ETSI TS 119 124-4 V1.1.1 (2016-06)

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

Reference
DTS/ESI-0019124-4

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

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 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 set of checks to be performed for testing conformance of CAdES signatures against CAdES baseline signatures as specified in ETSI EN 319 122-1 [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 CAdES [1].

Regarding CAdES attributes, the present document explicitly differentiates between structural requirements that are defined on building blocks, and the requirements specified for CAdES 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 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 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 319 122-1: "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] IETF RFC 5652 (09-2009): "Cryptographic Message Syntax (CMS)".

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 whole set of checks to be performed for testing conformance to ETSI EN 319 122-1 [1].

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 CAdES baseline signatures as specified in ETSI EN 319 122-1 [1], the present document classifies the whole set of requirements specified in ETSI EN 319 122-1 [1] in two groups as follows:

1) Requirements "CAdES_BS" (after "CAdES baseline signatures"): requirements defined in clauses 5 and 6 of ETSI EN 319 122-1 [1]. These are requirements specific to CAdES baseline signatures.

2) 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].

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 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 documents start with "CAdES_BS", after "CAdES baseline signatures" and "CAdES_BB", after "CAdES 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 CAdES baseline signatures [1] 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.

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 CAdES-B-B signatures

5.1 Introduction

The present clause specifies the set of assertions to be tested on applications claiming conformance to CAdES-B-B signatures as specified in ETSI EN 319 122-1 [1].

Clause 5.2 specifies assertions for testing those constraints imposed by the CAdES baseline signatures specification [1] to the CMS Signature elements.

Clause 5.3 specifies assertions for testing those constraints imposed or permitted by the CAdES signatures specifications [1] or [2] to the CMS Signature elements.

5.2 Testing CMS Signature elements

5.2.1 Testing algorithm requirements

This clause defines the test assertion for algorithm used as digest algorithm.

TA id: CAdES_BS/ALG/1
Normative source: [1] – Clause 6.2.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1]
Predicate: For new signatures, applications do not use MD5 algorithm as digest algorithm.
Prescription level: **mandatory**
Tag: CAdES baseline signatures.

5.2.2 Testing content-type

5.2.2.1 General

The following clauses define the test assertions for content-type attribute presence in CMS signature.

5.2.2.2 Test assertions common to CAdES baseline and extended signatures

TA id: CAdES_BB/CTY/1
Normative source: [1] – Clause 5.1.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include ContentType attribute in CMS signature.
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

5.2.2.3 Test assertions specific to CAdES baseline signatures

TA id: CAdES_BS/CTY/1
Normative source: [1] – Clause 6.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1]
Predicate: For new signatures, applications set the value id-data in ContentType attribute in CMS signature.
Prescription level: **mandatory**
Tag: CAdES baseline signatures.

5.2.3 Testing message-digest

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

TA id: CAdES_BB/MD/1
Normative source: [1] – Clause 5.1.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include message-digest attribute in CMS signature.
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

5.2.4 Testing CMSversion

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

TA id: CAdES_BB/CMSV
Normative source: [3] – Clause 5.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include SignedData.CMSversion attribute in CMS signature.
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

5.2.5 Testing DigestAlgorithmIdentifiers

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

TA id: CAdES_BB/DAI
Normative source: [3] – Clause 5.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include SignedData.DigestAlgorithmIdentifiers attribute in CMS signature.
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

5.2.6 Testing EncapsulatedContentInfo

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

TA id: CAdES_BB/ECI
Normative source: [3] – Clause 5.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include SignedData.EncapsulatedContentInfo attribute in CMS signature.
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

5.2.7 Testing SignedData.certificates

5.2.7.1 General

The following clauses define the test assertions for SignedData.certificates attribute presence in CMS signature.

5.2.7.2 Test assertions common to CAdES baseline and extended signatures

TA id: CAdES_BB/SDC/1
Normative source: [3] – Clause 5.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include all certificates needed for path building in the SignedData.certificates attribute.
Prescription level: **recommended**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_BB/SDC/2
Normative source: [3] – Clause 5.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications avoid duplication of certificate values in the SignedData.certificates attribute.
Prescription level: **recommended**
Tag: CAdES baseline and extended signatures.

5.2.7.3 Test assertions specific to CAdES baseline signatures

TA id: CAdES_BS/SDC/1
Normative source: [1] – Clause 6.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1]
Predicate: For new signatures, applications include the signing certificate in the SignedData.certificates attribute.
Prescription level: **mandatory**
Tag: CAdES baseline signatures.

5.2.8 Testing SignedData.crls

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

TA id: CAdES_BB/SDCRL/1
Normative source: [3] – Clause 5.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include the full set of CRL values needed for the validation of the signature itself in the SignedData.crls.crl attribute.
Prescription level: **permitted**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_BB/SDCRL/2
Normative source: [3] – Clause 5.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include the full set of OCSP responses values needed for the validation of the signature itself in the SignedData.crls.other attribute.
Prescription level: **permitted**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_BB/SDCRL/3
Normative source: [3] – Clause 5.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications avoid duplication of revocation values in the SignedData.crls attribute.
Prescription level: **recommended**
Tag: CAdES baseline and extended signatures.

5.2.9 Testing SignerInfos

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

TA id: CAdES_BB/SI/1
Normative source: [3] – Clause 5.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include one or more SignerInfos attributes in SignedData.
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

5.3 Testing basic attributes for CAdES signatures

5.3.1 Testing signing-time

5.3.1.1 General

The following clauses define the test assertions for signing-time attribute presence in CMS signature.

5.3.1.2 Test assertions common to CAdES baseline and extended signatures

TA id: CAdES_BB/STI/1
Normative source: [1] – Clause 5.2.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, the value to be included in SigningTime attribute in CMS signature by applications is encoded as UTC time for dates between 1 January 1950 and 31 December 2049 (inclusive) and as GeneralizedTime for any dates with year values before 1950 or after 2049.
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

5.3.1.3 Test assertions specific to CAdES baseline signatures

TA id: CAdES_BS/STI/1
Normative source: [1] – Clause 6.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1]
Predicate: For new signatures, applications include SigningTime attribute in CMS signature.
Prescription level: **mandatory**
Tag: CAdES baseline signatures.

5.3.2 Testing Enhanced Security Services (ESS)

5.3.2.1 General

The following clauses define the test assertions for ESS attribute presence in CMS signature.

5.3.2.2 Test assertions common to CAdES baseline and extended signatures

TA id: CAdES_BB/ESS/1
Normative source: [1] – Clause 5.2.2
Target: CAdES signature generator claiming conformance to CAdES 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: CAdES baseline and extended signatures.

TA id: CAdES_BB/ESS/2
Normative source: [1] – Clause 5.2.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
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: CAdES baseline and extended signatures.

TA id: CAdES_BB/ESS/3
Normative source: [1] – Clause 5.2.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
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: CAdES baseline and extended signatures.

TA id: CAdES_BB/ESS/4
Normative source: [1] – Clause 5.2.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications do not include the issuerSerial field in the encoding of the ESS-signing-certificate and ESS-signing-certificate-v2.
Prescription level: **recommended**
Tag: CAdES baseline and extended signatures.

5.3.2.3 Test assertions specific to CAdES baseline signatures

TA id: CAdES_BS/ESS/1
Normative source: [1] – Clause 6.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [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: CAdES baseline signatures.

5.3.3 Testing countersignature

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

TA id: CAdES_BB/CS/1
Normative source: [1] – Clause 5.2.7
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For a signer, CMS signature includes countersignature attribute.
Prescription level: **permitted**
Tag: CAdES baseline and extended signatures.

5.3.4 Testing content-reference

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

TA id: CAdES_BB/CR/1
Normative source: [1] – Clause 5.2.11
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include content-reference attribute in CMS signature.
Prescription level: **permitted**
Tag: CAdES baseline and extended signatures.

5.3.5 Testing content-identifier

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

TA id: CAdES_BB/CI/1
Normative source: [1] – Clause 5.2.12
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include content-identifier attribute in CMS signature.
Prescription level: **permitted**
Tag: CAdES baseline and extended signatures.

5.3.6 Testing content-hints

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

TA id: CAdES_BB/CH/1
Normative source: [1] – Clause 5.2.4.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include content-hints attribute in CMS signature.
Prescription level: **permitted**
Tag: CAdES baseline and extended signatures.

5.3.7 Testing commitment-type-indication

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

TA id: CAdES_BB/CTI/1
Normative source: [1] – Clause 5.2.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include commitment-type-indication attribute in CMS signature.
Prescription level: **permitted**
Tag: CAdES baseline and extended signatures.

5.3.8 Testing signer-location

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

TA id: CAdES_BB/SL/1
Normative source: [1] – Clause 5.2.5
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include signer-location attribute in CMS signature.
Prescription level: **permitted**
Tag: CAdES baseline and extended signatures.

5.3.9 Testing signer-attributes-v2

This clause defines the test assertions for signer-attributes-v2 attribute presence in CMS signature.

TA id: CAdES_BB/SA/1
Normative source: [1] – Clause 5.2.6
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include signer-attributes-v2 attribute in CMS signature.
Prescription level: **permitted**
Tag: CAdES baseline and extended signatures.

5.3.10 Testing content-time-stamp

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

TA id: CAdES_BB/CTS/1
Normative source: [1] – Clause 5.2.8
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include content-time-stamp attribute in CMS signature.
Prescription level: **permitted**
Tag: CAdES baseline and extended signatures.

5.3.11 Testing mime-type

This clause defines the test assertions for mime-type attribute presence in CMS signature.

TA id: CAdES_BB/MT/1
Normative source: [1] – Clause 5.2.4.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include mime-type attribute in CMS signature.
Prescription level: **permitted**
Tag: CAdES baseline and extended signatures.

5.3.12 Testing signature-policy-identifier

This clause defines the test assertions for signature-policy-identifier attribute presence in CMS signature.

TA id: CAdES_BB/SPID/1
Normative source: [1] – Clause 5.2.9
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications include signature-policy-identifier attribute in CMS signature.
Prescription level: **permitted**
Tag: CAdES baseline and extended signatures.

5.3.13 Testing signature-policy-store

This clause defines the test assertions for signature-policy-store attribute presence in CMS signature.

TA id: CAdES_BB/SPS/1
Normative source: [1] – Clause 5.2.10
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Prerequisites: CAdES_BB/SPID/1
Predicate: For new signatures, applications include signature-policy-store attribute in CMS signature.
Prescription level: **permitted**
Tag: CAdES baseline and extended signatures.

6 Testing conformance to CAdES-B-T signatures

6.1 General

CAdES-B-T signatures as specified in [1] are built on CAdES-B-B signatures. In consequence, CAdES-B-T signatures shall fulfill the requirements specified in clause 5 of the present document and all the requirements defined in clause 6.2.

The following clause specifies assertions for testing those constraints imposed or permitted by the CAdES-B-T signatures specification [1] to the CMS Signature elements.

6.2 Testing CAdES attributes

6.2.1 Testing SignatureTimeStamp

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

TA id: CAdES_BB/STS/1
Normative source: [1] – Clause 5.3
Target: CAdES signature generator claiming conformance to CAdES-B-T signatures as specified in [1] or to CAdES-E-T, -E-C, -E-X, -E-X-Long, -E-X-L, -E-A extended signatures as specified in [2]
Predicate: For new signatures, applications include signature-time-stamp attribute in CAdES signature.
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

7 Testing conformance to CAdES-B-LT signatures

7.1 General

CAdES-B-LT signatures as specified in [1] are built on CAdES-B-T signatures. In consequence, CAdES-B-LT signatures shall fulfill the requirements specified in clauses 5 and 6 of the present document and all the requirements defined in clause 7.2.

The following clauses specify assertions for testing those constraints imposed or permitted by the CAdES-B-LT signatures specification [1] to the CMS Signature elements.

7.2 Testing CAdES attributes

7.2.1 Testing Certificate and Revocation references and values

This clause defines the test assertion for certificate, attribute certificate and revocation references and values attributes presence in CAdES signatures.

TA id: CAdES_BS/CCR/1
Normative source: [1] – Clause 6.3
Target: CAdES signature generator claiming conformance to CAdES-B-LT signatures as specified in [1]
Predicate: For new signatures, applications do not include complete-certificate–references attribute in CAdES signature.
Prescription level: **mandatory**
Tag: CAdES-B-LT baseline signatures.

TA id: CAdES_BS/CRR/1
Normative source: [1] – Clause 6.3
Target: CAdES signature generator claiming conformance to CAdES-B-LT signatures as specified in [1]
Predicate: For new signatures, applications do not include complete-revocation–references attribute in CAdES signature.
Prescription level: **mandatory**
Tag: CAdES-B-LT baseline signatures.

TA id: CAdES_BS/ACR/1
Normative source: [1] – Clause 6.3
Target: CAdES signature generator claiming conformance to CAdES-B-LT signatures as specified in [1]
Predicate: For new signatures, applications do not include attribute-certificate–references attribute in CAdES signature.
Prescription level: **mandatory**
Tag: CAdES-B-LT baseline signatures.

TA id: CAdES_BS/ARR/1
Normative source: [1] – Clause 6.3
Target: CAdES signature generator claiming conformance to CAdES-B-LT signatures as specified in [1]
Predicate: For new signatures, applications do not include attribute-revocation–references attribute in CAdES signature.
Prescription level: **mandatory**
Tag: CAdES-B-LT baseline signatures.

TA id: CAdES_BS/CV/1
Normative source: [1] – Clause 6.3
Target: CAdES signature generator claiming conformance to CAdES-B-LT signatures as specified in [1]
Predicate: For new signatures, applications do not include certificate–values attribute in CAdES signature.
Prescription level: **mandatory**
Tag: CAdES baseline signatures.

TA id: CAdES_BS/RV/1
Normative source: [1] – Clause 6.3
Target: CAdES signature generator claiming conformance to CAdES-B-LT signatures as specified in [1]
Predicate: For new signatures, applications do not include revocation-values attribute in CAdES signature.
Prescription level: **mandatory**
Tag: CAdES-B-LT signatures.

7.2.2 Testing time-stamp attributes

This clause defines the test assertion for time-stamp attributes presence in CAdES signature.

TA id: CAdES_BS/ESCTS/1
Normative source: [1] – Clause 6.3
Target: CAdES signature generator claiming conformance to CAdES-B-LT signatures as specified in [1]
Predicate: For new signatures, applications do not include CAdES-C-time-stamp attribute in CAdES signature.
Prescription level: **mandatory**
Tag: CAdES-B-LT signatures.

TA id: CAdES_BS/TSCCR/1
Normative source: [1] – Clause 6.3
Target: CAdES signature generator claiming conformance to CAdES-B-LT signatures as specified in [1]
Predicate: For new signatures, applications do not include time-stamped-certs-crls-references attribute in CAdES signature.
Prescription level: **mandatory**
Tag: CAdES-B-LT signatures.

7.2.3 Testing SignedData.certificates attribute

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

TA id: CAdES_BS/SDC/2
Normative source: [1] – Clause 6.3
Target: CAdES signature generator claiming conformance to CAdES-B-LT signatures as specified in [1]
Predicate: For new signatures, applications include all certificates needed for path building in the SignedData.certificates attribute.
Prescription level: **mandatory**
Tag: CAdES-B-LT signatures.

7.2.4 Testing revocation values

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

TA id: CAdES_BS/SDCRL/1
Normative source: [1] – Clause 6.3
Target: CAdES signature generator claiming conformance to CAdES-B-LT signatures as specified in [1]
Predicate: For new signatures, applications include the full set of revocation data (CRL or OCSP responses) that have been used in the validation of the signature itself in the SignedData.crls attribute.
Prescription level: **mandatory**
Tag: CAdES-B-LT signatures.

8 Testing conformance to CAdES-B-LTA signatures

8.1 General

CAdES-B-LTA signatures as specified in [1] are built on CAdES-B-LT signatures. In consequence, CAdES-B-LTA signatures shall fulfill the requirements specified in clauses 5, 6 and 7 of the present document and all the requirements defined in clause 8.2.

The following clauses specify assertions for testing those constraints imposed or permitted by the CAdES-B-LTA signatures specification [1] to the CMS Signature elements.

8.2 Testing CAdES attributes

8.2.1 Testing ArchiveTimeStampV3

This clause defines the test assertion for archive-time-stamp-v3 attribute presence in CAdES signature.

TA id: CAdES_BB/ATSV3/1
Normative source: [1] – Clause 5.5.3
Target: CAdES signature generator claiming conformance to CAdES-B-LTA signatures as specified in [1] or to CAdES-E-A extended signatures as specified in [2]
Predicate: For new signatures, applications include archive-time-stamp-v3 attribute in CAdES signature.
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_BB/ATSHI/1
Normative source: [1] – Clause 5.5.2
Target: CAdES signature generator claiming conformance to CAdES-B-LTA signatures as specified in [1] or to CAdES-E-A extended signatures as specified in [2]
Prerequisites: CAdES_BS/ATSV3/1
Predicate: For new signatures, applications include ats-hash-index-v3 attribute in archive-time-stamp-v3 attribute in CAdES signature.
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

8.2.2 Testing time-stamp attributes

This clause defines the test assertion for time-stamp attributes presence in CAdES signature.

TA id: CAdES_BB/ATS/1
Normative source: [1]
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications do not include archive-time-stamp (OID 1.2.840.113549.1.9.16.2.27) attribute in CAdES signature.
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_BB/ATSV2/1
Normative source: [1] – Clause A.2.4
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications do not include archive-time-stampV2 (OID 1.2.840.113549.1.9.16.2.48) attribute in CAdES signature.
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_BB/LTV/1
Normative source: [1] – Clause A.2.5
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: For new signatures, applications do not include long-term-validation attribute in CAdES signature.
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

Annex A (normative): Test assertions derived from attributes definition

A.1 General

This annex specifies test assertions focused on testing the structure of the attributes specified by CAdES [1] and CMS [3].

A.2 Testing CMS defined attributes

A.2.1 Testing content-type attribute

TA id: CAdES_ASN/CTY/1
Normative source: [3] – Clause 11.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the content-type attribute id-contentType OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) 3 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CTY/2
Normative source: [3] – Clause 11.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: Content-type attribute values have ASN.1 type OBJECT IDENTIFIER
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.2.2 Testing data content-type

TA id: CAdES_ASN/CTY/3
Normative source: [3] – Clause 4
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the data content type id-data OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 1 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.2.3 Testing signed-data content-type

TA id: CAdES_ASN/CTY/4
Normative source: [3] – Clause 5
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the signed-data content type id-signedData OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 2 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.2.4 Testing message-digest attribute

TA id: CAdES_ASN/MD/1
Normative source: [3] – Clause 11.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the message-digest attribute id-messageDigest OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) 4 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/MD/2
Normative source: [3] – Clause 11.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: Message-digest attribute values have ASN.1 type OCTET STRING
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.2.5 Testing CMSVersion

TA id: CAdES_ASN/CMSV/1
Normative source: [3] – Clause 10.2.5
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: CMSVersion values have ASN.1 type INTEGER in the set {1, 2, 3, 4, 5}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.2.6 Testing DigestAlgorithmIdentifiers

TA id: CAdES_ASN/DAI/1
Normative source: [3] – Clause 10.1.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: DigestAlgorithmIdentifiers values have ASN.1 type SET of SEQUENCE in which every sequence includes, at least, an OBJECT IDENTIFIER identifying a cryptographic algorithm
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.2.7 Testing SignatureAlgorithmIdentifiers

TA id: CAdES_ASN/SAI/1
Normative source: [3] – Clause 10.1.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: SignatureAlgorithmIdentifiers values have ASN.1 type SET of SEQUENCE in which every sequence includes, at least, an OBJECT IDENTIFIER identifying a cryptographic algorithm
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.2.8 Testing EncapsulatedContentInfo

TA id: CAdES_ASN/ECI/1
Normative source: [3] – Clause 5.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: EncapsulatedContentInfo has ASN.1 type SEQUENCE including an OBJECT IDENTIFIER, identifying the content type, and, optionally, an OCTET STRING
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.2.9 Testing SignedData.certificates

TA id: CAdES_ASN/SDC/1
Normative source: [3] – Clause 10.2.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: SignedData.certificates values have ASN.1 type SET of CHOICES
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.2.10 Testing SignedData.crls

TA id: CAdES_ASN/SDCRL/1
Normative source: [3] – Clause 10.2.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: SignedData.crls values have ASN.1 type SET of CHOICES
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.2.11 Testing SignerInfo attribute

TA id: CAdES_ASN/SI/1
Normative source: [3] – Clause 5.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: SignerInfo has ASN.1 type SEQUENCE including CMSVersion, SignerIdentifier, DigestAlgorithmIdentifier, optional SignedAttributes, SignatureAlgorithmIdentifier, SignatureValue and optional UnsignedAttributes attributes.
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.2.12 Testing AlgorithmIdentifier

TA id: CAdES_ASN/AI/1
Normative source: [3] – Clause 10.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: AlgorithmIdentifier values have ASN.1 type SEQUENCE including at least, an OBJECT IDENTIFIER identifying a cryptographic algorithm
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3 Testing basic attributes for CAdES signatures

A.3.1 Testing signing-time attribute

TA id: CAdES_ASN/STI/1
Normative source: [3] – Clause 11.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the signing-time attribute id-signingTime OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) 5 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/STI/2
Normative source: [3] – Clause 11.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: Signing-time attribute values have ASN.1 type CHOICE of {UTCTime, GeneralizedTime}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/STI/3
Normative source: [3] – Clause 11.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: Dates between 1 January 1950 and 31 December 2049 (inclusive) are encoded as UTCTime. Any dates with year values before 1950 or after 2049 are encoded as GeneralizedTime
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.2 Testing ESS signing-certificate

TA id: CAdES_ASN/ESS/1
Normative source: [1] – Clause 5.2.2.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the ESS signing-certificate attribute id-aa-signingCertificate OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) id-aa(2) 12 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/ESS/2
Normative source: [1] – Clause 5.2.2.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: ESS signing-certificate attribute values have ASN.1 type SEQUENCE of {SEQUENCE of ESSCertID, SEQUENCE of PolicyInformation OPTIONAL}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/ESS/3
Normative source: [1] – Clause 5.2.2.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: ESSCertID values have ASN.1 type SEQUENCE of {Hash, IssuerSerial OPTIONAL}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/ESS/4
Normative source: [1] – Clause 5.2.2.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: Hash values have ASN.1 type OCTET STRING
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/ESS/5
Normative source: [1] – Clause 5.2.2.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: IssuerSerial values have ASN.1 type SEQUENCE of {GeneralNames, CertificateSerialNumber}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.3 Testing ESS signing-certificate-v2

TA id: CAdES_ASN/ESSv2/1
Normative source: [1] – Clause 5.2.2.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the ESS signing-certificate-v2 attribute id-aa-signingCertificateV2 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) id-aa(2) 47 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/ESSv2/2
Normative source: [1] – Clause 5.2.2.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: ESS signing-certificate-v2 attribute values have ASN.1 type SEQUENCE of {SEQUENCE of ESSCertIDv2, SEQUENCE of PolicyInformation OPTIONAL}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/ESSv2/3
Normative source: [1] – Clause 5.2.2.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: ESSCertIDv2 values have ASN.1 type SEQUENCE of {AlgorithmIdentifier, Hash, IssuerSerial OPTIONAL}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.4 Testing countersignature

TA id: CAdES_ASN/CS/1
Normative source: [3] – Clause 11.4
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the countersignature attribute id-countersignature OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) 6 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CS/2
Normative source: [3] – Clause 11.4
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: countersignature attribute values have ASN.1 type SignerInfo
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.5 Testing content-reference

TA id: CAdES_ASN/CR/1
Normative source: [1] – Clause 5.2.11
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the content-reference attribute id-aa-contentReference OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 10 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CR/2
Normative source: [1] – Clause 5.2.11
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: contentReference attribute values have ASN.1 type SEQUENCE of {ContentType, ContentIdentifier, OCTET STRING}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.6 Testing content-identifier

TA id: CAdES_ASN/CI/1
Normative source: [1] – Clause 5.2.12
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the content-identifier attribute id-aa-contentIdentifier OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 7 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CI/2
Normative source: [1] – Clause 5.2.12
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: contentIdentifier attribute values have ASN.1 type OCTET STRING
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.7 Testing content-hints

TA id: CAdES_ASN/CH/1
Normative source: [1] – Clause 5.2.4.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the content-hints attribute id-aa-contentHint OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 4}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CH/2
Normative source: [1] – Clause 5.2.4.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: contentHint attribute values have ASN.1 type SEQUENCE of {UTF8String, ContentType}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.8 Testing commitment-type-indication

TA id: CAdES_ASN/CTI/1
Normative source: [1] – Clause 5.2.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the commitment-type-indication attribute id-aa-ets-commitmentType OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 16}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CTI/2
Normative source: [1] – Clause 5.2.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: CommitmentTypeIndication attribute values have ASN.1 type SEQUENCE of {CommitmentTypeIdentifier, SEQUENCE of CommitmentTypeQualifier OPTIONAL}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CTI/3
Normative source: [1] – Clause 5.2.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: CommitmentTypeIdentifier attribute values have ASN.1 type OBJECT IDENTIFIER
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CTI/4
Normative source: [1] – Clause 5.2.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: CommitmentTypeQualifier attribute values have ASN.1 type SEQUENCE of {OBJECT IDENTIFIER, Qualifier OPTIONAL}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.9 Testing signer-location

TA id: CAdES_ASN/SL/1
Normative source: [1] – Clause 5.2.5
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the signer-location attribute id-aa-ets-signerLocation OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 17 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/SL/2
Normative source: [1] – Clause 5.2.5

Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: SignerLocation attribute values have ASN.1 type SEQUENCE of { countryName [0] DirectoryString OPTIONAL, localityName [1] DirectoryString OPTIONAL, postalAddress [2] PostalAddress OPTIONAL}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/SL/3
Normative source: [1] – Clause 5.2.5
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: PostalAddress attribute values have ASN.1 type SEQUENCE SIZE(1..6) OF DirectoryString
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/SL/4
Normative source: [1] – Clause 5.2.5
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: At least one of the fields countryName, localityName or postalAddress shall be present
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.10 Testing signer-attributes-v2

TA id: CAdES_ASN/SA/1
Normative source: [1] – Clause 5.2.6.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the signer-attributes-v2 attribute id-aa-ets-signerAttrV2 OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4) etsi(0) cades(19122) attributes(1) 1 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/SA/2
Normative source: [1] – Clause 5.2.6.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: signerAttrV2 attribute values have ASN.1 type SEQUENCE of {claimedAttributes [0] ClaimedAttributes OPTIONAL, certifiedAttributesV2 [1] CertifiedAttributesV2 OPTIONAL, signedAssertions [2] SignedAssertions OPTIONAL}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/SA/3
Normative source: [1] – Clause 5.2.6.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: ClaimedAttributes attribute values have ASN.1 type SEQUENCE of Attribute
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/SA/4
Normative source: [1] – Clause 5.2.6.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: CertifiedAttributesV2 attribute values have ASN.1 type SEQUENCE OF CHOICE {attributeCertificate [0] AttributeCertificate, otherAttributeCertificate [1] OtherAttributeCertificate}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/SA/5
Normative source: [1] – Clause 5.2.6.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: Attribute attribute values have ASN.1 type SEQUENCE of {OBJECT IDENTIFIER, SET OF DirectoryString}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/SA/6
Normative source: [1] – Clause 5.2.6.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: AttributeCertificate attribute values have ASN.1 type SEQUENCE of {AttributeCertificateInfo, AlgorithmIdentifier, BIT STRING}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/SA/7
Normative source: [1] – Clause 5.2.6.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: AttributeCertificateInfo attribute values have ASN.1 type SEQUENCE of {AttCertVersion, Holder, AttCertIssuer, AlgorithmIdentifier, CertificateSerialNumber, AttCertValidityPeriod, SEQUENCE OF Attribute, UniqueIdentifier OPTIONAL, Extensions OPTIONAL}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.11 Testing content-time-stamp

TA id: CAdES_ASN/CTS/1
Normative source: [1] – Clause 5.2.8
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the content-time-stamp attribute id-aa-ets-contentTimestamp OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 20 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CTS/2
Normative source: [1] – Clause 5.2.8
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: contentTimestamp attribute values have ASN.1 type TimeStampToken
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.12 Testing mime-type

TA id: CAdES_ASN/MT/1
Normative source: [1] – Clause 5.2.4.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the mime-type attribute id-aa-ets-mimeType OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4) etsi(0) electronic-signature-standard (1733) attributes(2) 1 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/MT/2
Normative source: [1] – Clause 5.2.4.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: mimeType attribute values have ASN.1 type UTF8String
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.13 Testing signature-policy-identifier

TA id: CAdES_ASN/SPI/1
Normative source: [1] – Clause 5.2.9.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the signature-policy-identifier attribute id-aa-ets-sigPolicyId OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) id-aa(2) 15 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/SPI/2
Normative source: [1] – Clause 5.2.9.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: sigPolicyId attribute values have ASN.1 type CHOICE {SignaturePolicyId, SignaturePolicyImplied -- not used in this version}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/SPI/3
Normative source: [1] – Clause 5.2.9.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: SignaturePolicyId attribute values have ASN.1 type SEQUENCE of {OBJECT IDENTIFIER, SigPolicyHash, SEQUENCE of SigPolicyQualifierInfo OPTIONAL}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/SPI/4
Normative source: [1] – Clause 5.2.9.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: SigPolicyHash attribute values have ASN.1 type SEQUENCE of {AlgorithmIdentifier, OCTET STRING}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/SPI/5
Normative source: [1] – Clause 5.2.9.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: SigPolicyQualifierInfo attribute values have ASN.1 type SEQUENCE of {noticeToUser | pointerToSigPolSpec | sigPolDocSpecification}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.14 Testing signature-policy-store

TA id: CAdES_ASN/SPS/1
Normative source: [1] – Clause 5.2.10
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the signature-policy-store attribute id-aa-ets-sigPolicyStore OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4) etsi(0) cades(19122) attributes(1) 3 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/SPS/2
Normative source: [1] – Clause 5.2.10
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: sigPolicyStore attribute values have ASN.1 type SEQUENCE of {SPDocSpecification, SignaturePolicyDocument}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/SPS/3
Normative source: [1] – Clause 5.2.10
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: SignaturePolicyDocument attribute values have ASN.1 type CHOICE of {OCTET STRING, IA5String}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.15 Testing signature-time-stamp

TA id: CAdES_ASN/STS/1
Normative source: [1] – Clause 5.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the signature-time-stamp attribute id-aa-signatureTimeStampToken OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 14 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/STS/2
Normative source: [1] – Clause 5.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: signatureTimeStampToken attribute values have ASN.1 type TimeStampToken
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.16 Testing complete-certificate-references

TA id: CAdES_ASN/CCR/1
Normative source: [1] – Clause A.1.1.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the complete-certificate-references attribute id-aa-ets-certificateRefs OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 21 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CCR/2
Normative source: [1] – Clause A.1.1.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: CompleteCertificateRefs attribute values have ASN.1 type SEQUENCE of {SEQUENCE of {OtherHash, IssuerSerial OPTIONAL}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CCR/3
Normative source: [1] – Clause A.1.1.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: OtherHash attribute values have ASN.1 type CHOICE of {OtherHashValue, OtherHashAlgAndValue}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CCR/4
Normative source: [1] – Clause A.1.1.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: OtherHashAlgAndValue attribute values have ASN.1 type SEQUENCE of {AlgorithmIdentifier, OtherHashValue}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CCR/5
Normative source: [1] – Clause A.1.1.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: OtherHashValue attribute values have ASN.1 type OCTET STRING
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.17 Testing complete-revocation-references

TA id: CAdES_ASN/CRR/1
Normative source: [1] – Clause A.1.2.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the complete-revocation-references attribute id-aa-ets-revocationRefs OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 22 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CRR/2
Normative source: [1] – Clause A.1.2.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: CompleteRevocationRefs attribute values have ASN.1 type SEQUENCE of { SEQUENCE of { crlids [0] CRLListID OPTIONAL, ocspids [1] OcspListID OPTIONAL, otherRev [2] OtherRevRefs OPTIONAL}}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CRR/3
Normative source: [1] – Clause A.1.2.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: CRLListID attribute values have ASN.1 type SEQUENCE of {SEQUENCE of {SEQUENCE of {OtherHash, CrlIdentifier OPTIONAL}}}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CRR/4
Normative source: [1] – Clause A.1.2.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: CrlIdentifier attribute values have ASN.1 type SEQUENCE of {Name, UTCTime, INTEGER OPTIONAL}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CRR/5
Normative source: [1] – Clause A.1.2.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: Name attribute values have ASN.1 type CHOICE of {SEQUENCE of {SET SIZE (1..MAX) of AttributeTypeAndValue}}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CRR/6
Normative source: [1] – Clause A.1.2.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: AttributeTypeAndValue attribute values have ASN.1 type SEQUENCE of {AttributeType, AttributeValue}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CRR/7
Normative source: [1] – Clause A.1.2.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: OcspListID attribute values have ASN.1 type SEQUENCE of {SEQUENCE of {SEQUENCE of {OcspIdentifier, OtherHash OPTIONAL}}}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CRR/8
Normative source: [1] – Clause A.1.2.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: OcspIdentifier attribute values have ASN.1 type SEQUENCE of {ResponderID, GeneralizedTime}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CRR/9
Normative source: [1] – Clause A.1.2.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: ResponderID attribute values have ASN.1 type CHOICE of {Name, KeyHash}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CRR/10
Normative source: [1] – Clause A.1.2.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: KeyHash attribute values have ASN.1 type OCTET STRING
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.18 Testing certificate-values

TA id: CAdES_ASN/CV/1
Normative source: [1] – Clause A.1.1.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the certificate-values attribute id-aa-ets-certValues OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 23 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/CV/2
Normative source: [1] – Clause A.1.1.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: CertificateValues attribute values have ASN.1 type SEQUENCE of {Certificate}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.19 Testing revocation-values

TA id: CAdES_ASN/RV/1
Normative source: [1] – Clause A.1.2.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the revocation-values attribute id-aa-ets-revocationValues OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 24 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/RV/2
Normative source: [1] – Clause A.1.2.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: RevocationValues attribute values have ASN.1 type SEQUENCE of {crlVals [0] SEQUENCE OF CertificateList OPTIONAL, ocspVals [1] SEQUENCE OF BasicOCSPResponse OPTIONAL, otherRevVals [2] OtherRevVals OPTIONAL}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.20 Testing CAdES-C-time-stamp

TA id: CAdES_ASN/ESCTS/1
Normative source: [1] – Clause A.1.5.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the CAdES-C-time-stamp attribute id-aa-ets-escTimeStamp OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 25}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/ESCTS/2
Normative source: [1] – Clause A.1.5.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: ESCTimeStampToken attribute values have ASN.1 type TimeStampToken
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.21 Testing time-stamped-certs-crls-references

TA id: CAdES_ASN/TSCCR/1
Normative source: [1] – Clause A.1.5.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the time-stamped-certs-crls-references attribute id-aa-ets-certCRLTimestamp OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 26}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/TSCCR/2
Normative source: [1] – Clause A.1.5.1
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: TimestampedCertsCRLs attribute values have ASN.1 type TimeStampToken
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.22 Testing ArchiveTimeStampV3

TA id: CAdES_ASN/ATSV3/1
Normative source: [1] – Clause 5.5.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the archive-time-stamp-v3 attribute id-aa-ets-archiveTimestampV3 OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4) etsi(0) electronic-signature-standard(1733) attributes(2) 4 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/ATSV3/2
Normative source: [1] – Clause 5.5.3
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: ArchiveTimeStampTokenV3 attribute values have ASN.1 type TimeStampToken
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.23 Testing ats-hash-index-v3

TA id: CAdES_ASN/ATSHI/1
Normative source: [1] – Clause 5.5.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the ats-hash-index-v3 attribute id-aa-ATSHashIndex-v3 OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4) etsi(0) cades(19122) attributes(1) 5 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/ATSHI/2
Normative source: [1] – Clause 5.5.2
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: ATSHashIndexV3 attribute values have ASN.1 type SEQUENCE of {AlgorithmIdentifier, SEQUENCE OF OCTET STRING, SEQUENCE OF OCTET STRING, SEQUENCE OF OCTET STRING}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.24 Testing long-term-validation

TA id: CAdES_ASN/LTV/1
Normative source: [1] – Clause A.2.5
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the long-term-validation attribute id-aa-ets-longTermValidation OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4) etsi(0) electronic-signature-standard (1733) attributes(2) 2 }
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/LTV/2
Normative source: [1] – Clause A.2.5
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: LongTermValidation attribute values have ASN.1 type SEQUENCE of {GeneralizedTime, CHOICE of {timeStamp [0] EXPLICIT TimeStampToken, evidenceRecord [1] EXPLICIT EvidenceRecord} OPTIONAL, extraCertificates [0] IMPLICIT CertificateSet OPTIONAL, extraRevocation [1] IMPLICIT RevocationInfoChoices OPTIONAL}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

A.3.25 Testing ArchiveTimeStampV2

TA id: CAdES_ASN/ATSV2/1
Normative source: [1] – Clause A.2.4
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: The following object identifier identifies the archive-time-stamp-v2 attribute id-aa-ets-archiveTimestampV2 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 48}
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

TA id: CAdES_ASN/ATSV2/2
Normative source: [1] – Clause A.2.4
Target: CAdES signature generator claiming conformance to CAdES signatures as specified in [1] or in [2]
Predicate: ArchiveTimeStampTokenV2 attribute values have ASN.1 type TimeStampToken
Prescription level: **mandatory**
Tag: CAdES baseline and extended signatures.

History

Document history		
V1.1.1	June 2016	Publication