SLOVENSKI STANDARD
SIST EN 319 142-1 V1.3.1:2027

01-januar-2027

Elektronski podpisi in infrastrukture zaupanja (ESI) - Digitalni podpisi PAdES - 1. del: Gradniki in izhodiščni podpisi PAdES

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

Sample Document

Ta slovenski standard je istoveten z: **ETSI EN 319 142-1 V1.3.1 (2026-11)**

get full document from standards.iteh.ai

ICS:

35.040.01	Kodiranje informacij na splošno	Information coding in general

SIST EN 319 142-1 V1.3.1:2027 **en**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

Sample Document

get full document from standards.iteh.ai

ETSI EN 319 142-1 V1.3.1 (2026-11)



EUROPEAN STANDARD

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

Sample Document

get full document from standards.iteh.ai

SIST EN 319 142-1 V1.3.1:2027

Reference
REN/ESI-0019142-1v131

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 of this document may be reproduced in any form, by any means and in any media, without the prior written authorization of ETSI and except as expressly permitted below.
By way of exception and when the document is a normative deliverable (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)), ETSI authorizes to reproduce and incorporate into products, services and technical documentation only those extracts (e.g. templates) that are strictly necessary for the technical implementation of the normative deliverable, to ensure compliance with the latter.
Nothing in this notice shall be construed as limiting any mandatory exceptions to copyright provided by applicable law.

© ETSI 2026.
All rights reserved.

SIST EN 319 142-1 V1.3.1:2027 • https://standards.iteh.ai/catalog/standards/sist/3eaaf77f-f9fd-4897-9274-bc185eda7351/sist-en-319-142-1-v1-3-1-2027

SIST EN 319 142-1 V1.3.1:2027

Contents

Intellectual Property Rights 4
Foreword 4
Modal verbs terminology 5
Introduction 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 7
3 Definition of terms, symbols and abbreviations 8
3.1 Terms 8
3.2 Symbols 8
3.3 Abbreviations 8
4 General syntax 9
4.1 General requirements for PAdES signatures based on PDF signatures 9
5 Attributes syntax and semantics 9
5.1 Introduction 9
5.2 CMS and CAdES defined attributes 10
5.3 ISO 32000 defined attributes 10
5.4 Validation data and archive validation data attributes 11
5.4.1 Overview 11
5.4.2 Document Security Store 13
5.4.2.1 Catalog 13
5.4.2.2 DSS Dictionary 13
5.4.2.3 Signature VRI Dictionary 15
5.4.3 Document Time-stamp 16
5.4.4 Validation of PAdES signatures 16
5.5 Requirements on encryption 17
5.6 Extensions dictionary and PDF 2.0 conformance 17
5.6.1 ISO 32000-1 (PDF 1.7) Compliant Documents 17
5.6.2 ISO 32000-2 (PDF 2.0) Compliant Documents 18
5.6.3 Version conformance across document revisions 18
6 PAdES baseline signatures 18
6.1 Signature levels 18
6.2 General requirements for PAdES baseline signatures 19
6.2.1 Algorithm requirements 19
6.2.2 Notation for requirements 19
6.3 PAdES baseline signatures 21
6.4 Legacy PAdES baseline signatures 27
Annex A (informative): Change history 28
History 29

Sample Document
Sample document from standards.iteh.ai

SIST EN 319 142-1 V1.3.1:2027 • https://standards.iteh.ai/catalog/standards/sist/3eaaf77f-f9fd-4897-9274-bc185eda7351/sist-en-319-142-1-v1-3-1-2027

SIST EN 319 142-1 V1.3.1:2027

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)) 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.

Sample Document
get full document from standards.iteh.ai

Foreword

This European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Trust Infrastructures (ESI).

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

ETSI EN 319 142-1: "Building blocks and PAdES baseline signatures";

ETSI EN 319 142-2: "Additional PAdES signatures profiles";

ETSI TS 119 142-3: "PAdES Document Time-stamp digital signatures (PAdES-DTS)".

National transposition dates	
Date of adoption of this EN:	9 November 2026
Date of latest announcement of this EN (doa):	28 February 2027
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 August 2027
Date of withdrawal of any conflicting National Standard (dow):	31 August 2027

SIST EN 319 142-1 V1.3.1:2027 • https://standards.iteh.ai/catalog/standards/sist/3eaaf77f-f9fd-4897-9274-bc185eda7351/sist-en-319-142-1-v1-3-1-2027

SIST EN 319 142-1 V1.3.1:2027

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.

Sample Document

get full document from standards.iteh.ai

SIST EN 319 142-1 V1.3.1:2027 • https://standards.iteh.ai/catalog/standards/sist/3eaaf77f-f9fd-4897-9274-bc185eda7351/sist-en-319-142-1-v1-3-1-2027

SIST EN 319 142-1 V1.3.1:2027

1 Scope

The present document specifies PAdES digital signatures. PAdES signatures build on PDF signature mechanisms defined in the ISO 32000 series. For documents conforming to ISO 32000-1 [1] PAdES utilizes an extended, alternative signature encoding. For documents conforming to ISO 32000-2 [9], these signature structures are incorporated natively by default within the core standard. Both approaches 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, augmentation, and validation of PAdES digital signatures are out of scope and specified in ETSI EN 319 102-1 [10]. Guidance on creation, augmentation and validation of PAdES digital signatures including the usage of the different attributes defined in the present document is provided in ETSI TR 119 100 [i.4]. The present document aims 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].

Sample Document

2 References

get full document from standards.iteh.ai

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 32000-1: "Document management — Portable document format — Part 1: PDF 1.7".

[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 (2 May 2008): "Canonical XML Version 1.1".

SIST EN 319 142-1 V1.3.1:2027 • https://standards.iteh.ai/catalog/standards/sist/3eaaf77f-f9fd-4897-9274-bc185eda7351/sist-en-319-142-1-v1-3-1-2027

SIST EN 319 142-1 V1.3.1:2027

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

[9] ISO 32000-2: "Document management — Portable document format —Part 2: PDF 2.0".

[10] 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".

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] Void.

[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); The framework for standardization of digital signatures and trust services; Overview".

[i.4] ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for signature creation and validation".

[i.5] Void.

[i.6] ETSI TS 119 312: "Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites".

[i.7] Adobe® XFA: "XML Forms Architecture (XFA) Specification" version 2.5, (June 2007), Adobe Systems Incorporated".

[i.8] ETSI TS 103 172: "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile".

[i.9] IETF RFC 2315 (1998): "PKCS #7: Cryptographic Message Syntax Version 1.5".

[i.10] ETSI TS 119 612: "Electronic Signatures and Trust Infrastructures (ESI); Trusted Lists".

[i.11] ETSI EN 319 142-2: "Electronic Signatures and Trust Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".

[i.12] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.13] ETSI TS 119 511: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques".

Sample Document
get full document from standards.iteh.ai

SIST EN 319 142-1 V1.3.1:2027 • https://standards.iteh.ai/catalog/standards/sist/3eaaf77f-f9fd-4897-9274-bc185eda7351/sist-en-319-142-1-v1-3-1-2027