ETSI TS 119 144-4 V1.1.1 (2016-06)

Electronic Signatures and Infrastructures (ESI); PAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance of PAdES baseline signatures

Reference

DTS/ESI-0019144-4

Keywords

conformance, e-commerce, electronic signature, PAdES, profile, security, testing

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/CommiteeSupportStaff.aspx

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 (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 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 covering PAdES digital signatures - Testing Conformance and Interoperability. Full details of the entire series can be found in part 1 [i.1].

A tool implementing the present document has been developed and is accessible at http://signatures-conformance-checker.etsi.org/.

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.

1 Scope

The present document defines the set of checks to be performed for testing conformance of PAdES signatures against PAdES baseline signatures as specified in ETSI EN 319 142-1 [1].

The present document does not specify checks leading to conclude whether a signature is technically valid or not (for instance, it does not specify checks for determining whether the cryptographic material present in the signature may be considered valid or not). In consequence, no conclusion may be inferred regarding the technical validity of a signature that has been successfully tested by any tool conformant to the present document.

Checks specified by the present document are exclusively constrained to elements specified by PAdES [1].

Regarding PAdES attributes, the present document explicitly differentiates between structural requirements that are defined on building blocks, and the requirements specified for PAdES baseline signatures conformance.

The present document is intentionally not linked to any software development technology and is also intentionally agnostic on implementation strategies. This is one of the reasons why the test assertions set specified in the present document includes tests on the correctness of the structure of all the elements specified by PAdES [1].

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] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

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

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 TR 119 144-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview".

[i.2] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.3] OASIS Committee Notes: "Test Assertions Guidelines Version 1.0" Committee Note 02, 19 June 2013.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TR 119 001 [i.2] apply.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.2] apply.

4 Overview

The present clause describes the main aspects of the technical approach used for specifying the whole set of checks to be performed for testing conformance to ETSI EN 319 142-1 [1].

ETSI EN 319 142-1 [1] defines requirements for building blocks and PAdES baseline signatures. For the purpose of identifying the whole set of test assertions required for testing conformance against PAdES baseline signatures as specified in ETSI EN 319 142-1 [1], the present document classifies the whole set of requirements specified in ETSI EN 319 142-1 [1] in two groups as follows:

1) Requirements "PAdES_BS" (after "PAdES baseline signatures"): requirements defined in clauses 5 and 6 of ETSI EN 319 142-1 [1]. These are requirements specific to PAdES baseline signatures.

2) Requirements "PAdES_BB" (after "PAdES building blocks"): requirements defined in clauses 4 and 5 of ETSI EN 319 142-1 [1] and clauses 4 and 5 of ETSI EN 319 142-2 [2] to be satisfied by both PAdES baseline signatures as specified in ETSI EN 319 142-1 [1] and additional PAdES signatures as specified in ETSI EN 319 142-2 [2].

a) In order to test conformance against the aforementioned specification, several types of tests are identified, namely:

   1) Tests on the signature structure.

   2) Tests on values of specific elements and/or attributes.

   3) Tests on interrelationship between different elements present in the signature.

   4) Tests on computations reflected in the contents of the signatures (message imprints for a time-stamping service, computed by digesting the concatenation of a number of elements of the signature, for instance).

b) No tests is included testing actual validity of the cryptographic material that might be present at the signature or to be used for its verification (status of certificates for instance).

c) Tests are defined as test assertions following the work produced by OASIS in "Test Assertions Guidelines Version 1.0" [i.3]. Each test assertion includes:

   1) Unique identifier for further referencing. The identifiers of the assertions start with "PAdES_BS", after "PAdES baseline signatures" and with "PAdES_BB", after "PAdES building blocks".

   2) Reference to the **Normative source** for the test.

   3) The **Target** of the assertion. In the normative part, this field identifies one of the four PAdES baseline signatures [1] Conformance Levels.

4) **Prerequisite** (optional) is, according to [i.3], "*a logical expression (similar to a Predicate) which further qualifies the Target for undergoing the core test (expressed by the Predicate) that addresses the Normative Statement*". It is used for building test assertions corresponding to requirements that are imposed under certain conditions.

5) **Predicate** fully and unambiguously defining the assertion to be tested.

6) **Prescription level.** Three levels are defined: mandatory, recommended and permitted, whose semantics is to be interpreted as described in clause 3.1.2 of [i.3].

7) **Tag:** information on the element tested by the assertion.

5 Testing conformance to PAdES-B-B signatures

5.1 Introduction

The present clause specifies the whole set of assertions to be tested on applications claiming conformance to PAdES-B-B signatures as specified in ETSI EN 319 142-1 [1].

Clause 5.2 specifies assertions for testing those constraints imposed by the PAdES building blocks and baseline signatures specification [1] to the signature dictionary elements.

Clause 5.3 specifies assertions for testing those constraints imposed by the PAdES building blocks and baseline signatures specification [1] to the CMS signature included in the signature dictionary entry with the key Contents.

5.2 Testing signature dictionary elements

This clause defines the test assertions for signature dictionary elements requirements.

TA id: PAdES_BS/SDM/1
Normative source: [1] – Clause 6.3
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [1]
Predicate: For new signatures, applications include the claimed time of signing in the signature dictionary entry with the key M.
Prescription level: **mandatory**
Tag: PAdES baseline signatures.

TA id: PAdES_BB/SDL/1
Normative source: [1] – Clause 6.3
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include the CPU host name or physical location of the signing in the signature dictionary entry with the key Location.
Prescription level: **permitted**
Tag: PAdES baseline and additional signatures.

TA id: PAdES_BB/SDR/1
Normative source: [1] – Clause 6.3
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications do not include the reason for the signing in the signature dictionary entry with the key Reason if the signature-policy-identifier attribute is present in the CMS signature.
Prescription level: **mandatory**
Tag: PAdES baseline and additional signatures.

TA id: PAdES_BB/SDR/2
Normative source: [1] – Clause 6.3
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications do not include the reason for the signing in the signature dictionary entry with the key Reason if the commitment-type-indication attribute is present in the CMS signature.
Prescription level: **mandatory**
Tag: PAdES baseline and additional signatures.

TA id: PAdES_BB/SDC/1
Normative source: [1] – Clause 4.1
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include the CMS signature in the signature dictionary entry with the key Contents.
Prescription level: **mandatory**
Tag: PAdES baseline and additional signatures.

TA id: PAdES_BB/SDCERT/1
Normative source: [1] – Clause 6.3
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications do not set the signature dictionary entry with the key Cert.
Prescription level: **mandatory**
Tag: PAdES baseline and additional signatures.

TA id: PAdES_BB/SDSF/1
Normative source: [1] – Clause 6.3
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include the value "ETSI.CAdES.detached" in the signature dictionary entry with the key SubFilter.
Prescription level: **mandatory**
Tag: PAdES baseline and additional signatures.

TA id: PAdES_BB/SDF/1
Normative source: [1] – Clause 6.3
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include the preferred signature handler to use when validating the signature itself in the signature dictionary entry with the key Filter.
Prescription level: **mandatory**
Tag: PAdES baseline and additional signatures.

TA id: PAdES_BB/SDBR/1
Normative source: [1] – Clause 6.3
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include an array of pairs of integers that shall describe the exact byte range for the digest calculation in the signature dictionary entry with the key ByteRange.
Prescription level: **mandatory**
Tag: PAdES baseline and additional signatures.

TA id: PAdES_BB/SDBR/2
Normative source: [1] – Clause 6.3
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [1] or in [2]
Prerequisites: PAdES_BS/SDBR/1
Predicate: For new signatures, the ByteRange value covers the entire file, including the signature dictionary but excluding the Contents value.
Prescription level: **mandatory**
Tag: PAdES baseline and additional signatures.

TA id: PAdES_BB/SDNAME/1
Normative source: [1] – Clause 6.3
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include the name of the person or authority signing the document in the signature dictionary entry with the key Name.
Prescription level: **permitted**
Tag: PAdES baseline and additional signatures.

TA id: PAdES_BB/SDCI/1
Normative source: [1] – Clause 6.3
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include a contact information of the signer in the signature dictionary entry with the key ContactInfo.
Prescription level: **permitted**
Tag: PAdES baseline and additional signatures.

5.3 Testing CMS signature elements

This clause defines the test assertions for the CMS signature, included in the signature dictionary entry with the key Contents, requirements.

Test assertions for SignedData.certificates attribute:

TA id: PAdES_BB/CER/1
Normative source: [1] – Clause 6.3
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include the signing certificate in the SignedData.certificates attribute of the CMS signature.
Prescription level: **mandatory**
Tag: PAdES baseline and additional signatures.

TA id: PAdES_BB/CER/2
Normative source: [1] – Clause 6.3
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [1] or in [2]
Prerequisites: PAdES_BB/CER/1
Predicate: For new signatures, applications include all certificates needed for path building in the SignedData.certificates attribute.
Prescription level: **recommended**
Tag: PAdES baseline and additional signatures.

Test assertions for ESS attribute:

TA id: PAdES_BB/ESS/1
Normative source: [1] – Clause 6.3
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include the ESS signing-certificate or signing-certificate-v2 attribute in signedAttrs for every signerInfo in CMS signature.
Prescription level: **mandatory**
Tag: conformance layer = B-Level of PAdES baseline profile.

TA id: PAdES_BB/ESS/2
Normative source: [1] – Clause 6.3
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [1] or in [2]
Prerequisites: PAdES_BS/ESS/1
Predicate: For new signatures, applications include the ESS-signing-certificate in signedAttrs for every signerInfo in CMS signature if SHA-1 hash algorithm is used.
Prescription level: **mandatory**
Tag: PAdES baseline and additional signatures.

TA id: PAdES_BB/ESS/3
Normative source: [1] – Clause 6.3
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [1] or in [2]
Prerequisites: PAdES_BS/ESS/1
Predicate: For new signatures, applications include the ESS-signing-certificate-v2 in signedAttrs for every signerInfo in CMS signature if another hash algorithm than SHA-1 is used.
Prescription level: **mandatory**
Tag: PAdES baseline and additional signatures.

TA id: PAdES_BB/ESS/4
Normative source: [1] – Clause 6.3
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [1] or in [2]
Prerequisites: PAdES_BS/ESS/1
Predicate: For new signatures, applications include the ESS signing-certificate-v2 attribute in signedAttrs for every signerInfo in CMS signature.
Prescription level: **recommended**
Tag: PAdES baseline and additional signatures.

Test assertion for message-digest attribute presence in CMS signature:

TA id: PAdES_BB/MD/1
Normative source: [1] – Clause 6.3
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include message-digest attribute in CMS signature.
Prescription level: **mandatory**
Tag: PAdES baseline and additional signatures.