ETSI TS 119 124-5 V1.1.1 (2016-06)

Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 5: Testing conformance of extended CAdES signatures

Reference

DTS/ESI-0019124-5

Keywords

CAdES, conformance, e-commerce, electronic signature, 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

Copyright Notification

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 CAdES 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 checks to be performed for testing conformance of CAdES signatures against extended CAdES signatures as specified in ETSI EN 319 122-2 [2]. It defines only the checks that are specific to extended CAdES signatures. The set of checks that are common to both extended and baseline CAdES signatures, are defined in ETSI TS 119 124-4 [3].

The complete set of checks to be performed by any tool on CAdES extended signatures is the union of the sets defined within the present document and the set of common checks for testing conformance against ETSI EN 319 122-1 [1] and ETSI EN 319 122-2 [2] defined in ETSI TS 119 124-4 [3], 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 CAdES [1].

Regarding CAdES attributes, the present document explicitly differentiates between structural requirements that are defined on building blocks, and the requirements specified for extended CAdES 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 CAdES [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 https://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 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[2] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[3] ETSI TS 119 124-4: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing conformance of CAdES 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 119 124-1: "Electronic Signatures and Infrastructures (ESI); CAdES 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.

3.2 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 set of checks to be performed for testing conformance to ETSI EN 319 122-2 [2].

ETSI EN 319 122-1 [1] defines requirements for building blocks and CAdES baseline signatures. For the purpose of identifying the whole set of test assertions required for testing conformance against extended CAdES signatures as specified in ETSI EN 319 122-2 [2], the present document classifies the whole set of requirements specified in ETSI EN 319 122-1 [1] and in ETSI EN 319 122-2 [2] in two groups as follows:

1) Requirements "CAdES_BB" (after "CAdES building blocks"): requirements defined in clauses 4, 5, and annex A of ETSI EN 319 122-1 [1] that have to be satisfied by both CAdES baseline signatures as specified in ETSI EN 319 122-1 [1] and extended CAdES signatures as specified in ETSI EN 319 122-2 [2]. The checks for these requirements are defined in ETSI TS 119 124-4 [3]. When needed in the present document, such checks are referred by their TA_id.

2) Requirements "CAdES_ES" (after "Extended CAdES signatures"): requirements defined in clauses 5 and 6 of ETSI EN 319 122-2 [2]. These are requirements specific to extended CAdES signatures.

a) In order to test conformance to ETSI EN 319 122-2 [2], 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.3]. Each test assertion includes:

1) Unique identifier for further referencing. The identifiers of the assertions defined within the present document start with "CAdES_ES", after "Extended CAdES signatures".

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 Extended CAdES signatures specification [2].

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.

The presentation of the checks are organized following the formats of extended CAdES signatures specified in [2]. The following signature levels are considered:

- CAdES-E-BES.
- CAdES-E-EPES.
- CAdES-E-T.
- CAdES-E-A.

5 Testing conformance to CAdES-E-BES extended signatures

5.1 Introduction

This clause specifies the set of assertions to be tested on signatures claiming conformance to the CAdES-E-BES signatures level as specified by ETSI EN 319 122-2 [2].

The next clauses specify the assertions for testing whether the elements that are profiled by ETSI EN 319 122-2 [2], are actually conformant to this level. The constraints imposed by the extended CAdES signatures specification [2] to the CMS Signature elements are tested.

5.2 Testing CMSversion

This clause defines the test assertions for SignedData.CMSversion attribute presence in CMS signature.

The CAdES_BB/CMSV check in ETSI TS 119 124-4 [3] shall apply.

5.3 Testing DigestAlgorithmIdentifiers

This clause defines the test assertions for SignedData.DigestAlgorithmIdentifiers attribute presence in CMS signature.

The CAdES_BB/DAI check in ETSI TS 119 124-4 [3] shall apply.

5.4 Testing EncapsulatedContentInfo

This clause defines the test assertions for SignedData.EncapsulatedContentInfo attribute presence in CMS signature.

The CAdES_BB/ECI check in ETSI TS 119 124-4 [3] shall apply.

5.5 Testing SignedData.certificates

This clause defines the test assertions for SignedData.certificates attribute presence in CMS signature.

The CAdES_BB/SDC/1 and 2 checks in ETSI TS 119 124-4 [3] shall apply.

5.6 Testing SignedData.crls

This clause defines the test assertions for SignedData.crls attribute.

The CAdES_BB/SDCRL/1, 2 and 3 checks in ETSI TS 119 124-4 [3] shall apply.

5.7 Testing SignerInfos

This clause defines the test assertions for SignedData.SignerInfos attribute presence in CMS signature.

The CAdES_BB/SI/1 check in ETSI TS 119 124-4 [3] shall apply.

5.8 Testing content-type

This clause defines the test assertions for ContentType attribute presence in CMS signature.

The CAdES_BB/CTY/1 check in ETSI TS 119 124-4 [3] shall apply.

5.9 Testing message-digest

This clause defines the test assertion for message-digest attribute presence in CMS signature.

The CAdES_BB/MD/1 check in ETSI TS 119 124-4 [3] shall apply.

5.10 Testing signing-time

This clause defines the test assertions for SigningTime attribute presence in CMS signature.

TA id: CAdES_ES/STI/1
Normative source: [2] - Clause 4.3
Target: CAdES signature generator claiming conformance to CAdES-E-BES signatures format as specified in [2]
Predicate: For new signatures, applications include SigningTime attribute in CAdES signature.
Prescription level: **permitted**
Tag: CAdES-E-BES signatures.

The CAdES_BB/STI/1 check in ETSI TS 119 124-4 [3] shall apply.

5.11 Testing Enhanced Security Services (ESS)

This clause defines the test assertions for ESS attribute presence in CMS signature.

The CAdES_BB/ESS/1, 2, 3 and 4 checks in ETSI TS 119 124-4 [3] shall apply.

5.12 Testing commitment-type-indication

This clause defines the test assertion for commitment-type-indication attribute presence in CMS signature.

The CAdES_BB/CTI/1 check in ETSI TS 119 124-4 [3] shall apply.

5.13 Testing signer-location

This clause defines the test assertion for signer-location attribute presence in CMS signature.

The CAdES_BB/SL/1 check in ETSI TS 119 124-4 [3] shall apply.

5.14 Testing signer-attributes-v2

This clause defines the test assertion for signer-attributes attribute presence in CMS signature.

The CAdES_BB/SA/1 check in ETSI TS 119 124-4 [3] shall apply.

5.15 Testing counter-signature

This clause defines the test assertion for counter-signature attribute presence in CMS signature.

The CAdES_BB/CS/1 check in ETSI TS 119 124-4 [3] shall apply.

5.16 Testing content-time-stamp

This clause defines the test assertion for content-time-stamp attribute presence in CMS signature.

The CAdES_BB/CTS/1 check in ETSI TS 119 124-4 [3] shall apply.

5.17 Testing content-reference

This clause defines the test assertion for content-reference attribute presence in CMS signature.

The CAdES_BB/CR/1 check in ETSI TS 119 124-4 [3] shall apply.

5.18 Testing content-identifier

This clause defines the test assertion for content-identifier attribute presence in CMS signature.

The CAdES_BB/CI/1 check in ETSI TS 119 124-4 [3] shall apply.

5.19 Testing content-hints

This clause defines the test assertion for content-hints attribute presence in CMS signature.

The CAdES_BB/CH/1 check in ETSI TS 119 124-4 [3] shall apply.