ETSI TS 119 124-2 V1.1.1 (2016-06)

Electronic Signatures and Infrastructures (ESI);
CAdES digital signatures -
Testing Conformance and Interoperability;
Part 2: Test suites for testing interoperability
of CAdES baseline signatures

Reference

DTS/ESI-0019124-2

Keywords

CAdES, e-commerce, electronic signature, interoperability, profile, security, testing

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 2 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].

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 a number of test suites to assess the interoperability between implementations claiming conformance to CAdES baseline signatures [1].

The test suites are defined with four different layers reflecting the four different levels of CAdES baseline signatures:

- Tests suite addressing interoperability between applications claiming B-B level conformance.
- Tests suite addressing interoperability between applications claiming B-T level conformance.
- Tests suite addressing interoperability between applications claiming B-LT level conformance.
- Tests suite addressing interoperability between applications claiming B-LTA level conformance.

Test suites also cover augmentation of CAdES baseline signatures and negative test cases.

These test suites are agnostic of the PKI infrastructure. Any PKI infrastructure can be used including the one based on EU Member States Trusted Lists.

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".

2.2 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] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

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] and the following apply:

negative test case: test case for a signature whose validation according to ETSI EN 319 102-1 [i.3] would not result in TOTAL-PASSED

3.2 Abbreviations

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

4 Overview

This clause describes the overall approach used throughout the present document to specify test suites for CAdES baseline signatures interoperability testing.

ETSI EN 319 122-1 [1] defines four different levels of CAdES baseline signatures.

The test suites are defined with different layers reflecting the levels of CAdES baseline signatures specified in [1]:

- Testing CAdES signatures interoperability between applications claiming B-B level conformance.
- Testing CAdES signatures interoperability between applications claiming B-T level conformance.
- Testing CAdES signatures interoperability between applications claiming B-LT level conformance.
- Testing CAdES signatures interoperability between applications claiming B-LTA level conformance.
- Testing augmentation of CAdES signatures from B-T level to B-LTA level.
- Negative test cases for CAdES baseline signatures:
  - CAdES-B-B signatures test cases.
  - CAdES-B-T signatures test cases.
  - CAdES-B-LTA signatures test cases.

5 Testing interoperability of CAdES-B-B signatures

The test cases in this clause have been defined for different combinations of CAdES-B-B signatures attributes.

Mandatory attributes for CAdES-B-B signatures described in [1], clause 6.3, shall be present.

Table 1 shows which attributes are required to generate CAdES-B-B signatures for each test case.

Table 1: Test cases for CAdES-B-B signatures

TC ID	Description	Pass criteria	Signature attributes
CAdES/BB/1	This is the simplest CAdES-B-B signatures interoperability test case. The signature ONLY CONTAINS the mandatory CAdES attributes.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, ESSSigningCertificateV2 and SigningCertificate (included in SignedData.certificates field) attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ContentType o SigningTime o ESSSigningCertificateV2
CAdES/BB/2	In this CAdES-B-B signatures interoperability test case the signature contains a CertifiedAttributeV2 in addition to the CAdES/BB/1 test case attributes.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, ESSSigningCertificateV2, CertifiedAttributesV2 (included in SignerAttributesV2) and SigningCertificate (included in SignedData.certificates field) attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ContentType o SigningTime o ESSSigningCertificateV2 o SignerAttributesV2 (CertifiedAttributeV2)
CAdES/BB/3	In this CAdES-B-B signatures interoperability test case the signature contains a ClaimedAttribute in addition to the CAdES/BB/1 test case attributes.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, ESSSigningCertificateV2, ClaimedAttribute (included in SignerAttributesV2) and SigningCertificate (included in SignedData.certificates field) attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ContentType o SigningTime o ESSSigningCertificateV2 o SignerAttributesV2 (CertifiedAttributeV2)
CAdES/BB/4	This test case tests a CAdES-B-B signature with multiple independent signatures. The input to this test is a CAdES signature as specified in CAdES/BB/1 test case.	Positive validation. The signature shall contain 2 SigningCertificates attributes (included in SignedData.certificates field) and 2 signerInfos containing ContentType, SigningTime, MessageDigest and ESSSigningCertificateV2 attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime
CAdES/BB/5	This test case tests a CAdES-B-B signature with a CounterSignature attribute. The input to this test is a CAdES signature as specified in CAdES/BB/1 test case.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, ESSSigningCertificateV2, CounterSignature and SigningCertificate (included in SignedData.certificates field) attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ContentType o SigningTime o ESSSigningCertificateV2 • UnsignedAttributes o CounterSignature
CAdES/BB/6	This test case tests a CAdES-B-B signature that contains SignerLocation and CommitmentTypeIndication attributes in addition to the CAdES/BB/1 test case attributes.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, ESSSigningCertificateV2, SignerLocation (containing at least the countryName and localityName values), CommitmentTypeIndication and SigningCertificate (included in SignedData.certificates field) attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ContentType o SigningTime o ESSSigningCertificateV2 o SignerLocation o CommitmentTypeIndication

TC ID	Description	Pass criteria	Signature attributes
CAdES/BB/7	This test case tests a CAdES-B-B signature that contains a ContentTimeStamp attribute in addition to the CAdES/BB/1 test case attributes.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, ESSSigningCertificateV2, ContentTimeStamp and SigningCertificate (included in SignedData.certificates field) attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ContentType o SigningTime o ESSSigningCertificateV2 o ContentTimeStamp
CAdES/BB/8	This test case tests a CAdES-B-B signature that contains an explicit SignaturePolicyIdentifier attribute in addition to the CAdES/BB/1 test case attributes.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, ESSSigningCertificateV2, SignaturePolicyIdentifier and SigningCertificate (included in SignedData.certificates field) attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ContentType o SigningTime o ESSSigningCertificateV2 o SignaturePolicyIdentifier
CAdES/BB/9	This test case tests a CAdES-B-B signature in which digest algorithm SHA1 is used to digest data to be signed. The signature ONLY CONTAINS the mandatory CAdES attributes.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, ESSSigningCertificate and SigningCertificate (included in SignedData.certificates field) attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ContentType o SigningTime o ESSSigningCertificate

6 Testing interoperability of CAdES-B-T signatures

The test cases in this clause have been defined for different combinations of CAdES-B-T signatures attributes. CAdES baseline signatures claiming conformance to B-T level of document [1] shall be built on baseline signatures conformant to B-B level.

A CAdES baseline signature conformant to B-T level shall be a baseline signature conformant to B-B level for which a Trust Service Provider has generated a trusted token (time-stamp token) proving that the signature itself actually existed at a certain date and time.

Mandatory attributes for CAdES-B-T signatures described in document [1], clause 6.3, shall be present.

Table 2 shows which attributes are required to generate CAdES-B-T signatures for each test case.

Table 2: Test cases for CAdES-B-T signatures

TC ID	Description	Pass criteria	Signature attributes
CAdES/BT/1	This is the simplest CAdES-B-T signatures interoperability test case. The signature ONLY CONTAINS the mandatory CAdES attributes for CAdES-B-B signatures and a SignatureTimeStamp unsigned attribute.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, ESSSigningCertificateV2, SignatureTimeStamp and SigningCertificate (included in SignedData.certificates field) attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime • UnsignedAttributes o SignatureTimeStamp
CAdES/BT/2	This test case tests the adding of an indipendent CAdES-B-T signature to an already signed document in CAdES-B-T signature format. The input to this test is a CAdES-B-T signature as specified in CAdES/BT/1 test case.	Positive validation. The signature shall contain 2 SigningCertificates attributes (included in SignedData.certificates field) and 2 signerInfos containing ContentType, SigningTime, MessageDigest, ESSSigningCertificateV2 and SignatureTimeStamp attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime • UnsignedAttributes o SignatureTimeStamp

TC ID	Description	Pass criteria	Signature attributes
CAdES/BT/3	This test case tests the adding of an independent CAdES-B-T signature to an already signed document in CAdES-B-B signature format. The input to this test is a CAdES-B-B signature as specified in CAdES/BB/1 test case.	Positive validation. The signature shall contain 2 SigningCertificates attributes (included in SignedData.certificates field) and 2 signerInfos containing ContentType, SigningTime, MessageDigest and ESSSigningCertificateV2 attributes. The second signerInfo contains a SignatureTimeStamp attribute too.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime • UnsignedAttributes o SignatureTimeStamp

7 Testing interoperability of CAdES-B-LT signatures

The test cases in this clause have been defined for different combinations of CAdES-B-LT signatures attributes. CAdES baseline signatures claiming conformance to B-LT level of document [1] shall be built on baseline signatures conformant to B-T level.

A CAdES baseline signature conformant to B-LT level shall be a baseline signature conformant to B-T level to which values of certificates and values of certificates status used to validate the signature have been added.

Mandatory attributes for CAdES-B-LT signatures described in document [1], clause 6.3, shall be present.

Table 3 shows which attributes are required to generate test CAdES-B-LT signatures for each test case.

Table 3: Test cases for CAdES-B-LT signatures

TC ID	Description	Pass criteria	Signature attributes
CAdES/BLT/1	This is the simplest CAdES-B-LT signatures interoperability test case. The signature contains the mandatory CAdES attributes for CAdES-B-T signatures. The full set of certificates that have been used to validate the signature is included. The revocation material that have been used in the validation of the signature is included. The revocation data used are CRLs.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, Certificates, Crls.crl, ESSSigningCertificateV2 and SignatureTimeStamp attributes.	• Certificates • Crls.crl • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime • UnsignedAttributes o SignatureTimeStamp
CAdES/BLT/2	This CAdES-B-LT signatures interoperability test case is similar to CAdES/BLT/1 one. The signature contains the mandatory CAdES attributes for CAdES-B-T signatures. The full set of certificates that have been used to validate the signature is included. The revocation material that have been used in the validation of the signature is included. The revocation data used are OCSP responses.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, Certificates, Crls.other, ESSSigningCertificateV2 and SignatureTimeStamp attributes.	• Certificates • Crls.other • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime • UnsignedAttributes o SignatureTimeStamp