



**Electronic Signatures and Trust Infrastructures (ESI);  
PAdES digital signatures;  
Part 2: Additional PAdES signatures profiles**

Document Preview

[ETSI EN 319 142-2 V1.2.0 \(2025-03\)](https://standards.iteh.ai/catalog/standards/etsi/69c69b76-f8c6-49ef-a5e5-f1ee75d94cd4/etsi-en-319-142-2-v1-2-0-2025-03)

<https://standards.iteh.ai/catalog/standards/etsi/69c69b76-f8c6-49ef-a5e5-f1ee75d94cd4/etsi-en-319-142-2-v1-2-0-2025-03>

---

**Reference**

---

REN/ESI-0019142-2v121

---

---

**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 - APE 7112B  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° w061004871

---

**Important notice**

---

The present document can be downloaded from the  
[ETSI Search & Browse Standards](#) application.

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed,  
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to  
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our  
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

---

**Notice of disclaimer & limitation of liability**

---

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.  
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

---

**Copyright Notification**

---

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2025.  
All rights reserved.

# Contents

Intellectual Property Rights .....	5
Foreword.....	5
Modal verbs terminology.....	5
Introduction .....	6
1 Scope .....	7
2 References .....	7
2.1 Normative references .....	7
2.2 Informative references.....	8
3 Definitions of terms, symbols and abbreviations .....	9
3.1 Definitions .....	9
3.2 Symbols.....	9
3.3 Abbreviations .....	9
4 Profile for CMS digital signatures in PDF .....	9
4.1 Features .....	9
4.2 Requirements of Profile for CMS Signatures in PDF .....	10
4.2.1 Requirements on PDF signatures.....	10
4.2.2 Requirements on PDF signature handlers.....	10
4.2.3 Requirements on signature validation.....	10
4.2.4 Requirements on Time Stamping.....	11
4.2.4.1 Requirements on electronic time-stamp creation .....	11
4.2.4.2 Requirements on electronic time-stamp validation .....	11
4.2.5 Requirements on revocation checking.....	11
4.2.6 Requirements on Seed Values .....	11
4.2.7 Requirements on encryption .....	11
5 Extended PAdES signature profiles .....	11
5.1 Features .....	11
5.2 General Requirements .....	12
5.2.1 Requirements from ETSI EN 319 142-1.....	12
5.2.2 Notation of Requirements.....	12
5.3 PAdES-E-BES Level.....	12
5.4 PAdES-E-EPES Level.....	14
5.5 PAdES-E-LTV Level .....	14
6 Profiles for XAdES Signatures signing XML content in PDF.....	15
6.1 Features .....	15
6.2 Profiles for XAdES signatures of signed XML documents embedded in PDF containers.....	15
6.2.1 Overview .....	15
6.2.2 Profile for Basic XAdES signatures of XML documents embedded in PDF containers .....	17
6.2.2.1 Features .....	17
6.2.2.2 General syntax and requirements .....	18
6.2.2.3 Requirements for applications generating signed XML document to be embedded .....	18
6.2.2.4 Mandatory operations.....	18
6.2.2.4.1 Protecting the signing certificate .....	18
6.2.2.5 Requirements on XAdES optional properties .....	19
6.2.2.6 Serial Signatures .....	19
6.2.2.7 Parallel Signatures.....	19
6.2.2.8 PAdES Signatures .....	19
6.2.3 Profile for long-term XAdES signatures of signed XML documents embedded in PDF containers .....	20
6.2.3.1 Features .....	20
6.2.3.2 Augmentation mechanism.....	20
6.2.3.3 Optional properties.....	20
6.2.3.4 Validation Process.....	20
6.3 Profiles for XAdES signatures on XFA Forms .....	20

6.3.1	Overview .....	20
6.3.2	Profile for Basic XAdES signatures on XFA forms .....	23
6.3.2.1	Features .....	23
6.3.2.2	General syntax and requirements .....	23
6.3.2.3	Mandatory operations.....	24
6.3.2.3.1	Protecting the signing certificate .....	24
6.3.2.4	Requirements on XAdES optional properties .....	24
6.3.2.5	Serial Signatures .....	25
6.3.2.6	Parallel Signatures.....	26
6.3.3	Profile for long-term validation XAdES signatures on XFA forms.....	26
6.3.3.1	Overview .....	26
6.3.3.2	Features .....	26
6.3.3.3	General Requirements.....	26
6.3.4	Extensions Dictionary .....	26
<b>Annex A (informative):</b>	<b>General Features.....</b>	<b>27</b>
A.1	PDF signatures .....	27
A.2	PDF Signature types.....	28
A.3	PDF Signature Handlers.....	28
A.4	PDF serial signatures.....	28
A.5	PDF signature Validation and Time-stamping .....	29
A.6	ISO 19005-1: 2005 (PDF/A-1).....	29
A.7	ISO 19005-4:2020 (PDF/A-4).....	30
A.8	Seed Values and Signature Policies .....	30
<b>Annex B (informative):</b>	<b>Bibliography.....</b>	<b>31</b>
History .....		32

ETSI EN 319 142-2 V1.2.0 (2025-03)

<https://standards.iteh.ai/catalog/standards/etsi/69c69b76-f8c6-49ef-a5e5-f1ee75d94cd4/etsi-en-319-142-2-v1-2-0-2025-03>

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 IPR online database](#).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

## Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

# Foreword

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

The present document is part 2 of a multi-part deliverable covering the PAdES digital signatures. Full details of the entire series can be found in part 1 [4].

## 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. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (i.e. repudiates; see ISO/IEC 10181-4 [i.1]) the validity of the signature.

Thus, the present document can be used for any document encoded in a Portable Document Format (PDF) produced by an individual and a company, and exchanged between companies, between an individual and a governmental body, etc. The present document is independent of any environment; it can be applied to any environment, e.g. smart cards, SIM cards, special programs for digital signatures, etc.

The present document is part of a rationalized framework of standards (see ETSI TR 119 000 [i.8]). See ETSI TR 119 100 [i.9] for getting guidance on how to use the present document within the aforementioned framework.

**iTeh Standards**  
**(<https://standards.iteh.ai>)**  
**Document Preview**

[ETSI EN 319 142-2 V1.2.0 \(2025-03\)](https://standards.iteh.ai/catalog/standards/etsi/69c69b76-f8c6-49ef-a5e5-f1ee75d94cd4/etsi-en-319-142-2-v1-2-0-2025-03)

<https://standards.iteh.ai/catalog/standards/etsi/69c69b76-f8c6-49ef-a5e5-f1ee75d94cd4/etsi-en-319-142-2-v1-2-0-2025-03>

---

# 1 Scope

The present document defines multiple profiles for PAdES digital signatures which are digital signatures embedded within a PDF file.

The present document contains a profile for the use of PDF signatures, as described in ISO 32000-2 [1] and based on CMS digital signatures [i.6], that enables greater interoperability for PDF signatures by providing additional restrictions beyond those of ISO 32000-2 [1]. This first profile is not related to ETSI EN 319 142-1 [4].

The present document also contains a second set of profiles that extend the scope of the profile in ETSI EN 319 142-1 [4], while keeping some features that enhance interoperability of PAdES signatures. These profiles define three levels of PAdES extended 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. These PAdES extended signatures offer a higher degree of optionality than the PAdES baseline signatures specified in ETSI EN 319 142-1 [4].

The present document also defines a third profile for usage of an arbitrary XML document signed with XAdES signatures that is embedded within a PDF file.

The profiles defined in the present document provide equivalent requirements to profiles found in ETSI TS 102 778 [i.10].

Procedures for creation, augmentation, and validation of PAdES digital signatures are out of scope and specified in ETSI EN 319 102-1 [i.11]. Guidance on creation, augmentation and validation of PAdES digital signatures including the usage of the different attributes is provided in ETSI TR 119 100 [i.9].

The present document does not repeat the base requirements of the referenced standards, but instead aims to maximize interoperability of digital signatures in various business areas.

---

## 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 referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the [ETSI docbox](#).

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 32000-2](#): "Document management — Portable document format —Part 2: PDF 2.0".
- [2] Void.
- [3] [IETF RFC 5280](#): "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
- [4] [ETSI EN 319 142-1](#): "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures"..
- [5] [ETSI EN 319 122-1](#): "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".
- [6] [ETSI EN 319 132-1](#): "Electronic Signatures and Trust Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

- [7] [ETSI EN 319 132-2](#): "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".
- [8] Adobe® XFA: "[XML Forms Architecture \(XFA\) Specification](#)" version 3.3, (January 2012), Adobe Systems Incorporated".
- [9] W3C® Recommendation: "[XML Signature Syntax and Processing Version 1.1](#)".
- [10] [IETF RFC 5035 \(2007\)](#): "Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility".
- [11] Void.
- [12] Void.
- [13] [IETF RFC 5652 \(2009\)](#): "Cryptographic Message Syntax (CMS)".

## 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 referenced 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] ISO/IEC 10181-4: "Information technology — Open Systems Interconnection — Security frameworks for open systems: Non-repudiation framework".
- [i.2] ETSI TS 119 312: "Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites".
- [i.3] IETF RFC 5755: "An Internet Attribute Certificate Profile for Authorization".
- [i.4] W3C® Working Group Note: "XML Signature Best Practices", 11 April 2013.
- [i.5] ISO 19005-1:2005: "Document management — Electronic document file format for long-term preservation — Part 1: Use of PDF 1.4 (PDF/A-1)".
- [i.6] Void.
- [i.7] ISO 19005-4 (2020): "Electronic document file format for long-term preservation — Part 4: Use of ISO 32000-2 (PDF/A-4)".
- [i.8] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of digital signatures and trust services; Overview".
- [i.9] ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for signature creation and validation".
- [i.10] ETSI TS 102 778: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles".
- [i.11] ETSI EN 319 102-1: "Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".
- [i.12] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".



---

## 3 Definitions of terms, symbols and abbreviations

### 3.1 Definitions

For the purposes of the present document, the terms given in ISO 32000-2 [1], ETSI TR 119 001 [i.12] and ETSI EN 319 142-1 [4] apply.

### 3.2 Symbols

Void.

### 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.12] and the following apply:

CA	Certification Authority
CMS	Cryptographic Message Syntax

NOTE: As specified in IETF RFC 5652 [13].

CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
ESS	Enhanced Security Services
MDP	Modification Detection and Prevention
PDF	Portable Document Format
SIM	Subscriber Identity Module
TSA	Time-Stamping Authority
UBL	Universal Business Language
UTC	Coordinated Universal Time
XML	XML Forms Architecture
XMP	eXtensible Metadata Platform

---

## 4 Profile for CMS digital signatures in PDF

### 4.1 Features

The present profile specifies digital signatures that:

- Are encoded in CMS as defined by CMS (see IETF RFC 5652 [13]).
- Support serial signatures.
- Optionally include signature time-stamps.
- Optionally include revocation information.
- Protect integrity of the document and authenticates the signer identity information included in the signing certificate.
- Can optionally include the "reasons" for the signature.
- Can optionally include a description of the location of signing.
- Can optionally include contact info of the signer.

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™).

## 4.2 Requirements of Profile for CMS Signatures in PDF

### 4.2.1 Requirements on PDF signatures

While ISO 32000-2 [1], clause 12.8 clearly states the majority of the requirements necessary for conformance with this profile, this clause specifies additional requirements for conformance.

- a) PDF Signatures shall be as specified in ISO 32000-2 [1], clause 12.8.
- b) 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.
- c) The PDF Signature (a DER-encoded CMS binary data object) shall be placed into the Contents entry of the signature dictionary.
- d) The CMS object shall conform to the CMS specification in IETF RFC 5652 [13]. At minimum, it shall include the signer's X.509 signing certificate.

NOTE 1: Although ISO 32000-2 [1] also allows the value of the Contents entry of signature dictionary to be a DER-encoded PKCS#1 binary data object, that format is not supported by this profile.

- e) 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 should be captured and validated before completing the creation of the PDF Signature.
- f) If present, any revocation information shall be a signed attribute of the PDF Signature.
- g) IETF RFC 5755 [i.3] attribute certificates associated with the signer certificate should not be used.

NOTE 2: ISO 32000-2 [1] allows the inclusion of one or more IETF RFC 5755 [i.3] attribute certificates associated with the signer certificate. However, attribute certificates are not widely supported and hence use of this attribute will reduce interoperability.

- h) There shall only be a single signer (i.e. one single component of "SignerInfo" type within "signerInfos" element) in any PDF Signature.

### 4.2.2 Requirements on PDF signature handlers

- a) A PDF reader may substitute a different signature handler, other than that specified in **Filter**, when validating the signature, as long as it supports the specified **SubFilter** format.
- b) Only the values for **SubFilter** listed in ISO 32000-2 [1], clause 12.8.3. 1 (i.e. **adbe.pkcs7.detached** and **ETSI.CAdES.detached**) shall be used.

NOTE: While the names of the SubFilters can imply specific algorithms, the actual list of supported algorithms can be found in ISO 32000-2 [1], clause 12.8.3.1, table 260. Consult ETSI TS 119 312 [i.2] for guidance on algorithm choices.

The use of SHA-1 is phased out and hence other hashing algorithms shall be used.

### 4.2.3 Requirements on signature validation

When the user opens a signed document and requests validation of the signature(s) present in the PDF, a reader shall invoke the appropriate signature handler that shall perform the following steps to validate them.

- a) Validate that the document digest matches that in the signature as specified in ISO 32000-2 [1], clause 12.8.1.
- b) Validate the path of certificates used to validate the binding between the subject distinguished name and subject public key as specified in IETF RFC 5280 [3]. The validity checks shall be carried out at the time indicated either by electronic time-stamp applied as per clause 4.2.4 or some other trusted indication of the signing time. The revocation status shall be checked as specified in clause 4.2.5.

- c) To achieve consistent validation results with existing signatures and existing implementations of signature handlers, that did not know this attribute, the signing certificate reference attribute itself should be ignored during validation if present.

NOTE: Unlike any other Profile in the present document inclusion of the certificate hash (see CAdES [5], clause 5.2.2) is not required by this profile. Applications requiring the existence of certificate hash can use signatures based on PAdES baseline profiles [4] or the profile defined in clause 5.3 or the profile defined in clause 5.4.

## 4.2.4 Requirements on Time Stamping

### 4.2.4.1 Requirements on electronic time-stamp creation

- a) An electronic time-stamp from a trusted TSA should be applied to the digital signature as soon as possible after the signature is created so the electronic time-stamp reflects the time after the document was signed.
- b) If a signature handler chooses to embed an electronic time-stamp into the PDF Signature, then it shall be embedded as described in ISO 32000-2 [1], clause 12.8.3.3.1.

### 4.2.4.2 Requirements on electronic time-stamp validation

- a) A signature handler shall take the signature field of the CMS signature, encode it and compute the digest of the resulting byte stream using the algorithm indicated in the electronic time-stamp.
- b) A signature handler shall check if the value obtained in the first step is the same as the digest present in the electronic time-stamp.

## 4.2.5 Requirements on revocation checking

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

## 4.2.6 Requirements on Seed Values

Seed values that would require a signature handler to violate this profile shall not be used.

EXAMPLE: Seed values that specify the use of PKCS#1 are not permitted as the present document requires use of CMS.

## 4.2.7 Requirements on encryption

The requirements in ETSI EN 319 142-1 [4], clause 5.5 shall apply.

---

# 5 Extended PAdES signature profiles

## 5.1 Features

The profiles in this clause define PAdES signatures based on the building blocks defined in ETSI EN 319 142-1 [4]. These profiles define three levels of PAdES extended signatures that offer a higher degree of optionality than the PAdES baseline signatures specified in ETSI EN 319 142-1 [4].

PAdES-E-BES level allows basic digital signatures embedded within a PDF file. There is an unambiguous connection from the signature to the identity of a certificate intended to identify the signer.

PAdES-E-EPES level is built on top of the PAdES-E-BES level and allows inclusion of signature policies.