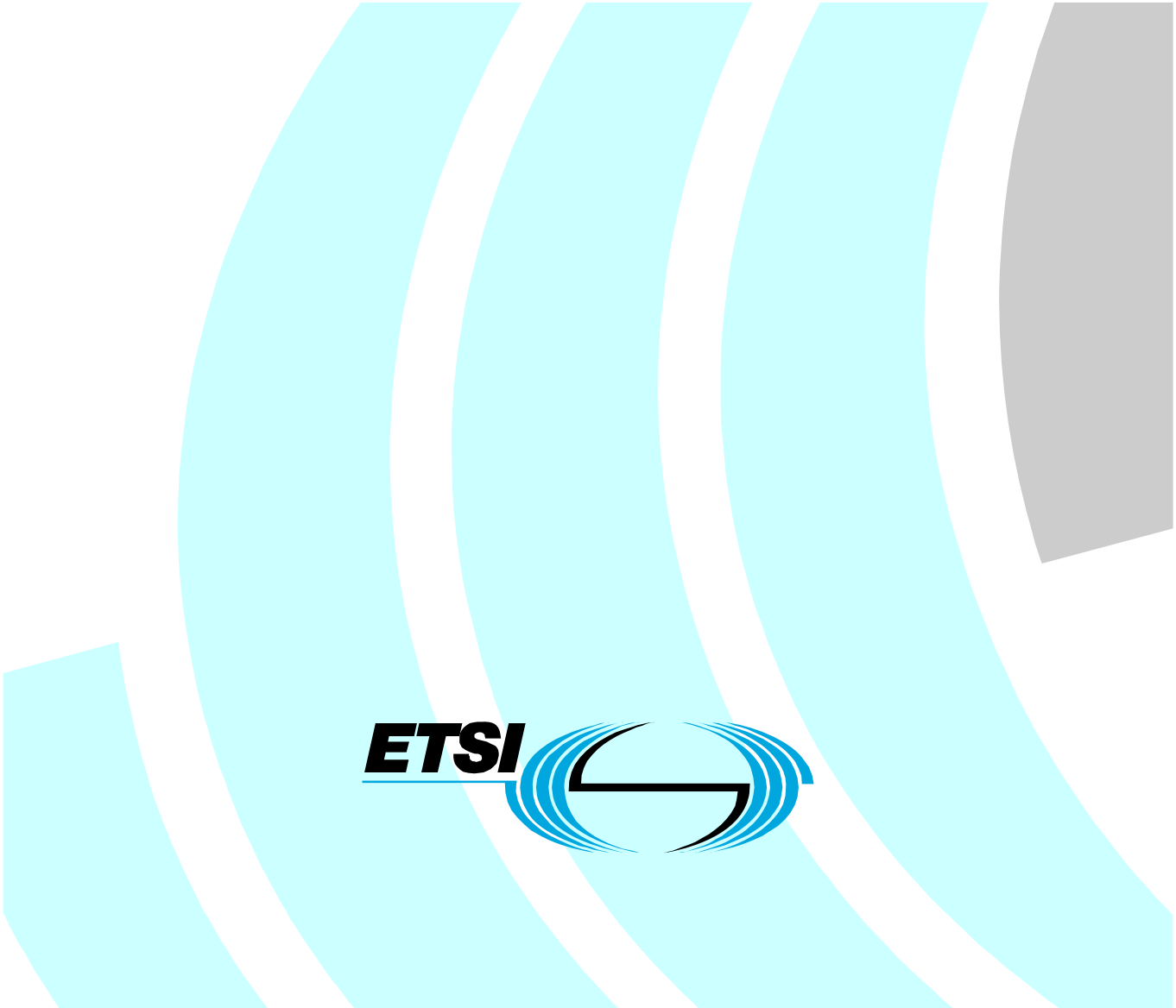
ETSI TR 102 923 V1.1.1 (2010-07)

Technical Report

Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signatures (PAdES); Usage and implementation guidelines



Reference
DTR/ESI-000086

Keywords
e-commerce, electronic signatures, security,
PAdES

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 Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

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.

ISO 32000-1 [i.6] 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 [i.6] 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 technology and techniques as TS 101 733 [i.3] (CAdES), but without the extended signature capabilities of CAdES.

TS 102 779 [i.16]: "PDF Advanced Electronic Signatures (PAdES)", in its parts 1 to 6 specify formats for including management of Advanced Electronic Signatures within PDF framework, as well as to deal with visual signatures and visual representation of Advanced Electronic Signatures verification. As such, PAdES is also a set of standards that support European requirements for electronic signatures and includes features to support validation of signatures which are stored for years or even decades.

1 Scope

The present document provides:

1) Guidance on expected usage of PAdES signatures for securing PDF documents.

2) Guidance on the implementation of PAdES requirements.

Readers should note that this is not a normative document, but an informative one. As such, no mandatory requirements are specified in the present document, but recommendations and suggestions on what authors of the document think that a correct usage of PAdES would be, and also details and recommendations that might be useful for PAdES implementers.

NOTE: These guidelines includes information collected derived from the ETSI PAdES FAQ web site at the time of publication. Further details and more up to date information may be found by reference to the web site at www.padesfaq.net

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.

Not applicable.

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

[i.2] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for Electronic Signatures.

[i.3] ETSI TS 101 733: "Electronic Signatures and Infrastructures(ESI); CMS Advanced Electronic Signatures (CAdES)".

[i.4] ETSI TS 101 903: "XML Advanced Electronic Signatures (XAdES)".

[i.5] OASIS-DSSX: "Profile for comprehensive multi-signature verification reports for OASIS Digital Signature Services. Committee Draft Version 1.0".

[i.6] 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.

[i.7] ETSI TS 102 778-1: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES".

[i.8] 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".

[i.9] 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".

[i.10] ETSI TS 102 778-4: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES LTV Profile".

[i.11] 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".

[i.12] ETSI TS 102 778-6: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 6: Visual Representations of Electronic Signatures".

[i.13] IETF RFC 3852 (2004): "Cryptographic Message Syntax (CMS)".

[i.14] IETF RFC 3709: "Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates".

[i.15] IETF RFC 3739: "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile".

[i.16] ETSI TS 102 779: "Speech and multimedia Transmission Quality (STQ); Multi-component KPI".

[i.17] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions 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 [i.6] 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 [i.13]) or related syntax containing a digital signature placed within a PDF document structure as specified in ISO 32000-1 [i.6], 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 [i.6], 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

3.2 Abbreviations

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

AdES	Advanced Electronic Signatures
CAdES	CMS Advanced Electronic Signature

NOTE: See TS 101 733 [i.3].

CMS Cryptographic Message Syntax

NOTE: As specified in RFC 3852 [i.13].

CRL Certificate Revocation List
DSS Document Security Store
ESI Electronic Signatures and Infrastructure
GSM Global System for Mobile communication
LTV Long Term Validation
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
XAdES XML Advanced Electronic Signatures

NOTE: See TS 101 903 [i.4].

XFA XML Forms Architecture
XML eXtensible Markup Language

4 Background: PAdES' historical context

Over the last decade, ETSI ESI TC has defined a complete framework for Advanced Electronic Signatures (AdES henceforth), specifying formats and management procedures for such signatures in the most popular syntaxes that currently deal with electronic documents and electronic signatures, namely: ASN.1 (CAdES), PDF (PAdES) and XML (XAdES).

Traditionally CAdES has been used in those environments that traditionally have used CMS (mostly binary documents) and where some of the features brought by AdES signatures are required. XAdES signatures have been used within environments where XML documents require usage of AdES signatures, although they have also been used for signing binary documents.

PAdES specification brings to the PDF signatures (and by doing this, to the PDF documents framework) features already incorporated to binary and XML electronic documents through the usage of CAdES and XAdES signatures, namely: capability for incorporating a soundful repertoire of signed properties qualifying both the signature and/or the signatory (i.e. role of the signer, claimed signing time, etc), and those ones that may deal with long term signatures (i.e. signatures that may correctly be verified long after the certificates in the certification path have expired). Under this perspective, PAdES constitutes a step forward in the path that is leading to bring the features of AdES signatures to the most relevant types of electronic documents.

5 Using PAdES

The present clause provides details and recommendations of the expected usage of PAdES signatures.

5.1 Parts of PAdES specification

PAdES specifications come in 6 parts. Below follows the list of parts as well as a short description of each part:

- TS 102 778-1 [i.7]: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES". This part provides a bird's eye view of the other 5 parts. More specifically, it provides a general description of support for Advanced Electronic Signatures in PDF documents including use of XML signatures to protect XML data in PDF documents; lists the features of the PAdES signatures profiled in the other parts; and describes how these profiles may be used in combination. This document will be referred as PAdES Part 1 henceforth.

- TS 102 778-2 [i.8]: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1 [i.6]". This part profiles the use of PDF signatures, as described in ISO 32000-1 [i.6]. This profile allows to generate PAdES signatures that are compatible with existing ISO 32000 [i.6] PDF readers. Among other features, PAdES part 2 supports serial signatures, may optionally include the "reasons" for the signature, a description of the location where the signature was generated, contact info of the signatory. This profile recommends inclusion of a signature time-stamp and revocation information. This profile serves as basis for building more evolved types of PAdES signatures. This document will be referred as PAdES Part 2 henceforth.

- TS 102 778-3 [i.9]: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles". This part profiles the inclusion of features offered by AdES-BES and AdES-EPES types, namely: secure the singing certificate itself with the signature and all the signed attributes in AdES-BES and AdES-EPES repertoire (including a reference to the Electronic Signature Policy under which the signatory has created the signature and that the verifier should use during the verification). PAdES-BES and PAdES-EPES signatures are encoded as CAdES-BES and CAdES-EPES. This document will be referred as PAdES Part 3 henceforth.

- TS 102 778-4 [i.10]: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES LTV Profile". This profile specify new PDF structures that, in combination with PAdES signatures specified in Part 3, support long term electronic signatures. These structures are specified for supporting the inclusion of validation data of electronic signatures (certificates, CRLs and/or OCSP responses) and document time-stamps (i.e. time-stamps that covers the whole existing PDF document when the time-stamp is generated) within PDF documents, so that similar features to the CAdES-A or XAdES-A are obtained within PDF framework using this combination of CAdES-BES/EPES signatures and additional PDF objects. This document will be referred as PAdES Part 4 henceforth.

- TS 102 778-5 [i.11]: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures". This profile deals with the usage of XAdES signatures for signing two different types of documents within the PDF framework: first a XML document that is first signed with a regular XAdES signature and afterwards embedded in a PDF container; secondly with the signing of XFA forms with regular XAdES signatures. These PAdES signatures are based on XML signatures rather than the binary signatures specified within PAdES Parts 2 and 3 . This document will be referred as PAdES Part 5 henceforth.

- TS 102 778-6 [i.12]: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 6: Visual Representations of Electronic Signatures". This profile provides requirements and recommendations for the visual appearance of signatures included within a PDF document and the representation of signature verification. This is particularly aimed to help the untrained human understanding of the signature and to further consistency between the visual appearance of signatures within a PDF document and the signature verification representation in order to help human comparison.

5.2 PAdES, ISO 32000-1, CAdES and XAdES

PAdES signatures are fully compatible with ISO 32000-1 [i.6]; as mentioned earlier, PAdES Part 2 actually defines a profile of ISO 32000-1 [i.6], and is compatible with PDF readers based on that standard. The more evolved types of PAdES signatures defined in parts 3 and 4 are based on this profile.

One of the most important consequences is that PAdES actually builds on the existing installed base of PDF readers and the range of tools available to sign and verify PDF documents.

Both PDF and PAdES are open standards which have been implemented by several suppliers. PDF is standardized by the International Standards Organisation as ISO 32000-1 [i.6], this was further develop as PAdES by ETSI (European Telecommunications Standards Institute). PAdES is being fed back into the ISO for inclusion in future versions of ISO 32000.

As with other forms of advanced electronic signatures (CAdES and XAdES), PAdES signatures:

- Supports Advanced Electronic Signatures compliant with EU Directive 1999/93 on Electronic Signatures as they use public key cryptographic techniques to protect both the integrity of the document so that any changes can be detected, and the authenticity of the origin of the document or a signature applied to the document.

- Provides a standard technique for assuring the long term validation of electronic signatures in PDFs, as it supports techniques to ensure that the integrity and authenticity of the document can be verified long (years or even decades) after the document was created.

5.3 Selecting the right PAdES Profile

To correctly apply PAdES it is important to understand when PAdES is applicable and in particular which part of PAdES is appropriate for different application scenarios.

The present clause provides guidelines that may help readers to identify when PAdES signatures suit the business scenario that they are facing, and what specific PAdES profile satisfy the requirements associated to that business scenario.

5.3.1 Selecting the right CMS/CAdES-based PAdES Profile

PAdES signatures profiled in Parts 2 to 4 are most applicable to any scenario where **a regular PDF document** needs to be electronically signed with a signature satisfying the EU legal requirements for electronic signatures as in EU Directive 1999/93 [i.2] or where there is a need of managing long term electronic signatures.

PAdES Part 2 is most appropriate where compatibility with PDF readers supporting ISO 32000-1 [i.6] is of major concern. Part 2 can be used in those scenarios where there is a need for signing a regular PDF document but there are no requirements for long term signatures, or for having an explicit reference to a Electronic Signature Policy, or for including any of the CAdES signed attributes that are profiled in Part 3.

PAdES Part 3 is most appropriate for those scenarios where there is a need for signing a regular PDF document and there is also a need for an explicit reference to an Electronic Signature Policy, or the inclusion of a signature time-stamp, or the inclusion of any of the CAdES signed attributes profiled in Part 3, BUT there are not requirements for long term signatures. PAdES signatures aligned with Part 3 are actually encoded as CAdES-BES, CAdES-EPES or CAdES–T signatures.

PAdES Part 4 is most appropriate for those scenarios where there is a need for signing a regular PDF document and in addition there is the requirement of having long term signatures. As already mentioned, PAdES Part 4 are CAdES signatures combined with PDF structures that contain validation data (certificates, CRLs, OCSP responses) and document time-stamps. Part 4 can be used in combination with PAdES signatures specified in Part 2 or Part 3.

5.3.2 Selecting the right XAdES-based PAdES Profile

From what has been already explained, PAdES signatures profiled in Parts 3 and 4 build on CAdES. PAdES does not specifies syntax for using XAdES-based electronic signatures as a native signatures for regular PDF document, the main reason being that at the moment of its production no use-cases for it were reported to the standardizing committee.

NOTE: This was one of the decisions where no unanimity was achieved and the decision was taken by majority of the standardizing team members.

XAdES-based PAdES signatures as profiled in Part 5, nicely fit in two additional usage scenarios:

- **XAdES-Signed-Object-And-PDF Packaged** scenario: whenever a XML document previously signed with one or more regular XAdES signatures, is embedded within a PDF container for its management and those signatures have to be aligned to the EU Directive and/or requires the inclusion of some XAdES signed property or require to be a long term electronic signatures.

- **XAdES-XFA-Signed** scenario: whenever a XFA form (PDF framework supporting the creation, management and signing of XML forms) is required to be signed with a XML signature that has to be aligned to the EU Directive and/or requires the inclusion of some XAdES signed property or requires to be a long term electronic signature.

5.4 PAdES types vs. CAdES/XAdES types

The security protection provided by the different PAdES profiles are equivalent to the CAdES [i.3] and XAdES [i.4] forms are follows:

1) The PAdES-BES profile as specified in part 3 supports CAdES-BES, CAdES-T.

2) The PAdES-EPES profile as specified in part 3 supports CAdES-EPES with the option of a signature time-stamp as for CAdES-T.

3) The PAdES-LTV profile as specified in part 4 without the document time-stamp provides an extended variation of CAdES-C (that includes certificate and certificate revocation values instead of reference).

4) The PAdES-LTV profile as specified in part 4 with the document time-stamp provides an extended variation of CAdES-X (that includes certificate and certificate revocation values instead of references, and time-stamp over the whole document, including the signature).

5) PAdES-LTV profile as specified in part 4 with the document time-stamp provides an extended variation of CAdES-X-L (that includes certificate and certificate revocation values instead of references, and additionally a time-stamp over the whole document, including the signature).

6) The PAdES-LTV profile as specified in part 4 with the document time-stamp provides equivalent to CAdES-A.

NOTE: The reason for not dealing with references is that PDF defines a documental framework and that in foreseen use cases of signed PDF documents, each document has to be self-contained, and in consequence, if a PDF document contains a long term electronic signature, all the material required for its possible arbitration has to be in the document.

7) PAdES Part 5 contains two groups of profiles, namely: 2 profiles for XAdES-signed XML documents embedded in PDF containers and 2 profiles for XAdES signatures on XFA forms . PAdES Part 5 profiles XAdES-signed XML documents embedded in PDF containers support all the forms of XAdES (-BES, -T, -EPES, -C, -X, -XL and -A).

8) PAdES Part 5 profiles XAdES signatures on XFA forms support XAdES-B, XAdES-EPES and XAdES-T. As for evolved forms, same considerations apply for the usage of PAdES-LTV profile as in 3 to 6, but applied to XAdES forms instead CAdES.

Table 1 summarize the remarks shown above.

Table 1: PAdES, XAdES and CAdES types correspondences

	CAdES	XAdES	PDF	PDF-XFA
Basic Advanced Electronic Signature (AdES-BES)	CAdES-BES	XAdES-BES	PAdES-BES	XAdES-BES
Advanced Electronic Signature with Explicit Signature Policy Reference (AdES-EPES)	CAdES-EPES	XAdES-EPES	PAdES-EPES	XAdES-EPES
Advanced Electronic Signature with Time (AdES-T)	CAdES-T	XAdES-T	PAdES (BES or EPES) with Time-stamp option	XAdES-T
With complete validation data references (AdES-C)	CAdES-C	XAdES-C	Extended version: PAdES LTV with values (no references) without document time-stamp	Extended version: PAdES LTV with values (no references) without document time-stamp
Extended validation data reference (AdES-X)	CAdES-X	XAdES-X	Extended version: PAdES LTV with values (no references) and document time-stamp	Extended version: PAdES LTV with values (no references) and document time-stamp
Extended validation data (AdES-X-L)	CAdES-X-L	XAdES-X-L	Extended version: PAdES LTV with values (no references) and document time-stamp	Extended version: PAdES LTV with values (no references) and document time-stamp
Archive validation data (AdES-A)	CAdES-A	XAdES-A	PAdES LTV with values and document time-stamp	PAdES LTV with values and document time-stamp

5.4.1 PAdES and CMS (PAdES Part 2)

Signatures profiled in PAdES Part 2 are regular CMS signatures fully aligned with ISO 32000-1 [i.6] specification and thus is compatible with existing readers based on ISO 32000-1 [i.6]. PAdES Part 2 imposes a number of constraints to ISO 32000-1 [i.6] signatures.

PAdES Part 2 signatures add the following features to the basic features provided by CMS:

1) Optionally may incorporate a signature time-stamp. This time-stamp is embedded as described in ISO 32000-1 [i.6], clause 12.8.3.3.1.

2) Also optionally may include revocation information. This information is embedded as signed attribute using the `adbe-revocationInfoArchival` signed attribute defined by ISO 32000-1 [i.6], clause 12.8.3.3.2.

3) Optionally may include the "reasons" for the signature. This is embedded as signed attribute using `Reason` signature dictionary entry defined by ISO 32000-1 [i.6], clause 12.8.1.

4) Optionally may include the "location" of signing. This is embedded as signed attribute using `Location` signature dictionary entry defined by ISO 32000-1 [i.6], clause 12.8.1.

5) Optionally may include contact information of the signatory. This is embedded as signed attribute using `ContactInfo` signature dictionary entry defined by ISO 32000-1 [i.6], clause 12.8.1.

6) Optionally may include a "legal content attestation" to indicate to the relying party the PDF capabilities which may affect the signed document (e.g. JavaScript).

5.4.2 PAdES Part 3 and CAdES

Signatures profiled in PAdES Part 3 are encoded as certain forms of regular CAdES signatures, with further profiling. PAdES Part 3 may be functionally equivalent to CAdES-BES, CAdES-EPES, and CAdES-T, depending on the signed attributes included in the signature.

Below follows the list of attributes that may be incorporated or not to PAdES part 3 signatures.:

1) ESS `signing-certificate` or the ESS `signing-certificate-v2` CAdES signed attributes are used.
2) May optionally incorporate `signature-policy-identifier` CAdES signed attribute.
3) Is recommended to incorporate `signature-time-stamp` CAdES unsigned attribute.
4) Does NOT incorporate the `signing-time` CAdES signed attribute (instead the M entry in the signature dictionary is used).
5) Does NOT incorporate `content-reference` CAdES signed attribute. Instead, mechanisms provided by PDF syntax may be used.
6) Does NOT incorporate `content-identifier` CAdES signed attribute.
7) Does NOT incorporate `content-hints` CAdES signed attribute.
8) May optionally incorporate `commitment-type-indication` CAdES signed attribute (see 6.2 Implementing PAdES Part 3 for details of its optional usage).
9) Does NOT incorporate `signed-location` CAdES signed attribute. Instead, it uses the `Location` entry of the signature dictionary.
10) May optionally incorporate `signer-attributes` CAdES signed attribute.
11) May optionally incorporate `content-time-stamp` CAdES signed attribute.
12) Does NOT incorporate counter-signature CAdES unsigned attribute.

If a PAdES Part 3 neither incorporates the `signature-policy-identifier` nor `signature-time-stamp` CAdES unsigned attributes, then this is a PAdES-BES, which provides same semantics as CAdES-BES.

If a PAdES Part 3 incorporates the `signature-policy-identifier` CAdES unsigned attribute, then this is a PAdES-EPES, which provides same semantics as CAdES-EPES.

If a PAdES Part 3 incorporates the `signature-time-stamp` CAdES unsigned attribute, then this is a PAdES-T, which provides same semantics as CAdES-T. PAdES-T may be indistinctly built on PAdES-BES or PAdES-EPES.

5.4.3 PAdES Part 4 and CAdES

Signatures profiled in PAdES Part 4 include signatures encoded as regular CAdES signatures plus the PDF structures in charge of incorporating validation information (certificates path, certificates status information in the so-called Document Security Store –DSS, and time-stamps on the whole contents of the documents, in the so-called Document-Ttimestamp).

More specifically, PAdES Part 3 signatures are built on PAdES Part 3 signatures by adding the validation information PDF structures.

This means that a PAdES Part 4 signature, with one Document Security Store (that includes all the certificates and all the certificate status information data, i.e., CRLs and/or OCSP responses), and one Document Timestamp, contains certificates and certificate status values as recollected during the verification process, and a *document* Time-stamp that also Time-stamps these values. This provides functional equivalence to what is provided by CAdES-X-L signatures but also functional equivalence to CAdES-A (as the document time-stamp actually time-stamps everything in the document, including signature and validation data).

The PAdES-LTV profile as specified in part 4 without the document time-stamp provides an extended variation of CAdES-C (including certificate and certificate revocation values instead of reference).

NOTE: The reason for not dealing with references is that PDF defines a documental framework and that in foreseen use cases of signed PDF documents, each document has to be self-contained, and in consequence, if a PDF document contains a long term electronic signature, all the material required for its possible arbitration has to be in the document.

5.4.4 PAdES and XAdES (PAdES Part 5)

PAdES Part 5 specifies profiles for usage of regular XAdES signatures for dealing with signed XML content that is managed within the PDF framework in one of the two scenarios detailed in clause 5.3.2.

In the **XAdES-Signed-Object-And-PDF Packaged** scenario the signatures included within the packaged XML content are XAdES signatures. If additional validation has to be added in order to get more evolved XAdES forms, the signed object may be extracted from the PDF package, the XAdES signature may be evolved and the modified signed object may be embedded in a PDF file.

In the **XAdES-XFA-Signed** scenario, however, once theXAdES signature has been generated and included, if additional validation has to be added in order to get features of the more evolved XAdES forms, the original XAdES signature is combined with the aforementioned PDF structures that contain validation data (certificates, CRLs, OCSP responses) and document time-stamps.

5.4.5 PAdES Part 6

Unlike the other parts of PAdES, part 6 is not concerned the format of the electronic signatures within the PDF but how information about the signature should be visually represented. This considers two aspects of signature presentation, firstly the appearance of signatures within a PDF and secondly the representation of the PAdES signature verification.

When PAdES electronic signature is generated a visual representation of that signature can appear as part of the document (signature appearance). This signature appearance is added by the signatory at signing time. Although the signature appearance may be derived from the signature and its certificate there is no guarantee that it is for the same identity as the advanced electronic signature encoded within the document.

When a signed PDF document is received and viewed the PAdES signature is commonly verified. The results of the verification are commonly displayed to the human user, but this often this information is in a form relating to the technology used rather than in a way that the human user may understand.

PAdES Part 6 provides requirements and recommendation for the signature appearance and representation of signature verification so that it can be easily read by an untrained human user, whilst also providing in depth information needed for the forensic expert in the case of dispute. It also aims to provide consistency between the signature appearance added on signing and representation of signature verification to assist the human user in clearly identifying the use of fraudulent names in the signature appearance.

6 Implementing PAdES

6.1 Implementing PAdES Part 2

PAdES Part 2 is a profile of ISO 32000 (so PAdES signatures compliant with this part are in fact ISO 3200 signatures). As such, it adds constraints to ISO 32000. For instance, the PDF signature defined in this profile will be a DER-encoded PKCS#7 binary data object, which will be placed into the Contents entry of the signature dictionary; "old style" DER-encoded PKCS#1 binary data object is not allowed to be present in that entry.

While producing PAdES Part 2 as a profile of ISO 32000, the following criteria were agreed and used:

1) Recommendations made by ISO 32000 were preserved within PAdES Part 2.
2) Features of PDF signatures not defined in ISO 32000 are not included in PAdES Part 2, thereby ensuring compatibility with PDF readers based on this standard.
3) Certain optional features offered by ISO 32000 (as the aforementioned "old style" DER-encoded PKCS#1 binary data object) were dropped from PAdES Part 2.

6.1.1 Serial and Parallel signatures

PAdES Part 2 allows for the so-called "serial signatures". Serial signatures are those ones that actually sign signatures already applied to the document, so that a chain of signatures is produced. This is used in workflows where the signature of certain entity actually "entitles" the signature being signed. PAdES Part 2 serial signatures, in addition to the previous signatures applied to the document also sign the document itself.

PAdES Part 2 does not allow usage of parallel signatures, i.e. signatures each one signing the document excluding the other existing signatures.

6.1.2 Signature time-stamp

PAdES Part 2 recommends the use of a time-stamp on the signature (the so-called signature time-stamp) "as soon as possible after the signature is created so that the timestamp reflects the time at which the document was created". This time-stamp plays a double role: as a trusted indication of the time before which the signature was applied, and also as a mechanism that avoids repudiation of the signature by the signatory. The time-stamp proves that the signature existed at the given time as it includes a digest of the signature.

The signature time-stamp is embedded into the PDF signature as described in ISO 32000-1 [i.6], clause 12.8.3.3.1.

6.1.3 Revocation information at the time of signing

PAdES Part 2 recommends that the signatory validate the signing certificate and the revocation information and to embed the revocation information within the PAdES Part 2 before signing. This feature does allow the signer to provide information that may be used by the verifier to avoid having to obtain this information itself. This may be considered, however, to have inherent weakness as the source of revocation information is chosen by the signer not the party verifying the signature. Verifiers may ignore such a revocation information "in favour of alternative storage or referenced data as per its own policies".

The revocation information is included in the adbe-revocationInfoArchival signed attribute as described in ISO 32000-1 [i.6], clause 12.8.3.3.2.

6.1.4 Signature validation

A conforming signature handler will check validity at the time indicated either by the signature time-stamp if present or some other trusted indication of signing time.

A conforming signature handler may ignore any embedded revocation information in favour of alternative storage or referenced data as per its own policies.

6.2 Implementing PAdES Part 3

6.2.1 Features provided

PAdES Part 3 signatures actually may provide those features provided by SOME forms of CAdES, namely: CAdES-BES, CAdES-EPES and CAdES-T,. PAdES Part 2 features are listed below:

1) Protection of the signing certificate by the signature itself (the signing certificate digest is incorporated as part of a signed attribute to the signature). This allows to counter the certificate substitution attack.
2) Incorporation of additional information as signed attributes to the signature:
    a) Indication of the time when the signatory purportedly generated the signature (claimed signing time).
    b) Identification of the set of rules that govern the generation and verification of the signature (signature policy identifier).
    c) Reason for signing (reason).
    d) Commitment taken when signing (commitment type indication).

e) Indication of the purported place where the signatory signs the document (signer location).

f) Indication of the claimed role played by the signatory when signing or any claimed attribute that the signatory may have (Claimed signer attributes).

g) Time-stamp on the contents to be signed.

3) Incorporation of CAdES unsigned attributes, namely:

a) Signature-time-stamp.

6.2.2 PDF signature dictionary

PAdES Part 3 signatures are DER-encoded `SignedData` object as specified in CMS [i.13] included within the `Content` entry of the PDF signature dictionary (no ISO 32000-1 [i.6] specifications on this entry apply in PAdES Part 3).

The PDF signature dictionary `SubFilter` entry will be set to "`ETSI.CAdES.detached`".

The PDF signature dictionary does not include the `Cert` entry.

The byte range specified in the PDF signature dictionary will cover the entire file, including the signature dictionary but excluding the PDF signature itself.

6.2.3 PAdES Part 3, CAdES and incorporation of signed attributes

PAdES Part 3 signatures are encoded as CAdES signatures BUT NOT all the signed attributes providing the features listed in the clause above are actually encoded as CAdES signed attributes in these CAdES signatures.

ISO 32000 signatures also allow certain information to be added (in PDF syntax) before signing, which, by the way in which these signatures worked, were also signed, becoming as a matter of fact, a kind of "signed attributes" expressed in PDF syntax. Some of this information is semantically similar to some of the CAdES signed attributes. Below follows the list of such pieces of information:

1) Indication of the purported signing time.

2) Indication of the Reason/Commitment taken when signing.

3) Indication of the purported location where the signature was generated

PAdES Part 3 criteria for dealing with them is to keep the PDF way of doing things unless there are unavoidable requirements for using the CAdES attributes. This means that PAdES Part 3 signatures are CAdES signatures that:

1) Do not incorporate the attribute `signing-time` CAdES signed attribute but instead have the value of this time within the `M` entry of the signature dictionary.

2) Do not incorporate the `signer-location` CAdES signed attribute but instead have the indication of such location within the `Location` entry of the signature dictionary.

3) Incorporate the Reason entry in the signature dictionary for expressing the semantics of reason for signing. Additionally, if the `signature-policy-identifier` CAdES signed attribute is present, then the `commitment-type-indication` CAdES signed attribute may also be used (as there is a very strong relationship between Signature Policies as specified by ETSI and this CAdES attribute).

6.2.4 Signature Policy and ISO 32000 seed values

It is important not to confuse `signature-policy-identifier` signed attribute in PAdES Part 3 signatures with the "seed values" defined ISO 32000-1 [i.6], clause 12.7.4.5. While both bears similarities, seed values should only be viewed as workflow constraints for a given document, whereas signature policies should be viewed as general endorsement rules agreed upon by the signer and the verifier.

Both, seed values and signature policy enforce constraints at signing time. Signature policy rules actually enforce certain rules during the verification process; seed values do not.

PAdES Part 3 defines two new optional entries for the "signature field seed value dictionary " specified in ISO 32000-1 [i.6], namely:

1) SignaturePolicyOID, an ASCII string, for containing the OID of a signature policy to be used.
2) SignaturePolicyCommitmentType, an array of ASCII strings, for defining the commitment types that can be used within the signature policy identified by the OID present in SignaturePolicyOID entry. If SignaturePolicyOID entry is not present, this entry is ignored.

6.2.5 Signature validation

A relevant issue when verifying PAdES Part 3 signatures is determining the signature verification time. PAdES Part 3 specifies that the signature may be verified against a time other than the current time if all validation information required is known to have existed at that time. Otherwise these signatures will be verified at verifier's current time.

An informative note in PAdES Part 3 specification mentions that, if when the validation is performed at the trusted signing time, the validating application discovers that some certificate was valid at that time but has been revoked after that time, the validating application may raise a warning to the user.

Unsigned attributes other than the ones specified in PAdES Part 3 may be ignored by the verification application unless they are used in conjunction with other profiles which place requirements on their usage.

The handling of unsupported signed attributes is a matter of the verifier.

6.2.6 Time-stamp on signed content

CAdES specifies that `content-time-stamp` signed attribute protects the value of the `eContent` field. In the case of PAdES, where the signature is detached, `content-time-stamp` protects all the data being signed as identified by the ByteRange.

6.3 Implementing PAdES Part 4

PAdES Part 4 specifies how to incorporate long term capabilities in PAdES signatures: more specifically, this part assures that a PDF signature can still be verified long after (even years) it has been generated. For doing this, PAdES Part 4 specifies how to add information to a signed document to enable a verifier to securely repeat an initial verification, such as applied when first storing a document, when retrieving the stored document years later.

The techniques specified in PAdES Part 4 are applicable to both CAdES based PDF signatures specified in Parts 2 and 3 and XAdES based signatures applied to XFA content as specified in PAdES Part 5.

6.3.1 Achieving long term signatures in PAdES

PAdES long term signatures are achieved using the same principles as in XAdES and CAdES, namely by:

1) Defining two new PDF container objects for containing signature validation data and document time-stamp to the signed PDF document. These can be used to repeat that verification process and prove that at that time the signature was valid.
2) Incorporating in to the signature, when it has been verified, all the validation data that have been used for verification in one of the new PDF container objects (called Document Security Store –DSS henceforth). This includes certificates and material reporting the status of these certificates (CRLs, OCSP responses).
3) Time-stamping the whole signed document with the aforementioned validation data and incorporating such "document time-stamp" in the second new PDF container object (called Document Time-stamp). This proves that at that time, all the time-stamped validation material existed and so could be used for the signature verification.
4) Allowing in this way, new document time-stamp tokens to be repeatedly added over a period of time to protect the validity of the signature in the previous time-stamp token before its certificate expires.

Henceforth, the validation data and the document time-stamp tokens are generically denoted as Long Term Validation material (LTV material).

NOTE: PAdES Part 5 uses these new PDF container objects for LTV material, in its **XAdES-XFA-Signed** profile.

6.3.2 Rationale for the new PDF container objects

Both, XAdES and CAdES already had their own elements for achieving long term electronic signatures. PAdES Part 4 does not re-use such elements. This is due to limitations in the PDF signature structures not allowing extension to the space used to carry the original signature. A PDF signature, such as specified in part 2 or 3 of PAdES, is placed within the PDF structure, rather than at the end. And so the additional validation data and time-stamps cannot be added directly to the signature without potentially overrunning the space available.

Once the signature is inserted, it MAY NOT grow, which means that the incorporation of the LTV material can not be directly added to the CAdES structure within the Content entry: a new place is specified for this.

Similar arguments apply to the use of the new PDF container objects for LTV material in PAdES Part 5 **XAdES-XFA-Signed** profile.

6.3.3 New PDF container objects for LTV material

As mentioned before, PAdES Part 4 defines two new PDF container objects:

1) Document security store;
2) The Document Time-stamp.

The Document Security Store (DSS) consists of:

1) a so-called "DSS dictionary" which links to certificates and revocation information (CRLs or OCSP responses) applicable to ANY signature within the PDF document;
2) optionally, one or more than one "Validation Related Information (VRI) dictionaries" which links this validation data to SPECIFIC signatures (as many dictionaries as signatures if desired); and
3) the actual certificates and revocation (CRLs or OCSP responses) values.

The Document time-stamp is a regular PDF DSS dictionary specially profiled to indicate that the contained information is not a regular signature but a time-stamp token, bound to a document for providing an upper bound time at which the whole document (including any potential validation data) can be proven to exist.

6.3.3.1 The Document Security Store

The DSS dictionary contains links (indirect references in PDF terminology) to ALL the certificates, CRLs and OCSP responses (validation data) that have been collected by the verifying application (conforming signature handler in PAdES terminology) that may be used for verifying ANY signature in the PDF document.

The DSS also contains links to VRI (Validation Relation Information) dictionaries. Each VRI Dictionary is bound to one PAdES signature and at the same time provides a link to the validation data for that specific signature.

In consequence the DSS dictionary provides the path to ALL the validation data stored within the PDF signed document. The VRI Dictionary provides yet a path to validation data for a specific signature (which means that, as anticipated, there may be more than one PAdES signature within a PDF document). Conforming signature handlers wanting to repeat the validation process long after the signatures were generated will find in the VRI and DSS dictionaries their way to retrieve it.

When no VRI dictionaries appear and there are more than one PAdES signature in the PDF document, the conforming signature handler will have to find its way between all the validation data and decide what part of that material should be used to repeat the validation process for each signature.

If VRI dictionaries are present, the conforming signature handler, once ascertained the binding between a certain VRI dictionary and a certain PAdES signature, will use the validation material pointed by such VRI dictionary for verifying the signature.

In fact, the PDF document contains a pool of validation data that is pointed from different places: the DSS dictionary and optionally VRI dictionaries referencing validation data for specific signatures.

6.3.3.2 The Document Time-stamp

As its name indicates the Document time-stamp is a PDF dictionary that contains a time-stamp on the whole document, including the signature(s), and any validation data with the associated DSS and VRI dictionaries that may be present within it.

In fact this structure is a standard PDF signature dictionary structure with some specific small but relevant changes that actually indicate that what is present within the `Content` entry is not a regular signature but a RFC 3161 [i.17] time-stamp. More specifically, the `Type` key is set to "`DocTimeStamp`", and the `SubFilter` key is set to "`ETSI.RFC3161`". Additionally, entries with the following keys are not present in this structure: `Cert`, `Reference`, `Changes`, R, `Prop_AuthTime` and `Prop_AuthType`. The Document time-stamp is added at the end of the PDF file and time-stamps all the document except its own `Content` entry.

The document time-stamp binds the validation data to the rest of the PDF document, and provides proof that the whole document (including validation data) existed at the indicated time.

Being the Document time-stamp based in RFC 3161 [i.17], and being this type of time-stamps digital signatures, they suffer problems with time (expiration of certificates, weaknesses of algorithms, keys, etc.). This is the reason why, after certain time has passed since the first Document time-stamp has been added, a new Document time-stamp is added that secures the signature(s) and the former document time-stamp. This process is recurrently repeated as time goes on.

Whenever a new Document time-stamp is about to be added, conforming signature handlers collect all the validation material corresponding to the former Document time-stamp, and add it to the PDF document. Only once you have done that, the new Document time-stamp may be generated and added in a new DSS dictionary. In this way it is ensured that in the future any conforming signature handler will be able to repeat the processes that allow it validate the signature(s) and all the Document time-stamp(s) present in the PDF document.

An example will help to clarify this: assume that there exists a PDF document that is signed with two PAdES Part 3 signatures. The inner structure of the PDF could correspond to something like:

Initial_Document_ToBeSigned

SignatureDictionary_1

SignatureDictionary_2

Now this goes to a conforming signature handler that, after verifying collects all the validation material and, knowing that these electronic signatures need to be preserved during 5 years, generates something like:

Initial_Document_ToBeSigned

SignatureDictionary_1

SignatureDictionary_2

DSS (points to VRI_1, VRI_2 and all of Validation Data Pool)

VRI_1 (points to those elements of Validation Data required for verifying signature_1)

VRI_2 (points to those elements of Validation Data required for verifying signature_2)

Validation Data

Now the relaying party that has validated the signature requests and gets a time-stamp, which incorporates to the PDF document as a Document time-stamp:

Initial_Document_ToBeSigned

SignatureDictionary_1

SignatureDictionary_2

DSS (points to VRI_1, VRI_2 and Validation Data Pool)

VRI_1 (points to those elements of Validation Data required for verifying signature_1)

VRI_2 (points to those elements of Validation Data required for verifying signature_2)

Validation Data

Document_TimeStamp_1

After some time, a new Document time-stamp is added (because the expiration date of some certificate of those ones that have to be used for verifying the previous time-stamp is approaching or because some weakness has been discovered in some algorithm used in that time-stamp). The conforming signature handler will collect all the validation data of the previous Document time-stamp, add it to the PDF document and add the new Document time-stamp:

Initial_Document_ToBeSigned

SignatureDictionary_1

SignatureDictionary_2

DSS (points to VRI_1, VRI_2 and Validation Data Pool)

VRI_1 (points to those elements of Validation Data required for verifying signature_1)

VRI_2 (points to those elements of Validation Data required for verifying signature_2)

Validation Data

Document_TimeStamp_1

DSS (pointing to the validation data of Document_TimeStamp_1)

Validation Data (for Document_TimeStamp_1)

Document_TimeStamp_2

6.3.4 Signature Validation

PAdES Part 4 recommends starting validation of document time-stamps by the most recent one (last one). This one is validated at the current time with validation data collected at the current time. The document time-stamp next to the last one is validated at the time indicated by the last document time-stamp with all the validation data present in the previous DSS (going from outermost to innermost). This strategy is repeated for all the other "inner" document time-stamps: i.e., each one is validated at the time present in the subsequent document time-stamp, with the validation data present in the previous DSS. Finally the signature and the signature time-stamp are verified at the latest innermost document time-stamp with the validation data present in the signature's DSS.

NOTE: PAdES Part 2 recommends inclusion of validation material before signing. Under these circumstances, a verifier may verify the signature against the time indicated in the signature time-stamp, as the validation material included represented the status of the certificate at that time. PAdES Part 4 however, deals with situations where the validation material is added to the signature after the signing time, and in consequence it may not be used the time indicated in the signature time-stamp as verification time.

6.3.5 No references to validation material in PAdES Part 4

References to the validation material as specified in CAdES and XAdES (i.e. data structures containing, among other data, the digest of the validation material values), have NOT been incorporated in PAdES. It was agreed by majority that for the usual PDF usage scenarios, it would be more convenient NOT to manage such references, as this reduces the different ways PAdES is implemented, hence improving interoperability, and avoids the complexities in implementations particularly for efficient handling of failure cases when referenced data is not available.

6.4 Implementing PAdES Part 5

PAdES Part 5 specifies profiles for usage of regular XAdES signatures for dealing with signed XML content that is managed within the PDF framework in two specific scenarios detailed in PAdES Part 5 clause 5.3.2.

In the **XAdES-Signed-Object-And-PDF Packaged** scenario the signatures included within the packaged XML content are XAdES signatures. If additional validation has to be added in order to get more evolved XAdES forms, the signed object may be extracted from the PDF package, the XAdES signature may be evolved and the modified signed object may be embedded in a PDF file.

In the **XAdES-XFA-Signed** scenario, however, once theXAdES signature has been generated and included, if additional validation has to be added in order to get features of the more evolved XAdES forms, the original XAdES signature is combined with the aforementioned PDF structures that contain validation data (certificates, CRLs, OCSP responses) and document time-stamps.

6.4.1 Implementing Profiles for XAdES-signed XML documents embedded in PDF containers

The starting point for these two profiles is an arbitrary XML document signed with one or more XAdES signatures. This document may have been created independently from any PDF framework.

The first profile (called Basic Profile) specifies requirements for embedding such a XAdES-signed XML document within a PDF file, when the XAdES signatures are XAdES-BES, XAdES-EPES or XAdES-T.

The second profile (called Long Term Profile) specify requirements for evolving XAdES signatures compliant with the aforementioned Basic Profile towards long term XAdES signatures.

6.4.1.1 Implementing Basic Profile

6.4.1.1.1 Serial and Parallel signatures

This profile allows for both serial and parallel signatures.

6.4.1.1.2 XAdES signed XML documents to be embedded

Any XAdES-signed XML document that embeds all the data objects signed by the XAdES signatures may be embedded within a PDF document aligned with this profile. Alternatively, if the XAdES-signed XML document does not embed all the signed data objects the corresponding XAdES signatures will include valid `ds:Reference` elements for correctly retrieving such data objects.

6.4.1.1.3 XAdES properties

This profile allows for the inclusion of a number of XAdES properties as summarized below:

1. It recommends to protect the signing certificate by inclusion of `the xades:SigningCertificate` signed property.
2. It allows to include the following optional XAdES signed properties with the semantics and usage as specified in XAdES [i.4]: `xades:SigningTime`, `xades:SignaturePolicyIdentifier`, `xades:SignatureProductionPlace`, `xades:SignerRole`, `xades:SignedDataObjectFormat`, `xades:CommitmentTypeIndication`, `xades:AllDataObjectsTimeStamp`, `xades:IndividualDataObjectsTimeStamp`.
3. It allows to include the `xades:SignatureTimeStamp` unsigned property to the signature.
4. It provides support for serial signatures by any of the two mechanisms specified by XAdES [i.4], i.e. adding the xades:CounterSignature unsigned property or by using a detached XAdES signatures which includes a ds:Reference (which contains a Type attribute set to `http://uri.etsi.org/01903#CountersignedSignature`) referencing the original signature.
5. It provides support for parallel signatures as long as all the XAdES signatures are embedded within the XAdES-signed XML document.

6.4.1.1.4 Signing the embedding PDF document

Implementers should be aware that any approval signature (see ISO 32000-1 [i.6] clause 12.8.1) as specified in TS 102 778-2 [i.8], TS 102 778-3 [i.9] or TS 102 778-4 [i.10], applied to the embedding PDF document 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 [i.6] clause 12.8.1) as specified in TS 102 778-2 [i.8], TS 102 778-3 [i.9] or TS 102 778-4 [i.10] signing the embedded signed XML document, may be used in conjunction with the DocMDP (Modification, Detection and Prevention) feature, allowing changes in the embedded signed XML document (by upgrading the XAdES signatures, for example) without invalidating such signatures.

6.4.1.2 Implementing Long Term Profile

This profile allows for upgrading the XAdES signatures present within the XML document embedded within the PDF document.

This upgrade requires extraction of the XAdES-signed embedded XML document, regular upgrade of XAdES signatures by incorporation of any of the unsigned properties specified in XAdES [i.4] for such purpose, and embedding of the modified XML document within the PDF document.

This profile does not impose any restriction of the XAdES unsigned properties that may be added to the original XAdES signatures. Whenever one of these properties is added, its syntax, semantics and usage will be as specified in XAdES [i.4].

6.4.1.2.1 Signature Validation

This profile recommends that the validation of the most recent (last one) `xades:ArchiveTimeStamp` (or `xadesv141:ArchiveTimeStamp`) is carried out at the current time with validation data collected at the current time. The `xades:ArchiveTimeStamp` next to the last one is validated at the time indicated by the last `xades:ArchiveTimeStamp` (or `xadesv141:ArchiveTimeStamp`) with the validation data present in that property or within the previous (going from outermost to innermost) `xadesv141:TimeStampValidationData` property. This strategy is repeated for all the other `xades:ArchiveTimeStamp` (or `xadesv141:ArchiveTimeStamp`) elements.

The profile also recommends to validate any present time-stamp contained in `xades:SigAndRefsTimeStamp` or `xades:RefsOnlyTimeStamp` at the latest innermost xades:ArchiveTimeStamp (or `xadesv141:ArchiveTimeStamp`) time using the validation data stored present in that property or within the previous (going from outermost to innermost) `xadesv141:TimeStampValidationData` property.

Finally, the profile recommends to validate the signature and the signature time-stamp at the time indicated in the time-stamp present within `xades:SigAndRefsTimeStamp` or `xades:RefsOnlyTimeStamp` or the latest innermost `xades:ArchiveTimeStamp` (or `xadesv141:ArchiveTimeStamp`) element if none of the two previous elements is present.

6.4.2 Implementing Profile for XAdES signatures on XFA forms

PAdES Part 5 defines two profiles for signing XFA dynamic forms, 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 TS 102 778-4 [i.10] to achieve equivalent functionality to XAdES-XL and XAdES-A forms.

These profiles can be used for signing only the XML data of XFA dynamic forms or for signing any XML content of XFA dynamic forms.

6.4.2.1 Implementing Basic Profile

Signatures aligned with this profile are encoded as XAdES-BES, XAdES-EPES or XAdES-T signatures.

6.4.2.1.1 Signing the signed properties

Signatures aligned with this profile sign the `xades:SignedProperties` element and the `ds:SignatureProperties` element, which includes the claiming signing time and the reasons for signing as specified by XFA [i.1].

6.4.2.1.2 Serial and Parallel signatures

This profile allows for both serial and parallel signatures using the standard mechanisms of XAdES. Any of the two mechanisms for serial signatures specified within XAdES may be used.

6.4.2.1.3 XAdES properties

This profile allows for the inclusion of a number of XAdES properties as summarized below:

1. It recommends to protect the signing certificate by inclusion of `the xades:SigningCertificate` signed property.
2. It allows the usage of `xades:SignaturePolicyIdentifier` signed property.
3. It allows the usage of `xades:SignatureProductionPlace` signed property.
4. It allows the usage of `xades:SignerRole` signed property.
5. It allows the usage of `xades:SignedDataObjectFormat` signed property.
6. It allows the usage of `xades:CommitmentTypeIndication` signed property if the signature also contains the `xades:SignaturePolicyIdentifier` signed property. If this property is not present, the signature will include the `description` element within the `ds:SignatureProperties` element.
7. It allows the usage of `xades:AllDataObjectsTimeStamp` signed property.
8. It allows the usage of `xades:IndividualDataObjectsTimeStamp` signed property.
9. It recommends the usage of `xades:SignatureTimeStamp` unsigned property.

This profile bans the inclusion of certain XAdES properties as summarized below:

1. It does not allow the usage of `xades:SigningTime`, as XFA [i.1] already imposes the usage of `CreateDate` element with identical semantics within the `ds:SignatureProperties` element.

6.4.2.2 Implementing Long Term Profile

This profile provides a means for maintaining the validity of the signatures on XFA dynamic forms over extended periods using the LTV techniques specified in PAdES Part 4 annex A.

Signatures aligned with this profile are encoded as XAdES-BES, XAdES-EPES or XAdES-T signatures, which are complemented with LTV PDF objects.

6.4.2.2.1 DSS Dictionary

For building DSS' VRI entry (which contains the base-16-encoded SHA1 digest of the signature referenced), the `ds:Signature` element is canonicalized using exclusive canonicalization (`http://www.w3.org/2001/10/xml-exc-c14n#`) .

6.4.2.2.2 Validation process

PAdES Part 5 recommends the following validation process for signatures aligned with this profile:

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)

6.5 Implementing PAdES Part 6

PAdES Part 6 specifies how to design a signature appearance and how to display the verification results to maximize the consistency between the signature appearance and the representation of the signature verification.

The requirements and recommendations for a conforming implementation can be divided into two sets: Implementing the creation of a signature appearance and implementing the representation of signature verification. Both sets of requirements aim at a common goal: To have a similar visual representation of the signature appearance and the verification result, in the common case that the signature appearance identifies the true signer of the document.

Specifications should refer to this document in order to streamline document exchange workflows that include signature appearances, keeping in mind that security targets are still met by the electronic signatures itself.

6.5.1 Content of signature appearance

PAdES Part 6 tries to take advantage of the certificate images defined in an IETF Draft. This lets the certificate issuer link images that represent the identity of the signatory to its own certifying signature, providing a trusted source for a visual representation of the signers identity.

Certificate images may not be available either because this extension was not used by the certificate issuer or because the certificate image is only referenced by the certificate and is temporarily not available from a remote source during signing time. In both cases a well defined set of other information from the certificate should be included, to identify a signer in a way consistent to the signature verification. This set will always include the common name of the signer that is included in the CN attribute of the user certificate. In most cases it will also contain the affiliation of the signer, that is found in the Organization field (O) of the certificate. The signers organization may be omitted in use-cases where it is not relevant. If logo images from RFC 3709 [i.14] or images of handwritten signatures as defined as biometric information in RFC 3739 [i.15] are used as extensions off the signers certificate, they should also be included into the signature appearance.

The use of this images in certificates is recommended by this profile, as they ensure an exact visual match between signature appearance and the signature verification representation.

6.5.2 Encoding of the signature appearance

There are some requirements on the encoding of the signature appearance that have an direct impact on the format of the PDF document that contains the signature. Conformance to most of this requirement could be tested in an automated way. These requirements are necessary to make the signature appearance visible inside a conforming reader according to ISO 32000.

There could be existing implementation that create signature appearances using multiple content streams for the signature appearance, that are intended to be displayed for different outcomes of the signature verification. This feature is deprecated by this profile and a conforming implementations should take care not using this feature.

Conformance to this requirements is also necessary but not sufficient to conform to PDF/A-1.

6.5.3 Implementing signature verification representation

When a conforming reader displays a PDF document that contains electronic signature to a user, it may validate this signatures and display the results of the verification to the user as well. In many use-cases this signature verification representation is required to be user-friendly and to fulfil certain legal requirements at the same time.

In a graphical user interface the visual representation of a signature verification is to be displayed in a frame or window different from the display of the page content. It is important that the display is separated from the page display in a way understandable to the untrained user and a way that can not be mocked by active content of the PDF document.

The representation of the signature verification should be done in a hierarchical way. An example could be a tree widget in a graphical user interface or a window with basic information that features links that display detailed information upon interaction by the user.

The basic information about any AdES will consist at the top level of two parts. The result of the signature verification and the identity of the signer. For a valid signature the first is intended to inform the user about the exact signed data or about the reasons if the verification does not validate the signature. The second is bound to be similar to a signature appearance by requirements of the standard. In the best case the signer certificate refers to a certificate image that was also used in the signature appearance, in which case this image is displayed. Without a certificate image available, information about the signer is displayed mostly in text form. If there is an option an implementation may stress the similarity to the signature appearance further by choosing matching layout and fonts as used in the signature appearance.

a) Name of signatory (as in CN).

b) The affiliation of signatory (as in O) is displayed in any case. This is unlike the signature appearance, but the verifier can not determine if the organization in the certificate ifs relevant to the signature or not.

c) Any logo image in the signatories certificate (as defined in RFC 3709 [i.14]).

d) Any image of a handwritten signature in certificate (as defined in RFC 3739 [i.15], section 3.2.5).

e) The identity of the trusted CA which is used as the basis for certificate path validation. This may be in the form of a "friendly name" which is configured for the conformant reader or information derived from the issuer name (e.g. using the O field). This information is normally not part of the signature appearance, to avoid confusion by an occasional mismatch between both representations. There is currently no common way to display the name of the certificate issuer in an user friendly way.

The detailed information can be split about several more levels, and documents all information used when validating the signature. The information used to verify the signature typical contains other electronic signatures, like time-stamps and OCSP-Responses. These signatures should be displayed in a similar way to the users signature.

As an example the representation of these details may created from on a verification report as defined in the OASIS Profile for Comprehensive Multi-signature Verification Reports [i.5].

History

Document history		
V1.1.1	July 2010	Publication