Draft EN 319 142-5 V0.0.3 (2013-11)

EUROPEAN STANDARD

Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures

STABLE DRAFT FOR PUBLIC REVIEW UNTIL 15 JANUARY 2014

Download the template for comments:

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

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

CAUTION: This DRAFT document is provided for information and is for future development work within the ETSI Technical Committee ESI only. ETSI and its Members accept no liability for any further use/implementation of this Specification.

Approved and published specifications and reports shall be obtained exclusively via the ETSI Documentation Service at

http://pda.etsi.org/pda/queryform.asp

Reference

DEN/ESI-0019142-5

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Logos on the front page

If a logo is to be included, it should appear on the right hand side of the front page.

Copyrights on page 2

This paragraph should be used for deliverables processed before WG/TB approval and used in meetings. It will replace the 1st paragraph within the copyright section.

If an additonal copyright is necessary, it shall appear on page 2 after the ETSI copyright notification

The additional EBU copyright applies for EBU and DVB documents.

The additional CENELEC copyright applies for ETSI/CENELEC documents.

The additional CEN copyright applies for CEN documents.

The additional WIMAX copyright applies for WIMAX documents.

Contents

If you need to update the table of content you would need to first unlock it.
To unlock the Table of Contents: select the Table of Contents, click simultaneously: Ctrl + Shift + F11.
Then lock it: reselect the Table of Contents and then click simultaneously: Ctrl + F11.

Logos on the front page 3

Copyrights on page 2 3

If an additonal copyright is necessary, it shall appear on page 2 after the ETSI copyright notification 3

Intellectual Property Rights 5

Foreword 5
Multi-part documents 5
Transposition table 6

Introduction 6

1 Scope 6

2 References 7
2.1 Normative references 7
2.2 Informative references 7

3 Definitions, symbols and abbreviations 8
3.1 Definitions 8
3.2 Symbols 8
3.3 Abbreviations 8

4 User defined clause(s) from here onwards 9
4.1 User defined subdivisions of clause(s) from here onwards 9
Annexes 9

Annex <A> (normative): Title of normative annex *(style H8)* **9**

Annex <X> (normative): ATS in TTCN-2 *(style H8)* **9**

<X.1> The TTCN-2 Machine Processable form (TTCN.MP) *(style H1)* 10

Annex <X+1> (normative): ATS in TTCN-3 *(style H8)* **10**

<X+1.1> TTCN-3 files and other related modules *(style H1)* 10

<X+1.2> HTML documentation of TTCN-3 files *(style H1)* 10

Annex <X+3> (informative): Change History **11**

Annex <X+4> (informative): Bibliography **11**

History 12
A few examples: 12

<PAGE BREAK>

Intellectual Property Rights

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

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

Foreword

This European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

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

The present document is part 5 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.1].

The present document was previously published as ETSI TS 102 778-5.

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 [4] 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 [4] 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 [6] technology and techniques as EN 319 122-1 [5] (CAdES), but without the extended signature capabilities of CAdES.

This profile specifies digital signatures on XML content that may be carried in a PDF document using XAdES based signatures.

1 Scope

The present document defines four profiles that together profile the usage of XAdES [1] signatures, as defined in EN 319 132-1 [1], for signing XML content within the PDF containers. The scope of the present document is limited to the following cases:

1) One XML document (compliant with an arbitrary XML language, like UBL for e-Invoicing) that is completely or partially signed with at least one enveloped XAdES signature and that is incorporated within a PDF container as a so-called "embedded" document. In this situation, both the XML document and the XAdES signature(s) are created independently of the PDF container and after their creation, embedded within this container.

NOTE 1: Implementers should be aware that any subsequent approval signature (see ISO 32000-1 [4] clause 12.8.1) as specified in EN 319 142-2 [i.7], EN 319 142-3 [i.8] or EN 319 142-4 [i.9] also signs the embedded signed XML document. Any upgrade of the XAdES signature of the present 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 [4] clause 12.8.1) as specified in EN 319 142-2 [i.7], EN 319 142-3 [i.8] or EN 319 142-4 [i.9] 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.

2) Signed (with XMLDSig or XAdES signature) dynamic XFA [2] forms. The present document specifies profiles that apply to two different scenarios, namely: signing only the XML data of the XFA form, or signing any part of the XFA form that may be signed with a XMLDSig signature.

NOTE 2: XFA forms build up an XML-based architecture for managing forms within the PDF framework. In this architecture data, structure and rendering details appear as XML contents. According to the XFA specification not all this XML content may be signed with XML Sig. Being XAdES signatures built on XMLDSig, XAdES signatures may sign only those XML contents that XFA specification allows to be signed with XMLDSig.

NOTE 3: Readers should be aware that although PDF documents are addressed for human beings, XFA forms, being them based on XML, may be consumed by software applications. In addition to that, conforming signature handlers may be able to identify what parts of a certain form are signed by an XAdES signature.

For each case two profiles are specified, namely:

1) One profile intended to be used by a signer, where basic forms of XAdES signatures (namely XAdES-BES, XAdES-EPES and XAdES-T) on the corresponding XML content are profiled.

2) One profile applicable to any party relying on a signature over a long period (e.g. longer than the lifetime of the signing certificate, also called long-term signature in the present document). It may be applied by a party receiving and verifying the document or the signing party who should also verify the document when applying long term verification. It specifies how to include validation information and to further protect the signature using time-stamps so that it is possible to subsequently verify a XAdES signature long after it was generated.

For the first case the present document specifies requirements for embedding a signed (with XAdES signatures) XML document within a PDF container as an embedded file.

For the second case the present document specifies requirements for generating XAdES signatures on only the XML data of the form, or on any XML content of the XFA form that may be signed with a XMLDSig signature.

For both cases the present document specifies requirements on the XAdES properties both signed and unsigned.

Also for both cases the present document specifies requirements for upgrading of XAdES signatures from basic to more advanced forms.

2 References

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

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

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

2.1 Normative references

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

[1] EN 319 132-1: "XML Advanced Electronic Signatures (XAdES)".

[2] Adobe XML Architecture, Forms Architecture (XFA) Specification, version 2.5, (June 2007), Adobe Systems Incorporated.

[3] W3C/IETF Recommendation: "XML-Signature Syntax and Processing".

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

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

[5] EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

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

[7] W3C Recommendation (16 August 2006): "Extensible Markup Language (XML) 1.0 (Fourth Edition)", edited in place 29 September 2006.

NOTE: The documents [1], [5] are published in the context of the work in Mandate M460. They might not yet be published

2.2 Informative references

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

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

[i.2] ETSI TR 102 038: "TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies".

[i.3] ETSI TR 102 272: "Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies".

[i.4] W3C Working Draft : "XML Signature Best Practices". 26 February 2009.

NOTE: Available at http://www.w3.org/TR/2009/WD-xmldsig-bestpractices-20090226/.

[i.5] Void.

[i.6] EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES".

[i.7] EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1".

[i.8] EN 319 142-3: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles".

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

3 Definitions, symbols and abbreviations

Definitions

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

conforming signature handler: software application, or part of a software application, that knows how to perform digital signature operations (e.g. signing and/or verifying) in conformance with ISO 32000-1 [4] and the requirements of the appropriate profile

data object: actual binary/octet data being operated on (transformed, digested, or signed) by an application

NOTE: The term and the definition have been taken from [3],

PDF Signature: binary data object based on the CMS (RFC 3852 [6]) or related syntax containing a digital signature placed within a PDF document structure as specified in ISO 32000-1 [4] 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 [4], clause 12.8.1, table 252 that contains all the information about the Digital Signature

signer: entity that creates an electronic signature

verifier: entity that validates an electronic signature

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)

XML document: data object that is well-formed, as defined in XML specification [i.4].

NOTE: The actual definition that is given in [i.4] is as follows: "(Definition: A data object is an XML document if it is well-formed, as defined in this specification. In addition, the XML document is valid if it meets certain further constraints)".

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 abbreviations given in [1], [2] and the following apply:

BES	Basic Electronic Signature
CA	Certification Authority
CAdES	CMS Advanced Electronic Signature
CMS	Cryptographic Message Syntax

NOTE: As specified in RFC 3852 [6].

DSS	Document Security Store
EPES	Explicit Policy-based Electronic Signature
LTV	Long Term Validation

OCSP	Online Certificate Status Protocol
PAdES	PDF Advanced Electronic Signature
PDF	Portable Document Format
VRI	Validation Related Information
XAdES	XML Advanced Electronic Signatures
XFA	XML Forms Architecture
XML	eXtensible Markup Language

NOTE: As specified in [7].

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

4.1 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 may be aligned with any XML language, i.e. a signed UBL e-Invoice.

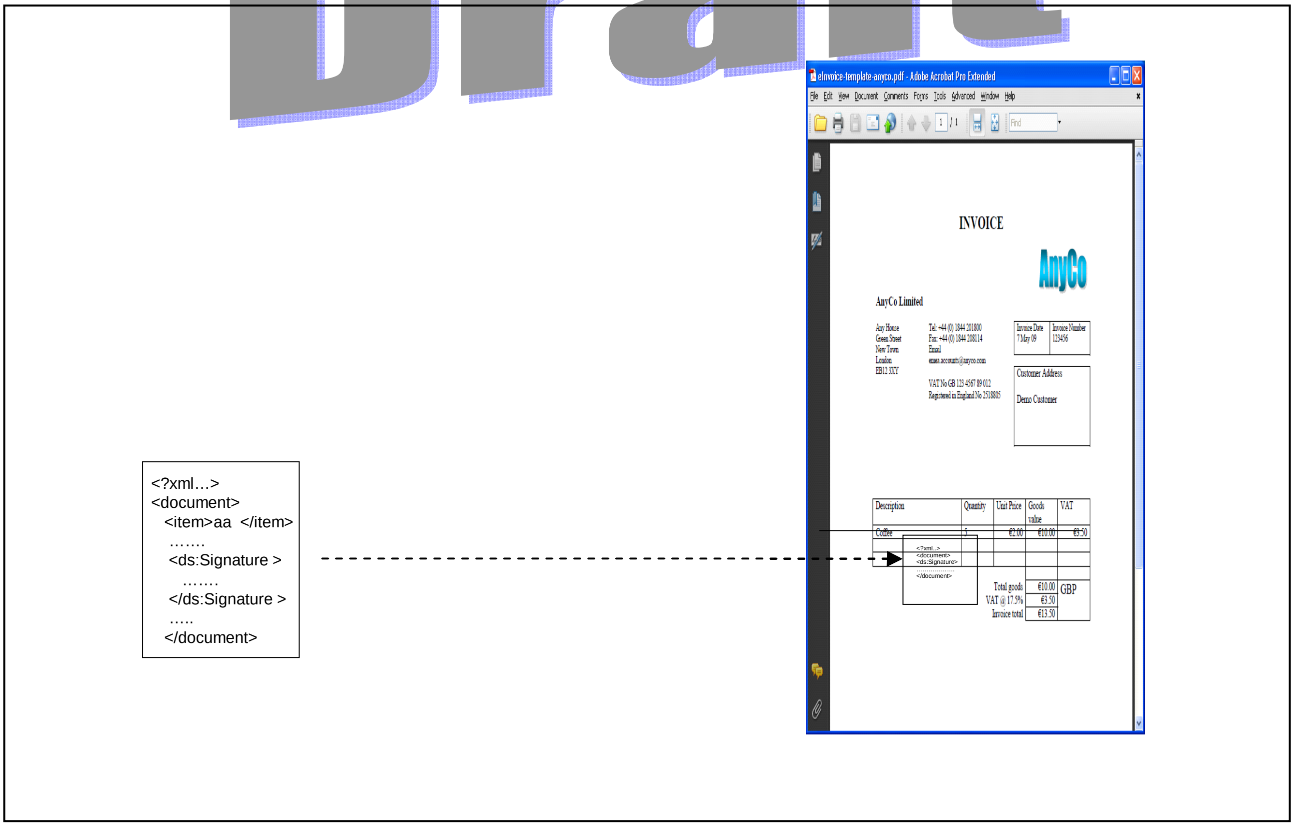
NOTE: The term "data object" applies to any resource that may be referenced by the XMLDSig mechanisms. It may then apply to the XML document when it is signed as a whole, and also to a collection of elements of the XML document if only these elements are signed.

This clause defines two profiles, namely: a basic profile for the basic XAdES forms (XAdES-BES, XAdES-EPES, and XAdES-T), and a profile for long-term XAdES signatures (from XAdES-C to XAdES-A forms).

The scenario for usage of the first profile, specified in clause 4.2, is described below and shown in figure 1:

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

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



```
<?xml…>
<document>
  <item>aa </item>
   …….
   <ds:Signature >
     …….
   </ds:Signature >
   …..
  </document>
```

eInvoice-template-anyco.pdf - Adobe Acrobat Pro Extended
File Edit View Document Comments Forms Tools Advanced Window Help
1 / 1
Find

INVOICE

AnyCo

AnyCo Limited

Any House
Green Street
New Town
London
EB12 3XY

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

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

Invoice Date	Invoice Number
7 May 09	123456

Customer Address

Demo Customer

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

```
<?xml..>
<document>
<ds:Signature>
……………….
</document>
```

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 4.3, is described below and shown in figure 2:

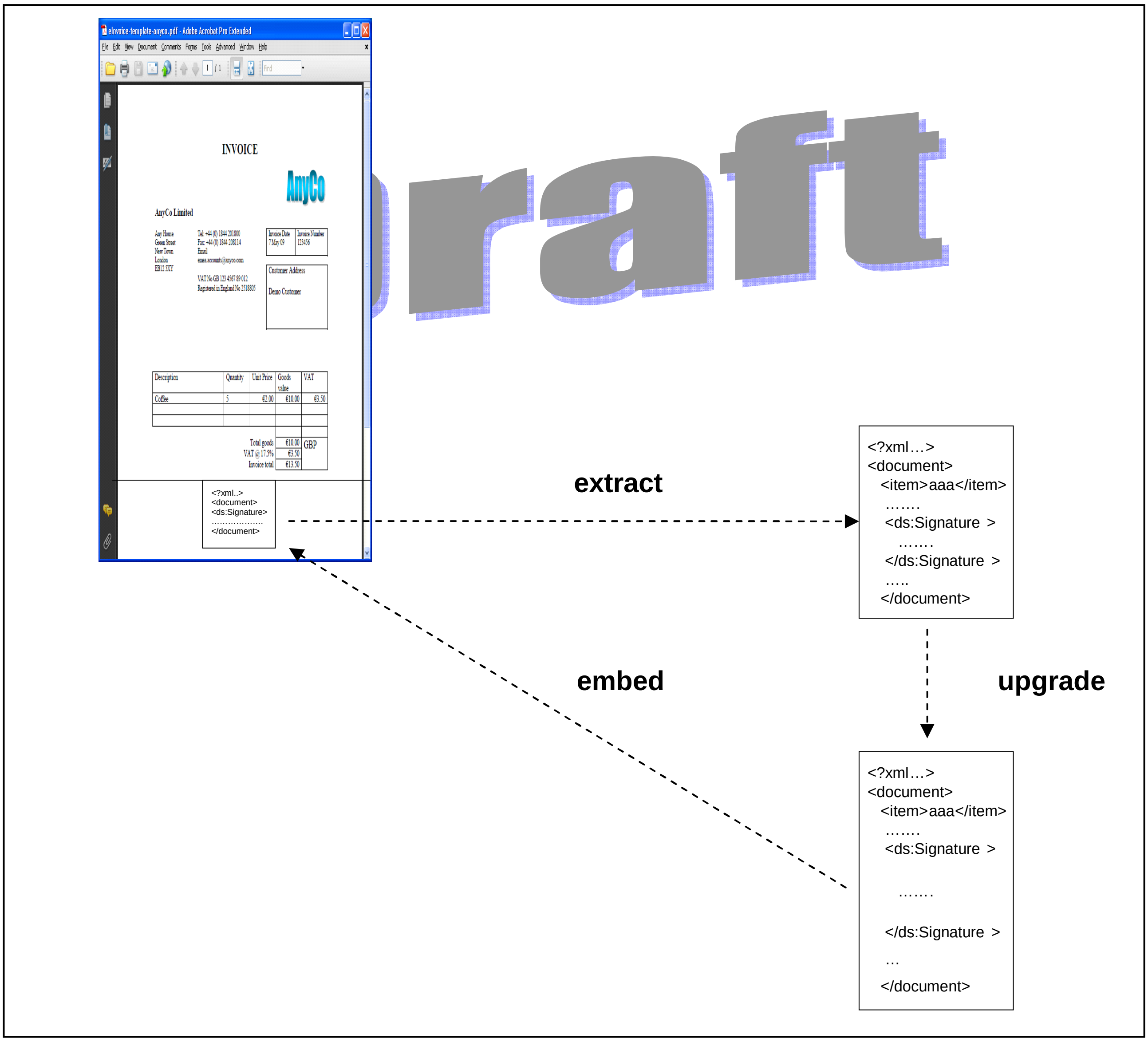
1) The PDF container with the signed XML document is received by the verifier. The verifier extracts the embedded file and verifies the XAdES signature.

2) The verifier may upgrade the XAdES signature to more evolved forms as specified in EN 319 132-1 [1]. As the XAdES signature is part of an embedded file, the Document Secure Store specified in EN 319 142-4 [i.9] may not contain the validation material added during the upgrade. This upgrade must, in consequence be done outside the PDF container and within the XAdES signature itself.

NOTE 1: It is understood that although upgrading the XAdES signature or upgrading the document by a Document Secure Store could provide the verifier with the same information to verify the document in the long run, but it is required to upgrade the XAdES signature in order to enhance interoperability between verifiers.

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

NOTE 2: Upgrading the XAdES signature can be done by extracting the stream object containing the XAdES signature from the containing document, upgrading the XAdES signature in that XML document and including the upgraded XML document in a new stream with the same pdf object number by an incremental update..


eInvoice-template-anyco.pdf - Adobe Acrobat Pro Extended
File Edit View Document Comments Forms Tools Advanced Window Help
1 / 1
Find
AnyCo
extract
embed
upgrade

INVOICE

AnyCo Limited

Any House
Green Street
New Town
London
EB12 3XY

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

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

Invoice Date	Invoice Number
7 May 09	123456

Customer Address

Demo Customer

Description	Quantity	Unit Price	Goods value	VAT
Coffee	5	€2.00	€10.00	€3.50

Total goods	€10.00	GBP
VAT @ 17.5%	€3.50	
Invoice total	€13.50	

```
<?xml..>
<document>
<ds:Signature>
..................
</document>
```

```
<?xml…>
<document>
  <item>aaa</item>
   …….
   <ds:Signature >
      …….
   </ds:Signature >
   …..
  </document>
```

```
<?xml…>
<document>
  <item>aaa</item>
   …….
   <ds:Signature >

      …….

   </ds:Signature >
   …
  </document>
```

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

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

4.2.1 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 4.2.3.

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 forms are profiled by this profile: XAdES-BES, XAdES-EPES, and XAdES-T forms in [1].

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

e) This profile supports parallel signatures.

4.2.2 General syntax and requirements

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

The signatures profiled by the present document are XAdES signatures, and as such, shall follow the syntax specified in EN 319 132-1 [1] with the restrictions specified in this profile.

The XAdES signatures forms profiled by the present document are the following ones: XAdES-BES, XAdES-EPES, and XAdES-T.

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

The handling of unsupported signed properties is a matter for the verifier.

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.

4.2.3 Requirements for applications generating signed XML document to be embedded

The signed XML document to be embedded within the PDF container shall satisfy the following requirements:

1) The signed XML document 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.

2) Applications generating XAdES signatures compliant with the present profile shall ensure that the signed XML document contains at least one XAdES signature and one or more signed data objects.

Applications generating XAdES signatures compliant with the present profile shall ensure that the signed data objects and the XAdES signature(s) within the signed XML document to be embedded satisfy one of the following requirements:

1) All the signed data objects are embedded within the signed XML document.

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 XML signature.

2) If a signed data object is detached from the signed XML document, it shall be possible to build up a valid ds:Reference element according to the rules of [3] for retrieving such data object by using the retrieval mechanism specified in [3].

NOTE 2: Readers should note that 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 [3].Readers should be aware of the interoperability issues that may 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. Nevertheless, implementers of these profiles are addressed to 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.

4.2.4 Mandatory operations

4.2.4.1 Protecting the signing certificate

XAdES specifies two mechanisms for protecting the signing certificate, namely: adding the xades: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 xades:SigningCertificate property for securing the signing certificate. Nevertheless, applications may use the other technique.

NOTE: Readers are warned, nevertheless that signing 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

4.2.5 Requirements on XAdES optional properties

4.2.5.1 The SigningTime element

The SigningTime element is an optional signed property. If present its syntax, semantics and usage shall be as specified in EN 319 132-1 [1].

4.2.5.2 The SignaturePolicyIdentifier element

The SignaturePolicyIdentifier element is an optional signed property. If present its syntax, semantics and usage shall be as specified in EN 319 132-1 [1].

4.2.5.3 The SignatureProductionPlace element

The SignatureProductionPlace element is an optional signed property. If present its syntax, semantics and usage shall be as specified in EN 319 132-1 [1].

4.2.5.4 The SignerRole element

The SignerRole element is an optional signed property. If present its syntax, semantics and usage shall be as specified in EN 319 132-1 [1].

4.2.5.5 The SignedDataObjectFormat element

The `SignedDataObjectFormat` element is an optional signed property. If present its syntax, semantics and usage shall be as specified in EN 319 132-1 [1].

4.2.5.6 The CommitmentTypeIndication element

The `CommitmentTypeIndication` element is an optional signed property. If present its syntax, semantics and usage shall be as specified in EN 319 132-1 [1].

4.2.5.7 The AllDataObjectsTimeStamp element

The `AllDataObjectsTimeStamp` element is an optional signed property. If present its syntax, semantics and usage shall be as specified in EN 319 132-1 [1].

4.2.5.8 The IndividualDataObjectsTimeStamp element

The `IndividualDataObjects` element is an optional signed property. If present its syntax, semantics and usage shall be as specified in EN 319 132-1 [1].

4.2.5.9 The `SignatureTimeStamp` element

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

4.2.6 Serial Signatures

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

The clauses below specify requirements for each mechanism.

4.2.6.1 The `CounterSignature` element

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

4.2.6.2 Detached serial signature

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 EN 319 132-1 [1], clause 7.2.4.1.

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.

4.2.7 Parallel Signatures

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

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

4.3.1 Features

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

a) Long-term signatures production.

b) Signature is encoded as XAdES-C, XAdES-X or XAdES-XL, XAdES-A (EN 319 132-1 [1]).

4.3.2 Upgrading 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 upgraded XAdES signature. Finally, conforming signature handlers shall embed again the signed XML document with the upgraded XAdES signature into the PDF container.

4.3.3 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 EN 319 132-1 [1].

4.3.4 Validation Process

It is recommended that that validation process be as follows:

1) Any time-stamp present within latest `xades:ArchiveTimeStamp` element should be validated at current time with validation data collected at the current time.

2) Any time-stamp present within "inner" `xades:ArchiveTimeStamp` elements should be validated at the time indicated in the time-stamp present in previous `xades:ArchiveTimeStamp`.

3) Any present time-stamp contained in `xades:SigAndRefsTimeStamp` or `xades:RefsOnlyTimeStamp` the signature and the signature time-stamp should be validated at the latest innermost LTV archive timestamp time using the validation data stored in the DSS and time-stamped (by the successive enveloping time-stamps).

4) The signature and any time-stamp present within `xades:SignatureTimeStamp` element should be validated at the time indicated in the time-stamp present within `xades:SigAndRefsTimeStamp` or `xades:RefsOnlyTimeStamp` or the latest innermost `xades:ArchiveTimeStamp` element if none of the two previous elements is present.

5 Profiles for XAdES signatures on XFA Forms

5.1 Overview

This clause defines two profiles for using XAdES signatures for signing dynamic XFA forms. Syntax and semantics of dynamic XFA forms are specified in [2].

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 XMLDSig signature.

XFA forms specification [2] allows signing XFA forms using XMLDSig signatures. XFA forms specification defines certain restrictions for these signatures. Being XAdES signatures built on XMLDSig signatures, the same restrictions shall apply for XAdES signatures as for XMLDSig signatures.

NOTE: Digital signatures of XFA forms are discussed in section "Signed Forms and Signed Submissions" of [2]. XML signatures for signing XFA forms are discussed in section "XML Digital Signatures" of [2].

This clause defines two profiles, namely:

1) A basic profile for the basic XAdES forms (XAdES-BES, XAdES-EPES, and XAdES-T).

2) A profile for long-term XAdES signatures, which uses DSS and VRI dictionaries specified in EN 319 142-4 [i.9] to achieve equivalent functionality to XAdES-XL and XAdES-A forms.

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.

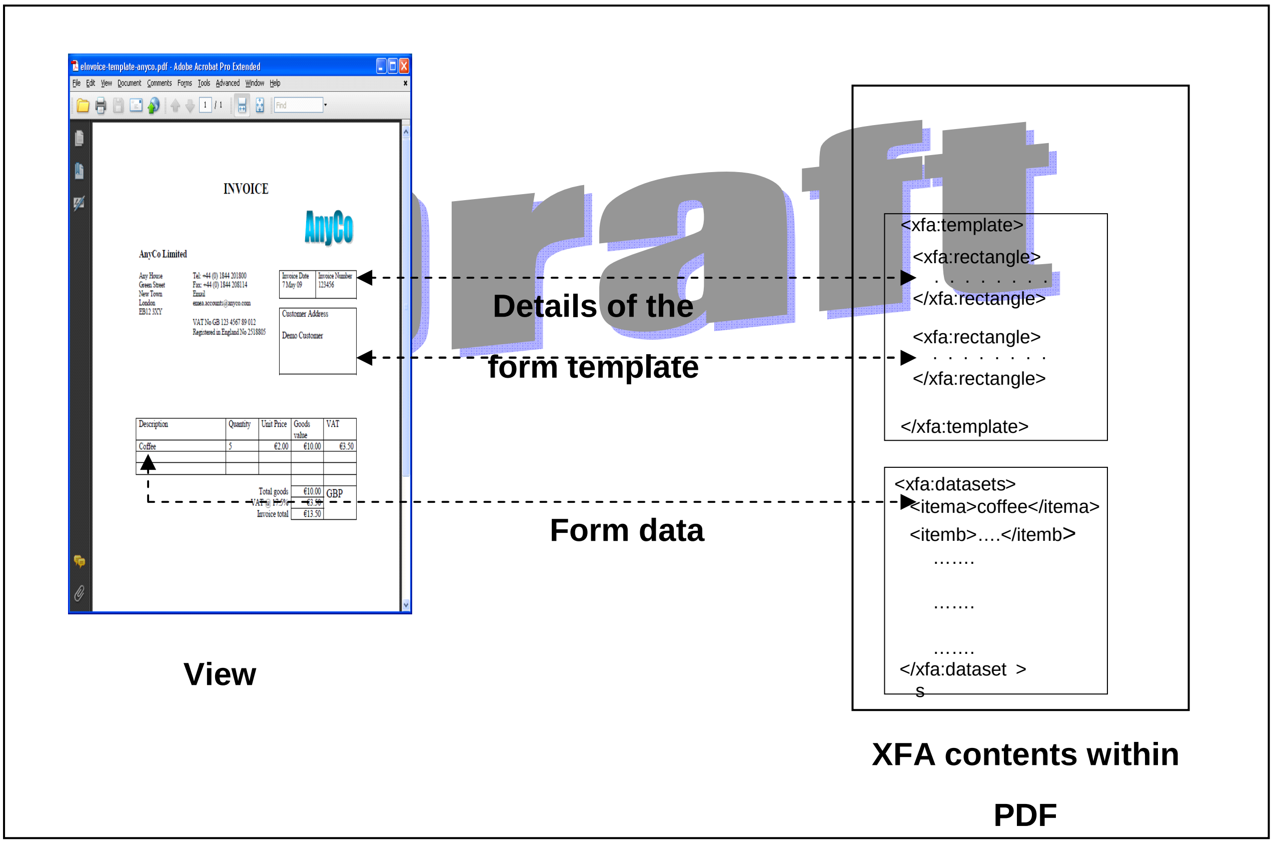
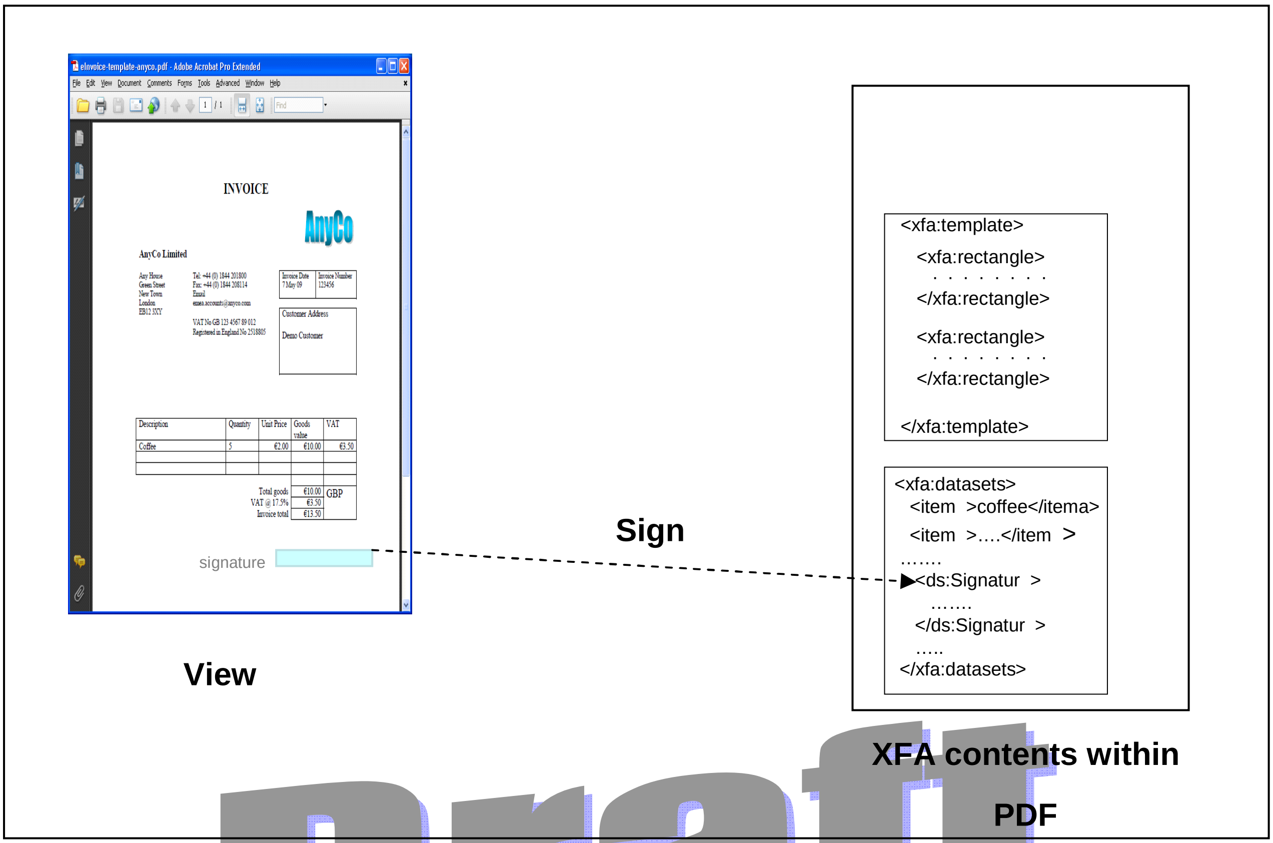


Figure 3: XFA framework

The scenario for usage of the profile for basic XAdES signatures on XFA forms, specified in clause 5.2, is shown in figure 4. After filling a form, a user may sign selected parts of the form (data only, or any XFA component that may actually be signed with a XMLDSig signature. The XAdES signature (XAdES-BES, XAdES-EPES or XAdES-T) is then incorporated within the XFA content.



INVOICE

AnyCo

AnyCo Limited

Any House
Green Street
New Town
London
EB12 3XY

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

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

Invoice Date	Invoice Number
7 May 09	123456

Customer Address

Demo Customer

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

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 5.3, is shown in figure 5. At any time after the signing of a form with a XAdES signature compliant with the profile for basic XAdES signatures on XFA form, a user may upgrade the signature on the XFA form using the Document Secure Store and VRI techniques specified in EN 319 142-4 [i.9]. 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.

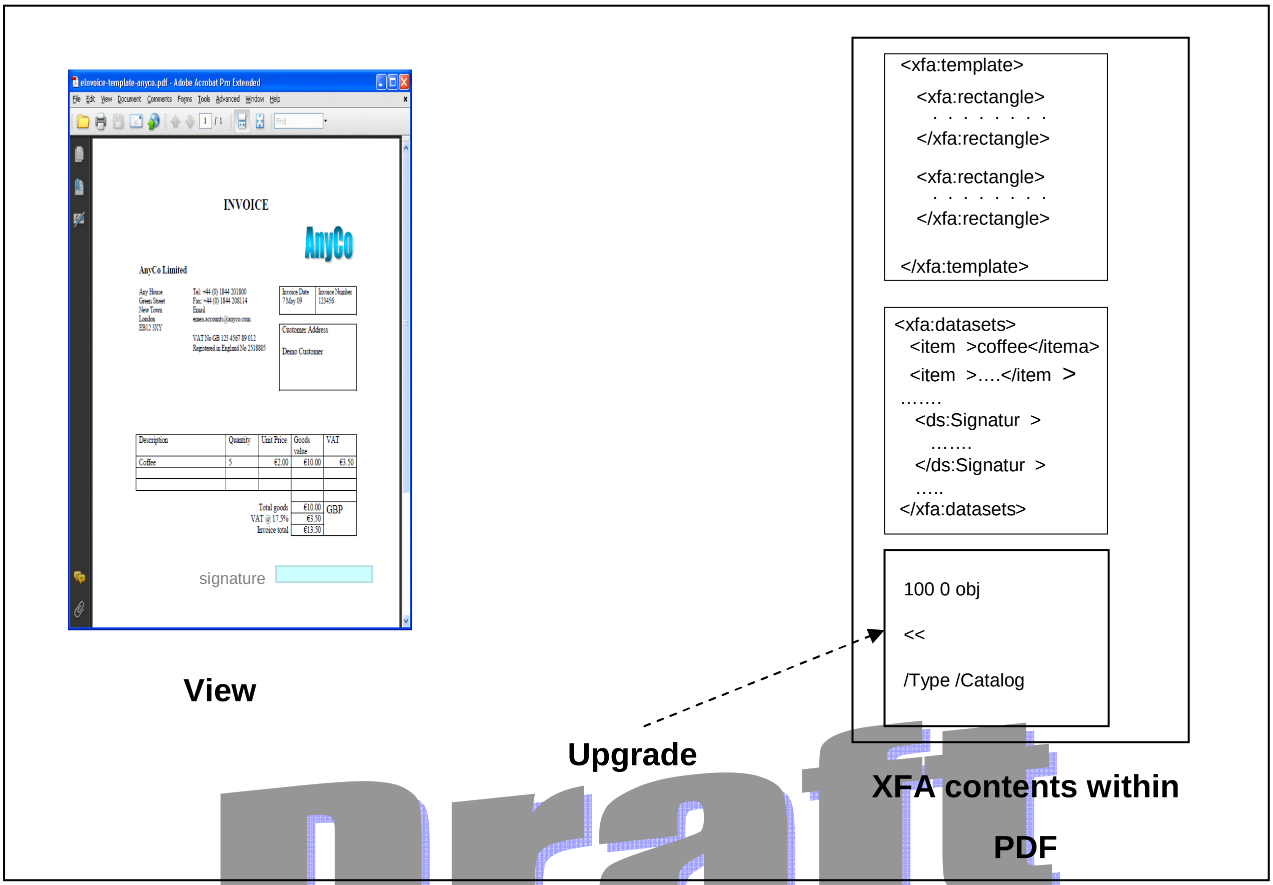


Figure 5: Scenario for profile for long-term validation XAdES signatures on XFA forms

5.2 Profile for Basic XAdES signatures on XFA forms

5.2.1 Features

The main features provided by this profile are listed below:

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

b) The XAdES signature protects 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 as XAdES-BES, XAdES-EPES or XAdES-T forms.

d) This profile supports serial signatures.

e) This profile supports parallel signatures.

5.2.2 General syntax and requirements

The signatures specified by this profile are XAdES signatures, and as such, they shall follow the syntax specified in EN 319 132-1 [1] with the restrictions specified in this profile.

The signatures specified by this profile are XAdES signatures built on XMLDSig signatures used for signing parts of XFA dynamic forms. As such they shall respect the requirements for XMLDSig signatures defined by XFA specification [2] except those ones that conflict with XAdES syntactic or semantic requirements.

The XAdES signatures forms profiled by the present document are XAdES-BES, XAdES-EPES and XAdES-T.

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

The handling of unsupported signed properties is a matter for the verifier.

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.

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

5.2.3 Mandatory operations

5.2.3.1 Protecting the signing certificate

XAdES specifies two mechanisms for protecting the signing certificate, namely: adding the `xades: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 `xades:SigningCertificate` property for securing the signing certificate. Nevertheless, conforming signature handlers may use the other technique.

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. Conforming signature handlers 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 .

5.2.4 Requirements on XAdES optional properties

5.2.4.1 The `SigningTime` element

The `SigningTime` element shall not be used.

NOTE: The XMLDSig signatures generated by XFA processors include additional XML elements not specified within [3]. 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.

Signatures aligned with this profile shall sign the ds:SignatureProperties element containing the additional XML elements not specified within [3] that are incorporated by XFA processors.

5.2.4.2 The SignaturePolicyIdentifier element

The `SignaturePolicyIdentifier` element is an optional signed property. If present its syntax, semantics and usage shall be as specified in EN 319 132-1 [1].

5.2.4.3 The SignatureProductionPlace element

The `SignatureProductionPlace` element is an optional signed property. If present its syntax, semantics and usage shall be as specified in EN 319 132-1 [1].

5.2.4.4 The SignerRole element

The SignerRole element is an optional signed property. If present its syntax, semantics and usage shall be as specified in EN 319 132-1 [1].

5.2.4.5 The SignedDataObjectFormat element

The SignedDataObjectFormat element is an optional signed property. If present its syntax, semantics and usage shall be as specified in EN 319 132-1 [1].

5.2.4.6 The CommitmentTypeIndication element

If the XAdES signature is not a XAdES-EPES form and it is not a XAdES form built on a XAdES-EPES form either, the commitment-type-indication property shall not be present.

NOTE 1: The XMLDSig signatures generated by XFA processors include additional XML elements not specified within [3]. 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 is a XAdES-EPES signature or another form built on a XAdES-EPES form, the commitment-type-indication attribute may be present. If it is present, its syntax, semantics and usage shall be as specified in EN 319 132-1 [1]. If the XAdES signature is a XAdES-EPES signature or another form built on a XAdES-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 2: The reason for this last requirement is that signature policies formats specified by ETSI in TR 102 038 [i.2] and TR 102 272 [i.3] may define different rules for each commitment type indication property present in the XAdES signature.

5.2.4.7 The AllDataObjectsTimeStamp element

The AllDataObjectsTimeStamp element is an optional signed property. If present its syntax, semantics and usage shall be as specified in EN 319 132-1 [1].

5.2.4.8 The IndividualDataObjectsTimeStamp element

The IndividualDataObjects element is an optional signed property. If present its syntax, semantics and usage shall be as specified in EN 319 132-1 [1].

5.2.4.9 The SignatureTimeStamp element

The SignatureTimeStamp element should be present as an unsigned property in signatures compliant with the present profile. Its syntax, semantics and usage shall be as specified in EN 319 132-1 [1].

5.2.5 Serial Signatures

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

The following clauses specify requirements for each mechanism.

5.2.5.1 The CounterSignature element

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

5.2.5.2 Detached serial signature

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 EN 319 132-1 [1] clause 7.2.4.1.

If this method of countersigning a XAdES signature is used the XAdES countersignature should also be present within XFA dynamic form.

5.2.6 Parallel Signatures

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

5.3 Profile for long-term validation XAdES signatures on XFA forms (XAdES-LTV)

5.3.1 Overview

Validation of an electronic signature requires data to validate the signature such as CA certificates, Certificate Revocation List (CRLs) or certificate status information (OCSP) provided by an online service (referred to in the present document as validation data). If the document is stored and the signatures verified multiple times over a long period (months, years or even decades), the original validation data may no longer available or there may uncertainty as to what validation data was used when the document was first verified. The LTV profiles provide a means for the signer or a verifier to attach validation data to the document at the time near when the document is signed as well as any future time that verification takes place if the information has changed. In addition, the LTV enables the validity to be maintained over extended periods through repeated application of time-stamps.

The present clause profiles the XAdES-BES, XAdES-EPES and XAdES-T signature forms aligned with the profile defined in clause 5.2 of the present document, 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 EN 319 132-1 [1], by upgrading XAdES signatures aligned with the profile defined in clause 5.2 of the present document, using the LTV mechanisms specified in annex A of EN 319 142-4 [i.9].

This profile does not specify an upgrade to support the equivalent to XAdES-C and XAdES-X forms, as the VRI dictionary specified in annex A of [i.8] does not provide resources for incorporating references to certificates and certificate status data (CRLs or OCSP responses) required by the aforementioned forms.

5.3.2 Features

The main features provided by this profile are listed below:

a) Features a), b), d) and e) of the profile defined in clause 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 [i.9]. 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.

5.3.3 General Requirements

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

a) Document security store information as specified in clause A.1 of [i.9].

b) Document time-stamps as specified in clause A.2 of [i.9].

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

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

5.3.4 Validation Process

It is recommended that that validation process be as follows:

1) The "latest" archive time-stamp should be validated at current time with validation data collected at the current time.

2) The "inner" archive time-stamps should be validated at previous archive timestamp time with the validation data present (and time-stamped for the successive enveloping time-stamps) in the previous DSS.

3) the signature and any time-stamp present within `xades:SignatureTimeStamp` element should be validated at the latest innermost LTV archive timestamp time using the validation data stored in the DSS and time-stamped (by the successive enveloping time-stamps)

Validation of documents without archive time-stamps is outside the scope of this profile.

5.4 Extensions Dictionary

The extensions dictionary (see ISO 32000-1 [4] 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.

The following text is to be used when appropriate:

Proforma copyright release text block

This text box shall immediately follow after the heading of an element (i.e. clause or annex) containing a proforma or template which is intended to be copied by the user. Such an element shall always start on a new page.

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the <proformatype> proforma in this {clause|annex} so that it can be used for its intended purposes and may further publish the completed <proformatype>.

<PAGE BREAK>

Annex A (informative): Matching of Basic PAdES-LTV XAdES-based profiles to XAdES

This informative annex shows how functional equivalence to different evolved XAdES forms is achieved by combining XAdES signatures aligned with the profile defined in clause 5.2 of the present document and LTV-related dictionaries defined in annex A of EN 319 142-4 [i.9].

The first column indicates what profile supports the functional equivalence. The second row indicates the XAdES form whose functionality is supported. The third column indicates the starting combination of XAdES signature and LTV related dictionaries on which the final combination is built. Finally, the fourth column indicates what has to be added to the starting combination for achieving something functionally equivalent to the XAdES form identified in the second column.

Entry	Profile	Functional equivalence to XAdES form	Built on	Adding
1	Not currently supported (see note 1)	XAdES-C		
2	Not currently supported(see note 1)	XAdES-X		
3	PAdES-LTV (based in XAdES as profiled in clause 5.3)	XAdES-X-L	PAdES-BES, PAdES-EPES as profiled in clause 5.2, either with `xades:SignatureTimeStamp` recommended (functionally equivalent to XAdES-T, XAdES-BES or XAdES-EPES).	• A DSS containing indirect references to the values of the certificates and cert status data (CRLs or OCSP responses) as specified in clause A.1 of EN 319 142-4. • Optionally VRI dictionary containing indirect references to the values of the certificates and cert status data (CRLs or OCSP responses) that were used for verifying a particular signature as specified in annex A.1 of EN 319 142-4 . • The certificates and cert status data (CRLs or OCSP responses) referenced by DSS and VRI as specified in annex A of EN 319 142-4. • A document Time-stamp as specified in clause A.2 of EN 319 142-4 [i.9].
4	PAdES-LTV (based in XAdES, as profiled in clause 5.3)	XAdES-A	PAdES signature identified in row 3 (functionally equivalent to XAdES-X-L)	• In the DSS: set of indirect references to the values of certificates and certificate status data (CRLs or OCSP responses) as specified in clause A.1 of EN 319 142-4. • Optionally VRI dictionary containing indirect references to the values of the certificates and cert status data (CRLs or OCSP responses) that were used for verifying the previous document time-stamp as specified in clause A.1 of EN 319 142-4. • The certificates and cert status data (CRLs or OCSP responses) referencing by DSS as specified in clause A.1 of EN 319 142-4. • A document Time-stamp as specified in clause A.2 of TS EN 319 142-4 [i.9].

Entry	Profile	Functional equivalence to XAdES form	Built on	Adding
5	PAdES-LTV (based in XAdES, as profiled in clause 5.3) (see note 2)	XAdES-A (with one more document time-stamp)	PAdES signature identified in row 4 (functionally equivalent to XAdES-A - with one document-time-stamp)	• In the DSS: set of indirect references to the values of certificates and certificate status data (CRLs or OCSP responses) including those that were used for verifying the previous document time-stamp. • Optionally VRI dictionary containing indirect references to the values of the certificates and cert status data (CRLs or OCSP responses) that were used for verifying the previous document time-stamp as specified in clause A.11 of EN 319 142-4. • The certificates and cert status data (CRLs or OCSP responses) referencing by DSS as specified in clause A.11 of EN 319 142-4. • A document Time-stamp as specified in clause A.2 1 of EN 319 142-4 [i.9]

NOTE 1: The reason for not supporting references is that they are difficult to manager. There may be situations where referenced data are not available and this may result in being locked-up while waiting for resolution of references.

NOTE 2: Row 5 in the table shows the process for upgrading the signature with successive document time-stamps and their corresponding validation data (certificates and certificate status).

Abstract Test Suite (ATS) text block

This text should be used for ATSs using either TTCN-2 or TTCN-3. In case:

- *TTCN-2 is used: attach the TTCN.MP;*
- *TTCN-3 is used: attach the TTCN-3 files and other related modules, as well as the HTML documentation of the TTCN-3 files.*

Annex <X> (normative): ATS in TTCN-2 *(style H8)*

This text shall only be used for ATSs using TTCN version 2 (TTCN-2):

This ATS has been produced using the Tree and Tabular Combined Notation version 2 (TTCN-2) according to ISO/IEC 9646-3 [<x>].

<X.1> The TTCN-2 Machine Processable form (TTCN.MP) *(style H1)*

The TTCN.MP representation corresponding to this ATS is contained in an ASCII file (<any_name>.MP contained in archive <Shortfilename>.ZIP) which accompanies the present document.

<PAGE BREAK>

Annex <X+1> (normative): ATS in TTCN-3 *(style H8)*

This text shall only be used for ATSs using TTCN version 3 (TTCN-3):

This ATS has been produced using the Testing and Test Control Notation (TTCN) according to ES 201 873-1 [<x>].

Indicated here which parts of the ES 201 873 series and its versions (editions) have been used; also indicate any extensions which have been used.

<X+1.1> TTCN-3 files and other related modules *(style H1)*

The TTCN-3 and other related modules are contained in archive <Shortfilename>.zip which accompanies the present document.

<X+1.2> HTML documentation of TTCN-3 files *(style H1)*

The HTML documentation of the TTCN-3 and other related modules are contained in archive <Shortfilename>.zip which accompanies the present document.

<PAGE BREAK>

Annex <X+2> (informative): Title of informative annex *(style H8)*

<Text>

<X+2.1> First clause of the annex *(style H1)*

<Text>

<X+2.1.1 >First subdivided clause of the annex *(style H2)*

<Text>

<PAGE BREAK>

Annex <X+3> (informative): Change History

This informative annex is optional. If present, it describes the list of changes implemented in a new version of the deliverable.

Its format is tabular, it may contain the Change Request numbers and titles or textual explanations of the changes that lead to each new version number of the deliverable.

date	Version	Information about changes
October 2011	v1.1.1	First publication of the TS after approval by TC SPAN at SPAN#19 (30 September - 2 October 2011; Prague) Rapporteur is John Smith
February 2012	v1.2.1	Implemented Change Requests: SPAN(12)20_019 Error message information clarifications SPAN(12)20_033 Revised error message information SPAN(12)20_046 update of figure 3 clause 9.2 These CRs were approved by TC SPAN#20 (3 - 5 February 2012; Sophia) Version 1.2.1 prepared by John Smith
July 2013	v1.3.1	Implemented Changes: Correction needed because the previously approved version did not contain the last version of the ASN.1 and XML attachments. Version 1.3.1 prepared by Mark Canterbury (NTAC)

<PAGE BREAK>

Annex <X+4> (informative): Bibliography

The annex entitled "Bibliography" is optional.

It shall contain a list of standards, books, articles, or other sources on a particular subject which are not mentioned in the document itselft (see clause 12.2 of the EDRs http://portal.etsi.org/edithelp/Files/other/EDRs_navigator.chm).

It shall not include references mentioned in the document.

*Use the **Heading 8 style** for the title and B1+ or Normal for the text.*

- <Publication>: "<Title>".

OR

<Publication>: "<Title>".

<PAGE BREAK>

History

Document history		
V1.1.1	July 2009	Publication as ETSI TS 102 778
V1.1.2	December 2009	Publication as ETSI TS 102 778
V1.1.2	April 2013	Draft forwarded by ***editHelp!*** for revision purposes
V0.0.0	May 2013	Draft version of EN inside ETSI STF458
V0.0.1	September 2013	Incomplete Draft for Review in ESI#40
V0.0.2	November 2013	Stable Draft for Review in ESI#41
V0.0.3	November 2013	Stable Draft for public review

Latest changes made on 2013-119-27