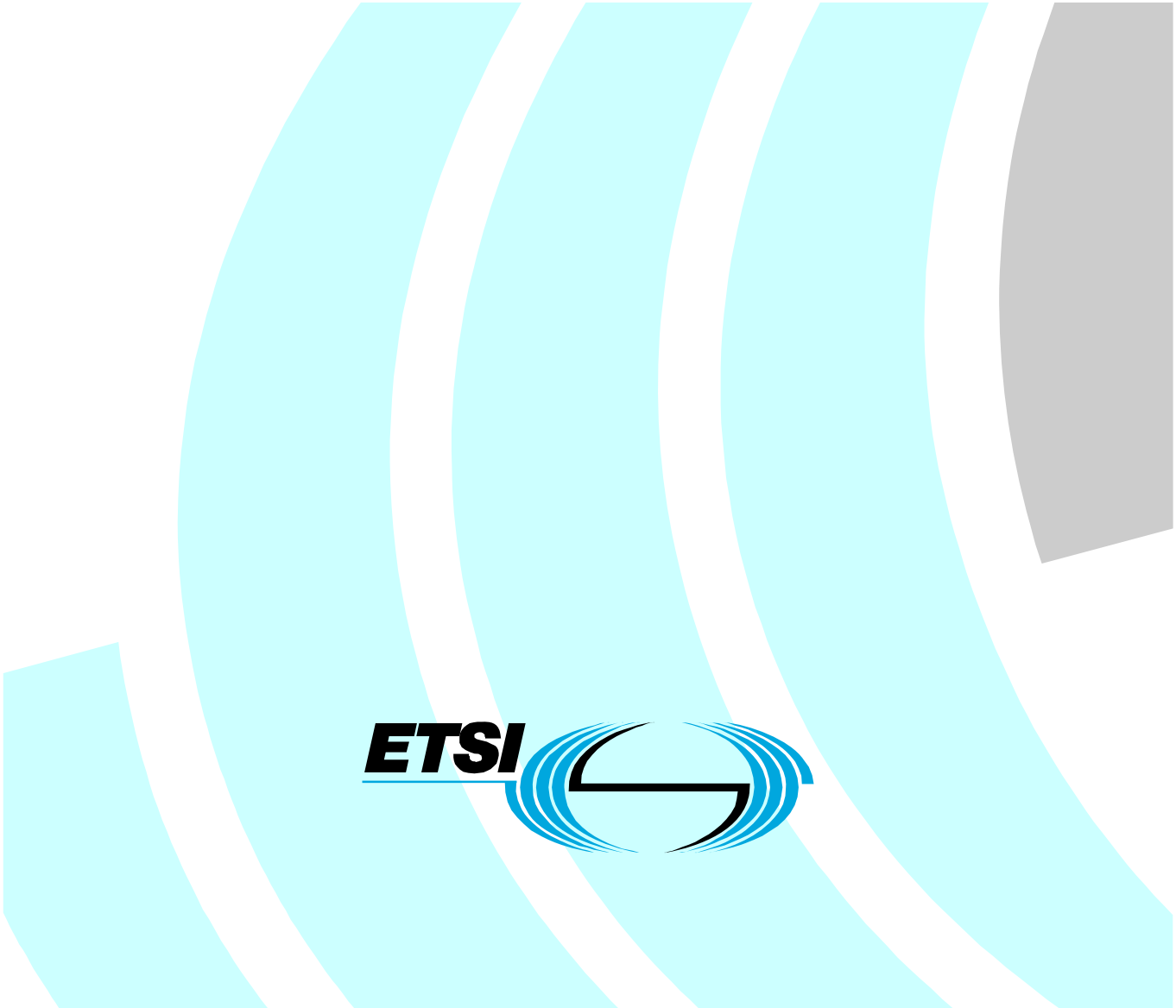
ETSI TS 102 778-1 V1.1.1 (2009-07)

Technical Specification

Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES



Reference
DTS/ESI-000072-1

Keywords
e-commerce, electronic signature, 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://webapp.etsi.org/IPR/home.asp).

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

Foreword

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

The present document is part 1 of a multi-part deliverable covering PDF Advanced Electronic Signature Profiles, as identified below:

Part 1: "PAdES Overview - a framework document for PAdES";

Part 2: "PAdES Basic - Profile based on ISO 32000-1";

Part 3: "PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles";

Part 4: "PAdES Long Term - PAdES-LTV Profile";

Part 5: "PAdES for XML Content - Profiles for XAdES signatures".

Introduction

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

The present document is intended to cover electronic signatures for electronic documents. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (i.e. repudiates; see ISO/IEC 10181-4 [i.1]) the validity of the signature.

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

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

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

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

ISO 32000-1 [1] identifies the ways in which an electronic signature, in the form of a digital signature, may be incorporated into a PDF document to authenticate the identity of the user and validate integrity of the document's content. These signatures are based on the same CMS [5] technology and techniques as TS 101 733 [2] (CAdES), but without the extended signature capabilities of CAdES.

1 Scope

The present document provides a framework for the set of profiles for PDF (Portable Document Format - as specified in ISO 32000-1 [1]) Advanced Electronic Signatures specified in this multi-part deliverable.

This multi-part deliverable profiles and extends the support for electronic signatures specified in ISO 32000-1 [1] to include the enhanced features for advanced electronic signatures. These profiles include features equivalent to those specified in TS 101 733 [2] (CAdES) and TS 101 903 [3] (XAdES) and include support for validation of signed documents stored over long periods.

The present document:

a) Provides a general description of support for signatures in PDF documents including use of XML signatures to protect XML data in PDF documents;

b) Lists the features of the PDF profiles specified in other parts of the document;

c) Describes how the profiles may be used in combination.

The present document is for information only. Reference should be made to the other parts of this deliverable for the normative requirements of each profile.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

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

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

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

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

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

[2] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[3] ETSI TS 101 903: "XML Advanced Electronic Signatures (XAdES)".

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

[5] IETF RFC 3852 (2004): "Cryptographic Message Syntax (CMS)".

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

[7] ETSI TS 102 778-3: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles".

[8] ETSI TS 102 778-4: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES LTV Profile".

[9] ETSI TS 102 778-5: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures".

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

[i.2] Adobe XFA: "XML Forms Architecture (XFA) Specification".

[i.3] ISO 19005-1 (2005): "Document management - Electronic document file format for long-term preservation - Part 1: Use of PDF 1.4 (PDF/A-1)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in [1], [2], [3] and the following apply:

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

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

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

PDF signature: binary data object based on the CMS (see RFC 3852 [5]) or related syntax containing a digital signature placed within a PDF document structure as specified in ISO 32000-1 [1], clause 12.8 with other information about the signature applied when it was first created

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

signer: entity that creates an electronic signature

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

verifier: entity that validates an electronic signature

The present document makes use of certain keywords to signify requirements. Below follows their definitions:

may: means that a course of action is permissible within a profile

shall: means that the definition is an absolute requirement of a profile

NOTE: It has to strictly be followed in order to conform to the present document

should: Means that among several possibilities one is recommended, in a profile, as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required

NOTE: Implementers may know valid reasons in particular circumstances to ignore this recommendation, but the full implications have to be understood and carefully weighed before choosing a different course.

3.2 Abbreviations

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

CAdES CMS Advanced Electronic Signature

NOTE: See TS 101 733 [2].

CMS Cryptographic Message Syntax

NOTE: As specified in RFC 3852 [5].

CRL Certificate Revocation List
GSM Global System for Mobile communication
LTV Long Term Validation
MDP Modification Detection Permissions
OCSP Online Certificate Status Protocol
PAdES PDF Advanced Electronic Signature
PAdES-BES PAdES Basic Electronic Signature
PAdES-EPES PAdES Explicit Policy Electronic Signature
PDF Portable Document Format
PKCS Public Key Cryptography Standards
SIM Subscriber Identity Mode
UBL Universal Business Language
XAdES XML Advanced Electronic Signatures

NOTE: See TS 101 903 [3].

XFA XML Forms Architecture
XML eXtensible Markup Language

4 General Features

4.1 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 encoded as a binary object using CMS [5] or related signature formats (including PKCS #7 [4] and CAdES [2]). 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 part2 and 3 make normative this requirement which is a recommendation in ISO 32000-1 [1], clause 12.8.1.

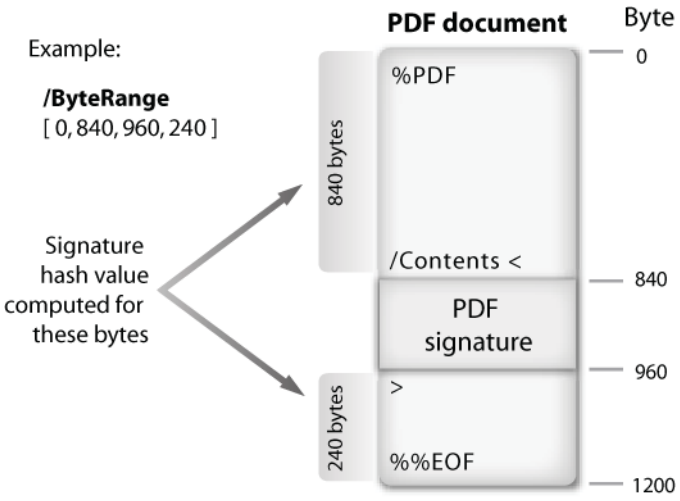


Figure 1

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 of the string is first written to disk as a series of 0x00 hex values and later filled in with the actual contents.

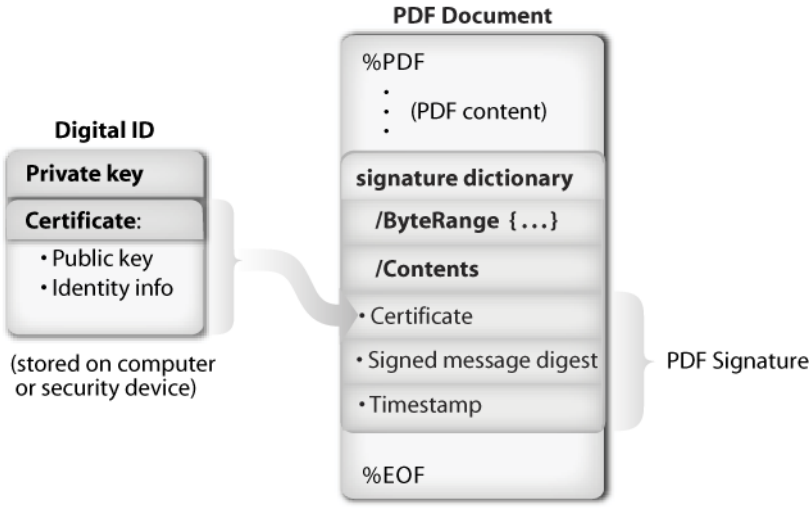


Figure 2

4.2 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 a 3rd 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.

4.3 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 [4] encoding as specified in ISO 32000-1 [1] clause 12.8.3.3.1 (see TS 102 778-2 [6]);

b) CAdES encoding as specified in TS 101 733 [2] (see TS 102 778-3 [7]).

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

4.4 PDF serial signatures

While other forms of CMS-based electronic 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 [4] envelope - ISO 32000-1 [1] does not support this. As such, there shall only be a single signer (e.g. a single "SignerInfo" structure) 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**.

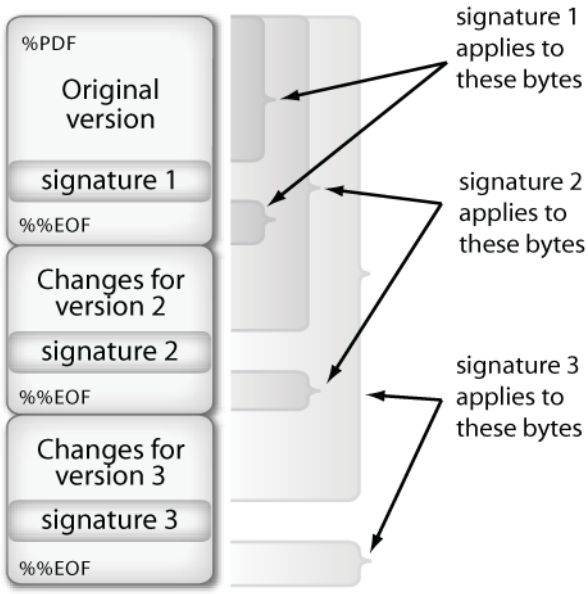


Figure 3

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 verifying serial signatures, each signature is verified 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.

4.5 PDF signature Validation and Time-stamping

The use of time-stamping with 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.

4.6 ISO 19005-1: 2005 (PDF/A-1)

PDF/A-1 [i.3] 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, it is recommended to convert the document to PDF/A before applying a digital signature.

As PDF/A-1 [i.3] 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 time-stamping. However, since such features are not explicitly forbidden there is nothing that prevents a PDF/A-1 conforming writer from putting these extended features into a file - but there should be no expectation that a PDF/A-1 conforming reader will process them accordingly. A PDF/A-1 conforming reader is, however, free to implement functionality beyond that specified in PDF/A-1.

PDF/A-2 (to be published as a new part of ISO 19005 [i.3]) will be based on ISO 32000-1 [1] and is expected to be published sometime in 2010. With full support for electronic signatures with extended features as described in this series of profiles, it will become the file format of choice for reliable long term archiving of digitally signed, PDF-based, digital content.

4.7 Signatures on XML Content in PDF

Data encoded in XML may be carried within a PDF document. This may be used, for example, to carry PDF form data mapped into the PDF document using the XML Forms Architecture (XFA [i.2]). An XML signature, using the XAdES [3] format, may be applied to this data.

The XML data, with or without an XML/XAdES signature, may be also signed along with the rest of the PDF document using a PDF signature as described above. Once signed with a PDF signature further information cannot be added directly to any XAdES Signature that may be present. Where a XAdES signature is applied using XFA the related validation data may be provided using PDF data structures to support long term validation (see clause 5.8). However, if raw XML structures are used (i.e. not using XFA) once a XAdES signature has been placed within a document signed with a PDF Signature it cannot be extended to support long term validation (see clause 5.6).

TS 102 778-5 [9] specifies profiles for the use of XAdES signatures to protect XML data within PDF documents and the use of PDF data structures to provide validation data which can be related to a XAdES signature.

5 Profiles

5.1 Part 2: PAdES Basic - Profile based on ISO 32000-1

5.1.1 Description

This profile specifies a PDF signature as currently specified in ISO 32000-1 [1]. The profile is specified in TS 102 778-2 [6].

The use of a PDF Signature conforming to this profile is illustrated in figure 4.

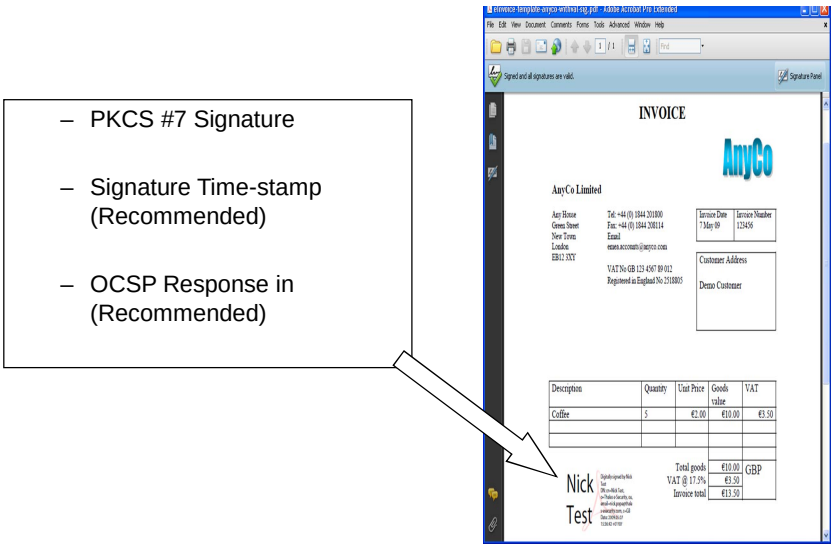


Figure 4

5.1.2 Features

a) Supports serial signatures.

b) Recommends inclusion of a signature time-stamp.

c) Recommends inclusion of revocation information.

d) Signature protects integrity of the document and authenticates the signatory.

e) Signature can optionally include the "reasons" for the signature.

f) Signature can optionally include a description of the location of signing.

g) Signature can optionally include contact info of the signatory.

h) 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).

5.2 Part 3: PAdES Enhanced - PAdES-BES Profile

5.2.1 Description

This profiles specifies a PDF advanced signature based upon CAdES-BES as specified in TS 101 733 [2] with the option of a signature time-stamp (CAdES-T).

The use of a PDF Signature conforming to this profile is illustrated in figure 5.

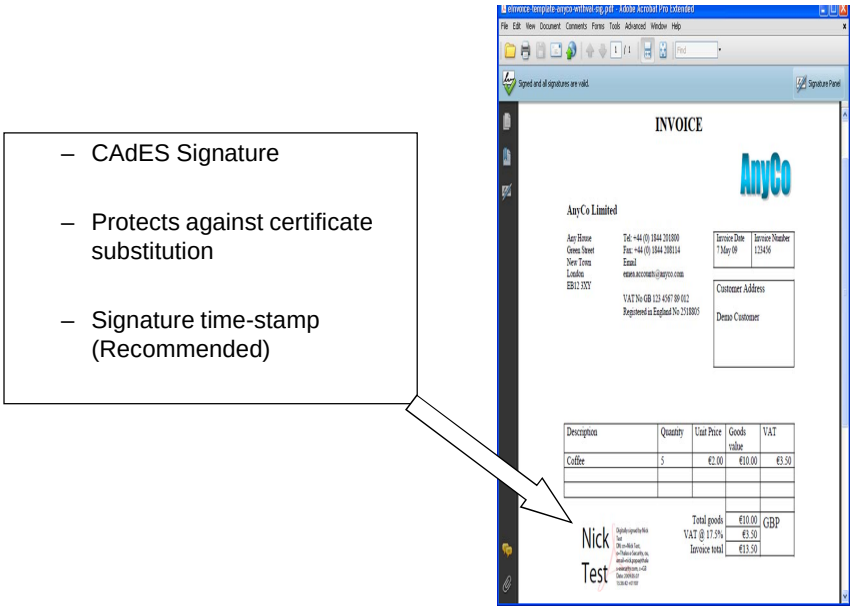


Figure 5

5.2.2 Features

The features provided by this profile are very similar to the PAdES profile as specified in TS 102 778-2 [6]. CAdES is used instead of CMS and the profile gives guidance to avoid embedding potentially duplicated information.

a) Signature encoded as CAdES-BES (see TS 101 733 [2]).

b) Must include signing certificate reference.

c) Recommends inclusion of a signature time-stamp.(CAdES-T).

d) Supports serial signatures.

e) Signature protects integrity of the document and authenticates the signatory.

f) Signature can optionally include CAdES simple attributes (Signing Time, Signer Attributes, Content-Timestamp).

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

5.3 Part 3: PAdES Enhanced - PAdES-EPES profile

5.3.1 Description

This profiles specifies a PDF advanced signature based upon CAdES-EPES as specified in TS 101 733 [2]. This profile is the same as the PAdES - BES profile with the addition of a signature policy identifier and optionally a commitment type indication.

The use of a PDF Signature conforming to this profile is illustrated in figure 6.

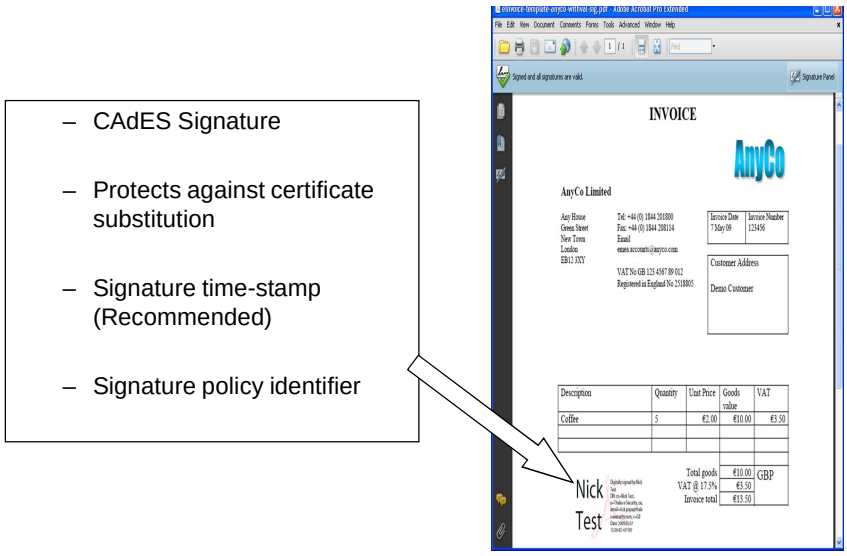


Figure 6

5.3.2 Features

The features provided by this profile are very similar to the PAdES - CMS profile as specified in TS 102 778-2 [6]. CAdES is used instead of CMS and the profile gives guidance to avoid embedding potentially duplicated information.

a) Signature encoded as CAdES-BES (TS 101 733 [2]).

b) Must include signing certificate reference.

c) Must include signature policy identifier.

d) Optionally includes signature time-stamp (CAdES-T).

e) Optionally includes commitment type indicator.

f) Supports serial signatures.

g) Signature protects integrity of the document and authenticates the signatory.

h) Signature can optionally include CAdES simple attributes (Signing Time, Signer Attributes, Content-Timestamp).

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

5.4 Part 4: Long Term - PAdES-LTV Profile

5.4.1 Description

This profile supports the long term validation of PDF Signatures. This profile can be used in conjunction with the PAdES-CMS, PAdES-BES or PAdES-EPES profiles.

This profile is applicable to any party relying on a signature over a long period (e.g. longer than the lifetime of the signing certificate). It may be applied by a party receiving and verifying the document or the signing party who should also verify the document when applying LTV.

The use of a PDF Signature conforming to this profile is illustrated in figure 7.

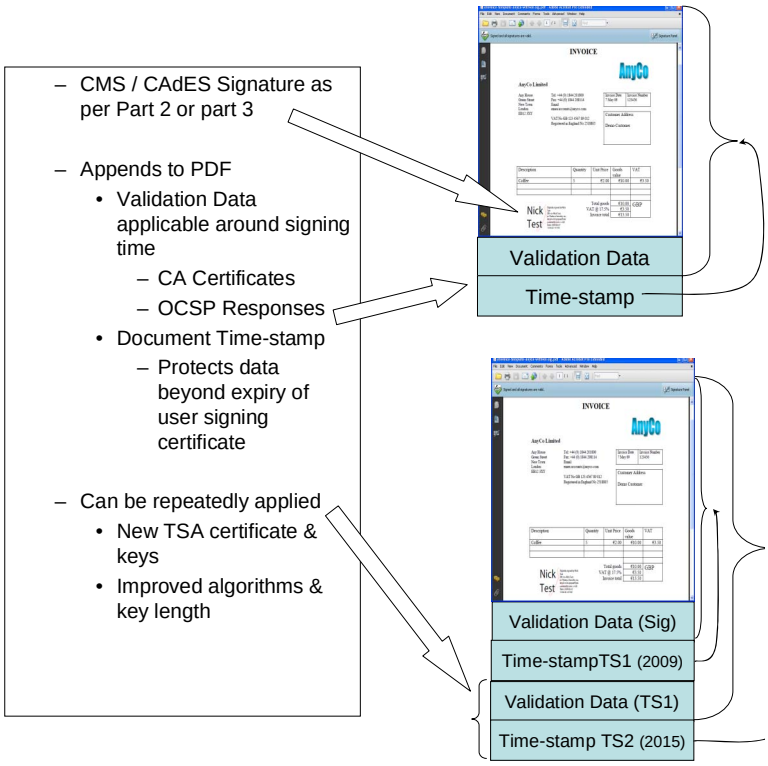


Figure 7

5.4.2 Features

This profile adds the following to the features the PAdES-CMS, PAdES-BES or PAdES-EPES profiles described above:

a) Addition of validation data to an existing PDF document which may be used to validate earlier signatures within the document (including PDF signatures and time-stamp signatures).

b) Addition of a document time-stamp which protects the existing document and any validation data.

c) Further validation data and document time-stamp may be added to a document over time to maintain its authenticity and integrity.

5.5 Part 5: PAdES for XML Content - Profile for Basic XAdES signatures of XML documents embedded in PDF Containers

5.5.1 Description

This is the first of two profiles that profile usage of a signed (with XAdES signatures [3]) XML document (that may be aligned with any XML language, i.e. a signed UBL e-Invoice) that is embedded within a PDF container, for providing integrity, authentication and non repudiation services on the XML data objects that are signed with the XAdES signature.

This profile specifies requirements for the basic XAdES forms (XAdES-BES, XAdES-EPES, and XAdES-T).

NOTE: Implementers should be aware that any subsequent **approval** signature (see ISO 32000-1 [1] clause 12.8.1) as specified in TS 102 778-2 [6], TS 102 778-3 [7] or TS 102 778-4 [8] also signs the embedded signed XML document. Any upgrade of the XAdES signature of this document to support validation long after the expiration of the signing certificate or other extended features such a countersignatures (e.g. using XAdES-C or XAdES-X or XAdES-A) would invalidate the aforementioned approval signatures. Implementers should also be aware that **certification** signatures (see ISO 32000-1 [1] clause 12.8.1) as specified in TS 102 778-2 [6], TS 102 778-3 [7] or TS 102 778-4 [8] signing the embedded signed XML document, may be used in conjunction with the DocMDP dictionary, allowing changes in the embedded signed XML document (by upgrading the XAdES signatures, for example) without invalidating such signatures.

The use of a PDF Signature conforming to this profile is illustrated in figure 8.

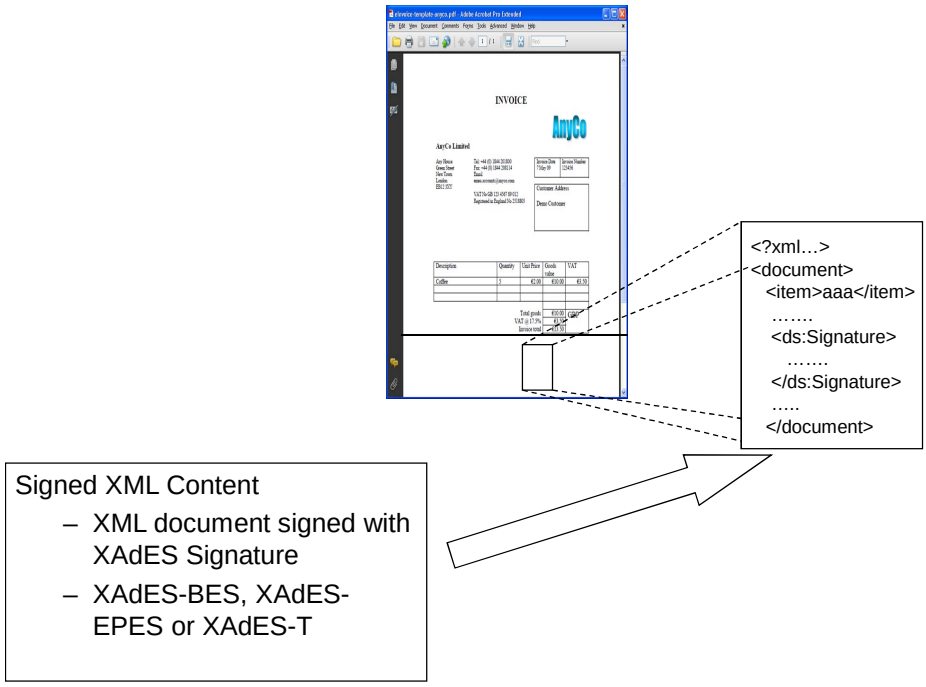


Figure 8

5.5.2 Features

The main features provided by this profile are listed as follows:

a) The XML signed document (including both data objects to be signed and the XAdES signatures) is created independent of the PDF container. The profile also puts requirements on the relative placement of XAdES signatures and the signed data objects.

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

c) The following XAdES signatures forms are profiled by this profile: XAdES-BES, XAdES-EPES, and XAdES-T forms (see TS 101 903 [3]).

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

e) This profile supports parallel signatures.

5.6 Part 5: PAdES for XML Content - Profile for long-term XAdES signatures of XML documents embedded in PDF containers

5.6.1 Description

This is the second of two profiles that profile usage of arbitrary Signed (with XAdES signatures) XML content (that may be aligned with any XML language, i.e. a signed UBL e-Invoice) that is embedded within a PDF container as an attached file, for providing integrity, authentication and no repudiation services on the XML data objects that are signed with the XAdES signature. This profile deals with requirements for upgrading the basic XAdES forms profiled in the profile identified in clause 5.5 to the more evolved forms of XAdES (XAdES-C, XAdES-X, XAdES-XL and XAdES-A (see TS 101 903 [3])).

The use of a PDF Signature conforming to this profile is illustrated in figure 9.

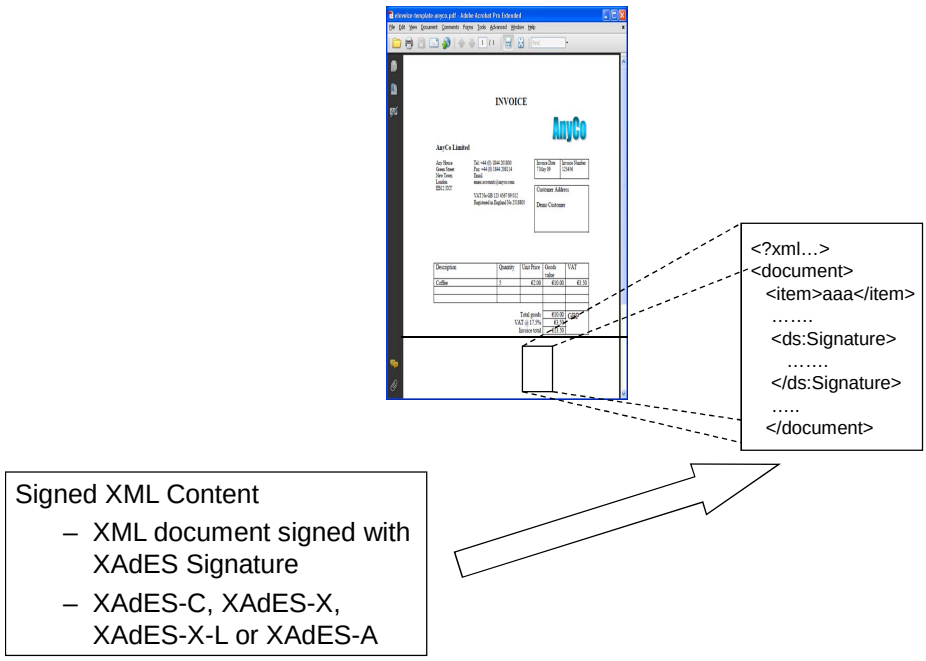


Figure 9

5.6.2 Features

This profile adds to the profile in clause 5.5.2 the features listed as follows:

a) Long-term signatures production.

b) Signature is encoded as XAdES-C, XAdES-X or XAdES-XL, XAdES-A (see TS 102 903 [3]).

5.7 Part 5: PAdES for XML Content - Profile for Basic XAdES signatures on XFA forms

5.7.1 Description

This is the first of two profiles that profile usage of XAdES signatures to sign dynamic XFA forms. XFA defines a XML-based architecture for building up and completing forms where the data is held as XML elements.

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

This profile specifies requirements for the basic XAdES forms (XAdES-BES, XAdES-EPES, and XAdES-T).

The use of a PDF Signature conforming to this profile is illustrated in figure 10.

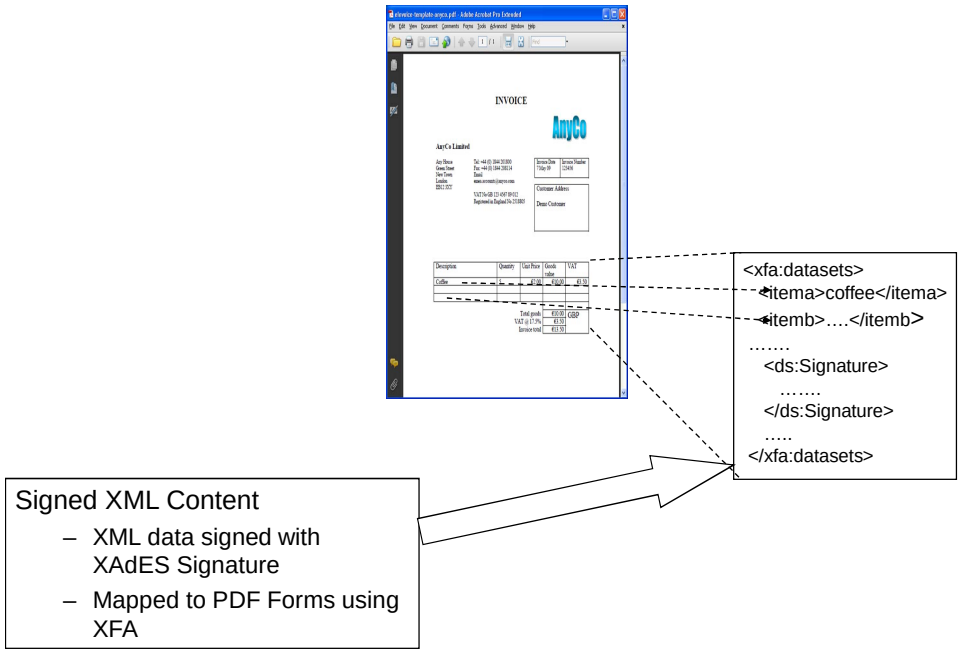


Figure 10

5.7.2 Features

The main features provided by this profile are listed as follows:

a) The XAdES signature will be able to sign XFA data only or any XML content from XFA allowed by XFA specification [i.2].

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

c) Signature is encoded from XAdES-T or XAdES-BES or XAdES-EPES (see TS 101 903 [3]).

d) This profile supports serial signatures.

e) This profile supports parallel signatures

5.8 Part 5: PAdES for XML Content - Profile for long-term validation XAdES signatures on XFA forms (XAdES-LTV)

5.8.1 Description

This is the second of two profiles that profile usage of XAdES signatures to sign dynamic XFA forms. XFA defines a XML-based architecture for building up and completing forms where the data is held as XML elements.

It profiles the upgrade of the signature forms compliant with the profile identified in clause 5.7, to support long term validation.

This profile defines requirements to support the equivalent to all the signature forms XAdES-XL and XAdES-A as specified in TS 101 903 [3], by upgrading XAdES signatures compliant with the profile identified in clause 5.7 of the present document, using the LTV mechanisms specified in annex A of TS 102 778-4 [8].

The use of a PDF Signature conforming to this profile is illustrated in figure 11.

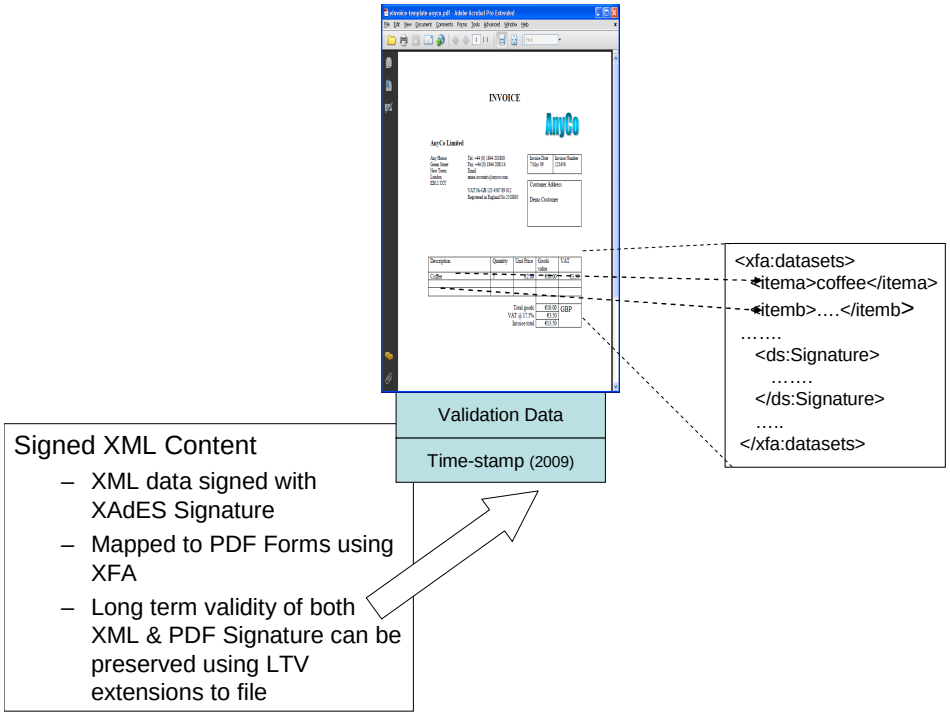


Figure 11

5.8.2 Features

The main features provided by this profile are listed as follows:

a) Features a), b), d) and e) of the profile defined in clause 5.2 of the present document.

b) The signatures aligned with this profile provide equivalent features as XAdES-XL and XAdES-A forms. 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 annex A of TS 102 778-4 [8]. Annex A of the present document shows how to build combinations of basic forms of XAdES signatures and LTV-related dictionaries for obtaining functionally equivalent signatures to XAdES-XL and XAdES-A signature forms.

6 Use of Profiles in Combination

The profiles described above may be used in combination as follows:

a) PAdES-LTV may be applied to an existing document with PAdES-CMS, PAdES-BES or PAdES-EPES signatures.

b) PAdES-CMS, PAdES-BES or PAdES-EPES, optionally extended using PAdES-LTV, may be applied to a document with a XAdES signature applied to XML Data.

c) Basic XAdES not using XFA, and XAdES-Basic and XAdES-LTV profiles may be used with the PDF Signatures following any PAdES profile. However, a XAdES signature cannot be upgraded once a PDF signature has been applied to the document.

History

Document history		
V1.1.1	July 2009	Publication