

|            |                                                                                                                                                                 |                                                       |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| <b>STN</b> | <b>Elektronické podpisy a infraštruktúry (ESI).<br/>Digitálne podpisy vo formáte PAdES. Časť 1:<br/>Stavebné bloky a základné podpisy vo formáte<br/>PAdES.</b> | <b>STN<br/>EN 319 142-1<br/>V1.1.1</b><br><br>87 9142 |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|

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

Táto norma obsahuje anglickú verziu európskej normy.  
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 01/17

Obsahuje: EN 319 142-1 V1.1.1:2016

**124091**

---

Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, 2017  
Podľa zákona č. 264/1999 Z. z. v znení neskorších predpisov sa môžu slovenské technické normy  
rozmnžovať a rozširovať iba so súhlasom Úradu pre normalizáciu, metrológiu a skúšobníctvo SR.

# ETSI EN 319 142-1 V1.1.1 (2016-04)



**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

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

---

**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.

© European Telecommunications Standards Institute 2016.

All rights reserved.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.  
**3GPP™** and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and  
of the 3GPP Organizational Partners.  
**GSM®** and the GSM logo are Trade Marks registered and owned by the GSM Association.

# Contents

|                                                                            |    |
|----------------------------------------------------------------------------|----|
| Intellectual Property Rights .....                                         | 4  |
| Foreword.....                                                              | 4  |
| Modal verbs terminology.....                                               | 4  |
| Introduction .....                                                         | 4  |
| 1 Scope .....                                                              | 6  |
| 2 References .....                                                         | 6  |
| 2.1 Normative references .....                                             | 6  |
| 2.2 Informative references.....                                            | 7  |
| 3 Definitions and abbreviations.....                                       | 7  |
| 3.1 Definitions.....                                                       | 7  |
| 3.2 Abbreviations .....                                                    | 8  |
| 4 General syntax.....                                                      | 8  |
| 4.1 General requirements for PAdES signatures based on PDF signatures..... | 8  |
| 5 Attributes syntax and semantics .....                                    | 9  |
| 5.1 Introduction .....                                                     | 9  |
| 5.2 CMS and CADES defined attributes.....                                  | 9  |
| 5.3 ISO 32000-1 defined attributes .....                                   | 9  |
| 5.4 Validation data and archive validation data attributes.....            | 10 |
| 5.4.1 Overview .....                                                       | 10 |
| 5.4.2 Document Security Store .....                                        | 11 |
| 5.4.2.1 Catalog .....                                                      | 11 |
| 5.4.2.2 DSS Dictionary .....                                               | 11 |
| 5.4.2.3 Signature VRI Dictionary .....                                     | 13 |
| 5.4.3 Document Time-stamp .....                                            | 14 |
| 5.5 Requirements on encryption.....                                        | 14 |
| 5.6 Extensions dictionary .....                                            | 15 |
| 6 PAdES baseline signatures.....                                           | 15 |
| 6.1 Signature levels .....                                                 | 15 |
| 6.2 General requirements for PAdES baseline signatures .....               | 16 |
| 6.2.1 Algorithm requirements.....                                          | 16 |
| 6.2.2 Notation for requirements.....                                       | 16 |
| 6.3 PAdES baseline signatures .....                                        | 18 |
| 6.4 Legacy PAdES baseline signatures .....                                 | 22 |
| History .....                                                              | 23 |

---

# 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 (<https://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 European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

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".

| National transposition dates                                                           |                 |
|----------------------------------------------------------------------------------------|-----------------|
| Date of adoption of this EN:                                                           | 1 April 2016    |
| Date of latest announcement of this EN (doa):                                          | 31 July 2016    |
| Date of latest publication of new National Standard or endorsement of this EN (dop/e): | 31 January 2017 |
| Date of withdrawal of any conflicting National Standard (dow):                         | 31 January 2017 |

---

## 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, augmentation, and validation of PAdES digital signatures are out of scope and specified in ETSI EN 319 102-1 [i.5]. 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].

---

## 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 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](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 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] 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); The framework for standardization of signatures: overview".
- [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 Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".
- [i.6] ETSI TS 119 312: "Electronic Signatures and 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 Infrastructures (ESI); Trusted Lists".
- [i.11] ETSI EN 319 142-2: "Electronic Signatures and 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".

---

**koniec náhľadu – text ďalej pokračuje v platenej verzii STN**