Draft ETSI EN 319 142-1 V1.0.0 (2015-06)

Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures

Reference
DEN/ESI-0019142-1

Keywords
electronic signature, PAdES, profile, security

ETSI

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

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

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

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://ipr.etsi.org).

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

Foreword

This draft European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI standards EN Approval Procedure.

The present document is part 1 of a multi-part deliverable covering the PDF digital signatures (PAdES), as identified below:

Part 1: "Building blocks and PAdES baseline signatures";

Part 2: "Additional PAdES signatures profiles".

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Electronic commerce has emerged as a frequent way of doing business between companies across local, wide area and global networks. Trust in this way of doing business is essential for the success and continued development of electronic commerce. It is therefore important that companies using this electronic means of doing business have suitable security controls and mechanisms in place to protect their transactions and to ensure trust and confidence with their business partners. In this respect digital signatures are an important security component that can be used to protect information and provide trust in electronic business.

The present document is intended to cover digital signatures supported by PKI and public key certificates, and aims to meet the general requirements of the international community to provide trust and confidence in electronic transactions, including, amongst other, applicable requirements from Regulation (EU) No 910/2014 [i.2].

The present document can be used for any transaction between an individual and a company, between two 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, SIM cards, special programs for electronic signatures, etc.

The present document is part of a rationalized framework of standards (see ETSI TR 119 000 [i.3]).
ETSI TR 119 100 [i.4] provides guidance on how to use the present document within the aforementioned framework.

1 Scope

The present document specifies PAdES digital signatures. PAdES signatures build on PDF signatures specified in ISO 32000-1 [1] with an alternative signature encoding to support digital signature formats equivalent to the signature format CAdES as specified in ETSI EN 319 122-1 [2], by incorporation of signed and unsigned attributes, which fulfil certain common requirements (such as the long term validity of digital signatures) in a number of use cases.

The present document specifies formats for PAdES baseline signatures, which provide the basic features necessary for a wide range of business and governmental use cases for electronic procedures and communications to be applicable to a wide range of communities when there is a clear need for interoperability of digital signatures used in electronic documents.

The present document defines four levels of PAdES baseline signatures addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it. Each level requires the presence of certain PAdES attributes, suitably profiled for reducing the optionality as much as possible.

Procedures for creation and validation of PAdES digital signatures are out of scope and specified in ETSI EN 319 102-1 [i.5].

The present document aim at supporting electronic signatures in different regulatory frameworks.

NOTE: Specifically but not exclusively, PAdES digital signatures specified in the present document aim at supporting electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, and qualified electronic seals as per Regulation (EU) No 910/2014 [i.2].

2 References

2.1 Normative 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.

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

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

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

[2] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[3] IETF RFC 5652 (2009): "Cryptographic Message Syntax (CMS)".

[4] IETF RFC 5280 (2008): "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[5] IETF RFC 6960 (2013): "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[6] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[7] W3C Recommendation (May 2008): "Canonical XML Version 1.1".

[8] IETF RFC 5816 (2010): "ESSCertIDv2 Update for RFC 3161".

2.2 Informative 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.

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

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] ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management".

[i.2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.3] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); Rationalized structure for Electronic Signature Standardization".

[i.4] ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Business Driven Guidance for Signature Creation and Validation".

[i.5] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Signature Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[i.6] Adobe® Supplement to ISO 32000-1. BaseVersion: 1.7 - ExtensionLevel: 5.

NOTE: Available at http://www.adobe.com/devnet/pdf/pdf_reference.html.

[i.7] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.8] Adobe® XFA: "XML Forms Architecture (XFA) Specification" version 2.5, (June 2007), Adobe Systems Incorporated".

[i.9] ETSI TS 103 172: "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile".

[i.10] IETF RFC 2315 (1998): "PKCS #7: Cryptographic Message Syntax Version 1.5".

[i.11] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.12] ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".

[i.13] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardisation of signatures; Definitions and abbreviations".3 Definitions and abbreviations.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ISO 32000-1 [1], TR 119 001 [i.13] and the following apply:

electronic time-stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time

NOTE 1: In the case of IETF RFC 3161 [6] updated by IETF RFC 5816 [8] protocol, the electronic time-stamp is referring to the `timeStampToken` field within the `TimeStampResp` element (the TSA's response returned to the requesting client).

NOTE 2: This can be the signer or the creator of a seal or any party that initially validates or further maintains the signature.

generator: any party which creates, or adds attributes to, a signature

NOTE: This can be the signer or any party that initially validates or further maintains the signature.

Legacy PAdES baseline signature: digital signature generated according to ETSI TS 103 172 [i.9]

PAdES signature: digital signature that satisfies the requirements specified within the present document and ETSI EN 319 142-2 [i.12]

proof of existence: information that can be used to prove that some data existed before a given time

signature handler: software module that implements a specific form of signing and/or authentication of digital signatures

trust service provider: body operating one or more (electronic) Trust Services

verifier: entity that validates a digital signature

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.13] and the following apply:

DSS	Document Security Store
ESS	Enhanced Security Services
TSL	Trust Status List
VRI	Validation Related Information

4 General syntax

4.1 General requirements for PAdES signatures based on PDF signatures

PAdES signatures profiled in the present document build on PDF signatures specified in ISO 32000-1 [1] with an alternative signature encoding to support digital signature formats equivalent to the signature format CAdES [2], by incorporation of signed and unsigned attributes described in clause 5.

The following requirements apply:

a) A DER-encoded SignedData object as specified in CAdES [2] shall be included as the PDF signature in the entry with the key `Contents` of the Signature Dictionary as described in ISO 32000-1 [1], clause 12.8.1. There shall only be a single signer (i.e. one single component of `SignerInfo` type within `signerInfos` element) in any PDF Signature.

b) Requirements for handling PDF Signatures specified in ISO 32000-1 [1], clause 12.8 shall apply except where overridden by the present document.

NOTE: Given that PAdES signatures are enveloped inside a PDF document and are detached in the sense of a CMS signature, the signature placement is implied by ISO 32000-1 [1].
In ISO 32000-1 [1], section 12.8.3.3.1 reads "No data shall be encapsulated in the PKCS#7 SignedData field".

c) Some signature attributes found in CAdES [2] have the same or similar meaning as keys in the Signature Dictionary described in ISO 32000-1 [1]. For signature attributes and keys that have the same or similar meaning only one of them should be used according to the requirements set in table defined in clause 6.3 in the present document.

5 Attributes syntax and semantics

5.1 Introduction

This clause provides details on attributes specified within ISO 32000-1 [1] and CAdES [2] and defines new attributes for building PAdES signatures.

The clause distinguishes between the following types of attributes: CMS and CAdES defined attributes, ISO 32000-1 [1] defined attributes, validation data and archive validation data attributes. The first ones are the attributes that build the DER-encoded `SignedData` object included as the PDF signature in the entry with the key `Contents` of the Signature Dictionary as described in ISO 32000-1 [1], clause 12.8.1. The second ones are the attributes that build the Signature Dictionary as described in ISO 32000-1 [1]. The other ones are the attributes where to include validation data and archive validation data that can guarantee long term validity of digital signatures.

Clause 6.3 provides the requirements concerning how to use the attributes described above.

5.2 CMS and CAdES defined attributes

The attributes included in the following list may be used to generate the DER-encoded `SignedData` object included as the PDF signature in the entry with the key `Contents` of the Signature Dictionary as described in ISO 32000-1 [1], clause 12.8.1. Their syntax shall be as defined in ETSI EN 319 122-1 [2], clause 5.

- `content-type`
- `message-digest`
- `signing certificate reference attributes`
  - `ESS signing-certificate`
  - `ESS signing-certificate-v2`
- `commitment-type-indication`
- `signer-attributes-v2`
- `content-time-stamp`
- `signature-policy-identifier`
- `signature-time-stamp`

5.3 ISO 32000-1 defined attributes

The entries of the Signature Dictionary shall be as defined in ISO 32000-1 [1], clause 12.8.1 unless specified otherwise in the present document.

In particular, the entries with the following keys in the Signature Dictionary are directly addressed: `M`, `Contents`, `Filter`, `SubFilter`, `ByteRange`. Further the entries with the `Location`, `Name`, `ContactInfo` and `Reason` keys in the Signature Dictionary are inherently addressed.

5.4 Validation data and archive validation data attributes

5.4.1 Overview

Validation of a digital signature requires data to validate the signature such as CA certificates, Certificate Revocation List (CRLs) or certificate status information (OCSP) commonly provided by online services (referred to in the present document as validation data).

This clause describes 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 5.4.2). The structure of **DSS** and **VRI** is illustrated in figure 1.

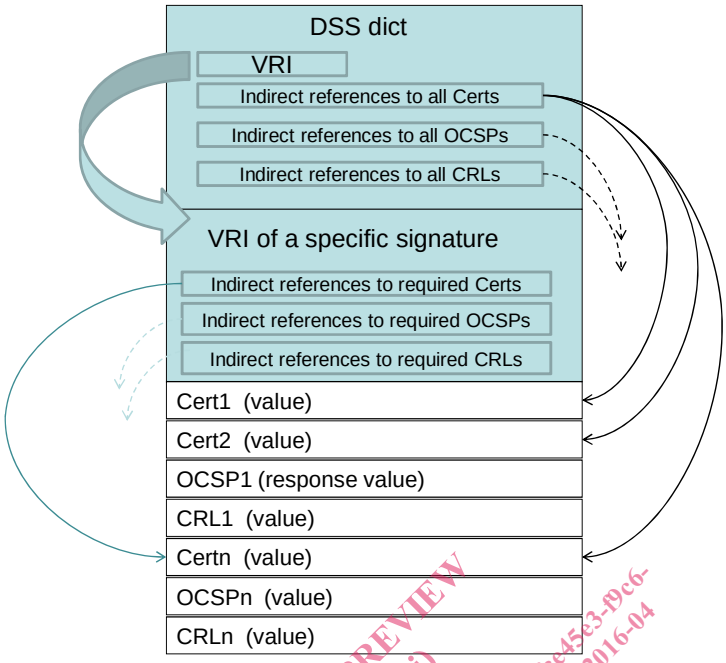

Figure 1: Illustration of DSS and VRI structures

This clause also defines another extension to ISO 32000-1 [1] called Document Time-stamp (see clause 5.4.3) to extend the life-time of protection to the document.

These extensions support Long Term Validation (LTV) of PDF Signatures. The structure of a PDF document with LTV is illustrated in figure 2.

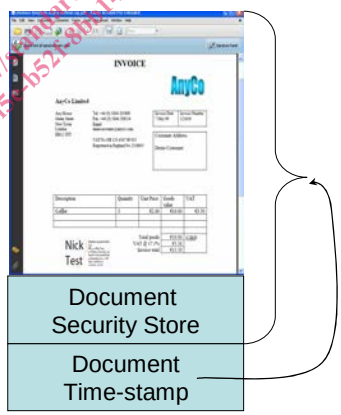

Figure 2: Illustration of PDF document with extended life-time protection

The life-time of the protection can be further extended beyond the life-time 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.