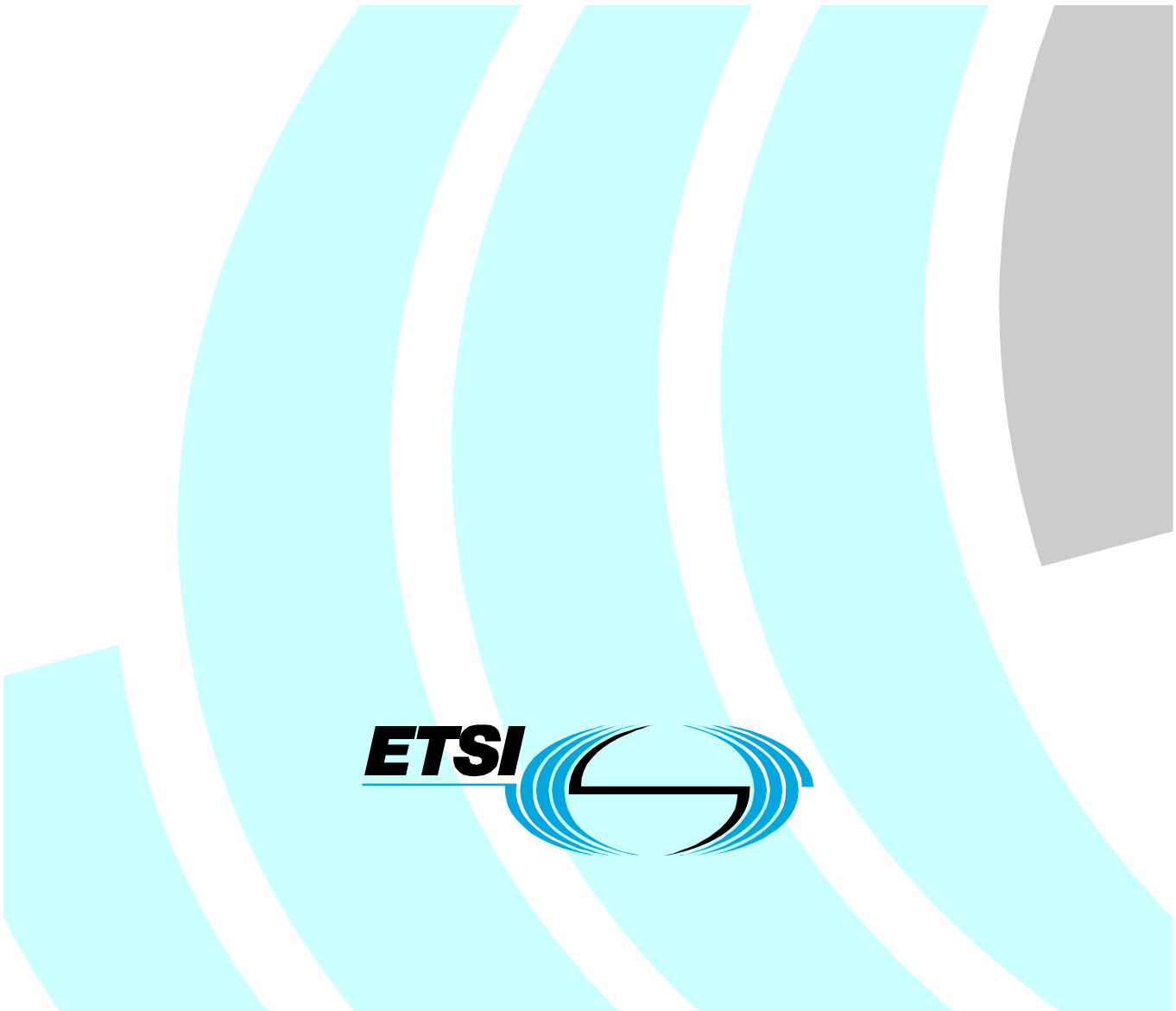
ETSI TS 102 778 V1.1.1 (2009-04)

Technical Specification

Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; CMS Profile based on ISO 32000-1



Reference
DTS/ESI-000063

Keywords
e-commerce, electronic signature, security

ETSI

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

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

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

Contents

Intellectual Property Rights

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

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

Foreword

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

Introduction

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

Clause 12.8 of ISO 32000-1 identifies the ways in which a digital signature may be used to authenticate the identity of a user and the accuracy of the document's content. These digital signatures are based on the same CMS [i.2] technology and techniques as TS 101 733 [i.1] (CAdES), but without the extensions defined in CAdES for the purposes of long term validation.

The present document defines the first of a series of profiles that describe how digital signatures in PDF can be used in a way that provide an Advanced Electronic Signature framework for the signing of electronic documents in PDF format.

Therefore the following provisions represent a general consensus of the use of these standards and hence provide a reliable basis for maximizing interoperability. Nevertheless, in particular business areas and niches there may be specific needs and/or regulations that may require variations to these profiles.

1 Scope

The present document profiles the use of PDF signatures, as described in ISO 32000-1 [1] and based on CMS [i.2], for its use in any application areas where PDF is the appropriate technology for exchange of digital documents including interactive forms. Further profiles in this series will specify additional features which add to the non-repudiation and long-term validation properties of PDF Signatures.

This profile does not repeat the base requirements of the referenced standards, but instead aims to maximize interoperability of CMS-based electronic signatures in various business areas. Clause 4 provides a general informative description of the profile, while clause 5 specifies the normative conformance requirements of this profile.

2 References

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

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

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

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

2.1 Normative references

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

[1] ISO 32000-1 (2008): "Document Management - Portable Document Format - PDF 1.7".

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

[3] ITU-T Recommendation X.509 / ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[4] IETF RFC 3280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[5] IETF RFC 2560: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

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

[7] ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

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

2.2 Informative references

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

[i.1] ETSI TS 101 733 (V1.7.4): "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[i.2] IETF RFC 3852: "Cryptographic Message Syntax (CMS)".

[i.3] IETF RFC 3281: "An Internet Attribute Certificate Profile for Authorization".

3 Definitions and abbreviations

3.1 Definitions

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

NOTE: The words "may", "shall" and "should" are used in the present document as keywords to signify requirements.

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

conforming reader: software application that is able to read and process PDF files that have been made in conformance with ISO 32000-1 [1]

may: means that a course of action is permissible within this 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: DER-encoded PKCS#7 binary data object containing a digital signature and other information necessary to verify the digital signature such as the signer's certificate along with any supplied revocation information

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

shall: means that the definition is an absolute requirement of this profile and it has to strictly be followed in order to conform to the present document

should: means that among several possibilities one is recommended, in this 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 must be understood and carefully weighed before choosing a different course.

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

3.2 Abbreviations

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

CAdES CMS Advanced Electronic Signatures

NOTE: As per TS 101 733 [i.1].

CMS Cryptographic Message Syntax
CRL Certificate Revocation List
MDP Modification Detection Permissions
OCSP Online Certificate Status Protocol
PDF Portable Document Format

4 Description of Profile for CMS signatures in PDF

4.1 Introduction

This profile specifies a PDF signature as specified in ISO 32000-1:2008 [1] that enables greater interoperability for PDF signatures by providing additional restrictions beyond those of ISO 32000-1 [1].

4.2 Features

Signature encoded in CMS as defined by PKCS #7 1.5 (RFC 2315 [2]).

Supports serial signatures.

Optionally includes signature time-stamp.

Optionally includes revocation information.

Signature protects integrity of the document and authenticates the signatory.

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

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

Signature can optionally include contact info of the signatory.

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

4.3 PDF signatures

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

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

NOTE 1: This makes normative a recommendation in ISO 32000-1 [1], clause 12.8.1.

NOTE 2: By restricting the ByteRange entry this way, it ensures that there are no bytes in the PDF that are not covered by the digest, other than the PDF signature itself.

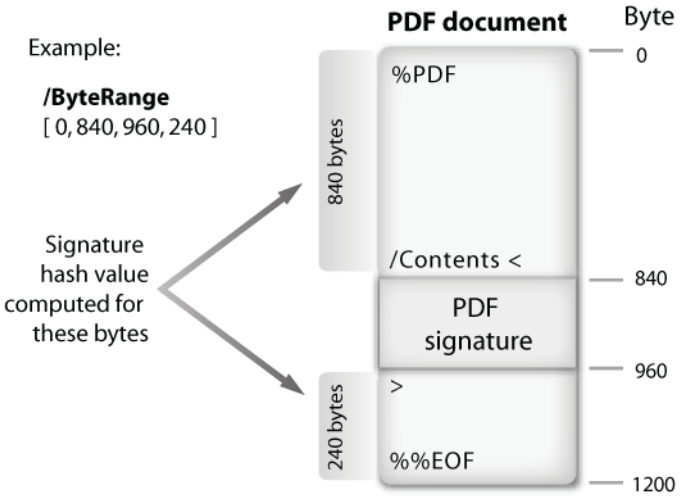


Figure 1

The PDF Signature (a DER-encoded PKCS#7 binary data object) shall be placed into the **Contents** entry of the signature dictionary. The PKCS#7 object shall conform to the PKCS#7 specification in RFC 2315 [2]. At minimum, it shall include the signer's X.509 [3] signing certificate.

NOTE 3: Although ISO 32000-1 [1] also allows the value of the **Contents** entry of signature dictionary to be a DER-encoded PKCS#1 binary data object, that format does not conform with this profile.

NOTE 4: The size of the **Contents** entry is computed based on a best guess of the maximum size needed to contain the PDF signature and any addition revocation and timestamping information. The contents of the string is first written to disk as a series of 0x00 hex values and later filled in with the actual contents.

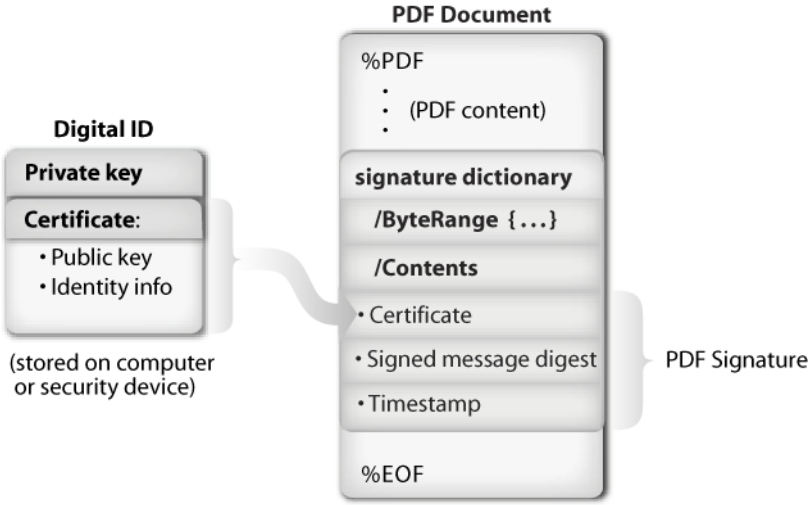


Figure 2

As recommended by ISO 32000-1 [1], clause 12.8.3.3.1, timestamping and revocation information should be included in order to improve the long-term non-repudiation properties of the signature. This revocation information and as much of the complete chain of certificates, as is available, shall be captured and validated before completing the creation of the PDF Signature. In addition, the revocation information shall be a signed attribute of the PDF Signature.

NOTE 5: The above requirements for PDF signatures differ from the behaviour of other CMS-based electronic signature solutions.

ISO 32000-1 [1] allows the inclusion of one or more RFC 3281 [i.3] attribute certificates to be associated with the signer certificate. However, their use is not recommended as attribute certificates are not widely supported and hence use of this attribute will reduce interoperability.

NOTE 6: A conforming reader is not required to process any attribute certificates.

4.4 Signature types

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

Finally, PDF uses signatures in a 3rd way (Usage Rights, ISO 32000-1 [1], clause 12.8.2.3) which is to enhance a document with additional rights and privileges in a particular workflow, using the signature to ensure that the document and rights have not been tampered with in any way.

4.5 Handlers

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

NOTE 1: A conforming reader may substitute a different signature handler when verifying the signature, as long as it supports the specified SubFilter format.

However, ISO 32000-1 [1] permits values for **Filter** and **SubFilter** other than those documented. As such, the details of any **SubFilter** that is not documented in ISO 32000-1 [1] is unknown. Since there can be no guarantee that these non-documented implementations meet the requirements of this profile, only the two values for **SubFilter** listed in ISO 32000-1 [1], clause 12.8.3.3.1 (i.e. **adbe.pkcs7.detached** and **adbe.pkcs7.sha1**) shall be used in order to comply with this profile.

NOTE 2: While the names of the SubFilters may imply specific algorithms, the actual list of supported algorithms that can be used can be found in ISO 32000-1 [1], clause 12.8.3.3.2, table 257. Consult TS 102 176-1 [7] for guidance on algorithm choices.

NOTE 3: The use of SHA-1 is being phased out in some countries and hence use of other hashing algorithms is recommended.

4.6 PDF serial signatures

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

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

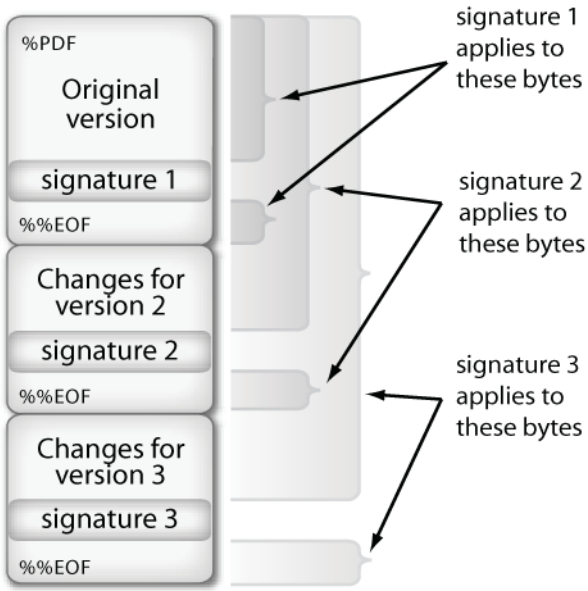


Figure 3

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

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

4.7 Signature validation

When the user opens a signed document and requests verification of the signature(s) present in the PDF, a conforming reader shall perform the following steps to verify them.

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

2) Validate the path of certificates used to verify the binding between the subject distinguished name and subject public key as specified in RFC 3280 [4]. The validity checks shall be carried out at the time indicated either by time-stamp applied as per clause 4.8 or some other trusted indication of the signing time. The revocation status shall be checked as specified in clause 4.9.

4.8 Time stamping

When a digital signature is applied to a document, a conforming reader may choose to stamp it with the signer's local machine time, and that is what may appear in the signature appearance. Because a user can set that time forward or back on their computer, that time is usually not trusted. Therefore a timestamp from a trusted timestamp server should instead be applied on the digital signature as soon as possible after the signature is created so the timestamp reflects the time at which the document was signed. A conforming reader that is signing a document should be sure that no other user actions take place between the creation of the signature and obtaining the timestamp. Timestamps fulfil a critical need in the validation process: if a conforming reader validates and timestamps the signature using a trusted timestamp server then the signer cannot later claim that it was signed by someone else, that the document was altered after they signed it, or that it was signed at another time.

The process for timestamping a digital signature is described in RFC 3161 [6]. If a conforming reader chooses to embed a timestamp into the PDF Signature, then it shall be embedded as described in ISO 32000-1 [1], clause 12.8.3.3.1.

4.9 Revocation checking

A conforming reader should embed the revocation information with the signature to save time when the signature is verified by the recipient. In addition, the inclusion of the revocation information protects against some threats relating to use of previously revoked certificates which affect the non-repudiation properties of the signature. If the revocation information is to be included in the PDF Signature, then it should be captured and validated before completing the creation of the PDF Signature (clause 4.3).

NOTE ISO 32000-1 [1], clause 12.8.3.3.2 describes the adbe-revocationInfoArchival attribute that should be used, as a signed attribute, to include this information into the PDF Signature.

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

To check the revocation status, a conforming reader may use either (or both) of the following methods:

- Certificate Revocation List (CRL) [4] is one common method that public key infrastructures use to maintain access to networked servers. With CRL, the certificate is checked against a list of revoked certificates. In addition to the certificate issue date and the issuing entities, the list specifies revoked certificates as well as the reasons for revocation.
- Online Certificate Status Protocol (OCSP) [5] defines a protocol for obtaining the revocation status of a given certificate from a server.

4.10 Seed values and signature policies

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

A **seed value dictionary** (ISO 32000-1 [1], clause 12.7.4.5, table 234) contains information that conveys a set of rules (or policies) that the form's author wishes the conforming reader to enforce at the time the signature is applied. These wishes can be specified either as requirements or recommendations. These seed values perform a similar function as the signature policies specified in TS 101 733 [i.1].

Common uses for seed values are to specify digest methods, revocation information, timestamping authorities and certificate attributes. Seed values that would require a conforming reader to violate this profile shall not be used.

EXAMPLE: Use of a seed value that specifies the use of PKCS#1 instead of PKCS#7 would not be permitted by this profile.

Because the seed values are part of the PDF data structures, they are covered by any signatures that are applied to the document.

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

PDF/A-1 [8] is a subset of PDF that enables reliable long term archiving of digital content in PDF format. It does so by tightening the normative requirements of the PDF file structure, requiring the inclusion of all required resources (such as fonts and images) and by restricting the use of interactive content and scripting facilities (i.e. JavaScript).

NOTE: Because the conversion of most PDF documents to PDF/A requires modification of the file, it is recommended to convert the document to PDF/A before applying a digital signature.

As PDF/A-1 is based on Adobe PDF 1.4 and not on ISO 32000-1 [1], it does not fully support all of its features available to digital signatures - specifically lacking are embedded revocation information and timestamping. However, since such features are not explicitly forbidden there is nothing that prevents a PDF/A-1 conforming writer from putting these extended features into a file - but there should be no expectation that a conforming PDF/A-1 reader will process them accordingly. A conforming PDF/A-1 reader is, however, free to implement functionality beyond that specified in PDF/A-1.

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

5 Requirements of profile for CMS signatures in PDF

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

5.1 Requirements from clause 4.3 (PDF signatures)

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

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

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

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

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

f) Use of RFC 3281 [i.3] attribute certificates associated with the signer certificate is not recommended.

5.2 Requirements from clause 4.5 (handlers)

a) Only the two values for **SubFilter** listed in ISO 32000-1 [1], clause 12.8.3.3.1 (i.e. **adbe.pkcs7.detached** and **adbe.pkcs7.sha1**) shall be used in order to comply with this profile.

5.3 Requirements from clause 4.6 (PDF serial signatures)

a) There shall only be a single signer (e.g. a single "SignerInfo" structure) in any PDF Signature.

5.4 Requirements from clause 4.7 (signature validation)

a) When the user opens a signed document and requests verification of the signature(s) present in the PDF, a conforming reader shall perform the steps listed in clause 4.7.

5.5 Requirements from clause 4.8 (time stamping)

a) A timestamp from a trusted timestamp server should be applied on the digital signature immediately after the signature is created so the timestamp reflects the time at which the document was signed.

b) If a conforming reader chooses to embed a timestamp into the PDF Signature, then it shall be embedded as described in ISO 32000-1 [1], clause 12.8.3.3.1.

5.6 Requirements from clause 4.9 (revocation checking)

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

5.7 Requirements from clause 4.10 (seed values and signature policies)

a) Seed values that would require a conforming reader to violate this profile shall not be used.

History

Document history		
V1.1.1	April 2009	Publication