



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

---

**Reference**

---

DTS/ESI-0019124-2

---

**Keywords**

---

CAAdES, 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>

---

**Copyright Notification**

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.  
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016.  
All rights reserved.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.  
**3GPP™** and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.  
**GSM®** and the GSM logo are Trade Marks registered and owned by the GSM Association.

---

# Contents

Intellectual Property Rights .....	4
Foreword.....	4
Modal verbs terminology.....	4
1 Scope .....	5
2 References .....	5
2.1 Normative references .....	5
2.2 Informative references.....	5
3 Definitions and abbreviations.....	6
3.1 Definitions .....	6
3.2 Abbreviations .....	6
4 Overview .....	6
5 Testing interoperability of CADES-B-B signatures.....	6
6 Testing interoperability of CADES-B-T signatures.....	8
7 Testing interoperability of CADES-B-LT signatures .....	9
8 Testing interoperability of CADES-B-LTA signatures.....	10
9 Testing CADES baseline signatures augmentation interoperability .....	13
10 Negative test cases for CADES baseline signatures .....	14
10.1 CADES-B-B signatures test cases.....	14
10.2 CADES-B-T signatures test cases .....	16
10.3 CADES-B-LTA signatures test cases.....	17
History .....	18

---

## 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.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ContentType</li> <li>○ SigningTime</li> <li>○ ESSSigningCertificateV2</li> </ul> </li> </ul>
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.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ContentType</li> <li>○ SigningTime</li> <li>○ ESSSigningCertificateV2</li> <li>○ SignerAttributesV2 (CertifiedAttributeV2)</li> </ul> </li> </ul>
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.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ContentType</li> <li>○ SigningTime</li> <li>○ ESSSigningCertificateV2</li> <li>○ SignerAttributesV2 (CertifiedAttributeV2)</li> </ul> </li> </ul>
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.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> </ul>
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.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ContentType</li> <li>○ SigningTime</li> <li>○ ESSSigningCertificateV2</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ CounterSignature</li> </ul> </li> </ul>
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.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ContentType</li> <li>○ SigningTime</li> <li>○ ESSSigningCertificateV2</li> <li>○ SignerLocation</li> <li>○ CommitmentTypeIndication</li> </ul> </li> </ul>

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.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ContentType</li> <li>○ SigningTime</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentTimeStamp</li> </ul> </li> </ul>
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.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ContentType</li> <li>○ SigningTime</li> <li>○ ESSSigningCertificateV2</li> <li>○ SignaturePolicyIdentifier</li> </ul> </li> </ul>
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.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ContentType</li> <li>○ SigningTime</li> <li>○ ESSSigningCertificate</li> </ul> </li> </ul>

## 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.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> </ul> </li> </ul>
CAdES/BT/2	This test case tests the adding of an independent 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.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> </ul> </li> </ul>



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.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> </ul> </li> </ul>

## 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.	<ul style="list-style-type: none"> <li>• Certificates</li> <li>• Crls.crl</li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> </ul> </li> </ul>
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.	<ul style="list-style-type: none"> <li>• Certificates</li> <li>• Crls.other</li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> </ul> </li> </ul>

TC ID	Description	Pass criteria	Signature attributes
CAAdES/BLT/3	In this CAAdES-B-LT signatures interoperability test case the signature contains a CertifiedAttributeV2 attribute in addition to the CAAdES/BLT/1 test case attributes. The full set of certificates that have been used to validate the signature is included and contains the Attribute Authority certificate too. 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, CertifiedAttributesV2 (included in SignerAttributesV2), Certificates, Crls.crl, ESSSigningCertificateV2 and SignatureTimeStamp attributes.	<ul style="list-style-type: none"> <li>• Certificates</li> <li>• Crls.crl</li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> <li>○ SignerAttributesV2 (CertifiedAttributeV2)</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> </ul> </li> </ul>
CAAdES/BLT/4	In this CAAdES-B-LT signatures interoperability test case the signature contains a CertifiedAttributeV2 attribute in addition to the CAAdES/BLT/2 test case attributes. The full set of certificates that have been used to validate the signature is included and contains the Attribute Authority certificate too. 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, CertifiedAttributesV2 (included in SignerAttributesV2), Certificates, Crls.other, ESSSigningCertificateV2 and SignatureTimeStamp attributes.	<ul style="list-style-type: none"> <li>• Certificates</li> <li>• Crls.other</li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> <li>○ SignerAttributesV2 (CertifiedAttributeV2)</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> </ul> </li> </ul>

## 8 Testing interoperability of CAAdES-B-LTA signatures

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

A CAAdES baseline signature conformant to B-LTA level shall be a baseline signature conformant to B-LT level to which one or more archive-time-stamp-v3 attributes (each one including one ats-hash-index-v3 unsigned attribute as specified in document [1]) have been added.

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

Table 4 shows which attributes are required to generate test CAAdES-B-LTA signatures for each test case.

Table 4: Test cases for CAES-B-LTA signatures

TC ID	Description	Pass criteria	Signature attributes
CAES/BLTA/1	This is the simplest CAES-B-LTA signatures interoperability test case. The signature contains the mandatory CAES attributes for CAES-B-LT signatures (the revocation data used are CRLs). One ArchiveTimeStampV3 attribute is included (including one ats-hash-index-v3 unsigned attribute).	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, Certificates, Crls.crl, ESSSigningCertificateV2, SignatureTimeStamp and ArchiveTimeStampV3 (including one ats-hash-index-v3 unsigned attribute) attributes.	<ul style="list-style-type: none"> <li>• Certificates</li> <li>• Crls.crl</li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> <li>○ ArchiveTimeStampV3 <ul style="list-style-type: none"> <li>○ ats-hash-index-v3</li> </ul> </li> </ul> </li> </ul>
CAES/BLTA/2	This CAES-B-LTA signatures interoperability test case is similar to CAES/BLTA/1 one. The signature contains the mandatory CAES attributes for CAES-B-LT signatures (the revocation data used are OCSP responses). One ArchiveTimeStampV3 attribute is included (including one ats-hash-index-v3 unsigned attribute).	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, Certificates, Crls.other, ESSSigningCertificateV2, SignatureTimeStamp and ArchiveTimeStampV3 (including one ats-hash-index-v3 unsigned attribute) attributes.	<ul style="list-style-type: none"> <li>• Certificates</li> <li>• Crls.other</li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> <li>○ ArchiveTimeStampV3</li> <li>○ ats-hash-index-v3</li> </ul> </li> </ul>
CAES/BLTA/3	In this case the CAES-B-LT signature was time-stamped with an ArchiveTimeStampV2. Afterwards, the resulting long-term-validation signature is time-stamped again with an ArchiveTimeStampV3. The validation material corresponding to the first ArchiveTimeStampV2 is added within time-stamp token itself by one of the following methods: (1) the TSU provides the information in the SignedData of the time-stamp token; (2) adding the certificate-values attribute and the revocation-values attribute of the TSP as an unsigned attribute within the time-stamp token. The revocation data used are CRLs.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, Certificates, Crls.crl, CompleteCertificateRefs, CompleteRevocationRefs, ESSSigningCertificateV2, SignatureTimeStamp, ArchiveTimeStampV2 and ArchiveTimeStampV3 (including one ats-hash-index-v3 unsigned attribute) attributes.	<ul style="list-style-type: none"> <li>• Certificates</li> <li>• Crls.crl</li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ CompleteCertificateRefs</li> <li>○ CompleteRevocationRefs</li> <li>○ SignatureTimeStamp</li> <li>○ ArchiveTimeStampV2 <ul style="list-style-type: none"> <li>○ Certificates</li> <li>○ Crls.crl</li> </ul> </li> <li>○ ArchiveTimeStampV3 <ul style="list-style-type: none"> <li>○ ats-hash-index-v3</li> </ul> </li> </ul> </li> </ul>

TC ID	Description	Pass criteria	Signature attributes
CAAdES/BLTA/4	In this case the CAAdES-B-LT signature was time-stamped with an ArchiveTimeStampV2. Afterwards, the resulting long-term-validation signature is time-stamped again with an ArchiveTimeStampV3. The validation material corresponding to the first ArchiveTimeStampV2 is added within time-stamp token itself by one of the following methods: (1) the TSU provides the information in the SignedData of the time-stamp token; (2) adding the certificate-values attribute and the revocation-values attribute of the TSP as an unsigned attribute within the time-stamp token. The revocation data used are OCSP responses.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, Certificates, Crls.other, CompleteCertificateRefs, CompleteRevocationRefs, ESSSigningCertificateV2, , ArchiveTimeStampV2 and ArchiveTimeStampV3 (including one ats-hash-index-v3 unsigned attribute) attributes.	<ul style="list-style-type: none"> <li>• Certificates</li> <li>• Crls.other</li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ CompleteCertificateRefs</li> <li>○ CompleteRevocationRefs</li> <li>○ SignatureTimeStamp</li> <li>○ ArchiveTimeStampV2 <ul style="list-style-type: none"> <li>○ Certificates</li> <li>○ Crls.other</li> </ul> </li> <li>○ ArchiveTimeStampV3 <ul style="list-style-type: none"> <li>○ ats-hash-index-v3</li> </ul> </li> </ul> </li> </ul>
CAAdES/BLTA/5	In this case the CAAdES-B-LT signature was time-stamped with an ArchiveTimeStampV3. Afterwards, the resulting CAAdES-B-LTA signature is time-stamped again with an ArchiveTimeStampV3. The validation material corresponding to the first ArchiveTimeStampV3 is added in root SignedData. The revocation data used are CRLs.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, Certificates, Crls.crl, ESSSigningCertificateV2, SignatureTimeStamp and 2 different ArchiveTimeStampV3 attributes.	<ul style="list-style-type: none"> <li>• Certificates</li> <li>• Crls.crl</li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> <li>○ ArchiveTimeStampV3 <ul style="list-style-type: none"> <li>○ ats-hash-index-v3</li> </ul> </li> <li>○ ArchiveTimeStampV3 <ul style="list-style-type: none"> <li>○ ats-hash-index-v3</li> </ul> </li> </ul> </li> </ul>
CAAdES/BLTA/6	In this case the CAAdES-B-LT signature was time-stamped with an ArchiveTimeStampV3. Afterwards, the resulting CAAdES-B-LTA signature is time-stamped again with an ArchiveTimeStampV3. The validation material corresponding to the first ArchiveTimeStampV3 is added in root SignedData. The revocation data used are OCSP responses.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, Certificates, Crls.other, ESSSigningCertificateV2, SignatureTimeStamp and 2 different ArchiveTimeStampV3 attributes.	<ul style="list-style-type: none"> <li>• Certificates</li> <li>• Crls.other</li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> <li>○ ArchiveTimeStampV3 <ul style="list-style-type: none"> <li>○ ats-hash-index-v3</li> </ul> </li> <li>○ ArchiveTimeStampV3 <ul style="list-style-type: none"> <li>○ ats-hash-index-v3</li> </ul> </li> </ul> </li> </ul>
CAAdES/BLTA/7	In this test case the CAAdES-B-LT signature contains an explicit SignaturePolicyIdentifier attribute in addition to the mandatory CAAdES attributes. The revocation data used are OCSP responses. One ArchiveTimeStampV3 attribute is included (including one ats-hash-index-v3 unsigned attribute).	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), SignaturePolicyIdentifier, Crls.crl, ESSSigningCertificateV2 and ArchiveTimeStampV3 attributes.	<ul style="list-style-type: none"> <li>• Certificates</li> <li>• Crls.crl</li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SignaturePolicyIdentifier</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> <li>○ ArchiveTimeStampV3 <ul style="list-style-type: none"> <li>○ ats-hash-index-v3</li> </ul> </li> </ul> </li> </ul>

## 9 Testing CAdES baseline signatures augmentation interoperability

The test cases in this clause have been defined for testing augmentation of CAdES-B-T signatures to CAdES-B-LTA signatures and subsequent validation of the augmented signatures.

A CAdES baseline signature conformant to B-LTA 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 and one or more archive-time-stamp-v3 attributes (each one including one ats-hash-index-v3 unsigned attribute as specified in document [1]) have been added.

Table 5 shows which attributes are required to augment a CAdES-B-T signature to a CAdES-B-LTA signature for each test case.

**Table 5: Test cases for augmentation of CAdES-B-T signatures to CAdES-B-LTA signatures**

TC ID	Description	Pass criteria	Signature attributes
CAdES/Aug/1	The CAdES-B-T signature, passed as input, shall be validated, the validation material concerning the signing certificate and the certificate that generated the signature timestamp shall be added (the revocation data used are CRLs) and, after that, one ArchiveTimeStampV3 attribute shall be added too (including one ats-hash-index-v3 unsigned attribute).	Positive validation. The signature shall contain a CAdES-B-T signature with ContentType, SigningTime, MessageDigest, ESSSigningCertificateV2 and SignatureTimeStamp to which Certificates, Crls.crl and ArchiveTimeStampV3 (including one ats-hash-index-v3 unsigned attribute) attributes have been added.	<ul style="list-style-type: none"> <li>• CAdES-B-T signature <ul style="list-style-type: none"> <li>○ Certificates</li> <li>○ Crls.crl</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ ArchiveTimeStampV3</li> <li>○ ats-hash-index-v3</li> </ul> </li> </ul>
CAdES/Aug/2	The CAdES-B-T signature, passed as input, shall be validated, the validation material concerning the signing certificate and the certificate that generated the signature timestamp shall be added (the revocation data used are OCSP responses) and, after that, one ArchiveTimeStampV3 attribute shall be added too (including one ats-hash-index-v3 unsigned attribute).	Positive validation. The signature shall contain a CAdES-B-T signature with ContentType, SigningTime, MessageDigest, ESSSigningCertificateV2 and SignatureTimeStamp to which Certificates, Crls.other and ArchiveTimeStampV3 (including one ats-hash-index-v3 unsigned attribute) attributes have been added.	<ul style="list-style-type: none"> <li>• CAdES-B-T signature <ul style="list-style-type: none"> <li>○ Certificates</li> <li>○ Crls.other</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ ArchiveTimeStampV3</li> <li>○ ats-hash-index-v3</li> </ul> </li> </ul>
CAdES/Aug/3	The input to this test case is a CAdES-B-LTA signature. The signature, passed as input, shall be validated, the validation material concerning the certificate that generated the ArchiveTimeStampV3 shall be added (the revocation data used are CRLs) and, after that, one ArchiveTimeStampV3 attribute shall be added too (including one ats-hash-index-v3 unsigned attribute).	Positive validation. The signature shall contain a CAdES-B-LTA signature with ContentType, SigningTime, MessageDigest, ESSSigningCertificateV2, SignatureTimeStamp, Certificates, Crls.crl and ArchiveTimeStampV3 to which Certificates, Crls.crl and a second ArchiveTimeStampV3 (including one ats-hash-index-v3 unsigned attribute) attributes have been added.	<ul style="list-style-type: none"> <li>• CAdES-B-T signature <ul style="list-style-type: none"> <li>○ Certificates</li> <li>○ Crls.crl</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ ArchiveTimeStampV3</li> <li>○ ats-hash-index-v3</li> <li>○ ArchiveTimeStampV3</li> <li>○ ats-hash-index-v3</li> </ul> </li> </ul>

TC ID	Description	Pass criteria	Signature attributes
CAdES/Aug/4	The input to this test case is a CAdES-B-LTA signature. The signature, passed as input, shall be validated, the validation material concerning the certificate that generated the ArchiveTimeStampV3 shall be added (the revocation data used are OCSP responses) and, after that, one ArchiveTimeStampV3 attribute shall be added too (including one ats-hash-index-v3 unsigned attribute).	Positive validation. The signature shall contain a CAdES-B-LTA signature with ContentType, SigningTime, MessageDigest, ESSSigningCertificateV2, SignatureTimeStamp, Certificates, Crls.other and ArchiveTimeStampV3 to which Certificates, Crls.other and a second ArchiveTimeStampV3 (including one ats-hash-index-v3 unsigned attribute) attributes have been added.	<ul style="list-style-type: none"> <li>• CAdES-B-T signature <ul style="list-style-type: none"> <li>○ Certificates</li> <li>○ Crls.other</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ ArchiveTimeStampV3 <ul style="list-style-type: none"> <li>○ ats-hash-index-v3</li> </ul> </li> <li>○ ArchiveTimeStampV3 <ul style="list-style-type: none"> <li>○ ats-hash-index-v3</li> </ul> </li> </ul> </li> </ul>

## 10 Negative test cases for CAdES baseline signatures

### 10.1 CAdES-B-B signatures test cases

The test cases in this clause have been defined for CAdES-B-B signatures.

Table 6 summarizes negative test cases for CAdES-B-B signatures.

**Table 6: Negative test cases for CAdES-B-B signatures**

TC ID	Description	Pass criteria	Signature attributes
CAdES/BBN/1	Verify a CAdES-B-B signature that DOES NOT CONTAIN the mandatory SigningTime attribute	Negative validation because the signature does not contain the mandatory SigningTime attribute. The signature shall contain ContentType, MessageDigest, SigningCertificate and ESSSigningCertificateV2 attributes.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> </ul> </li> </ul>
CAdES/BBN/2	Verify a CAdES-B-B signature that DOES NOT CONTAIN the mandatory SigningCertificate reference attribute	Negative validation because the signature does not contain the mandatory SigningCertificate reference attribute. The signature shall contain ContentType, MessageDigest, SigningCertificate and SigningTime attributes.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> </ul>
CAdES/BBN/3	Verify a CAdES-B-B signature that DOES NOT CONTAIN the mandatory ContentType attribute qualifying the signed data object	Negative validation because the signature does not contain the mandatory ContentType attribute. The signature shall contain ESSSigningCertificateV2, MessageDigest, SigningCertificate and SigningTime attributes.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ SigningTime</li> <li>○ ESSSigningCertificateV2</li> </ul> </li> </ul>
CAdES/BBN/4	Verify a CAdES-B-B signature that DOES NOT CONTAIN the mandatory certificates component into CMS signedData object	Negative validation because the signature does not contain the mandatory certificates component. The signature shall contain ESSSigningCertificateV2, MessageDigest, ContentType and SigningTime attributes.	<ul style="list-style-type: none"> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ContentType</li> <li>○ SigningTime</li> <li>○ ESSSigningCertificateV2</li> </ul> </li> </ul>

TC ID	Description	Pass criteria	Signature attributes
CAdES/BBN/5	Verify a CAdES-B-B signature having a wrong signature (the hash that was signed isn't the hash computed on the content being signed together with the signed attributes)	Negative validation because the hash that was signed isn't the hash of the specified MessageDigest attribute. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate and ESSSigningCertificateV2 attributes.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> </ul>
CAdES/BBN/6	Verify a CAdES-B-B signature created with an untrusted signing certificate	Negative validation because the signing certificate is untrusted. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate and ESSSigningCertificateV2 attributes.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> </ul>
CAdES/BBN/7	Verify a CAdES-B-B signature created with an expired signing certificate	Negative validation because the signing certificate is expired (at the time specified in signingTime attribute). The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate and ESSSigningCertificateV2 attributes.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> </ul>
CAdES/BBN/8	Verify a CAdES-B-B signature created with a revoked/suspended signing certificate	Negative validation because the signing certificate is revoked/suspended (at the time specified in signingTime attribute). The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate and ESSSigningCertificateV2 attributes.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> </ul>
CAdES/BBN/9	Verify a CAdES-B-B signature created with a signing certificate generated by a CA whose certificate is revoked/suspended	Negative validation because the signing certificate is generated by a CA whose certificate is revoked/suspended (at the time specified in signingTime attribute). The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate and ESSSigningCertificateV2 attributes.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> </ul>
CAdES/BBN/10	Verify a CAdES-B-B signature that includes a SignaturePolicyIdentifier attribute with explicit SignaturePolicyId. However its value of SignaturePolicyId.sigPolicyHash field does *NOT* match to the hash value of signature policy file	Negative validation because the hash value in SignaturePolicyId.sigPolicyHash included in SignaturePolicyIdentifier attribute does not match to the hash value of signer policy file. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, SignaturePolicyIdentifier and ESSSigningCertificateV2 attributes.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> <li>○ SignaturePolicyIdentifier</li> </ul> </li> </ul>

TC ID	Description	Pass criteria	Signature attributes
CAdES/BBN/11	Verify a CAdES-B-B signature in which the hash value of the signing certificate is different from the hash value in ESS signing certificate V2 attribute	Negative validation because the certHash value in ESSSigningCertificateV2 attribute does not match to the hash value of signing certificate. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate and ESSSigningCertificateV2 attributes.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> </ul>

## 10.2 CAdES-B-T signatures test cases

The test cases in this clause have been defined for CAdES-B-T signatures.

Table 7 summarizes negative test cases for CAdES-B-T signatures.

**Table 7: Negative test cases for CAdES-B-T signatures**

TC ID	Description	Pass criteria	Signature attributes
CAdES/BTN/1	Verify a CAdES-B-T signature in which, at the time in SignatureTimeStamp, the signer certificate had been already expired	Negative validation because at the time in SignatureTimeStamp, the signing certificate had been already expired. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate ESSSigningCertificateV2 and SignatureTimeStamp attributes.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> </ul> </li> </ul>
CAdES/BTN/2	Verify a CAdES-B-T signature in which, at the time in SignatureTimeStamp, the signer certificate had been already revoked	Negative validation because at the time in SignatureTimeStamp, the signing certificate had been already revoked. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate ESSSigningCertificateV2 and SignatureTimeStamp attributes.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> </ul> </li> </ul>
CAdES/BTN/3	Verify a CAdES-B-T signature in which the hash value of messageImprint in SignatureTimeStamp does *NOT* match to the hash value of corresponding signature value in signerInfo	Negative validation because the hash value of messageImprint in SignatureTimeStamp does *NOT* match to the hash value of corresponding signature value of signerInfo. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate ESSSigningCertificateV2 and SignatureTimeStamp attributes.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> </ul> </li> </ul>
CAdES/BTN/4	Verify a CAdES-B-T signature in which, at the time in SignatureTimeStamp, the timestamp signer certificate had been already revoked	Negative validation because at the time in SignatureTimeStamp, the timestamp signing certificate had been already revoked. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate ESSSigningCertificateV2 and SignatureTimeStamp attributes.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> </ul> </li> </ul>



TC ID	Description	Pass criteria	Signature attributes
CAdES/BTN/5	Verify a CAdES-B-T signature in which, at the time in SignatureTimeStamp, the timestamp signer certificate had been already expired	Negative validation because at the time in SignatureTimeStamp, the timestamp signing certificate had been already expired. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, ESSSigningCertificateV2 and SignatureTimeStamp attributes.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> </ul> </li> </ul>
CAdES/BTN/6	Verify a CAdES-B-T signature in which the timestamp signer certificate was generated by an untrusted CA	Negative validation because the anchor CA of the SignatureTimeStamp signing chain trust is unknown. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, ESSSigningCertificateV2 and SignatureTimeStamp attributes.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> </ul> </li> </ul>
CAdES/BTN/7	Verify a CAdES-B-T signature in which the timestamp signer certificate was generated by a CA whose certificate was revoked/suspended at the time of timestamp signer certificate generation	Negative validation because the anchor CA of the SignatureTimeStamp signing chain trust is revoked/suspended. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, ESSSigningCertificateV2 and SignatureTimeStamp attributes.	<ul style="list-style-type: none"> <li>• Certificates <ul style="list-style-type: none"> <li>○ SigningCertificate</li> </ul> </li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> </ul> </li> </ul>

## 10.3 CAdES-B-LTA signatures test cases

The test cases in this clause have been defined for CAdES-B-LTA signatures.

Table 8 summarizes negative test cases for CAdES-B-LTA signatures.

**Table 8: Negative test cases for CAdES-B-LTA signatures**

TC ID	Description	Pass criteria	Signature attributes
CAdES/BLTAN/1	Verify a CAdES-B-LTA signature in which the time in the SignatureTimeStamp is ulterior than the time in ATSV3	Negative validation because the time in the SignatureTimeStamp is ulterior than the time in ArchiveTimeStampV3. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, ESSSigningCertificateV2, SignatureTimeStamp and ArchiveTimeStampV3 attributes.	<ul style="list-style-type: none"> <li>• Certificates</li> <li>• Crls.crl</li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> <li>○ ArchiveTimeStampV3 <ul style="list-style-type: none"> <li>○ ats-hash-index-v3</li> </ul> </li> </ul> </li> </ul>
CAdES/BLTAN/2	Verify a CAdES-B-LTA signature in which the content in ats-hash-index-v3 element has not the right value related to the signature itself to which the ATSV3 has been applied	Negative validation because the content in ats-hash-index-v3 element has not the right value related to the CAdES signature to which the ArchiveTimeStampV3 has been applied. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, ESSSigningCertificateV2, SignatureTimeStamp and ArchiveTimeStampV3 attributes.	<ul style="list-style-type: none"> <li>• Certificates</li> <li>• Crls.crl</li> <li>• SignedAttributes <ul style="list-style-type: none"> <li>○ MessageDigest</li> <li>○ ESSSigningCertificateV2</li> <li>○ ContentType</li> <li>○ SigningTime</li> </ul> </li> <li>• UnsignedAttributes <ul style="list-style-type: none"> <li>○ SignatureTimeStamp</li> <li>○ ArchiveTimeStampV3 <ul style="list-style-type: none"> <li>○ ats-hash-index-v3</li> </ul> </li> </ul> </li> </ul>

---

## History

<b>Document history</b>		
V1.1.1	June 2016	Publication