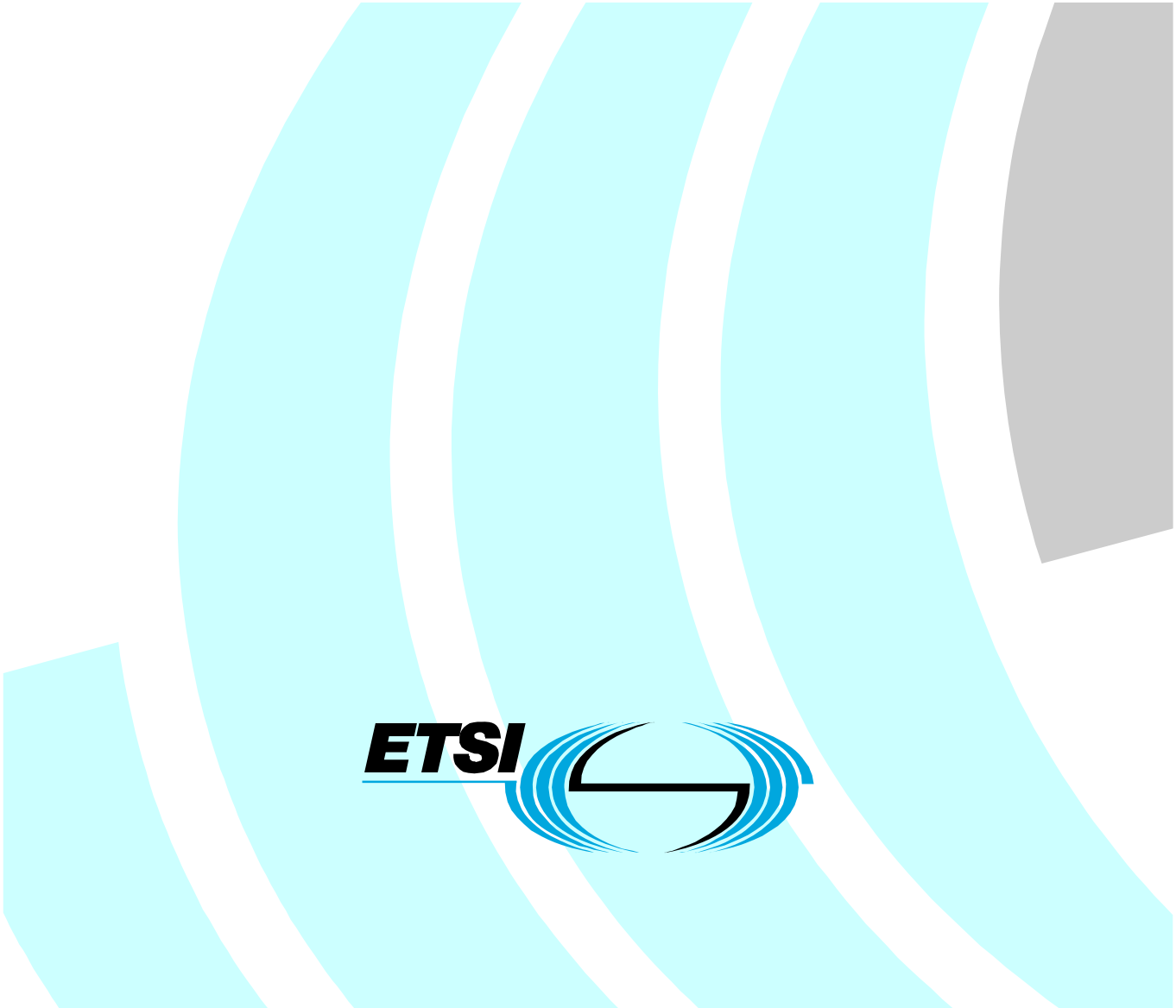
ETSI TS 102 778-4 V1.1.1 (2009-07)

Technical Specification

Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile



Reference
DTS/ESI-000072-4

Keywords
e-commerce, electronic signature, security

ETSI

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

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

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

Contents

Intellectual Property Rights

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

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

Foreword

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

The present document is part 4 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.3].

Introduction

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

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

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

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

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

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

ISO 32000-1 [1] identifies the ways in which an electronic signature, in the form of a digital signature, may be incorporated into a PDF document to authenticate the identity of the user and validate integrity of the document's content. This profile specifies digital signatures in PDF to provide Advanced Electronic Signature with long term validation equivalent to the, CAdES-X-Long and CAdES-A forms.

1 Scope

The present document profiles the electronic signature formats found in ISO 32000-1 [1] to support Long Term Validation (LTV) of PDF Signatures. This profile does not repeat the base requirements of the referenced standards, but instead aims to disambiguate between the techniques used in the different referenced standards.

The present document specifies how to include validation information in a PDF Document and to further protect the document using time-stamps so that it is possible to subsequently verify a PDF Signature long after it was signed. This profile may be used to support long term validation of:

a) PDF Signatures to profiles specified in TS 102 778-2 [i.4]; or

b) PDF Signatures to profiles specified in TS 102 778-3 [i.5]; or

c) PDF Signatures to profiles specified in TS 102 778-5 [i.6].

The present document specifies a profile to support the equivalent functionality to the signature forms CAdES-X Long and CAdES-A as specified in TS 101 733 [2] in a single profile PAdES-LTV (see annex B for further information on matching this profile to CAdES signature forms).

The same LTV mechanism specified in this profile is used to support the equivalent to all the signature forms XAdES-XL and XAdES-A as specified in TS 101 903 [3], by upgrading XAdES signatures aligned with the profile defined in clause 5.2 of TS 102 778-5 [i.6] (see annex A of TS 102 778-5 [i.6] for further information on matching this profile to XAdES signature forms).

The present document also specifies extensions to ISO 32000-1 [1] to provides features required to support LTV (see annex A).

NOTE: It is planned to submit these extensions to ISO as a proposal for a revision to ISO 32000-1 [1]. If accepted, future versions of this profile may reference any future ISO standard instead of the extensions specified in annex A.

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

The present document is part of a series of profiles for advanced electronic signature formats applied to PDF documents. General information on the series of profiles is specified in TS 102 778-1 [i.3].

The requirements specified in the present document take precedence over those specified in ISO 32000-1 [1].

2 References

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

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

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

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

2.1 Normative references

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

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

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

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

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

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

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

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

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

[9] W3C Recommendation (18 July 2002): "Exclusive XML Canonicalization Version 1.0".

NOTE: Available at http://www.w3.org/TR/xml-exc-c14n/#

2.2 Informative references

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

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

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

[i.3] 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.4] 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.5] 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.6] 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".

3 Definitions and abbreviations

3.1 Definitions

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

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

Document Security Store (DSS): information appended to a PDF document relating to its security including Validation-Related Information (VRI) and indirect references to the values of validation data for all signatures

document time-stamp: time-stamp applied to a document along with any document security-related information applied to that document

PDF Signature: a binary data object based on the PKCS#7 (see RFC 2315 [4]) or related syntax containing a digital signature placed within a PDF document structure as specified in ISO 32000-1 [1], clause 12.8 with other information about the signature applied when it was first created

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

Validation Related Information (VRI): indirect references to validation data used to validate a specific signature

verifier: entity that validates an electronic signature

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

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

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

3.2 Abbreviations

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

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

NOTE: As specified in RFC 3852 [5].

CRL	Certificate Revocation List
DSS	Document Security Store
EPES	Explicit Policy-based Electronic Signature
GSM	Global System for Mobile Telecommunications
LTV	Long Term Validation
OCSP	Online Certificate Status Protocol

PAdES	PDF Advanced Electronic Signature
PAdES-LTV	PAdES Long Term Validation
PDF	Portable Document Format
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
VRI	Validation Related Information
XADES	XML Advanced Electronic Signatures
XFA	XML Forms Architecture

4 Profile for PAdES-LTV

4.1 Overview

Validation of an electronic signature requires data to validate the signature such as CA certificates, Certificate Revocation List (CRLs) or Certificate status information (OCSP) commonly provided by an online service (referred to in the present document as validation data). If the document is stored and the signatures are to be verifiable long after first created, in particular after the signing certificate has expired, the original validation data may no longer available or there may uncertainty as to what validation data was used when the document was first verified.

Also, the cryptographic protection afforded by the signature may not be guaranteed after the certificate has expired.

This profile uses an extension to ISO 32000-1 [1] called Document Security Store (DSS) to carry such validation data as necessary to validate a signature, optionally with Validation Related Information (VRI) which relates the validation data to a specific signature (see clause A.1). The structure of DSS and VRI is illustrated in figure 1.

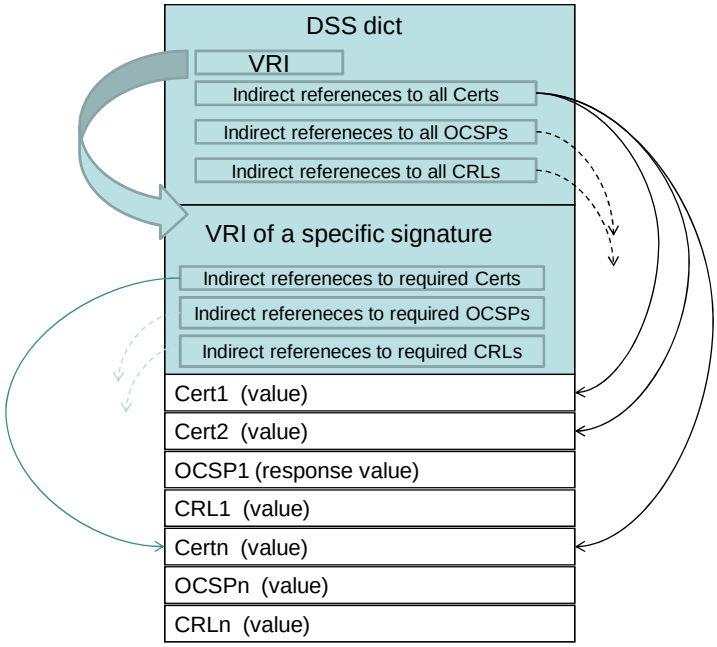


Figure 1: Illustration of DSS and VRI Structures

This profile also uses another extension to ISO 32000-1 [1] called Document Time-stamp (see clause A.2) to extend the life-time of protection to the document. The Document Time-stamp also protects the DSS binding it to the document to which it applies. The Document Time-stamp also protects the DSS by binding it to the document to which it applies. Furthermore, because the DSS is collected, and the signature first verified, at a time before the time indicated in the first Document Time-stamp, this indicated time can be used as the assumed signing time in a re-verification using the protected validation data from the DSS.

The structure of a PDF document to which LTV is applied is illustrated in figure 2.

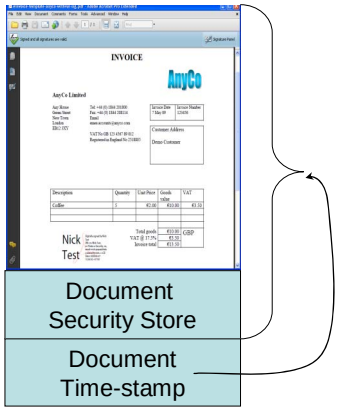


Figure 2: Illustration of PDF Document with LTV

The life-time of the protection can be further extended beyond the life-of the last document Time-stamp applied by adding further DSS information to validate the previous last document Time-stamp along with a new document Time-stamp. This is illustrated in figure 3.

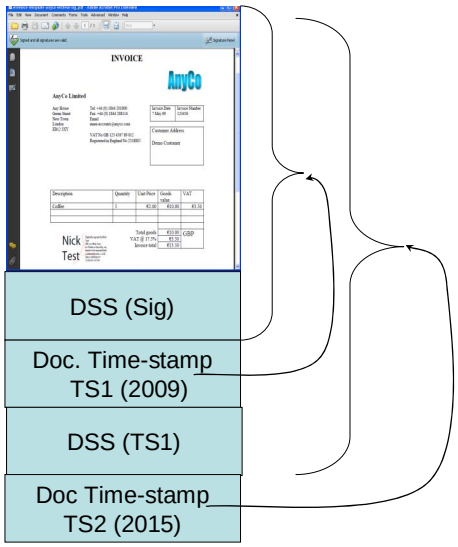


Figure 3: Illustration of PDF Document with repeated LTV

This profile is based on extensions to the PDF document structure described in ISO 32000-1 [1] as specified in annex A which describes how to use the **DSS dictionary** and **VRI dictionaries** to incorporate information for the purposes of performing long-term signature validation.

4.2 General Requirements

Conforming signature handlers creating and/or verifying PDF documents with PAdES-LTV shall support PDF documents with:

a) Document security store information as specified in clause A.1.

b) Document time-stamps as specified in clause A.2.

It is recommended that signed PDF documents, conforming to this profile, contain DSS followed by a document Time-stamp.

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

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

Systems supporting this profile shall support creation and/or validation of signatures with one or more DSS entries and document Time-stamps.

4.3 Validation Process

It is recommended that that validation process be as follows:

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

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

3) The signature and the signature Time-stamp should be validated at the latest innermost LTV document Time-stamp time using the validation data stored in the DSS and time-stamped (by the successive enveloping time-stamps)

Validation of documents without document Time-stamps is outside the scope of this profile.

Annex A (normative): ISO 32000-1 LTV Extensions

A.1 Document Security Store

Background

The long-term validation of an electronic signature is a well recognized problem. The problem stems from the fact that the signature may not be successfully verified when its collateral components (validation data) eventually expire unless certain conditions are met. To facilitate long term signature validation, PDF supports the inclusion of various types of validation data into the signed document. This enables the validation process of a conforming signature handler to re-verify the signature as occurred when the signature was first verified.

In order to trust the signing time, the signature should include a time-stamp. A time-stamp is itself signed, and so it is possible for the time-stamp's own validation data also to eventually expire. As with signatures, DSS may also include signature validation data relating to the signature time-stamp (or later document time-stamps).

Another problem is that at the time of signing not all of the validation-related components are available for various reasons including the inability to connect to remote servers that provide them (e.g. the user is offline) or the inability of the signer to bear the financial or time costs associated with obtaining these components. Also, in many workflows it is the recipient of a signed PDF document who is interested in a long term validation of the signatures and not the signer of the document.

In order to address these problems, this validation-related information needs to be dissociated from the signature itself providing the ability to add validation-related information to an existing signed PDF document at some time after a signature has been created. Therefore, a new separate "security store" (a repository of all security-related information) is defined in the PDF in which to place the components.

NOTE: An additional benefit of separating out the components is that those components which are common to several signatures (e.g. certificates and revocation lists) can be stored in this repository once and referenced from all places where they are needed. This will greatly reduce the size of a PDF document that contains several signatures.

"The relevant validation data for each signature may be identified from the security store (see VRI below) for optimization or to remove ambiguity of the validation data used to validate a specific signature."

Catalog

Added to ISO 32000-1 Table 28 "Entries in catalogue dictionary"		
KEY	**TYPE**	**VALUE**
DSS	dictionary	*(Optional)* Document-wide security-related information.

DSS Dictionary

This dictionary is used to provide a single place where all of the validation-related information for some or all signatures in the document should be placed.

The **DSS** dictionary, if present, shall contain validation-related information only for document signatures represented in PKCS#7 (and its derivatives) format or for XAdES signatures of forms signing dynamic XFA [i.2]. The **VRI** entry for a signature in a **DSS** dictionary shall be located in an incremental update section (see clause 7.5.6 of ISO 32000-1 [1]) that is located after the section with the signature to which it applies.

Entries in a DSS Dictionary		
KEY	**TYPE**	**VALUE**
Type	Name	*(Optional)* The type of this dictionary and its value shall be **DSS**, if present.
VRI	Dictionary	*(Optional)* This dictionary contains **Signature VRI** dictionaries in the document. The key of each entry in this dictionary is the base-16-encoded (uppercase) SHA1 digest of the signature to which it applies and the value is the **Signature VRI** dictionary which contains the validation-related information for that signature. See notes 1 and 2.
Certs	Array	*(Optional)* An array of (indirect references to) streams, each containing one BER-encoded X.509 certificate (see RFC 5280 [7]). This array contains certificates that may be used in the validation of any signatures in the document.
OCSPs	Array	*(Optional)* An array of (indirect references to) streams, each containing a BER-encoded Online Certificate Status Protocol (OCSP) response (see RFC 2560 [8]). This array contains OCSPs that may be used in the validation of any signatures in the document.
CRLs	Array	*(Optional)* An array of (indirect references to) streams, each containing a BER-encoded Certificate Revocation List (CRL) (see RFC 5280 [7]). This array contains CRLs that may be used in the validation of any signatures in the document.
NOTE 1: For a document signature the bytes that are hashed are those of the signature's DER-encoded PKCS#7 (and its derivatives) binary data object (base-16 decoded byte string in the **Contents** entry in the signature dictionary). For the signatures of the CRL and OCSP response, it is the respective signature object represented as a BER-encoded OCTET STRING encoded with primitive encoding. For a Time-stamp's signature it is the bytes of the Time-stamp itself since the Time-stamp token is a signed data object. NOTE 2: When computing the digest of a XAdES signature found in dynamic XFA [i.2], the contents of the ds:Signature is canonicalized using exclusive canonicalization (http://www.w3.org/2001/10/xml-exc-c14n#) as specified in [9] and then hashed.		

Signature VRI Dictionary

This dictionary relates validation data to a specific signature to which the validation data applies. This validation data shall be that used by the party adding the DSS to verify a signature or validation data known to be appropriate to another party later relying on the signature. The information consists of the validation time (indicated either by a date object, or a secure time represented by a Time-stamp, or implied by Document Time-stamp applied to the PDF document immediately after the DSS) and revocation information (which can be either a CRL or an OCSP).

Any values in the **Cert, CRL** and **OCSP** arrays of a **Signature VRI** dictionary shall also be present in the **DSS** dictionary applicable to the signature for which this **Signature VRI** dictionary is associated. If this signature does have any associated Certs, CRLs or OCSPs, then the corresponding key shall not be present in the VRI dictionary.

A **Signature VRI** dictionary shall not be used to record the information used in an unsuccessful validation attempt.

Entries in a Signature VRI Dictionary		
KEY	**TYPE**	**VALUE**
Type	Name	*(Optional)* Shall be **VRI**
Cert	array	*(Optional,* shall not be an empty array*)* An array of (indirect references to) streams, each containing one BER-encoded X.509 certificate (see RFC 5280 [7]). This array should contain all certificates that were used in the validation of this signature.
CRL	array	(*Optional*, shall not be an empty array) An array of (indirect references to) streams that should represent all CRLs that were used to determine the validity of the certificates related to this signature. Each array entry is an indirect reference to a stream that represents the BER-encoded Certificate Revocation List (CRL)
OCSP	array	(*Optional*, shall not be an empty array) An array of (indirect references to) streams that should represent all OCSPs that were used to determine the validity of the certificates in the chain related to this signature. Each array entry is an indirect reference to a stream that represents the BER-encoded Online Certificate Status Protocol (OCSP) response.
TU	date	*(Optional)* The date/time at which this VRI dictionary was obtained. The conforming reader may ignore this entry and use a different time for the signature validation. This entry shall be absent when the **TS** entry is present. Date shall be a date string as defined in ISO 32000-1 [1], clause 7.9.4. (See note 1).
TS	stream	*(Optional)* A stream containing the BER-encoded Time-stamp (see RFC 3161 [6]) which represents the secure time at which this VRI dictionary was obtained. This entry shall be absent when a **TU** entry is present. (See notes 2 and 3).
NOTE 1: The use of this key is not recommend by this profile and is only provided for informational purposes by other implementations. As such, this value should be ignored by this profile.		
NOTE 2: The datum that is hashed and included in the Time-stamp's messageImprint field (see RFC 3161 [6]) is the encryptedDigest field in the signature's PKCS#7 object (see RFC 2315 [4]).		
NOTE 3: The use of this key is not recommend by this profile and is only provided for informational purposes by other implementations. As such, this value should be ignored by this profile.		

DocMDP restrictions (see ISO 32000-1 [1] clause 12.8.2.2) shall not apply to incremental updates to a PDF document containing a DSS dictionary and associated VRI, Certs, CRLs and OCSPs.

NOTE: *ISO 32000-1 [1], 12.8.2.2, discusses the **DocMDP** (Modification, Detection and Prevention) feature whereby a set of permissions can be associated with a PDF in conjunction with a certification signature. The permissions of **DocMDP** are present in the **P** key of the **DocMDP** transform parameters dictionary, as an integer in the range 1 through 3. Values of 2 and 3 allow for additional signatures to be included after the certification but a value of 1 does not allow any change so allow Document Time-stamps.* This provision will need to be changed from that in ISO 32000-1 [1], to allow for the inclusion of LTV, including DSS and Document Time-stamps.

Example DSS dictionary (and associated objects)

```
100 0 obj
<<
/Type /Catalog
/DSS 101 0 R
%other stuff here...
>>
endobj

101 0 obj
<<
    /VRI 102 0 R
    /OCSPs [103 0 R]
    /CRLs [104 0 R]
    /Certs [105 0 R 106 0 R]
>>
endobj

102 0 obj
<<
    /4B783B9A6D0D69E4E881BFDF080835E896735416   << /OCSP [103 0 R] /CRL [104 0 R] >>
>>
```

```
endobj

103 0 obj
<<
    /Length 3085    %whatever the length of the stream is
>>
stream
%OCSP data goes here...
endstream

104 0 obj
<<
    /Length 909     %whatever the length of the stream is
>>
stream
%CRL data goes here...
endstream

105 0 obj
<<
    /Length 1042    %whatever the length of the stream is
>>
stream
%Certificate data goes here...
endstream

106 0 obj
<<
    /Length 960 %whatever the length of the stream is
>>
stream
%Certificate data goes here...
Endstream
```

Example with Two Signatures

```
101 0 obj
<<
                /VRI 102 0 R
                /OCSPs [103 0 R 107 0 R]
                /CRLs [104 0 R]
                /Certs [105 0 R 106 0 R]
>>
endobj
102 0 obj
<<
                /4B783B9A6D0D69E4E881BFDF080835E896735416            << /OCSP [103 0 R] /CRL [104 0
R] >>
                /123456789ABCDEF987654321FEDCBA1234567890            << /OCSP [107 0 R] >>
>>

107 0 obj
<<
                /Length 5012      %whatever the length of the stream is
>>
stream
%OCSP data goes here...
endstream
```

Usage of the DSS VRI in the Process of Signature Creation and Validation

In the process of a signature validation a conforming reader may have available multiple sources of validation-related components including those embedded in the signature itself, a local repository of such components, and those retrieved from on-line sources. In the presence of a **DSS** entry in a PDF's **Catalog** the preferred order of the search for components that can be used to validate a signature from the verifier's trust anchors by the conforming reader should be as follows:

1) Validation data referenced in VRI component in DSS.

2) Validation data referenced in DSS.

3) Validation data embedded in the signature (e.g. OCSP data see part 2 [i.4], clause 4.4).

4) Validation data referenced in from the local repository.

5) Validation data referenced in retrieved from an on-line source.

For backward compatibility, conforming writers should embed any validation-related information into the signature itself, when possible.

A.2 Document Time-stamp

A **Document Time-stamp** dictionary is a standard **Signature** dictionary (see ISO 32000-1 [1], 12.8.1) but with the following changes.

Modifications to table 252 for a Document Time-stamp Dictionary		
KEY	**TYPE**	**VALUE**
Type	Name	*(Optional)* If present, shall be **DocTimeStamp.**
SubFilter	Name	*(Required)* The value of **SubFilter** identifies the format of the data contained in the stream. A conforming reader may use any conforming signature handler that supports the specified format. When the value of Type is *DocTimestamp*, the value of SubFilter shall be *ETSI.RFC 3161*. Other values may be defined by developers, and when used, shall be prefixed with the registered developer identification as described in ISO 32000-1 [1], annex E.
Contents	Byte string	*(Required)* The value shall be a hexadecimal string (see clause 7.3.4.3, "Hexadecimal Strings") representing the value of the byte range digest. When the value of SubFilter is *ETSI.RFC3161,* Contents shall be the TimeStampToken as specified in RFC 3161 [6]. The value of the messageImprint field within the TimeStampToken shall be a hash of the bytes of the document indicated by the ByteRange. Space for the Contents value is required to be allocated before the message digest is computed (see clause 7.3.4, "String Objects").
V	Integer	*(Optional) The version of the signature dictionary format. For Document Time-stamp dictionaries the value, if present, shall be 0.* *Default value: 0.*

In addition, the following keys shall not be present in a **Document Time-stamp** dictionary: **Cert, Reference, Changes, R, Prop_AuthTime, and Prop_AuthType**.

The following keys should not be present in a Document Time-stamp dictionary: **Name**, **M, Location, Reason,** and **ContactInfo.** Since this information may already be present inside of the timestamptoken contained in **Contents**, a conforming reader should ignore these keys.

When a PDF already contains a PAdES signature, there is the likely scenario that future updates to that signature and its revocation information may need to take place. This process is done using the same LTV methodology already described

When evaluating the DocMDP restrictions (see ISO 32000-1 [1], clause 12.8.2.2) the presence of a Document Time-stamp dictionary item shall be ignored.

NOTE: *ISO 32000-1 [1], 12.8.2.2, discusses the **DocMDP** (Modification, Detection and Prevention) feature whereby a set of permissions can be associated with a PDF in conjunction with a certification signature. The permissions of **DocMDP** are present in the **P** key of the DocMDP transform parameters dictionary, as an integer in the range 1 through 3. Values of 2 and 3 allow for additional signatures to be included after the certification but a value of 1 does not currently allow any change but should allow Document Time-stamps.* This provision will need to be changed in ISO 32000-2, to allow for the inclusion of LTV, including DSS and Document Time-stamps.

Example Document Time-stamp

```
1 0 obj
<<
/Type /Catalog
/Pages 2 0 R
/AcroForm 5 0 R
>>
endobj
2 0 obj
<<
/Kids [ 3 0 R ]
/Count 1
/Type /Pages
>>
endobj
3 0 obj
<<
/Type /Page
/Parent 2 0 R
/MediaBox [ 0 0 612 792 ]
/Annots 4 0 R
% other keys goes here...
>>
endobj
4 0 obj
<<
/Type /Annot /Subtype /Widget
/Rect [ 0 0 0 0 ]
/F 4 /P 3 0 R
/FT /Sig /T (Sig)
/V 6 0 R
>>
endobj
5 0 obj
<<
/Fields [ 4 0 R ]
/SigFlags 3
>>
endobj
6 0 obj
<<
/Type /DocTimeStamp
/Filter /Adobe.PPKLite
/SubFilter /ETSI.RFC3161
/Contents <00000>           % values go here inside of <>
/ByteRange [0 0 0 0 ] % values go here inside of []
>>
endobj
```

Annex B (informative): Matching of PAdES-LTV-profiles to CAdES

This informative annex provides a match between the different CAdES forms and the combinations of PDF objects included within VRI dictionaries and Document Timestamp PDF objects.

Entry	Profile	Functional equivalence to CAdES form	Built on	Adding
1	Not currently supported (see note 1 below the table)	CAdES-C		
2	Not currently supported (see note 1 below the table)	CAdES-X		
3	PAdES-LTV (see note 2 below the table)	CAdES-X-Long	PAdES-BES or PAdES-EPES, either with signature time-stamps recommended (functionally equivalent to CAdES-T, CAdES-BES or CAdES-EPES)	A DSS containing indirect references to the values of the certificates and cert status data (CRLs or OCSP responses) as specified in clause A.1. Optionally VRI dictionary containing indirect references to the values of the certificates and cert status data (CRLs or OCSP responses) that were used for verifying a particular signature as specified in clause A.1. The certificates and cert status data (CRLs or OCSP responses) referencing by DSS and VRI as specified in clause A.1. A document Time-stamp as specified in clause A.2.
4	PAdES-LTV	CAdES-A	PAdES-LTV Signature identified in row 3 (functionally equivalent to CAdES-X-Long)	In the DSS: set of indirect references to the values of certificates and certificate status data (CRLs or OCSP responses) including those that were used for verifying the previous document Time-stamp as specified in clause A.1. Optionally VRI dictionary containing indirect references to the values of the certificates and cert status data (CRLs or OCSP responses)) including those that were used for verifying a particular signature as specified in clause A.1. The certificates and cert status data (CRLs or OCSP responses) referencing by DSS as specified in clause A.1. A document Time-stamp as specified in clause A.2.

Entry	Profile	Functional equivalence to CAdES form	Built on	Adding
5	PAdES-LTV (see note 3 below the table)	CAdES-A (with two document time-stamps)	PAdES-LTV Signature identified in row 4 (functionally equivalent to CAdES-A with one documentTime-stamp)	In the DSS: set of indirect references to the values of certificates and certificate status data (CRLs or OCSP responses) including those that were used for verifying the previous document Time-stamp. Optionally VRI dictionary containing indirect references to the values of the certificates and cert status data (CRLs or OCSP responses) that were used for verifying a particular signature as specified in clause A.1. The certificates and cert status data (CRLs or OCSP responses) referencing by DSS as specified in clause A.1. A document Time-stamp as specified in clause A.2.

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

NOTE 2: Strictly speaking, CAdES-X-Long builds on CAdES-X, which contains references to certificates, certificates status and time-stamp on the references or on the references and the signature, by adding certificates and certificates status values. The present profile provides functional equivalence in the sense that the form detailed in row 3 contains certificates and certificate status values as recollected during the verification process, and a *document* Time-stamp that also Time-stamps these values. In summary, this form allows to ascertain one time when the verifier had gained access to the validation data (as does CAdES-X) and includes the validation data within the signature (as does CAdES-X-Long).

NOTE 3: Row 5 in the table shows the process for upgrading the signature with successive document Time-stamps and their corresponding validation data (certificates and certificate status).

History

Document history		
V1.1.1	July 2009	Publication