ETSI TS 119 134-2 V1.1.1 (2016-06)

TECHNICAL SPECIFICATION

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

Reference

DTS/ESI-0019134-2

Keywords

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

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 2 of a multi-part deliverable covering XAdES digital signatures - Testing Conformance and Interoperability. Full details of the entire series can be found in part 1 [i.3].

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 XAdES baseline signatures as specified in ETSI EN 319 132-1 [1].

The test suites are defined with four different layers reflecting the four different levels of XAdES 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 XAdES baseline 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 http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES 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 applications of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.2] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview".

[i.3] ETSI TR 119 134-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview".

[i.4] 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.1] and the following apply:

negative test case: test case either for a signature that is not a XAdES baseline signature, or for a signature whose validation according to ETSI EN 319 102-1 [i.4] 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.1] and the following apply:

CA	Certification Authority
CRL	Certificate Revocation List
OCSP	Online Certificate Status Provider
TSA	Time-Stamping Authority
TSA1	Time-Stamping Authority 1
TSA2	Time-Stamping Authority 2

4 Overview

This clause describes the overall approach used throughout the present document to specify test suites for testing interoperability of XAdES baseline signature a specified in ETSI EN 319 132-1 [1].

ETSI EN 319 132-1 [1] defines four different levels of XAdES baseline signatures.

The test suites are defined with different layers reflecting the levels of XAdES signatures specified in ETSI EN 319 132-1 [1]:

- Testing XAdES signatures interoperability between applications claiming B-B level conformance.
- Testing XAdES signatures interoperability between applications claiming B-T level conformance. .
- Testing XAdES signatures interoperability between applications claiming B-LT T level conformance.
- Testing XAdES signatures interoperability between applications claiming B-LTA T level conformance.

Table 1 shows the prefixes used throughout the present document to refer to specific elements in the XAdES signature associated to the URIs of the corresponding namespaces.

Table 1: Prefixes used

XML Namespace URI	Prefix
http://www.w3.org/2000/09/xmldsig#	ds
http://uri.etsi.org/01903/v1.3.2#	xades
http://uri.etsi.org/01903/v1.4.1#	xadesv141

5 Test-suite for testing interoperability of XAdES-B-B signatures

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

Mandatory properties for XAdES-B-B signatures as specified in ETSI EN 319 132-1 [1] clause 6.3 shall be present.

Table 2 shows the test suite for testing interoperability of XAdES-B-B signatures as specified in ETSI EN 319 132-1 [1] that do not incorporate `xades:SignaturePolicyIdentifier` qualifying property.

Table 3 shows the test suite for testing interoperability of XAdES-B-B signatures as specified in ETSI EN 319 132-1 [1] that do incorporate `xades:SignaturePolicyIdentifier` and `xades:SignaturePolicyDocumentStore` qualifying properties.

Table 2: Test cases for XAdES-B-B signatures that do not incorporate xades:SignaturePolicyIdentifier qualifying property

TC ID	Description	Pass criteria	Signature qualifying properties
XAdES/BB/1	This is the simplest test case for XAdES-B-B signatures. XAdES-B-B signature signing one data object (a text file) and the `xades:SignedProperties` element. The signature only contains the mandatory XAdES properties according to the B-level, namely: `xades:SigningTime`. `xades:SigningCertifiatev2`. `xades:DataObjectFormat`. The `xades:DataObjectFormat` should point to a `ds:Reference` whose `URI` attribute points to the signed simple text file.	Positive validation.	• `xades:SigningCertificateV2` • `xades:SigningTime` • `xades:DataObjectFormat`
XAdES/BB/2	XAdES-B-B signature signing two data objects and the `xades:SignedProperties` element. This brings the presence of two `xades:DataObjectFormat` signed properties.	Positive validation.	• `xades:SigningCertificateV2` • `xades:SigningTime` • `xades:DataObjectFormat` • `xades:DataObjectFormat`
XAdES/BB/3	XAdES-B-B signature signing two data objects and the `xades:SignedProperties` element. Incorporates one `xades:CommitmentTypeIndication` qualifying property expressing a commitment for all the signed data objects.	Positive validation.	• `xades:SigningCertificateV2` • `xades:SigningTime` • `xades:DataObjectFormat` • `xades:DataObjectFormat` • `xades:CommitmentTypeIndication (with xades:AllSignedDataObjects element)`
XAdES/BB/4	XAdES-B-B signature signing two data objects and the `xades:SignedProperties` element. Incorporates one `xades:CommitmentTypeIndication` qualifying property expressing a commitment for one of the signed data objects.	Positive validation.	• `xades:SigningCertificateV2` • `xades:SigningTime` • `xades:DataObjectFormat` • `xades:DataObjectFormat` • `xades:CommitmentTypeIndication (with one xades:ObjectReference element)`
XAdES/BB/5	XAdES-B-B signature signing one data object (a text file) and the `xades:SignedProperties` element. Incorporates one `xades:SignatureProductionPlaceV2` qualifying property.	Positive validation.	• `xades:SigningCertificateV2` • `xades:SigningTime` • `xades:DataObjectFormat` • `xades:SignatureProductionPlaceV2`
XAdES/BB/6	XAdES-B-B signature signing one data object (a text file) and the `xades:SignedProperties` element. Incorporates one X509 Attribute certificate within the `xades:SignerRoleV2` qualifying property.	Positive validation.	• `xades:SigningCertificateV2` • `xades:SigningTime` • `xades:DataObjectFormat` • `xades:SignerRoleV2 (with one X509 Attribute certificate within one CertifiedRole/X509AttributeCertificate element)`
XAdES/BB/7	XAdES-B-B signature signing one data object (a text file) and the `xades:SignedProperties` element. Incorporates one claimed attribute within the `xades:SignerRoleV2` qualifying property.	Positive validation.	• `xades:SigningCertificateV2` • `xades:SigningTime` • `xades:DataObjectFormat` • `xades:SignerRoleV2 (with one xades:Claimed element)`

TC ID	Description	Pass criteria	Signature qualifying properties
XAdES/BB/8	XAdES-B-B signature signing one data object (a text file) and the `xades:SignedProperties` element. Incorporates one signed assertion within the `xades:SignerRoleV2` qualifying property.	Positive validation.	• `xades:SigningCertificateV2` • `xades:SigningTime` • `xades:DataObjectFormat` • `xades:SignerRoleV2 (with one xades:SignedAssertion element)`
XAdES/BB/9	XAdES-B-B signature signing one data object (a text file) and the `xades:SignedProperties` element. Incorporates one X509 Attribute certificate and one signed assertion within the `xades:SignerRoleV2` qualifying property.	Positive validation.	• `xades:SigningCertificateV2` • `xades:SigningTime` • `xades:DataObjectFormat` • `xades:SignerRoleV2 (with one xades:SignedAssertion element and with one CertifiedRole/X509AttributeCertificate element)`
XAdES/BB/10	XAdES-B-B signature signing one data object (a text file) and the `xades:SignedProperties` element. Incorporates one `xades:CounterSignature` qualifying property.	Positive validation.	• `xades:SigningCertificateV2` • `xades:SigningTime` • `xades:DataObjectFormat` • `xades:CounterSignature`
XAdES/BB/11	XAdES-B-B signature signing two data objects and the `xades:SignedProperties` element. Incorporates one `xades:AllDataObjectsTimeStamp` encapsulating a time-stamp token that time-stamps the signed data objects as specified in ETSI EN 319 132-1 [1].	Positive validation	• `xades:SigningCertificateV2` • `xades:SigningTime` • `xades:DataObjectFormat` • `xades:DataObjectFormat` • `xades:AllDataObjectTimeStamp`
XAdES/BB/12	XAdES-B-B signature signing two data objects and the `xades:SignedProperties` element. Incorporates one `xades:IndividualDataObjectsTimeStamp` encapsulating a time-stamp token that time-stamps one of the signed data objects as specified in ETSI EN 319 132-1 [1].	Positive validation	• `xades:SigningCertificateV2` • `xades:SigningTime` • `xades:DataObjectFormat` • `xades:DataObjectFormat` • `xades:IndividualDataObjectsTimeStamp`
XAdES/BB/13	XAdES-B-B signature signing two data objects and the `xades:SignedProperties` element. Incorporates one `xades:CommitmentTypeIndication` qualifying property expressing a commitment for one of the signed data objects. Incorporates one `xades:SignatureProductionPlaceV2` qualifying property. Incorporates one X509 Attribute certificate and one signed assertion within the `xades:SignerRoleV2` qualifying property. Incorporates one `xades:CounterSignature` qualifying property. Incorporates one `xades:IndividualDataTimeStamp` encapsulating a time-stamp token that time-stamps one of the signed data objects as specified in ETSI EN 319 132-1 [1].	Positive validation	• `xades:SigningCertificateV2` • `xades:SigningTime` • `xades:DataObjectFormat` • `xades:DataObjectFormat` • `xades:CommitmentTypeIndication (with one xades:ObjectReference element)` • `xades:SignatureProductionPlaceV2` • `xades:SignerRoleV2 with one xades:SignedAssertion element and with one CertifiedRole/X509AttributeCertificate` • `xades:CounterSignature` • `xades:IndividualDataObjectTimeStamp`

Table 3: Test cases for XAdES-B-B signatures incorporating xades:SignaturePolicyIdentifier qualifying property

TC ID	Description	Pass criteria	Signature qualifying properties
XAdES/BB/14	XAdES-B-B signature signing one data object (a text file) and the `xades:SignedProperties` element. Incorporates one `xades:SignaturePolicyIdentifier` qualifying property containing a `xades:SignaturePolicyHash` element and the following qualifiers: `xades:SPURI`, and `xades:UserNotice`.	Positive validation	• `xades:SigningCertificateV2` • `xades:SigningTime` • `xades:DataObjectFormat` • `xades:SignaturePolicyIdentifier (with xades:SignaturePolicyHash element and xades:SPURI and xades:UserNotice qualifiers)`
XAdES/BB/15	XAdES-B-B signature signing one data object (a text file) and the `xades:SignedProperties` element. Incorporates one `xades:SignaturePolicyIdentifier` qualifying property containing a `xades:SignaturePolicyHash` element and the following qualifiers: `xades:SPURI`, and `xadesv141:SPDocSpecification`. This last qualifier will specify how to compute the digest value of the signature policy document. NOTE: At the time the present document was produced no technical specification within ETSI TR 119 000 [i.2] was available specifying a syntax for defining a signature policy. The test case is nevertheless incorporated in order it can be used when such specification(s) are produced.	Positive validation	• `xades:SigningCertificateV2` • `xades:SigningTime` • `xades:DataObjectFormat` • `xades:SignaturePolicyIdentifier (with xades:SignaturePolicyHash element and xades:SPURI and xadesv141:SPDocSpecification qualifiers)`
XAdES/BB/16	XAdES-B-B signature signing one data object (a text file) and the `xades:SignedProperties` element. Incorporates one `xades:SignaturePolicyIdentifier` qualifying property containing a `xades:SignaturePolicyHash` element and the following qualifiers: `xades:SPURI`, and `xades:UserNotice`. Incorporates one `xadesv141:SignaturePolicyStore` qualifying property containing a `xadesv141:SignaturePolicyDocument` element.	Positive validation	• `xades:SigningCertificateV2` • `xades:SigningTime` • `xades:DataObjectFormat` • `xades:SignaturePolicyIdentifier (with xades:SignaturePolicyHash element and xades:SPURI and xades:UserNotice qualifiers)` • `xadesv141:SignaturePolicyStore (with xadesv141:SignaturePolicyDocument element)`
XAdES/BB/17	XAdES-B-B signature signing one data object (a text file) and the `xades:SignedProperties` element. Incorporates one `xades:SignaturePolicyIdentifier` qualifying property containing a `xades:SignaturePolicyHash` element and the following qualifiers: `xades:SPURI`, and `xades:UserNotice`. Incorporates one `xadesv141:SignaturePolicyStore` qualifying property containing a `xadesv141:SigPolDocLocalURI` element.	Positive validation	• `xades:SigningCertificateV2` • `xades:SigningTime` • `xades:DataObjectFormat` • `xades:SignaturePolicyIdentifier (with xades:SignaturePolicyHash element and xades:SPURI and xades:UserNotice qualifiers)` • `xadesv141:SignaturePolicyStore (with xadesv141:SigPolDocLocalURI element)`

6 Test-suite for testing interoperability of XAdES-B-T signatures

The test cases in this clause have been defined for different combinations of XAdES-B-T signatures properties.

Mandatory properties for XAdES-B-T signatures as specified in ETSI EN 319 132-1 [1], clause 6.3 shall be present.

Table 4 shows the test suite for testing interoperability of XAdES-B-T signatures as specified in ETSI EN 319 132-1 [1].