ETSI TS 119 144-5 V1.1.1 (2016-06)

Electronic Signatures and Infrastructures (ESI);
PAdES digital signatures -
Testing Conformance and Interoperability;
Part 5: Testing Conformance of additional PAdES signatures

Reference
DTS/ESI-0019144-5

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

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 5 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 additional PAdES signatures profiles as specified in ETSI EN 319 142-2 [3]. It defines only the checks that are specific to additional PAdES signatures. The set of checks that are common to both additional and baseline PAdES signatures, are defined in ETSI TS 119 144-4 [6].

The complete set of checks to be performed by any tool on additional PAdES signatures is the union of the sets defined within the present document and the set of common checks for testing conformance against ETSI EN 319 142-1 [1] and ETSI EN 319 142-2 [3] defined in ETSI TS 119 144-4 [6], as indicated in the normative clauses of the present document.

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 additional PAdES 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 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

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

[4] ETSI TS 119 134-4: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance of XAdES baseline signatures".

[5] IETF RFC 2315: "PKCS #7: Cryptographic Message Syntax Version 1.5".

[6] ETSI TS 119 144-4: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance against building blocks and PAdES baseline signatures".

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

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

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.3] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.3] apply.

4 Overview

The present clause describes the main aspects of the technical approach used for specifying the set of checks to be performed for testing conformance to ETSI EN 319 142-2 [3].

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 additional PAdES signatures as specified in ETSI EN 319 142-2 [3], the present document classifies the whole set of requirements specified in ETSI EN 319 142-1 [1] and in ETSI EN 319 142-2 [3] in two groups as follows:

1) Requirements "PAdES_BB" (after "PAdES building blocks"): requirements defined in clause 4, clause 5, clause 6 of ETSI EN 319 142-1 [1] 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 [3]. The checks for these requirements are defined in ETSI TS 119 144-4 [6]. When needed in the present document, such checks are referred by their TA_id.

2) Requirements "PAdES_AS" (after "Additional PAdES signatures"): requirements defined in clauses 4, 5 and 6 of ETSI EN 319 142-2 [3]. These are requirements specific to Extended CAdES signatures.

a) In order to test conformance to ETSI EN 319 142-2 [3], 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 are 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.2]. Each test assertion includes:

1) Unique identifier for further referencing. The identifiers start with "PAdES_AS", after "Additional PAdES signature".

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 format specified in Additional PAdES signatures specification [3].

4) **Prerequisite** (optional) is, according to [i.2], "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 optional, whose semantics is to be interpreted as described in clause 3.1.2 of [i.2].

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

The presentation of the checks is organized following the formats of Additional PAdES signatures specified in ETSI EN 319 142-2 [3]. The following signature formats is considered:

- CMS Signatures in PDF.
- PAdES-E-BES.
- PAdES-E-EPES.
- PAdES-E-LTV.
- XAdES Signatures signing XML content in PDF.

5 Testing conformance to CMS signatures in PDF profile

5.1 Introduction

The present clause specifies the set of assertions to be tested on signatures claiming conformance to the CMS signatures in PDF profile as specified by clause 4 of ETSI EN 319 142-2 [3].

The next clauses specify the assertions for testing the elements that are profiled by clause 4 of ETSI EN 319 142-2 [3]. The constraints imposed by clause 4 of ETSI EN 319 142-2 [3] and PKCS #7 syntax [5] to the signature elements are tested.

Clause 5.2 specifies the assertions for testing the elements that are profiled by clause 4 of ETSI EN 319 142-2 [3].

Clause 5.3 specifies the assertions for testing the properties that are specified by the PKCS #7 syntax [5].

5.2 Testing signature dictionary elements

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

PAdES_BB/SDC/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

TA id: PAdES_AS/SDC/1
Normative source: [3] – Clause 4.2.1
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [3]
Prerequisites: PAdES_BB/DSC/1
Predicate: For new signatures, applications encode the signature, included in the signature dictionary entry with the key Contents, as a DER-encoded PKCS#7 binary data object.
Prescription level: **mandatory**
Tag: Additional PAdES signatures.

PAdES_BB/SDBR/1-2 checks as specified in ETSI TS 119 144-4 [6] shall apply.

PAdES_BB/SDF/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

TA id: PAdES_AS/SDSF/1
Normative source: [3] – Clause 4.2.2
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [3]
Predicate: For new signatures, applications include the string "adbe.pkcs7.detached" in the SubFilter entry of the signature dictionary.
Prescription level: **mandatory**
Tag: Additional PAdES signatures.

TA id: PAdES_AS/SDSF/2
Normative source: [3] – Clause 4.2.2
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [3]
Predicate: While validating signatures, applications accept the string "adbe.pkcs7.detached" or "adbe.pkcs7.sha1" in the SubFilter entry of the signature dictionary.
Prescription level: **recommended**
Tag: Additional PAdES signatures.

TA id: PAdES_AS/SDM/1
Normative source: [3] – Clause 4
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [3]
Predicate: For new signatures, applications include the claimed time of signing in the M entry of the signature dictionary.
Prescription level: **permitted**
Tag: Additional PAdES signatures.

PAdES_BB/SDL/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

PAdES_BB/SDR/1-2 checks as specified in ETSI TS 119 144-4 [6] shall apply.

PAdES_BB/SDCERT/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

PAdES_BB/SDCI/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

PAdES_BB/SDNAME/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

5.3 Testing PKCS #7 signature elements

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

Test assertions for SignedData.certificates attribute:

PAdES_BB/CER/1-2 checks as specified in ETSI TS 119 144-4 [6] shall apply.

Test assertion for revocation data attribute:

TA id: PAdES_AS/CRL/1
Normative source: [3] – Clause 4.2.1
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [3]
Predicate: For new signatures, applications include all crls or ocsp responses needed for certificates validation in the signed attributes of the signature.
Prescription level: **recommended**
Tag: Additional PAdES signatures.

Test assertion for timestamp signature attribute:

TA id: PAdES_AS/TST/1
Normative source: [1] – Clause 4.2.1
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [3]
Predicate: For new signatures, applications include a timestamp in the unsigned attributes of the signature.
Prescription level: **recommended**
Tag: Additional PAdES signatures.

Test assertion for signing time attribute:

TA id: PAdES_AS/STI/1
Normative source: [1] – Clause 4
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [3]
Predicate: For new signatures, applications include a claimed signing time in the signed attributes of the signature.
Prescription level: **permitted**
Tag: Additional PAdES signatures.

Test assertion for signer-location attribute:

TA id: PAdES_AS/SL/1
Normative source: [1] – Clause 4
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [3]
Predicate: For new signatures, applications include a signer-location in the signed attributes of the signature.
Prescription level: **permitted**
Tag: Additional PAdES signatures.

6 Testing conformance to PAdES-E-BES and PAdES-E-EPES additional signatures

6.1 Introduction

The present clause specifies the set of assertions to be tested on signatures claiming conformance to PAdES-E-BES and PAdES-E-EPES signatures level as specified by clause 5 of ETSI EN 319 142-2 [3].

The next clauses specify the assertions for testing whether the elements that are profiled by ETSI EN 319 142-2 [3], are actually conformant to these levels. The constraints imposed by the PAdES-E-BES and PAdES-E-EPES levels and CAdES specification [2] to the signature elements are tested.

Clause 6.2 specifies the assertions for testing whether the elements that are profiled by PAdES-E-BES level in ETSI EN 319 142-2 [3], are actually conformant to this level.

Clause 6.3 specifies the assertions for testing whether the elements that are profiled by PAdES-E-EPES level in ETSI EN 319 142-2 [3] are actually conformant to this level.

6.2 Testing PAdES-E-BES signature dictionary and CMS signature elements

6.2.1 Testing signature dictionary elements

This clause specifies assertions for testing those constraints imposed by the CAdES specification [2] and the PAdES-E-BES level [3] to the signature dictionary elements.

PAdES_BB/SDC/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

PAdES_BB/SDBR/1-2 checks as specified in ETSI TS 119 144-4 [6] shall apply.

PAdES_BB/SDF/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

PAdES_BB/SDSF/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

PAdES_AS/SDM/1 check in clause 5.1 shall apply.

PAdES_BB/SDL/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

PAdES_BB/SDR/1-2 checks as specified in ETSI TS 119 144-4 [6] shall apply.

PAdES_BB/SDCERT/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

PAdES_BB/SDCI/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

PAdES_BB/SDNAME/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

6.2.2 Testing CMS signature elements

This clause specifies assertions for testing those constraints imposed by the CAdES specification [2] and the PAdES-E-BES level [3] to the CMS signature elements.

Test assertions for SignedData.certificates attribute:

- PAdES_BB/CER/1-2 checks as specified in ETSI TS 119 144-4 [6] shall apply.

Test assertion for timestamp signature attribute:

- PAdES_AS/TST/1 in clause 5.2 shall apply.

Test assertion for signing time attribute:

- PAdES_AS/STI/1 in clause 5.2 shall apply.

Test assertion for signer-location attribute:

- PAdES_AS/SL/1 in clause 5.2 shall apply.

Test assertions for ESS attribute:

- PAdES_BB/ESS/1-2-3-4 checks as specified in ETSI TS 119 144-4 [6] shall apply.

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

- PAdES_BB/MD/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

Test assertions for ContentType attribute in CMS signature:

- PAdES_BB/CTY/1-2 checks as specified in ETSI TS 119 144-4 [6] shall apply.

Test assertion for counter-signature attribute presence in CMS signature:

- PAdES_BB/CS/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

Test assertion for content-reference attribute presence in CMS signature:

- PAdES_BB/CR/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

Test assertion for content-identifier attribute presence in CMS signature:

- PAdES_BB/CI/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

Test assertion for content-hints attribute presence in CMS signature:

- PAdES_BB/CH/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

Test assertion for commitment-type-indication attribute presence in CMS signature:

- PAdES_BB/CTI/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

Test assertion for signer-location attribute presence in CMS signature:

- PAdES_BB/SL/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

Test assertion for signer-attributes-v2 attribute presence in CMS signature:

- PAdES_BB/SA/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

Test assertion for content-time-stamp attribute presence in CMS signature:

- PAdES_BB/CTS/1 check as specified in ETSI TS 119 144-4 [6] shall apply.

6.3 Testing PAdES-E-EPES signature dictionary and CMS signature elements

6.3.1 Testing signature dictionary elements

This clause specifies assertions for testing those constraints imposed by the CAdES specification [2] and the PAdES-E-EPES level [3] to the signature dictionary elements.

PAdES_BB/SDBR/1-2 checks as specified in ETSI TS 119 144-4 [6] shall apply.

6.3.2 Testing CMS signature elements

This clause specifies assertions for testing those constraints imposed by the CAdES specification [2] and the PAdES-E-EPES level [3] to the CMS signature elements.

It defines the test assertion for signature-policy-identifier attribute presence in CMS signature.

TA id: PAdES_AS/SPID/1
Normative source: [3] – Clause 5.4
Target: PAdES signature generator claiming conformance to PAdES signatures as specified in [3]
Predicate: For new signatures, applications include signature-policy-identifier attribute in CMS signature.
Prescription level: **mandatory**
Tag: Additional PAdES signatures.

7 Testing conformance to PAdES-E-LTV additional signatures

7.1 General requirements

The present clause specifies the set of assertions to be tested on signatures claiming conformance to the PAdES-E-LTV signatures level as specified by clause 5 of ETSI EN 319 142-2 [3].

The next clauses specify the assertions for testing whether the elements that are profiled by ETSI EN 319 142-2 [3], are actually conformant to this level. The constraints imposed by the PAdES-E-LTV signatures level to the signature elements are tested.

Clause 7.1 specifies the assertions for testing Document Security Store dictionary elements requirements.

Clause 7.2 specifies the assertions for testing Document Time-Stamp dictionary elements requirements.

PAdES signatures conformant to PAdES-E-LTV level as specified in ETSI EN 319 142-2 [3] are built on PAdES signatures already conformant to PAdES-E-BES or PAdES-E-EPES levels. In consequence, PAdES signatures conformant to PAdES-E-LTV level shall fulfil the requirements specified in clauses 5.1 or 5.2 of the present document and all the requirements defined in the clauses 7.2 and 7.3.

7.2 Testing DSS dictionary

This clause defines the test assertion for Document Security Store dictionary elements requirements.

PAdES_BB/DSS/1-2-3-4-5 checks as specified in ETSI TS 119 144-4 [6] shall apply.

7.3 Testing DTS dictionary

This clause defines the test assertion for Document Time-Stamp dictionary element requirements.

PAdES_BB/DTS/2-3-4-5 checks as specified in ETSI TS 119 144-4 [6] shall apply.

8 Testing conformance to profiles for XAdES signatures signing XML content in PDF specification

A PAdES signature conformant to the profiles for XAdES signatures signing XML content in PDF specified in ETSI EN 319 142-2 [3] is built on arbitrary XML document signed with XAdES signatures that is embedded within a PDF file. In consequence, PAdES signatures conformant to the above profiles specified in ETSI EN 319 142-2 [3] contain XAdES signatures that shall fulfil the requirements specified in clause 5 of ETSI TS 119 134-4 [4].

History

Document history		
V1.1.1	June 2016	Publication