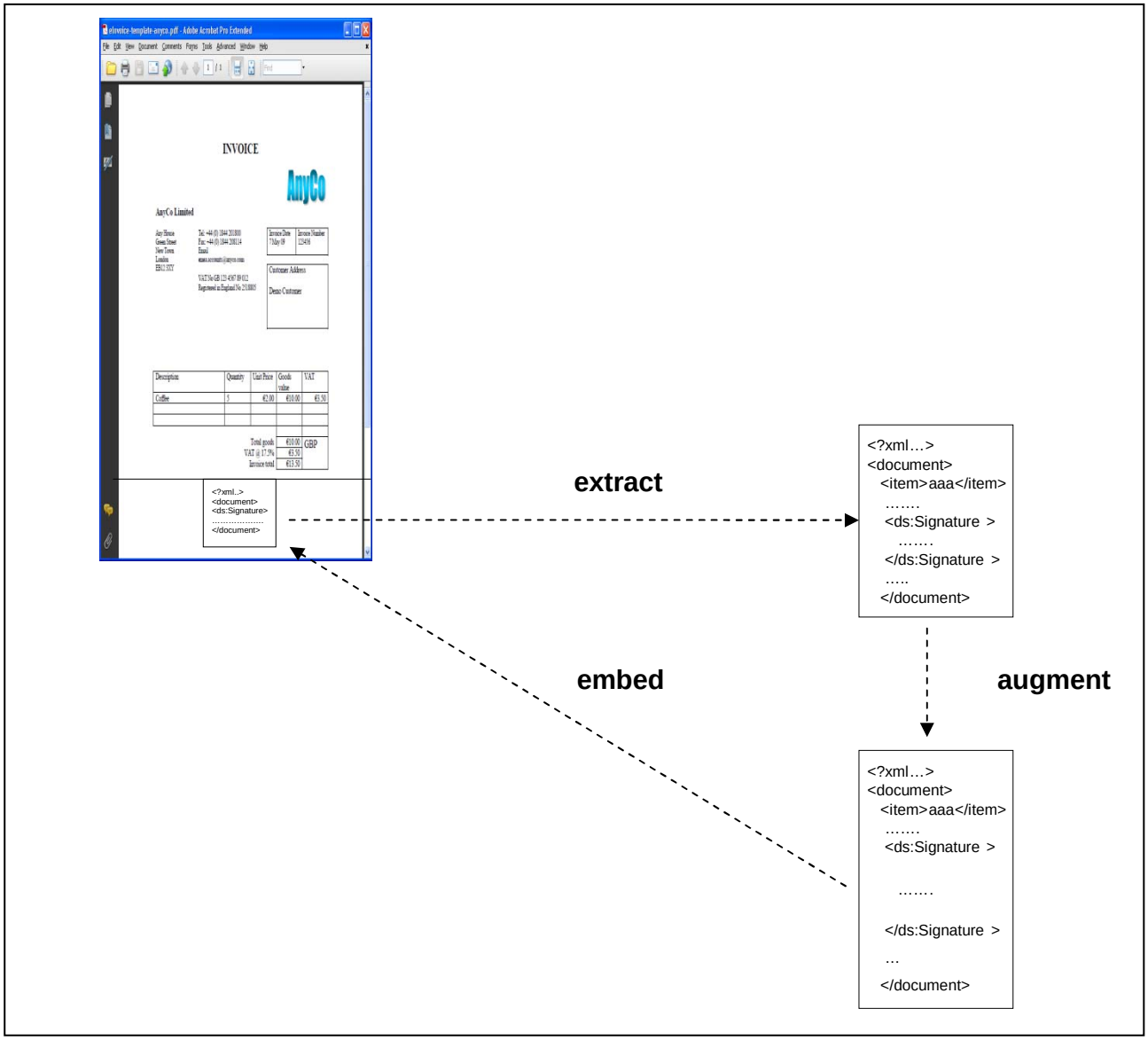


**Figure 2: Scenario for profile for long-term XAdES signatures of signed XML documents embedded in PDF containers**

## 6.2.2 Profile for Basic XAdES signatures of XML documents embedded in PDF containers

### 6.2.2.1 Features

The main features provided by this profile are listed below:

a) The signed XML document (including the XAdES signatures) is created independent from the PDF container. The relative placement of XAdES signatures and the signed data objects are restricted as specified in clause 6.2.2.3.

b) XAdES signatures embedded within the signed XML document protect the signed data objects providing integrity and authenticity. Additionally, the incorporation of a signature time-stamp allows non repudiation of signature production.

c) The following XAdES signatures levels are profiled by this profile: XAdES-E-BES, XAdES-E-EPES, and XAdES-E-T levels in ETSI EN 319 132-2 [7].

d) This profile supports serial signatures using XAdES countersignatures mechanisms.

e) This profile supports parallel signatures.

#### 6.2.2.2 General syntax and requirements

This profile applies to a signed XML document including one or more XAdES signatures that is embedded within PDF containers as an embedded file.

The signatures shall be XAdES signatures XAdES-E-BES, XAdES-E-EPES, or XAdES-E-T with the syntax specified in ETSI EN 319 132-2 [7] with the restrictions specified in the present document.

Unsigned properties not found in this profile may be present and may be ignored unless used in conjunction with other profiles which place requirements on the use of such attributes.

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

#### 6.2.2.3 Requirements for applications generating signed XML document to be embedded

The signed XML document to be embedded within the PDF container shall be created independently of the final PDF container. No further requirements are specified on the environment for creating this XML document or the XAdES signature(s) within the document.

The signed XML document to be embedded within the PDF container shall contain at least one XAdES signature and one or more signed data objects.

The signed data objects and the XAdES signature(s) within the signed XML document to be embedded shall satisfy one of the following requirements:

1) All the signed data objects shall be embedded within the signed XML document. Or

NOTE 1: This would cover any relative placement (enveloped, enveloping or detached) between XAdES signatures and signed data objects as long as these last ones are embedded within the XML document that contains the XAdES signature.

2) If a signed data object is detached from the signed XML document, a `ds:Reference` element shall reference it according to the rules of W3C Recommendation: "XML-Signature Syntax and Processing. Version 1.1" [9].

NOTE 2: This requirement allows situations where some XAdES signature actually signs data objects that are detached from the signed XML document embedded within the PDF container. These data objects could be outside of the PDF container or even within the PDF container assuming that it is possible to build up a valid `ds:Reference` element aligned with the principles specified within W3C Recommendation: "XML-Signature Syntax and Processing. Version 1.1" [9]. Interoperability issues can arise from referencing data objects outside of the PDF container as well as referencing data objects outside of the XML stream but inside of the PDF container.

NOTE 3: The two profiles specified in clause 4 do not impose any further requirement on the XML data objects to be signed as the signature protects the digest values including the digest values of the external data objects. Additional guidance can be found in the W3C Working Draft: "XML Signature Best Practices" [i.4] (or to more evolved versions of that document) that addresses a number of relevant security issues related to specific XMLDSig features, including dereferencing and transforming of the XML data objects to be signed.

#### 6.2.2.4 Mandatory operations

##### 6.2.2.4.1 Protecting the signing certificate

XAdES specifies two mechanisms for protecting the signing certificate, namely: adding the `SigningCertificate` element or including the signing certificate itself within the `ds:KeyInfo` element and cover at least this certificate with the signature itself.

The signing certificate shall be referenced in the SigningCertificate element or shall be included in the ds:KeyInfo element. The SigningCertificate qualifying property should be used.

NOTE: The whole `ds:KeyInfo`, locks the element and any addition of a certificate or validation data will invalidate the signature. Applications may, alternatively, use Xpath transforms for signing at least the signing certificate, leaving the rest of the `ds:KeyInfo` element open for addition of new data after signing.

#### 6.2.2.5 Requirements on XAdES optional properties

The following properties defined in XAdES may be used. If present their syntax, semantics and usage shall be as specified in ETSI EN 319 132-1 [6].

**Table 3: Requirements for the main attributes in basic XAdES signatures of XML documents embedded in PDF containers**

| Properties | References |
|---|---|
| `SigningTime` | ETSI EN 319 132-1 [6], clause 5.2.1 |
| `SignaturePolicyIdentifier` | ETSI EN 319 132-1 [6], clause 5.2.9 |
| `SignatureProductionPlaceV2` | ETSI EN 319 132-1 [6], clause 5.2.5 |
| `SignerRoleV2` | ETSI EN 319 132-1 [6], clause 5.2.6 |
| `DataObjectFormat` | ETSI EN 319 132-1 [6], clause 5.2.4 |
| `CommitmentTypeIndication` | ETSI EN 319 132-1 [6], clause 5.2.3 |
| `AllDataObjectsTimeStamp` | ETSI EN 319 132-1 [6], clause 5.2.8.1 |
| `IndividualDataObjects` | ETSI EN 319 132-1 [6], clause 5.2.8.2 |
| `SignatureTimeStamp` | ETSI EN 319 132-1 [6], clause 5.3 |
| `SignaturePolicyStore` | ETSI EN 319 132-1 [6], clause 5.2.10 |

#### 6.2.2.6 Serial Signatures

The present profile supports serial signing of XAdES signatures by any of the two mechanisms specified within ETSI EN 319 132-1 [6], clause 5.2.7.

The `CounterSignature` element is an optional unsigned qualifying property. If present its syntax, semantics and usage shall be as specified in ETSI EN 319 132-1 [6], clause 5.2.7.2.

Optionally, a XAdES signature aligned with this profile may be countersigned by a detached XAdES signature, which includes a `ds:Reference` element containing a `Type` attribute whose value is as specified in ETSI EN 319 132-1 [6], clause 5.2.7.1. If this method of countersigning a XAdES signature is used the XAdES countersignature should also be present within the Signed XML content embedded within the PDF container.

#### 6.2.2.7 Parallel Signatures

A Signed XML content embedded within the PDF container may include several XAdES signatures signing in parallel the same data objects.

#### 6.2.2.8 PAdES Signatures

CMS digital signatures in PDF (clause 4) , PAdES-E-BES (clause 5.3) or PAdES-E-EPES (clause 5.4), optionally augmented using PAdES-E-LTV (clause 5.5) , can be applied to a document with a XAdES signature applied to XML Data.

NOTE: A XAdES signature cannot be augmented once a PDF signature has been applied to the document.

### 6.2.3 Profile for long-term XAdES signatures of signed XML documents embedded in PDF containers

#### 6.2.3.1 Features

This profile adds to the former profile the features listed below:

a) Long-term signatures production.

b) Signature level can be XAdES-E-C, XAdES-E-X or XAdES-E-XL, XAdES-E-A (ETSI EN 319 132-2 [7]).

#### 6.2.3.2 Augmentation mechanism

For upgrading a XAdES signature form present within the signed XML document, conforming readers shall detach the signed XML document from the PDF container. After that, a suitable combination of the unsigned XAdES properties will be added to the XAdES signature for obtaining the corresponding augmented XAdES signature. Finally, signature handlers shall embed again the signed XML document with the augmented XAdES signature into the PDF container.

#### 6.2.3.3 Optional properties

This profile does not add additional requirements on the unsigned properties that are added for upgrading XAdES signatures. All of them are optional. If any of them is present, its syntax, semantics and usage shall be as specified in ETSI EN 319 132-1 [6].

#### 6.2.3.4 Validation Process

The Document Secure Store specified in ETSI EN 319 142-1 [4] should not be accessed during validation.

## 6.3 Profiles for XAdES signatures on XFA Forms

### 6.3.1 Overview

This clause defines two profiles for using XAdES signatures for signing dynamic XFA forms. Syntax and semantics of dynamic XFA forms are specified inXML Forms Architecture (XFA) Specification [8]:

1) A basic profile for XAdES-E-BES, XAdES-E-EPES, and XAdES-E-T signature levels defined in ETSI EN 319 132-2 [7].

2) A profile for long-term XAdES signatures, which uses DSS and VRI dictionaries specified in ETSI EN 319 142-1 [4] PAdES-B-LTV to achieve equivalent functionality to XAdES-E-XL and XAdES-E-A levels.

These profiles cover two different scenarios, namely: signing only the XML data of the XFA form, or signing any XML content of the XFA form that can be signed with a XMLDSig signature.

The XFA framework is summarized in figure 3. At the right of the figure the PDF incorporating XFA data is shown. Part of its XFA consists of XML elements providing details of the template of the form to be presented to the user (`xfa:template` element in the figure). Other part of the XFA consists of XML elements whose values are those introduced by the user when filling the form (`xfa:datasets` element in the figure). The left part of the figure shows the view presented to the user filling the form. Dashed arrows link the rendered or filled parts of the form with the corresponding XML data within the XFA.

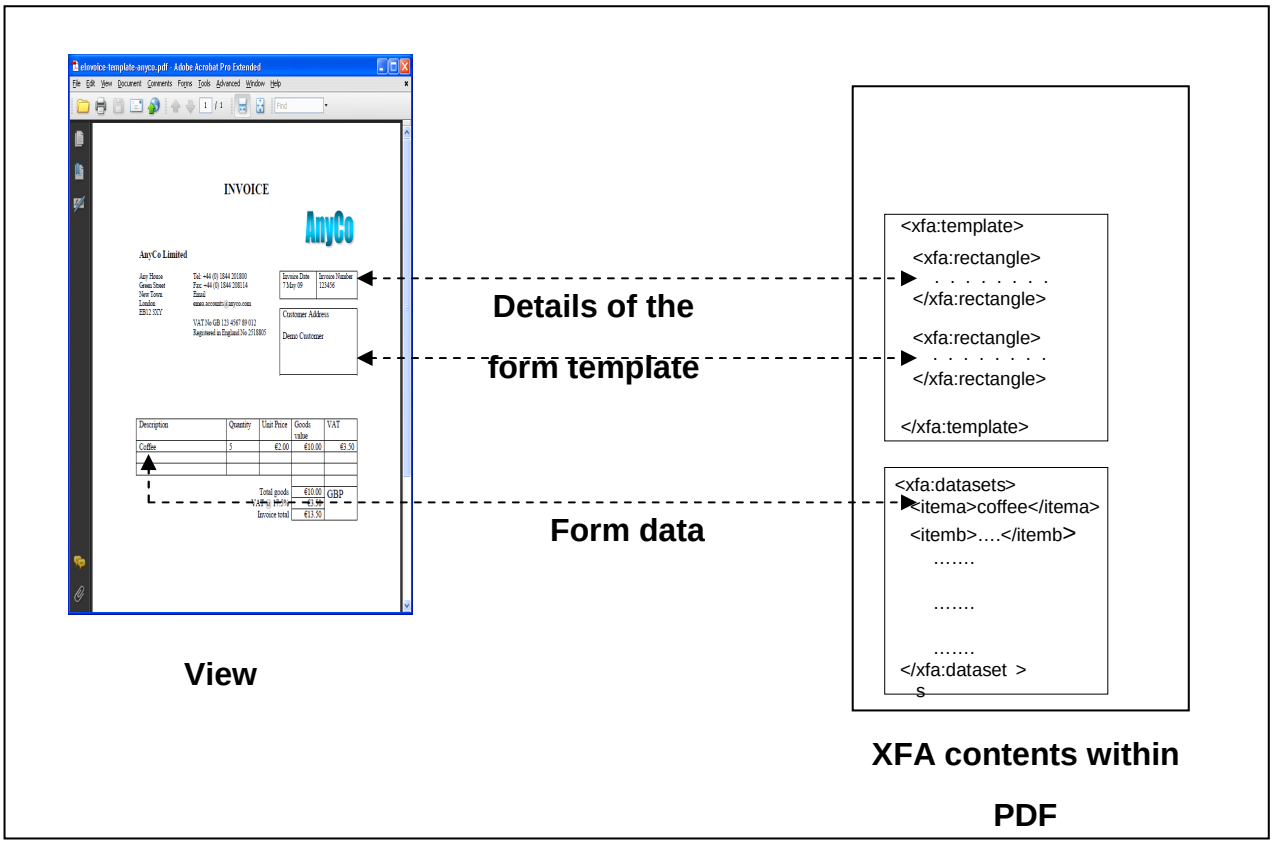


**Figure 3: XFA framework**

The scenario for usage of the profile for basic XAdES signatures on XFA forms, specified in clause 6.3.2, is shown in figure 4. After filling a form, a user can sign selected parts of the form (data only, or any XFA component that can actually be signed with a XAdES signature). The XAdES signature (XAdES-E-BES, XAdES-E-EPES or XAdES-E-T) is then incorporated within the XFA content.

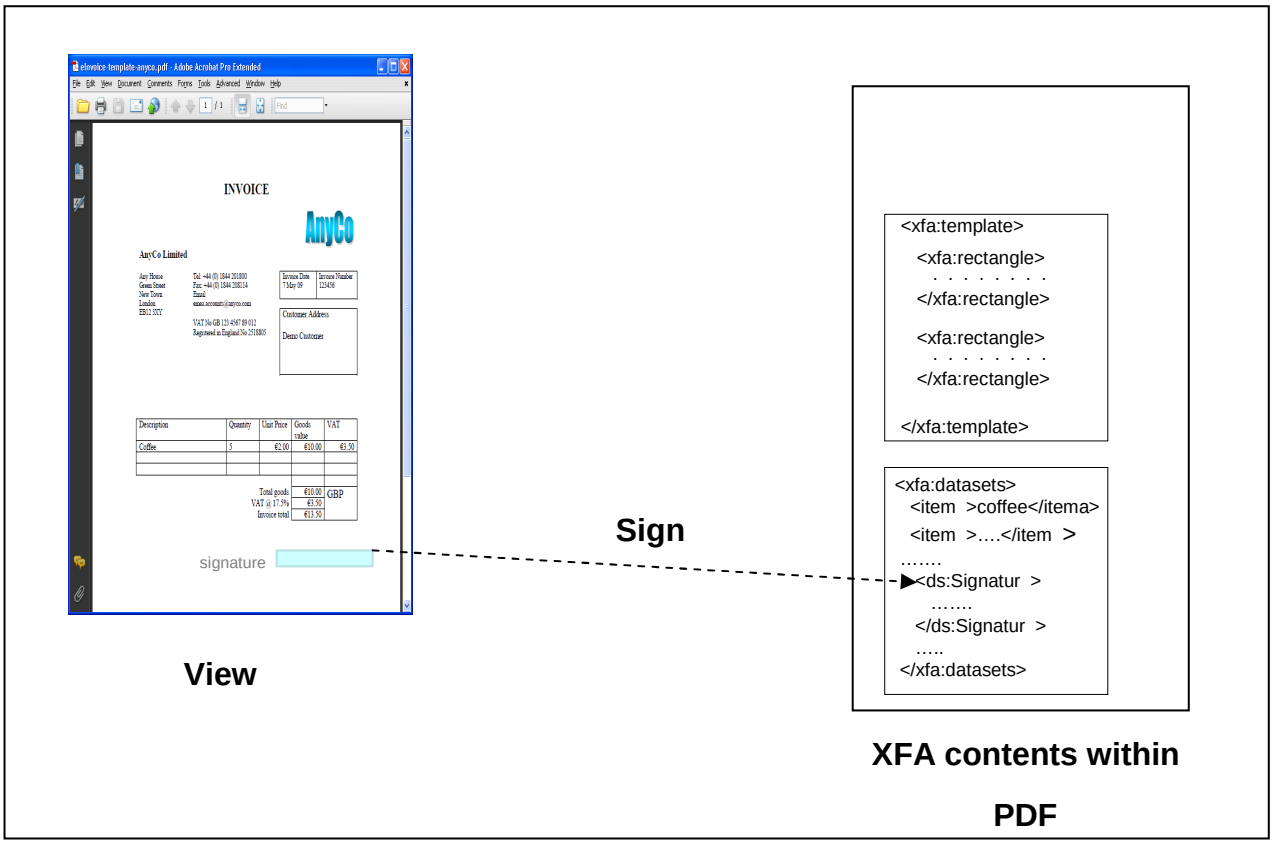


**Figure 4: Scenario for profile for basic XAdES signatures on XFA forms**

The scenario for usage of the profile for long-term validation XAdES signatures on XFA forms, specified in clause 6.3.3, is shown in figure 5. At any time after signing a XFA form with a XAdES signature, a user can augment the signature on the XFA form using the Document Secure Store and VRI techniques specified in ETSI EN 319 142-1 [4]. The validation data is then accordingly incorporated in these dictionaries, as the XAdES signature on the XFA form is a signature fully acknowledged by the XFA framework.

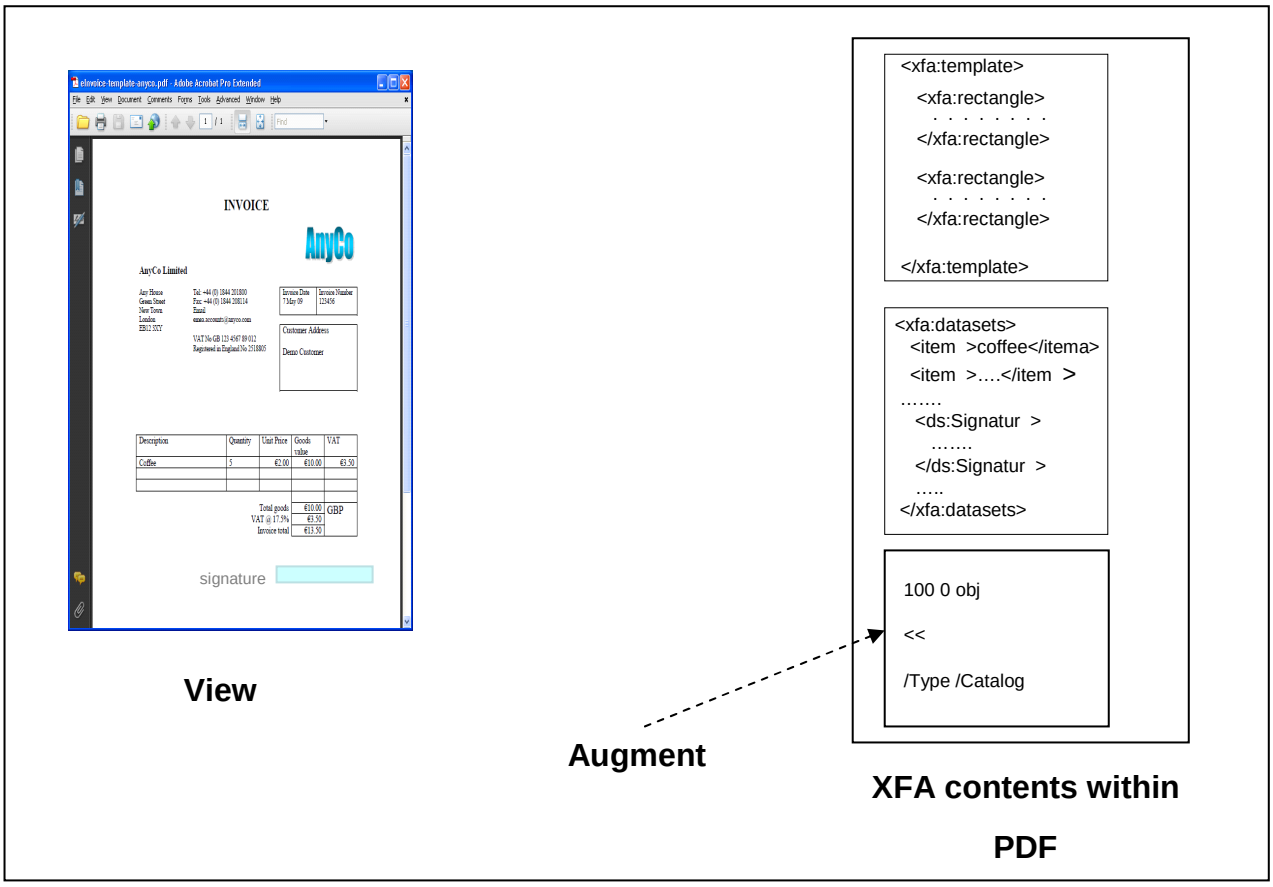


**Figure 5: Scenario for profile for long-term validation XAdES signatures on XFA forms**

## 6.3.2 Profile for Basic XAdES signatures on XFA forms

### 6.3.2.1 Features

The main features provided by this profile are listed below:

a) The XAdES signature signs XFA data only or any XML content from XFA allowed by XML Forms Architecture (XFA) Specification [8].

b) The XAdES signature protects integrity of what is signed and authenticates the signatory identity information included in the signing certificate. Additionally, the incorporation of a signature time-stamp also allows non repudiation of signature production time.

c) Signature levels are XAdES-E-BES, XAdES-E-EPES or XAdES-E-T.

d) This profile supports serial signatures.

e) This profile supports parallel signatures.

### 6.3.2.2 General syntax and requirements

The signatures shall be XAdES signatures, with the syntax specified in ETSI EN 319 132-1 [6] with the restrictions specified in this profile.

The signatures shall respect the requirements for XMLDSig signatures defined by XML Forms Architecture (XFA) Specification [8] except those ones that conflict with XAdES syntactic or semantic requirements.

Unsigned properties not found in this profile may be present and may be ignored unless used in conjunction with other profiles which place requirements on the use of such properties.

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

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

Signature handlers shall sign the `SignedProperties` element and the `ds:SignatureProperties` containing the signing time and the reasons for signing without having listed these elements within the signature manifest.

#### 6.3.2.3 Mandatory operations

##### 6.3.2.3.1 Protecting the signing certificate

XAdES specifies two mechanisms for protecting the signing certificate, namely: adding the `SigningCertificate` element or including the signing certificate itself within the `ds:KeyInfo` element and cover at least this certificate with the signature itself.

This profile recommends using the inclusion of the `SigningCertificate` qualifying property for securing the signing certificate. Nevertheless, signature handlers may use the other technique. At least one of the `SigningCertificate` element and the signed certificate in `ds:KeyInfo` shall be present.

NOTE: Readers are warned nevertheless that signing the whole `ds:KeyInfo` , locks the element and any addition of a certificate or validation data invalidate the signature. Signature handlers can, alternatively, use Xpath filtering for signing at least the signing certificate, leaving the rest of the `ds:KeyInfo` element open for addition of new data after signing.

#### 6.3.2.4 Requirements on XAdES optional properties

The table 4 specifies requirements on XAdES qualifying properties. If present their syntax, semantics and usage shall be as specified in ETSI EN 319 132-1 [6]. The column "Presence" shall contain the specification of the presence of the signature's element as follows:

- "shall be present": means that the attributes or signature fields shall be present, 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 attributes or signature fields shall not be present.
- "may be present": means that the attributes or signature fields may be present, 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".
- "conditioned presence": means that the presence 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".

**Table 4: Requirements for the main attributes for Basic XAdES signatures on XFA forms**

| Properties | Presence | References |
|---|---|---|
| SigningTime | shall not be present | ETSI EN 319 132-1 [6], clause 5.2.1 |
| SignaturePolicyIdentifier | may be present | ETSI EN 319 132-1 [6], clause 5.2.9 |
| SignatureProductionPlaceV2 | may be present | ETSI EN 319 132-1 [6], clause 5.2.5 |
| SignerRoleV2 | may be present | ETSI EN 319 132-1 [6], clause 5.2.6 |
| DataObjectFormat | may be present | ETSI EN 319 132-1 [6], clause 5.2.4 |
| CommitmentTypeIndication | conditioned presence | ETSI EN 319 132-1 [6], clause 5.2.3 |
| AllDataObjectsTimeStamp | may be present | ETSI EN 319 132-1 [6], clause 5.2.8.1 |
| IndividualDataObjects | may be present | ETSI EN 319 132-1 [6], clause 5.2.8.2 |
| SignatureTimeStamp | may be present | ETSI EN 319 132-1 [6], clause 5.3 |
| SignaturePolicyStore | may be present | ETSI EN 319 132-1 [6], clause 5.2.10 |

NOTE 1: The XMLDSig signatures generated by XFA processors include additional XML elements not specified within XML-Signature Syntax and Processing [9]. This information is included within the `ds:SignatureProperties` element. The signing time is present as content of the `CreateDate` element defined within the XMP ns.adobe.com/xap/1.0/ namespace.

The `SignatureTimeStamp` element should be present as an unsigned qualifying property in signatures.

Signatures shall sign the ds:SignatureProperties element containing the additional XML elements not specified withinXML-Signature Syntax and Processing [9] that are incorporated by XFA processors.

If the XAdES signature does not contain the `SignaturePolicyIdentifier` qualifying property, the `CommitmentTypeIndication` qualifying property shall not be present.

NOTE 2: The XMLDSig signatures generated by XFA processors include additional XML elements not specified within XML-Signature Syntax and Processing [9]. This information is included within the `ds:SignatureProperties` element, which is signed. The reason for signing is present as content of the `description` element defined within the Dublin Core http://purl.org/dc/elements/1.1/ namespace.

If the XAdES signature contains the `SignaturePolicyIdentifier` qualifying property, `CommitmentTypeIndication` qualifying property may be present. If it is present, its syntax, semantics and usage shall be as specified in ETSI EN 319 132-1 [6]. If the XAdES signature is a XAdES-E-EPES signature level or another level built on a XAdES-E-EPES form, the `ds:SignatureProperties` element shall not include the reason for signing within `description` element defined within the Dublin Core http://purl.org/dc/elements/1.1/ namespace.

NOTE 3: The reason for this last requirement is that signature policies formats specified by ETSI may define different rules for each commitment type indication qualifying property present in the XAdES signature.

### 6.3.2.5 Serial Signatures

The present profile supports serial signing of XAdES signatures by any of the two mechanisms specified within ETSI EN 319 132-1 [6], clause 5.2.7.

The `CounterSignature` element is an optional unsigned qualifying property. If present its syntax, semantics and usage shall be as specified in ETSI EN 319 132-1 [6], clause 5.2.7.2.

Optionally, a XAdES signature aligned with this profile may be countersigned by a detached XAdES signature, which includes a `ds:Reference` element containing a `Type` attribute whose value is as specified in ETSI EN 319 132-1 [6], clause 5.2.7.1. If this method of countersigning a XAdES signature is used the XAdES countersignature should also be present within XFA dynamic form.

#### 6.3.2.6 Parallel Signatures

A dynamic XFA form may include several XAdES signatures signing in parallel the XML content.

### 6.3.3 Profile for long-term validation XAdES signatures on XFA forms

#### 6.3.3.1 Overview

The present clause profiles the XAdES-E-BES, XAdES-E-EPES and XAdES-E-T signature levels aligned with the profile defined in clause 6.3.2 of the present document, to support long term validation.

This profile defines requirements to support the equivalent to XAdES-E-XL and XAdES-E-A signature levels as specified in ETSI EN 319 132-2 [7], by augmenting XAdES signatures aligned with the profile defined in clause 5.2.2 of the present document, using the LTV mechanisms specified in clause 5.4 of ETSI EN 319 142-1 [4].

#### 6.3.3.2 Features

The main features provided by this profile are listed below:

a) Features a), b), d) and e) of the profile defined in clause 6.3.2 of the present document.

b) The signatures aligned with this profile provide equivalent features as XAdES-E-XL and XAdES-E-A levels. These features are obtained by the incorporation of different pieces of validation data in the LTV-related PDF objects (namely DSS and VRI dictionaries) specified in clause 5.3.2 of ETSI EN 319 142-1 [4]. Clause 5.4 of the present document shows how to build combinations of some XAdES signatures levels and LTV-related dictionaries for obtaining functionally equivalent signatures to XAdES-E-XL and XAdES-E-A signature levels.

#### 6.3.3.3 General Requirements

Signature handlers shall be able to sign and/or validate signed XFA dynamic forms with XAdES signatures aligned with the present profile. In addition, signature handlers shall support PDF documents with:

a) Document security store information as specified in clause 5.4.2 of ETSI EN 319 142-1 [4].

b) Document time-stamps as specified in clause 5.4.3 of ETSI EN 319 142-1 [4].

This profile supports validation data carried by value within the DSS.

Signature handlers shall support generation and/or validation of signatures with one or more DSS entries and document time-stamps.

### 6.3.4 Extensions Dictionary

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

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

to identify that a PDF document includes extensions as identified in clause 5.4 of ETSI EN 319 142-1 [4].

# Annex A (informative): General Features

## A.1 PDF signatures

Digital signatures in ISO 32000-1 [1] currently support three activities: adding a digital signature immediately to a document, providing a placeholder field where signatures will go in the future, and checking signatures for validity. The signature itself along with various optional information is contained in a data structure of the PDF called the signature dictionary (ISO 32000-1 [1], clause 12.8.1, table 252).

The signature value is a binary object using CMS [i.6] or related signature formats (including PKCS #7 [2] and CAdES [5]). The specific format and content of the signature value depends on the profile.

As with other CMS-based signature implementations, a digest is computed over a range of bytes of the file. However with PDF, as the signature information is to be embedded into the document itself, this range is the entire file, including the signature dictionary but excluding the PDF Signature itself. The range is then indicated by the **ByteRange** entry of the signature dictionary.

By restricting the ByteRange entry this way, it ensures that there are no bytes in the PDF that are not covered by the digest, other than the PDF signature itself.

NOTE: The profiles defined in parts 2 and 3 make normative this requirement which is a recommendation in ISO 32000-1 [1], clause 12.8.1.

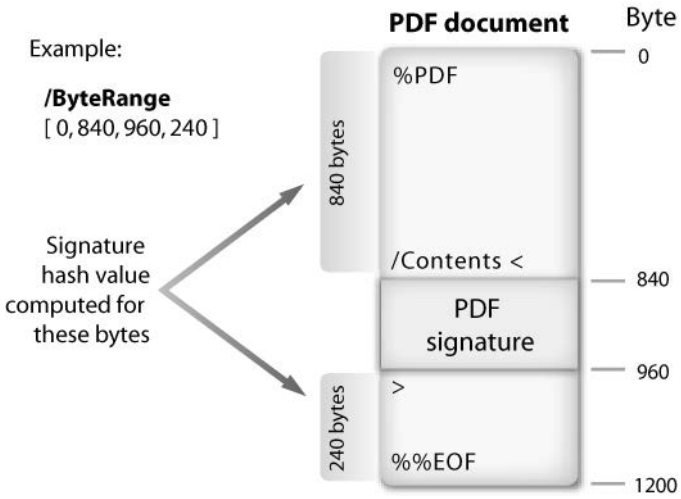


**Figure A.1**

The PDF Signature binary value is placed into the Contents entry of the signature dictionary.

The size of the Contents entry is computed based on a best guess of the maximum size needed to contain the PDF signature and any addition revocation and time-stamping information. The Contents entry is first written as a series of 0x00 hex values and later filled in with the actual values.

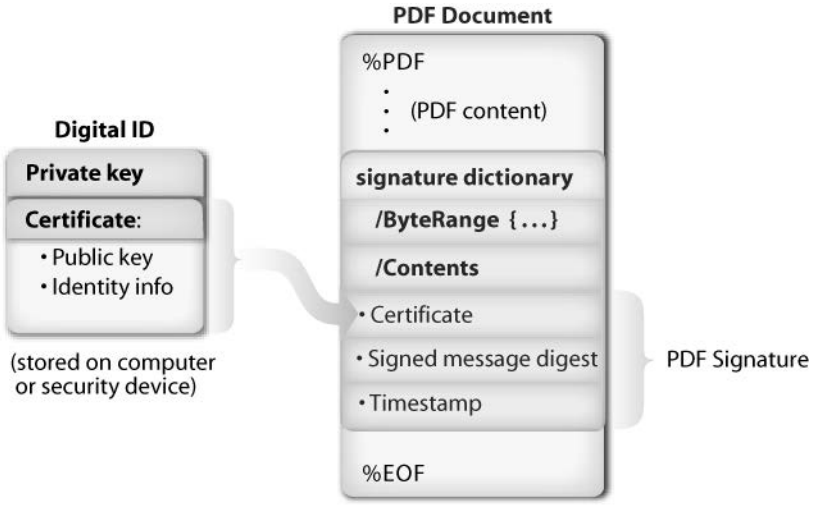


**Figure A.2**

# A.2 PDF Signature types

In addition to the traditional document signature, PDF signatures introduce the concept of certification signatures which work with modification detection permissions (MDP, ISO 32000-1 [1], clause 12.8.4). MDP functionality in PDF, which is specified by a signature reference dictionary, enables a document to be modified in certain ways (such as subsequent form fill-in or commenting) and still have the original signature interpreted as valid.

Finally, PDF uses signatures in another way (Usage Rights, ISO 32000-1 [1], clause 12.8.2.3) which is to enhance a document with additional rights and privileges in a particular workflow, using the signature to ensure that the document and rights have not been tampered with in any way.

# A.3 PDF Signature Handlers

ISO 32000-1 [1] defines multiple implementations for the inclusion of CMS-based digital signatures into a PDF document. Each implementation is defined by a pair of values in the signature dictionary called the **Filter** and **SubFilter**. **Filter** defines the name of the preferred signature handler to use when validating this signature, where **SubFilter** is a name that describes the encoding of the PDF Signature and key information in the signature dictionary.

The profiles specified in this multi-part deliverable specify use of two encodings both of which are CMS based:

a) PKCS #7 [2] encoding as specified in ISO 32000-1 [1], clause 12.8.3.3.1;

b) CAdES encoding as specified in ETSI EN 319 122-1 [5].

See other parts of the present document for requirements on signature handlers.

# A.4 PDF serial signatures

While other forms of CMS-based digital signatures support the ability to have parallel signatures, where multiple individuals sign the same byte range (and by association, the hash) and this collection of signing certificates is then included in a single PKCS#7 [2] envelope, ISO 32000-1 [1] does not support this. As such, there is only a single signer (e.g. one single component of "SignerInfo" type within "signerInfos" element) in any PDF signature. Instead, it offers an alternative solution to multiple signers of a document which has some benefits for certain types of workflows.

Each signature in a PDF can contain only a single signing certificate, but there can be as many signature dictionaries as one wishes in a PDF, each one with its own associated **ByteRange**.

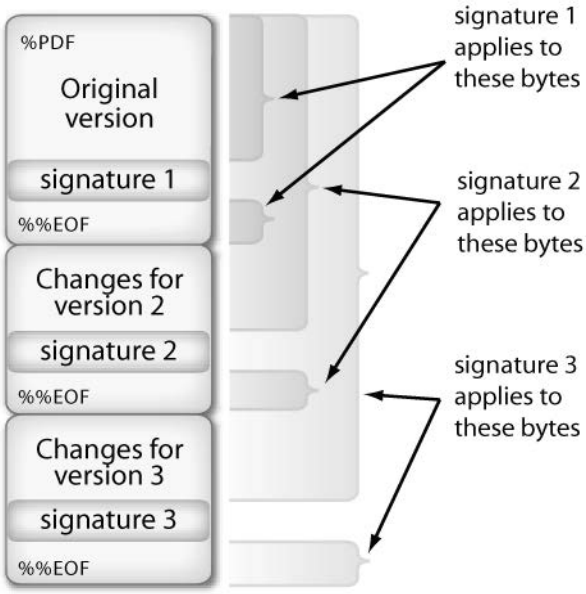


**Figure A.3**

The normal workflow for serial signatures in PDF is that after the first individual has signed, the document is then passed on to subsequent signers who not only sign the document but also the previous PDF signatures. In addition, in the case of a PDF form, subsequent signatories can also fill in additional fields (e.g. date and time) and then sign both their entered data along with the rest of the document.

ISO 32000-1 [1] states that when validating serial signatures, each signature is validated individually, but then the aggregate result of the validations is treated as the final status of the document. This means that it is possible to have a situation where some signatures do not pass validation (either due to document changes or trust concerns) but others do, and so it is necessary to determine a single document state from the collection.

Signatures applied in parallel are currently not supported.

## A.5 PDF signature Validation and Time-stamping

The use of time-stamping, CA certificates and revocation status information in validation of PDF signatures varies between the profiles employed. For further information see the other parts of this multi-part deliverable.

## A.6 ISO 19005-1: 2005 (PDF/A-1)

PDF/A-1 [i.5] is a subset of PDF that enables reliable long term archiving of digital content in PDF format. It does so by tightening the normative requirements of the PDF file structure, requiring the inclusion of all required resources (such as fonts and images) and by restricting the use of interactive content and scripting facilities (i.e. JavaScript).

NOTE: Because the conversion of most PDF documents to PDF/A requires modification of the file, the document should be converted to PDF/A before applying a digital signature.

As PDF/A-1 is based on Adobe ®PDF 1.4 and not on ISO 32000-1 [1], it does not fully support all of its features available to digital signatures - specifically lacking are embedded revocation information and electronic time-stamps. However, since such features are not explicitly forbidden there is nothing that prevents a PDF/A-1 writer from putting these extended features into a file - but a PDF/A-1 reader cannot be expected to process them accordingly. A PDF/A-1 reader is, however, free to implement functionality beyond that specified in PDF/A-1.

## A.7 ISO 19005-2:2011 (PDF/A-2)

PDF/A-2 [i.7] is the second part to the standard and is based on ISO 32000-1 [1]. PDF/A-2 address some of the new features added with versions 1.5, 1.6 and 1.7 of the PDF Reference. PDF/A-2 is backwards compatible, so all valid PDF/A-1 documents are compatible with PDF/A-2. However PDF/A-2 compatible files will not necessarily be PDF/A-1 compatible.

Part 2 [i.7] of the PDF/A Standard is based on a more recent version, PDF 1.7 (ISO 32000-1 [1]), rather than PDF 1.4 and offers a number of new features among which the provisions for digital signatures in accordance with the PDF digital signatures - PAdES profiles. It is the file format of choice for reliable long term archiving of digitally signed, PDF-based, digital content.

## A.8 Seed Values and Signature Policies

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

A *seed value dictionary* (ISO 32000-1 [1], clause 12.7.4.5, table 234) contains information that conveys a set of rules (or policies) that the form's author wishes the signature handler to enforce at the time the signature is applied. These wishes can be specified either as requirements or recommendations. It is important not to confuse this "seed values" attribute with signature policies signature-policy attribute as specified in ETSI EN 319 122-1 [5]. While both bear similarities, seed values are workflow constraints for a given document, whereas signature policies represent general endorsement rules agreed upon by the signer and the verifier.

Common uses for seed values are to specify digest methods, revocation information, timestamping authorities and certificate attributes.

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

# History

| Document history | | | |
|---|---|---|---|
| V1.0.0 | June 2015 | EN Approval Procedure | AP 20151028: 2015-06-30 to 2015-10-28 |
| | | | |
| | | | |
| | | | |
| | | | |