ETSI TS 119 124-3 V1.1.1 (2016-06)

TECHNICAL SPECIFICATION

Electronic Signatures and Infrastructures (ESI);
CAdES digital signatures -
Testing Conformance and Interoperability;
Part 3: Test suites for testing interoperability
of extended CAdES signatures

ETSI

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

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

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

Important notice

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

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

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

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

Copyright Notification

Contents

Intellectual Property Rights

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

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

Foreword

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

The present document is part 3 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 extended CAdES signatures [2].

The present document defines test suites for each level defined in ETSI EN 319 122-2 [2].

Test suites also cover augmentation of extended CAdES 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] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES 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".

[i.4] IETF RFC 3125 (09-2001): "Electronic Signature Policies".

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 to specify test suites for extended CAdES signatures interoperability testing.

ETSI EN 319 122-2 [2] defines different signature levels.

The test suites are defined with different layers reflecting the levels of extended CAdES signatures specified in [2].

Testing CAdES signatures:

- CAdES-E-BES signatures test cases;

- CAdES-E-EPES signatures test cases;

- CAdES-E-T signatures test cases;

- CAdES-E-C test cases;

- CAdES-E-X test cases;

- CAdES-E-X Long test cases;

- CAdES-E-A signatures (with ATSv2 and ATSv3) built on CAdES-E-T signatures test cases.

Testing negative CAdES signatures:

- CAdES-E-BES test cases;

- CAdES-E-EPES test cases;

- CAdES-E-T test cases;

- CAdES-E-A test cases.

Testing augmentation of CAdES signatures:

- augmentation to CAdES-E-C levels test cases;

- augmentation to CAdES-E-X levels test cases;

- augmentation to CAdES-E-XL levels test cases;

- augmentation to CAdES-E-A levels test cases.

5   Testing extended CAdES signatures interoperability

5.1   CAdES-E-BES test cases

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

Mandatory attributes for CAdES-E-BES described in [2] specification, clauses 4.2 and 4.3, shall be present.

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

Table 1: Test cases for CAdES-E-BES signatures

TC ID	Description	Pass criteria	Signature attributes

CAdES/BES/1	This is the simplest CAdES-E-BES signature without signing time. The signature ONLY CONTAINS the mandatory CAdES attributes.	Positive validation. The signature shall contain ContentType, MessageDigest, SigningCertificate (included in SignedData.certificates field) and ESSSigningCertificateV2 attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType

CAdES/BES/2	This is the simplest CAdES-E-BES signature with signing time. The signature ONLY CONTAINS a signing time attribute in addition to all the mandatory CAdES attributes.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field) and ESSSigningCertificateV2 attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime

CAdES/BES/3	In this CAdES-E-BES signature test case the signature contains a CertifiedAttributeV2 in addition to the CAdES/BES/2 test case attributes.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2 and CertifiedAttributeV2 attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			  o SignerAttributesV2 (CertifiedAttributeV2)

CAdES/BES/4	This test case tests a CAdES-E-BES signature with ContentTimeStamp attribute.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2 and ContentTimeStamp attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			  o ContentTimeStamp

CAdES/BES/5	This test case tests a CAdES-E-BES signature with CounterSignature attribute. The input to this test is a CAdES-E-BES signature as specified in CAdES/BES/2 test case.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2 and CounterSignature attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o CounterSignature

CAdES/BES/6	This test case tests a CAdES-E-BES signature with multiple independent signatures. The input to this test is a CAdES-E-BES signature as specified in CAdES/BES/2 test case.	Positive validation. The signature shall contain 2 SigningCertificates (included in SignedData.certificates field) attributes and 2 signerInfos containing ContentType, SigningTime, MessageDigest and ESSSigningCertificateV2 attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime

TC ID	Description	Pass criteria	Signature attributes

CAdES/BES/7	This test case tests a CAdES-E-BES signature with the following attributes at once:
	- MessageDigest
	- SigningTime
	- ESSSigningCertificateV2
	- SignerLocation
	- SignerAttributesV2 (only Claimed Attributes included)
	- ContentType
	- ContentHints
	- ContentIdentifier
	- CommitmentTypeIndication.
		Positive validation.
		The signature shall contain the following attributes:
		SigningCertificate (included in SignedData.certificates field), MessageDigest, SigningTime, ESSSigningCertificateV2, SignerLocation, SignerAttributesV2 (only Claimed Attributes included), ContentType, ContentHints, ContentIdentifier, CommitmentTypeIndication.
			• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			  o SignerLocation
			  o SignerAttributesV2 (ClaimedAttribute)
			  o ContentHints
			  o ContentIdentifier
			  o CommitmentTypeIndication
			  o ContentTimeStamp

5.2   CAdES-E-EPES test cases

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

Mandatory attributes for CAdES-E-EPES described in [2] specification, clauses 4.2 and 4.3, shall be present.

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

Table 2: Test cases for CAdES-E-EPES signatures

TC ID	Description	Pass criteria	Signature attributes

CAdES/EPES/1	This is the simplest CAdES-E-EPES signature. The signature ONLY CONTAINS the mandatory CAdES attributes.	Positive validation.
		The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2, SignaturePolicyIdentifier attributes.
			• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			  o SignaturePolicyIdentifier

CAdES/EPES/2	In this CAdES-E-EPES signature test case the signature-policy-identifier attribute is qualified with additional information within sigPolicyQualifiers. The sigPolicyQualifiers shall include the oid of sp-user-notice (1.2.840.113549.1.9.16.5.2) and a UTF8String as explicitText.	Positive validation.
		The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2, SignaturePolicyIdentifier attributes.
			• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			  o SignaturePolicyIdentifier
			    o sigPolicyId
			    o sigPolicyHash
			    o SigPolicyQualifierInfo SigPolicyQualifierId Unotice (explicitText)

CAdES/EPES/3	This test case tests CAdES-E-EPES signature with the following attributes at once:
	- MessageDigest
	- SigningTime
	- ESSSigningCertificateV2
	- SignerLocation
	- SignaturePolicyIdentifier
	- ContentType
	- CommitmentTypeIndication.
		Positive validation.
		The signature shall contain the following attributes:
		MessageDigest, SigningTime, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2, SignerLocation, ContentType, SignaturePolicyIdentifier, CommitmentTypeIndication.
			• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			  o SignerLocation
			  o SignaturePolicyIdentifier
			  o CommitmentTypeIndication

5.3   CAdES-E-T test cases

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

Mandatory attributes for CAdES-E-T described in [2] specification, clause 4.3, shall be present.

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

Table 3: Test cases for CAdES-E-T signatures

TC ID	Description	Pass criteria	Signature attributes

CAdES/T/1	This is the simplest CAdES-E-T signature. The signature ONLY CONTAINS the mandatory CAdES attributes.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2, SignatureTimeStamp attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp

CAdES/T/2	This test case tests the adding of an indipendent CAdES-E-T signature to an already signed document in CAdES-E-T format. The input to this test is a CAdES-E-T signature as specified in CAdES/T/1 test case to which a new SignerInfo instance will be added containing another CAdES-E-T signature.	Positive validation. The signature shall contain 2 SigningCertificates (included in SignedData.certificates field) attributes 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

5.4   CAdES-E-C test cases

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

Mandatory attributes for CAdES-E-C described in [2] specification, clause A.1, shall be present.

Table 4 shows which attributes are required to generate CAdES-E-C signatures for each test case.

Table 4: Test cases for CAdES-E-C signatures

TC ID	Description	Pass criteria	Signature attributes

CAdES/C/1	This test case tests a CAdES-E-C signature. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue shall be included. In the CompleteRevocationRefs only CRLListIDs shall be included.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs and CompleteRevocationRefs attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o CompleteCertificateRefs
			    o IssuerSerial
			    o OtherHashAlgAndValue
			  o CompleteRevocationRefs
			    o CRLListIDs

TC ID	Description	Pass criteria	Signature attributes

CAdES/C/2	This test case tests a CAdES-E-C signature. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue shall be included. In the CompleteRevocationRefs only OcspListIDs shall be included. Every OcspListID shall include the ocspIdentifier and the ocspRepHash elements.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs and CompleteRevocationRefs attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o CompleteCertificateRefs
			    o IssuerSerial
			    o OtherHashAlgAndValue
			  o CompleteRevocationRefs
			    o OcspListIDs
			      ▪ ocspIdentifier
			      ▪ ocspRepHash

CAdES/C/3	In this CAdES-E-C signatures interoperability test case the signature contains a CertifiedAttributeV2 in addition to the CAdES/C/1 test case attributes.
	In the AttributeCertificateRefs both IssuerSerial and OtherHashAlgAndValue shall be included. In the AttributeRevocationRefs only CRLListIDs shall be included.
		Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, AttributeCertificateRefs and AttributeRevocationRefs attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			  o SignerAttributesV2 (CertifiedAttributeV2)
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o CompleteCertificateRefs
			    o IssuerSerial
			    o OtherHashAlgAndValue
			  o CompleteRevocationRefs
			    o CRLListIDs
			  o AttributeCertificateRefs
			    o IssuerSerial
			    o OtherHashAlgAndValue
			  o AttributeRevocationRefs
			    o CRLListIDs

CAdES/C/4	In this CAdES-E-C signatures interoperability test case the signature contains a CertifiedAttributeV2 in addition to the CAdES/C/2 test case attributes.
	In the AttributeCertificateRefs both IssuerSerial and OtherHashAlgAndValue shall be included. In the AttributeRevocationRefs only OcspListIDs shall be included.
	Every OcspListID shall include the ocspIdentifier and the ocspRepHash elements.
		Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, AttributeCertificateRefs and AttributeRevocationRefs attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			  o SignerAttributesV2 (CertifiedAttributeV2)
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o CompleteCertificateRefs
			    o IssuerSerial
			    o OtherHashAlgAndValue
			  o CompleteRevocationRefs
			    o OcspListIDs
			      ▪ ocspIdentifier
			      ▪ ocspRepHash
			  o AttributeCertificateRefs
			    o IssuerSerial
			    o OtherHashAlgAndValue
			  o AttributeRevocationRefs
			    o OcspListIDs
			      ▪ ocspIdentifier
			      ▪ ocspRepHash

5.5   CAdES-E-X test cases

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

Mandatory attributes for CAdES-E-X described in [2] specification, clause A.1, shall be present.

Table 5 shows which attributes are required to generate test CAdES-E-X signatures for each test case.

Table 5: Test cases for CAdES-E-X signatures

TC ID	Description	Pass criteria	Signature attributes
CAdES/X/1	This test case tests a CAdES-E-X Type 1 signature format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue shall be included. In the CompleteRevocationRefs only CRLListIDs shall be included. A CAdES-C timestamp covering the signature, the signature timestamp, the complete-certificate-references attribute and complete-revocation-references attribute shall be included.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, ESCTimeStamp attributes.	• Certificates 　o SigningCertificate • SignedAttributes 　o MessageDigest 　o ESSSigningCertificateV2 　o ContentType 　o SigningTime • UnsignedAttributes 　o SignatureTimeStamp 　o CompleteCertificateRefs 　　o IssuerSerial 　　o OtherHashAlgAndValue 　o CompleteRevocationRefs 　　o CRLListIDs 　o ESCTimeStamp
CAdES/X/2	This test case tests a CAdES-E-X Type 2 signature format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue shall be included. In the CompleteRevocationRefs only CRLListIDs shall be included. A TimestampedCertsCRLs timestamp covering the complete-certificate-references and complete-revocation-references attributes shall be included.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, TimestampedCertsCRLs attributes.	• Certificates 　o SigningCertificate • SignedAttributes 　o MessageDigest 　o ESSSigningCertificateV2 　o ContentType 　o SigningTime • UnsignedAttributes 　o SignatureTimeStamp 　o CompleteCertificateRefs 　　o IssuerSerial 　　o OtherHashAlgAndValue 　o CompleteRevocationRefs 　　o CRLListIDs 　o TimestampedCertsCRLs
CAdES/X/3	This test case tests a CAdES-E-X Type 1 signature format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue shall be included. In the CompleteRevocationRefs only OcspListIDs shall be included. Every OcspListID shall include the ocspIdentifier and the ocspRepHash elements. A CAdES-C timestamp covering the signature, the signature timestamp, the complete-certificate-references attribute and complete-revocation-references attribute shall be included.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, ESCTimeStamp attributes.	• Certificates 　o SigningCertificate • SignedAttributes 　o MessageDigest 　o ESSSigningCertificateV2 　o ContentType 　o SigningTime • UnsignedAttributes 　o SignatureTimeStamp 　o CompleteCertificateRefs 　　o IssuerSerial 　　o OtherHashAlgAndValue 　o CompleteRevocationRefs 　　o OcspListIDs 　　　▪ ocspIdentifier 　　　▪ ocspRepHash 　o ESCTimeStamp

TC ID	Description	Pass criteria	Signature attributes

CAdES/X/4	This test case tests a CAdES-E-X Type 2 signature format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue shall be included. In the CompleteRevocationRefs only OcspListIDs shall be included. Every OcspListID shall include the ocspIdentifier and the ocspRepHash elements. A TimestampedCertsCRLs timestamp covering the complete-certificate-references and complete-revocation-references attributes shall be included.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, TimestampedCertsCRLs attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o CompleteCertificateRefs
			    o IssuerSerial
			    o OtherHashAlgAndValue
			  o CompleteRevocationRefs
			    o OcspListIDs
			      ▪ ocspIdentifier
			      ▪ ocspRepHash
			  o TimestampedCertsCRLs

5.6   CAdES-E-XL test cases

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

Mandatory attributes for CAdES-E-XL described in [2] specification, clause A.1, shall be present.

Table 6 shows which attributes are required to generate test CAdES-E-XL signatures for each test case.

Table 6: Test cases for CAdES-E-XL signatures

TC ID	Description	Pass criteria	Signature attributes

CAdES/XL/1	This test case tests a CAdES-E-XL Type 1 signature format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue shall be included. In the CompleteRevocationRefs only CRLListIDs shall be included. In the RevocationValues only crlVals shall be included.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, ESCTimeStamp, CertificateValues, RevocationValues attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o CompleteCertificateRefs
			    o IssuerSerial
			    o OtherHashAlgAndValue
			  o CompleteRevocationRefs
			    o CRLListIDs
			  o ESCTimeStamp
			  o CertificateValues
			  o RevocationValues
			    o crlVals

TC ID	Description	Pass criteria	Signature attributes

CAdES/XL/2	This test case tests a CAdES-E-XL Type 2 signature format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue shall be included. In the CompleteRevocationRefs only CRLListIDs shall be included. In the RevocationValues only crlVals shall be included.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, TimestampedCertsCRLs, CertificateValues, RevocationValues attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o CompleteCertificateRefs
			    o IssuerSerial
			    o OtherHashAlgAndValue
			  o CompleteRevocationRefs
			    o CRLListIDs
			  o TimestampedCertsCRLs
			  o CertificateValues
			  o RevocationValues
			    o crlVals

CAdES/XL/3	This test case tests a CAdES-E-XL Type 1 signature format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue shall be included. In the CompleteRevocationRefs only OcspListIDs shall be included. Every OcspListID shall include the ocspIdentifier and the ocspRepHash elements. In the RevocationValues only ocspVals shall be included.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, ESCTimeStamp, CertificateValues, RevocationValues attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o CompleteCertificateRefs
			    o IssuerSerial
			    o OtherHashAlgAndValue
			  o CompleteRevocationRefs
			    o OcspListIDs
			      ▪ ocspIdentifier
			      ▪ ocspRepHash
			  o ESCTimeStamp
			  o CertificateValues
			  o RevocationValues
			    o ocspVals

CAdES/XL/4	This test case tests a CAdES-E-XL Type 2 signature format. In the CompleteCertificateRefs both IssuerSerial and OtherHashAlgAndValue shall be included. In the CompleteRevocationRefs only OcspListIDs shall be included. Every OcspListID shall include the ocspIdentifier and the ocspRepHash elements. In the RevocationValues only ocspVals shall be included.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, TimestampedCertsCRLs, CertificateValues, RevocationValues attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o CompleteCertificateRefs
			    o IssuerSerial
			    o OtherHashAlgAndValue
			  o CompleteRevocationRefs
			    o OcspListIDs
			      ▪ ocspIdentifier
			      ▪ ocspRepHash
			  o TimestampedCertsCRLs
			  o CertificateValues
			  o RevocationValues
			    o ocspVals

5.7   CAdES-E-A test cases

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

Mandatory attributes for CAdES-E-A described in [2] specification, clauses 6.3 and A.2, shall be present.

Table 7 shows which attributes are required to generate test CAdES-E-A signatures for each test case.

Table 7: Test cases for CAdES-E-A signatures

TC ID	Description	Pass criteria	Signature attributes

CAdES/A/1	This test case tests a CAdES-E-A signature with ATSv3 built on a CAdES-E-T as specified in CAdES/T/1 test case. Validation data shall be included adding the certificate-values attribute and the revocation-values attribute before applying archive-time-stamp-v3. The revocation data used are CRLs.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, ESSSigningCertificateV2, SigningCertificate (included in SignedData.certificates field), SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, CertificateValues, RevocationValues and ArchiveTimeStampV3 attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o CompleteCertificateRefs
			      o IssuerSerial
			      o OtherHashAlgAndValue
			  o CompleteRevocationRefs
			      o CRLListIDs
			  o CertificateValues
			  o RevocationValues
			      o crlVals
			  o ArchiveTimeStampV3
			      o ats-hash-index-v3

CAdES/A/2	This test case tests a CAdES-E-A signature with ATSv3 built on a CAdES-E-T as specified in CAdES/T/1 test case. Validation data shall be included adding the certificate-values attribute and the revocation-values attribute before applying archive-time-stamp-v3. The revocation data used are OCSP responses.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, ESSSigningCertificateV2, SigningCertificate (included in SignedData.certificates field), SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, CertificateValues, RevocationValues and ArchiveTimeStampV3 attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o CompleteCertificateRefs
			      o IssuerSerial
			      o OtherHashAlgAndValue
			  o CompleteRevocationRefs
			      o OcspListIDs
			  o CertificateValues
			  o RevocationValues
			      o ocspVals
			  o ArchiveTimeStampV3
			      o ats-hash-index-v3

TC ID	Description	Pass criteria	Signature attributes
CAdES/A/3	This test case tests a CAdES-E-A signature with ATSv3 built on a CAdES-E-T as specified in CAdES/T/1 test case. Validation data shall be included adding the certificate-values attribute and the revocation-values attribute before applying archive-time-stamp-v3. The revocation data used are CRLs. A CAdES-C timestamp covering the signature, the signature timestamp, the complete-certificate-references attribute and complete-revocation-references attribute shall be included.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, ESSSigningCertificateV2, SigningCertificate (included in SignedData.certificates field), SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, ESCTimeStamp, CertificateValues, RevocationValues and ArchiveTimeStampV3 attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime • UnsignedAttributes o SignatureTimeStamp o CompleteCertificateRefs o IssuerSerial o OtherHashAlgAndValue o CompleteRevocationRefs o CRLListIDs o ESCTimeStamp o CertificateValues o RevocationValues o crlVals o ArchiveTimeStampV3 o ats-hash-index-v3
CAdES/A/4	This test case tests a CAdES-E-A signature with ATSv3 built on a CAdES-E-T as specified in CAdES/T/1 test case. Validation data shall be included adding the certificate-values attribute and the revocation-values attribute before applying archive-time-stamp-v3. The revocation data used are OCSP responses. A CAdES-C timestamp covering the signature, the signature timestamp, the complete-certificate-references attribute and complete-revocation-references attribute shall be included.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, ESSSigningCertificateV2, SigningCertificate (included in SignedData.certificates field), SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, ESCTimeStamp, CertificateValues, RevocationValues and ArchiveTimeStampV3 attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime • UnsignedAttributes o SignatureTimeStamp o CompleteCertificateRefs o IssuerSerial o OtherHashAlgAndValue o CompleteRevocationRefs o OcspListIDs o ESCTimeStamp o CertificateValues o RevocationValues o ocspVals o ArchiveTimeStampV3 o ats-hash-index-v3
CAdES/A/5	This test case tests a CAdES-E-A signature with ATSv3 built on a CAdES-E-T signature as specified in CAdES/T/1 test case. Validation data shall be included in SignedData before applying archive-time-stamp-v3.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), Crls.crl, ESSSigningCertificateV2, SignatureTimeStamp and ArchiveTimeStampV3 attributes.	• Certificates o SigningCertificate • Crls.crl • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime • UnsignedAttributes o SignatureTimeStamp o ArchiveTimeStampV3 o ats-hash-index-v3

TC ID	Description	Pass criteria	Signature attributes
CAdES/A/6	This test case tests a CAdES-E-A signature with ATSv3 built on a CAdES-E-C signature as specified in CAdES/C/1 test case. Validation data shall be included in SignedData before applying archive-time-stamp-v3.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), Crls.crl, ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs and ArchiveTimeStampV3 attributes.	• Certificates o SigningCertificate • Crls.crl • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime • UnsignedAttributes o SignatureTimeStamp o CompleteCertificateRefs o IssuerSerial o OtherHashAlgAndValue o CompleteRevocationRefs o CRLListIDs o ArchiveTimeStampV3 o ats-hash-index-v3
CAdES/A/7	This test case tests a CAdES-E-A signature with ATSv3 built on a CAdES-E-X Type 1 signature as specified in CAdES/X/1 test case. Validation data shall be included in SignedData before applying archive-time-stamp-v3.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), Crls.crl, ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, ESCTimeStamp and ArchiveTimeStampV3 attributes.	• Certificates o SigningCertificate • Crls.crl • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime • UnsignedAttributes o SignatureTimeStamp o CompleteCertificateRefs o IssuerSerial o OtherHashAlgAndValue o CompleteRevocationRefs o CRLListIDs o ESCTimeStamp o ArchiveTimeStampV3 o ats-hash-index-v3
CAdES/A/8	This test case tests a CAdES-E-A signature with ATSv3 built on a CAdES-E-X Type 2 signature as specified in CAdES/X/2 test case. Validation data shall be included in SignedData before applying archive-time-stamp-v3.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), Crls.crl, ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, TimestampedCertsCRLs and ArchiveTimeStampV3 attributes.	• Certificates o SigningCertificate • Crls.crl • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime • UnsignedAttributes o SignatureTimeStamp o CompleteCertificateRefs o IssuerSerial o OtherHashAlgAndValue o CompleteRevocationRefs o CRLListIDs o TimestampedCertsCRLs o ArchiveTimeStampV3 o ats-hash-index-v3

TC ID	Description	Pass criteria	Signature attributes

CAdES/A/9	This test case tests a CAdES-E-A signature with ATSv3 built on a CAdES-E-XL Type 1 signature as specified in CAdES/XL/1 test case.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, ESCTimeStamp, CertificateValues, RevocationValues and ArchiveTimeStampV3 attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o CompleteCertificateRefs
			    o IssuerSerial
			    o OtherHashAlgAndValue
			  o CompleteRevocationRefs
			    o CRLListIDs
			  o ESCTimeStamp
			  o CertificateValues
			  o RevocationValues
			    o crlVals
			  o ArchiveTimeStampV3
			    o ats-hash-index-v3

CAdES/A/10	This test case tests a CAdES-E-A signature with ATSv3 built on a CAdES-E-XL Type 2 signature as specified in CAdES/XL/2 test case.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, TimestampedCertsCRLs, CertificateValues, RevocationValues and ArchiveTimeStampV3 attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o CompleteCertificateRefs
			    o IssuerSerial
			    o OtherHashAlgAndValue
			  o CompleteRevocationRefs
			    o CRLListIDs
			  o TimestampedCertsCRLs
			  o CertificateValues
			  o RevocationValues
			    o crlVals
			  o ArchiveTimeStampV3
			    o ats-hash-index-v3

CAdES/A/11	This test case tests the CAdES-E-A with ATSv3 built on a CAdES-E-A with ATSv2. Validation data related to ATSv2 shall be included in SignedData.Certificates and SignedData.Crls within time-stamp-token.	Positive validation. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate (included in SignedData.certificates field), ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, ESCTimeStamp, CertificateValues, RevocationValues, ArchiveTimeStampV2 and ArchiveTimeStampV3 attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o CompleteCertificateRefs
			    o IssuerSerial
			    o OtherHashAlgAndValue
			  o CompleteRevocationRefs
			    o CRLListIDs
			  o TimestampedCertsCRLs
			  o CertificateValues
			  o RevocationValues
			    o crlVals
			  o ArchiveTimeStampV2
			    o Certificates
			    o Crls
			  o ArchiveTimeStampV3
			    o ats-hash-index-v3

6   Testing extended CAdES signatures augmention interoperability

6.1   Introduction

This clause describes augmentation tests where a signer generates a basic signature and a verifier, after verifying, augments it to a more evolved form.

The following clauses contain augmentation test cases grouped by CAdES level.

6.2   Augmentation to CAdES-E-C signatures test cases

The test cases in this clause deal with the augmentation to CAdES-E-C signatures.

Table 8 shows 2 augmentation to CAdES-E-C signatures test cases.

Table 8: Test cases for augmentation to CAdES-E-C signatures

TC ID	Description	Pass criteria	Signature attributes
CAdES/Aug/1	This test case tests the augmentation of a CAdES-E-BES signature as specified in CAdES/BES/2 test case to a CAdES-E-C signature as specified in CAdES/C/1 test case.	Positive validation. The signature to be augmented shall be successfully validated before upgrading. The augmented signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime • UnsignedAttributes o SignatureTimeStamp o CompleteCertificateRefs o IssuerSerial o OtherHashAlgAndValue o CompleteRevocationRefs o CRLListIDs
CAdES/Aug/2	This test case tests the augmentation of a CAdES-E-T signature as specified in CAdES/T/1 test case to a CAdES-C signature as specified in CAdES/C/1 test case.	Positive validation. The signature to be augmented shall be successfully validated before augmentation. The augmented signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime • UnsignedAttributes o SignatureTimeStamp o CompleteCertificateRefs o IssuerSerial o OtherHashAlgAndValue o CompleteRevocationRefs o CRLListIDs

6.3   Augmentation to CAdES-E-X signatures test cases

The test cases in this clause deal with the augmentation to CAdES-E-X signatures.

Table 9 shows 3 augmentation to CAdES-E-X signatures test cases.

Table 9: Test cases for augmentation to CAdES-E-X signatures

TC ID	Description	Pass criteria	Signature attributes

CAdES/Aug/3	This test case tests the augmentation of a CAdES-E-BES signature as specified in CAdES/BES/2 test case to a CAdES-E-X signature as specified in CAdES/X/1 test case.	Positive validation. The signature to be augmented shall be successfully validated before augmentation. The augmented signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, ESCTimeStamp attributes.	• Certificates
			○ SigningCertificate
			• SignedAttributes
			○ MessageDigest
			○ ESSSigningCertificateV2
			○ ContentType
			○ SigningTime
			• UnsignedAttributes
			○ SignatureTimeStamp
			○ CompleteCertificateRefs
			    ○ IssuerSerial
			    ○ OtherHashAlgAndValue
			○ CompleteRevocationRefs
			    ○ CRLListIDs
			○ ESCTimeStamp

CAdES/Aug/4	This test case tests the augmentation of a CAdES-E-T signature as specified in CAdES/T/1 test case to a CAdES-E-X signature as specified in CAdES/X/1 test case.	Positive validation. The signature to be augmented shall be successfully validated before augmentation. The augmented signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, ESCTimeStamp attributes.	• Certificates
			○ SigningCertificate
			• SignedAttributes
			○ MessageDigest
			○ ESSSigningCertificateV2
			○ ContentType
			○ SigningTime
			• UnsignedAttributes
			○ SignatureTimeStamp
			○ CompleteCertificateRefs
			    ○ IssuerSerial
			    ○ OtherHashAlgAndValue
			○ CompleteRevocationRefs
			    ○ CRLListIDs
			○ ESCTimeStamp

CAdES/Aug/5	This test case tests the augmentation of a CAdES-E-C signature as specified in CAdES/C/1 test case to a CAdES-E-X signature as specified in CAdES/X/1 test case.	Positive validation. The signature to be augmented shall be successfully validated before augmentation. The augmented signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, ESCTimeStamp attributes.	• Certificates
			○ SigningCertificate
			• SignedAttributes
			○ MessageDigest
			○ ESSSigningCertificateV2
			○ ContentType
			○ SigningTime
			• UnsignedAttributes
			○ SignatureTimeStamp
			○ CompleteCertificateRefs
			    ○ IssuerSerial
			    ○ OtherHashAlgAndValue
			○ CompleteRevocationRefs
			    ○ CRLListIDs
			○ ESCTimeStamp

6.4 Augmentation to CAdES-E-XL signatures test cases

The test cases in this clause deal with the augmentation to CAdES-E-XL signatures.

Table 10 shows 3 augmentation to CAdES-E-XL signatures test cases.

Table 10: Test cases for augmentation to CAdES-E-XL signatures

TC ID	Description	Pass criteria	Signature attributes
CAdES/Aug/6	This test case tests the augmentation of a CAdES-E-BES signature as specified in CAdES/BES/2 test case to a CAdES-E-XL signature as specified in CAdES/XL/1 test case.	Positive validation. The signature to be augmented shall be successfully validated before augmentation. The augmented signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, ESCTimeStamp, CertificateValues, RevocationValues attributes.	- Certificates - SigningCertificate - SignedAttributes - MessageDigest - ESSSigningCertificateV2 - ContentType - SigningTime - UnsignedAttributes - SignatureTimeStamp - CompleteCertificateRefs - IssuerSerial - OtherHashAlgAndValue - CompleteRevocationRefs - CRLListIDs - ESCTimeStamp - CertificateValues - RevocationValues - crlVals
CAdES/Aug/7	This test case tests the augmentation of a CAdES-E-T signature as specified in CAdES/T/1 test case to a CAdES-E-XL signature as specified in CAdES/XL/1 test case.	Positive validation. The signature to be augmented shall be successfully validated before augmentation. The augmented signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, ESCTimeStamp, CertificateValues, RevocationValues attributes.	- Certificates - SigningCertificate - SignedAttributes - MessageDigest - ESSSigningCertificateV2 - ContentType - SigningTime - UnsignedAttributes - SignatureTimeStamp - CompleteCertificateRefs - IssuerSerial - OtherHashAlgAndValue - CompleteRevocationRefs - CRLListIDs - ESCTimeStamp - CertificateValues - RevocationValues - crlVals
CAdES/Aug/8	This test case tests the augmentation of a CAdES-E-C signature as specified in CAdES/C/1 test case to a CAdES-E-XL signature as specified in CAdES/XL/1 test case.	Positive validation. The signature to be augmented shall be successfully validated before augmentation. The augmented signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, ESCTimeStamp, CertificateValues, RevocationValues attributes.	- Certificates - SigningCertificate - SignedAttributes - MessageDigest - ESSSigningCertificateV2 - ContentType - SigningTime - UnsignedAttributes - SignatureTimeStamp - CompleteCertificateRefs - IssuerSerial - OtherHashAlgAndValue - CompleteRevocationRefs - CRLListIDs - ESCTimeStamp - CertificateValues - RevocationValues - crlVals

6.5   Augmentation to CAdES-E-A signatures test cases

The test cases in this clause deal with the augmentation to CAdES-E-A signatures.

Table 11 shows 3 augmentations to CAdES-E-A signatures test cases.

Table 11: Test cases for upgrading to CAdES-A forms

TC ID	Description	Pass criteria	Signature attributes

CAdES/Aug/9	This test case tests the augmentation of a CAdES-E-BES signature as specified in CAdES/BES/2 test case to a CAdES-E-A signature as specified in CAdES/A/5 test case.	Positive validation. The signature to be augmented shall be successfully validated before augmentation.
		The augmented signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, Crls, ESSSigningCertificateV2, SignatureTimeStamp and ArchiveTimeStampV3 attributes.
			• Certificates
			  o SigningCertificate
			• Crls
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o ArchiveTimeStampV3

CAdES/Aug/10	This test case tests the augmentation of a CAdES-E-T signature as specified in CAdES/T/1 test case to a CAdES-E-A signature as specified in CAdES/A/5 test case.	Positive validation. The signature to be augmented shall be successfully validated before augmentation.
		The augmented signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, Crls, ESSSigningCertificateV2, SignatureTimeStamp and ArchiveTimeStampV3 attributes.
			• Certificates
			  o SigningCertificate
			• Crls
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o ArchiveTimeStampV3

CAdES/Aug/11	This test case tests the upgrade of a CAdES-E-C signature as specified in CAdES/C/1 test case to a CAdES-E-A signature as specified in CAdES/A/1 test case.	Positive validation. The signature to be upgraded shall be successfully validated before upgrading. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, CertificateValues, RevocationValues and ArchiveTimeStampV3 attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o CompleteCertificateRefs
			    o IssuerSerial
			    o OtherHashAlgAndValue
			  o CompleteRevocationRefs
			    o CRLListIDs
			  o CertificateValues
			  o RevocationValues
			    o crlVals
			  o ArchiveTimeStampV3

7   Testing negative extended CAdES signatures

7.1   CAdES-E-BES test cases

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

Table 12 shows which attributes are defined in the negative CAdES-E-BES signatures for each test case.

Table 12: Negative test cases for CAdES-E-BES signatures

TC ID	Description	Pass criteria	Signature attributes
CAdES/BESN/1	Verify a signed document having a wrong signature (the hash that was signed is not the hash of the specified MessageDigest element).	Negative validation because the hash that was signed is not the hash of the specified MessageDigest attribute. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate and ESSSigningCertificateV2 attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime
CAdES/BESN/2	Verify a document signed 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.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime
CAdES/BESN/3	Verify a document signed with a revoked/suspended signing certificate.	Negative validation because the signing certificate is revoked (at the time specified in signingTime attribute). The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate and ESSSigningCertificateV2 attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime
CAdES/BESN/4	Verify a signed document 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 signer certificate. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate and ESSSigningCertificateV2 attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime
CAdES/BESN/5	Verify a signed document whose format is not CAdES-E-BES.	Negative validation because the signature format is not a CAdES-E-BES form. The signature shall contain ContentType, SigningTime, MessageDigest and SigningCertificate attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ContentType o SigningTime
CAdES/BESN/6	Verify a document signed with an untrusted signing certificate.	Negative validation because the signing certificate is untrusted. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate and ESSSigningCertificateV2 attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime

7.2   CAdES-E-EPES test cases

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

Table 13 shows which attributes are defined in the negative CAdES-E-EPES signatures for each test case.

Table 13: Negative test cases for CAdES-E-EPES signatures

TC ID	Description	Pass criteria	Signature attributes
CAdES/EPESN/1	Verify a signed document having the value of SignaturePolicyId.sigPolicyHash field that does *NOT* match to the hash value of signer 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.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime o SignaturePolicyIdentifier
CAdES/EPESN/2	Verify a signed document in which the sigPolicyHash field value of SignaturePolicyIdentifier attribute in the CAdES-EPES signature is identical to signPolicyHash field value of IETF RFC 3125 [i.4] ASN.1 signature policy file. However in the policy file, signPolicyHash is *NOT* identical to the hash value which was calculated by the SignPolicyInfo without ASN.1 tag and length.	Negative validation because the sigPolicyHash field value of SignaturePolicyIdentifier attribute in the CAdES-E-EPES signature, while being identical to signPolicyHash field value of ASN.1 signature policy file, is not identical to the hash value which is calculated by the SignPolicyInfo without ASN.1 tag and length. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, SignaturePolicyIdentifier and ESSSigningCertificateV2 attributes.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime o SignaturePolicyIdentifier

7.3   CAdES-E-T test cases

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

Table 14 shows which attributes are defined in the negative CAdES-E-T signatures for each test case.

Table 14: Negative test cases for CAdES-E-T signatures

TC ID	Description	Pass criteria	Signature attributes
CAdES/TN/1	Verify a signed document in which the signing certificate, at the time in SignatureTimeStamp, 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.	• Certificates o SigningCertificate • SignedAttributes o MessageDigest o ESSSigningCertificateV2 o ContentType o SigningTime • UnsignedAttributes o SignatureTimeStamp

TC ID	Description	Pass criteria	Signature attributes

CAdES/TN/2	Verify a signed document in which the signing certificate, at the time in SignatureTimeStamp, 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.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp

CAdES/TN/3	Verify a signed document in which the hash value of messageImprint in SignatureTimeStamp does *NOT* match to the hash value of corresponding signature value of 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.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp

CAdES/TN/4	Verify a signed document in which the timestamp signing certificate, at the time in SignatureTimeStamp, 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.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp

CAdES/TN/5	Verify a signed document in which the timestamp signing certificate, at the time in SignatureTimeStamp, 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.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp

CAdES/TN/6	Verify a signed document in which the timestamp signing certificate is untrusted.	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.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp

7.4   CAdES-E-A test cases

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

Table 15 shows which attributes are defined in the negative CAdES-E-A signatures for each test case.

Table 15: Negative test cases for CAdES-A signatures

TC ID	Description	Pass criteria	Signature attributes

CAdES/AN/1	Verify a signed document 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, CompleteCertificateRefs, CompleteRevocationRefs, TimestampedCertsCRLs, CertificateValues, RevocationValues and ArchiveTimeStampV3 attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o CompleteCertificateRefs
			      o IssuerSerial
			      o OtherHashAlgAndValue
			  o CompleteRevocationRefs
			      o CRLListIDs
			  o TimestampedCertsCRLs
			  o CertificateValues
			  o RevocationValues
			      o crlVals
			  o ArchiveTimeStampV3

CAdES/AN/2	Verify a signed document in which the time in the TimestampedCertsCRLs is ulterior than the time in ATSv3.	Negative validation because the time in the TimestampedCertsCRLs is ulterior than the time in ArchiveTimeStampV3. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, TimestampedCertsCRLs, CertificateValues, RevocationValues and ArchiveTimeStampV3 attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o CompleteCertificateRefs
			      o IssuerSerial
			      o OtherHashAlgAndValue
			  o CompleteRevocationRefs
			      o CRLListIDs
			  o TimestampedCertsCRLs
			  o CertificateValues
			  o RevocationValues
			      o crlVals
			  o ArchiveTimeStampV3

TC ID	Description	Pass criteria	Signature attributes

CAdES/AN/3	Verify a signed document in which the time in the ESCTimeStamp is ulterior than the time in ATSv3.	Negative validation because the time in the ESCTimeStamp is ulterior than the time in ArchiveTimeStampV3. The signature shall contain ContentType, SigningTime, MessageDigest, SigningCertificate, ESSSigningCertificateV2, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, ESCTimeStamp, CertificateValues, RevocationValues and ArchiveTimeStampV3 attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o CompleteCertificateRefs
			    o IssuerSerial
			    o OtherHashAlgAndValue
			  o CompleteRevocationRefs
			    o CRLListIDs
			  o ESCTimeStamp
			  o CertificateValues
			  o RevocationValues
			    o crlVals
			  o ArchiveTimeStampV3

CAdES/AN/4	Verify a signed document in which the content in ats-hash-index element has not the right value related to the CAdES signature to which the ATSv3 has been applied.	Negative validation because the content in ats-hash-index 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, CompleteCertificateRefs, CompleteRevocationRefs, ESCTimeStamp, CertificateValues, RevocationValues and ArchiveTimeStampV3 attributes.	• Certificates
			  o SigningCertificate
			• SignedAttributes
			  o MessageDigest
			  o ESSSigningCertificateV2
			  o ContentType
			  o SigningTime
			• UnsignedAttributes
			  o SignatureTimeStamp
			  o CompleteCertificateRefs
			    o IssuerSerial
			    o OtherHashAlgAndValue
			  o CompleteRevocationRefs
			    o CRLListIDs
			  o ESCTimeStamp
			  o CertificateValues
			  o RevocationValues
			    o crlVals
			  o ArchiveTimeStampV3

History

Document history		
V1.1.1	June 2016	Publication