ETSI TS 119 134-3 V1.1.1 (2016-06)

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

Reference

DTS/ESI-0019134-3

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

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 XAdES 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 XAdES signatures as specified in ETSI EN 319 132-2 [2].

The present document defines test suites for each level defined in ETSI EN 319 132-2 [2].

Test suites also cover augmentation of extended XAdES 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 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] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: extended XAdES signatures".

[3] ETSI TS 119 134-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signature - Testing Conformance and Interoperability; Part 2: Test suites for testing Interoperability of 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 application of the present document but they assist the user with regard to a particular subject area.

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

[i.2] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.3] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: 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, symbols 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 either for a signature that is not an extended XAdES 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.2] and the following apply:

CA	Certification Authority
CRL	Certificate Revocation List
OCSP	Online Certificate Status Provider
TSA	Time-Stamping Authority

4 Overview

This clause describes the overall approach used throughout the present document to specify test suites for extended XAdES signatures as specified in ETSI EN 319 132-2 [2].

ETSI EN 319 132-2 [2] defines eight different levels of extended XAdES signatures.

The test suites are defined with different layers reflecting the levels of XAdES signatures specified in ETSI EN 319 132-2 [2]. Below follows an overview.

The test suites for testing interoperability of extended XAdES signatures include:

- XAdES-E-BES signatures test cases;
- XAdES-E-EPES signatures test cases;
- XAdES-E-T signatures test cases;
- XAdES-E-C test cases;
- XAdES-E-X test cases;
- XAdES-E-X Long test cases; and
- XAdES-E-A signatures.

The test suites including negative test cases for extended XAdES signatures include:

- Negative test cases for XAdES-E-BES signatures;
- Negative test cases for XAdES-E-EPES signatures;
- Negative test cases for XAdES-E-T signatures; and
- Negative test cases for XAdES-E-A signatures.

The test suites for testing augmentation of extended XAdES signatures include:

- Augmentation to XAdES-E-C signatures;
- Augmentation to XAdES-E-X signatures;
- Augmentation to XAdES-E-XL signatures; and
- Augmentation to XAdES-E-A signatures.

Certain XAdES extended signatures are also XAdES baseline signatures. In consequence, the present document defines test suites for testing interoperability of extended XAdES signatures that include certain test cases already defined in ETSI TS 119 134-2 [3].

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 suites for testing interoperability of extended XAdES signatures

5.1 Introduction

Clause 5 presents a test suite for testing interoperability of extended XAdES signatures as specified in in ETSI EN 319 132-2 [2].

5.2 Testing interoperability of XAdES-E-BES signatures

This clause presents a test suite for testing interoperability of XAdES-E-BES signatures as specified in in ETSI EN 319 132-2 [2].

The test suite for testing interoperability XAdES-E-BES signatures as specified in ETSI EN 319 132-2 [2] shall include the test cases defined in ETSI TS 119 134-2 [3], clause 5, Table 2 and the test cases defined in Table 2.

Table 2: Test cases for XAdES-E-BES not covered in ETSI TS 119 134-2 [3] clause 5

TC ID	Description	Pass criteria	Signature qualifying properties
XAdES/EBES/1	XAdES-E-BES signature signing one data object (a text file) and the `ds:KeyInfo` element, which includes the signing certificate of the signature. The signature does not incorporate the `xades:QualifyingProperties` container. NOTE: This test case allows testing how applications process XAdES-E-BES signatures that do not incorporate the `xades:SigningCertificateV2`.	Positive validation.	• `No xades:QualifyingProperties` • `ds:KeyInfo with signing certificate of the signature` • `ds:KeyInfo is also signed by the signature`
XAdES/EBES/2	XAdES-E-BES signature signing one data object (a text file) and the `xades:SignedProperties` element. Incorporates the `xades:SigningCertificateV2` qualifying property.	Positive validation.	• `xades:SigningCertificateV2`
XAdES/EBES/3	XAdES-E-BES signature signing two data objects, the `xades:SignedProperties` container, and the `ds:KeyInfo` element, which includes the signing certificate of the signature. The signature does not incorporate the `xades:SigningCertificateV2` qualifying property. Incorporates the `xades:SigningTime` qualifying property. Incorporates one `xades:DataObjectFormat` for one of the signed data objects. 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 the `xades:SignatureProductionPlaceV2` 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] generated by a TSA that is within the same hierarchy as the signing certificate of the signature.	Positive validation	• `ds:KeyInfo with signing certificate of the signature` • `ds:KeyInfo is also signed by the signature` • `xades:SigningTime` • `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`

5.3 Test-suite for testing interoperability of XAdES-E-EPES signatures

This clause defines one test suite for testing interoperability of XAdES-E-EPES signatures.

The test suite for testing interoperability XAdES-E-EPES signatures as specified in ETSI EN 319 132-2 [2] shall include the test cases defined in ETSI TS 119 134-2 [3], clause 5, Table 3 and the test cases defined in Table 3.

Table 3: Test cases for XAdES-E-EPES signatures not covered in ETSI TS 119 134-2 [3] clause 5

TC ID	Description	Pass criteria	Signature qualifying properties
XAdES/EEPES/1	XAdES-E-EPES signature signing one data object (a text file), the `ds:KeyInfo` element, which includes the signing certificate of the signature, and the `xades:SignedProperties` container. The signature does not incorporate the `xades:SigningCertificateV2` qualifying property. Incorporates one `xades:SignaturePolicyIdentifier` qualifying property containing a `xades:SignaturePolicyHash` element and the following qualifiers: `xades:SPURI`, and `xades:UserNotice`.	Positive validation	• `ds:KeyInfo with signing certificate of the signature` • `ds:KeyInfo is also signed by the signature` • `xades:SignaturePolicyIdentifier (with xades:SignaturePolicyHash element and xades:SPURI and xades:UserNotice qualifiers)`
XAdES/EEPES/2	XAdES-E-EPES signature signing one data object (a text file), the `ds:KeyInfo` element, which includes the signing certificate of the signature, and the `xades:SignedProperties` container. The signature does not incorporate the `xades:SigningCertificateV2` qualifying property. Incorporates one `xades:SignaturePolicyIdentifier` qualifying property containing a `xades:SignaturePolicyHash` element and the following qualifiers: `xades:SPURI`, and `xadesv141:SPDocSpecification`. This last qualifier specifies 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.3] 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	• `ds:KeyInfo with signing certificate of the signature` • `ds:KeyInfo is also signed by the signature` • `xades:SignaturePolicyIdentifier (with xades:SignaturePolicyHash element and xades:SPURI and xadesv141:SPDocSpecification qualifiers)`
XAdES/EEPES/3	XAdES-E-EPES signature signing one data object (a text file), the `ds:KeyInfo` element, which includes the signing certificate of the signature, and the `xades:SignedProperties` container. The signature does not incorporate the `xades:SigningCertificateV2` qualifying property. 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	• `ds:KeyInfo with signing certificate of the signature` • `ds:KeyInfo is also signed by the signature` • `xades:SignaturePolicyIdentifier (with xades:SignaturePolicyHash element and xades:SPURI and xades:UserNotice qualifiers)` • `xadesv141:SignaturePolicyStore (with xadesv141:SignaturePolicyDocument element)`

5.4 Test-suite for testing interoperability of XAdES-E-T signatures

This clause defines one test suite for testing interoperability of XAdES-E-T signatures.

The test suite for testing interoperability XAdES-E-T signatures as specified in ETSI EN 319 132-2 [2] shall include the test cases defined in ETSI TS 119 134-2 [3], clause 6 and the test cases defined in Table 4.

Table 4: Test cases for XAdES-E-T signatures that are not covered in ETSI TS 119 134-2 [3] clause 6

TC ID	Description	Pass criteria	Signature qualifying properties
XAdES/ET/1	XAdES signature as specified in test case XAdES/EBES/1 with the incorporation of a `xades:SignatureTimeStamp` qualifying property encapsulating one time-stamp token generated by a TSA that is within the same hierarchy as the signing certificate of the signature.	Positive validation	• `ds:KeyInfo with signing certificate of the signature` • `ds:KeyInfo is also signed by the signature` • `xades:SignatureTimeStamp (encapsulating one time-stamp token)`
XAdES/ET/2	XAdES-E-T signature signing one data object (text file) and the `xades:IndividualDataObjectsTimeStamp` container. It incorporates the `xades:SigningCertificateV2` qualifying property. It incorporates a `xades:SignatureTimeStamp` qualifying property encapsulating TWO time-stamp tokens. One of them is generated by a TSA1 that is within the same hierarchy as the signing certificate of the signature. The other is generated by a TSA2 that is not within the hierarchy of the signing certificate of the signature.	Positive validation	• `xades:SigningCertificateV2` • `xades:SignatureTimeStamp (with two time-stamp tokens generated by TSA1 and TSA2)`
XAdES/ET/3	XAdES signature as specified in test case XAdES/EBES/1 with the incorporations mentioned below. 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]. Incorporates a `xades:SignatureTimeStamp` qualifying property encapsulating one time-stamp token. The two time-stamps are generated by the same TSA that is within the same hierarchy as the signing certificate of the signature.	Positive validation	• `ds:KeyInfo with signing certificate of the signature` • `ds:KeyInfo is also signed by the signature` • `xades:IndividualDataObjectsTimeStamp` • `xades:SignatureTimeStamp (encapsulating one time-stamp token)`
XAdES/ET/4	XAdES signature as specified in test case XAdES/EBES/1 with the incorporations mentioned below. Incorporates two `xades:SignatureTimeStamp` qualifying properties, each one encapsulating one time-stamp token generated by different TSAs. These TSAs are within different trust hierarchies. NOTE: This will allow to define test cases for having different `xadesv141:TimeStampValidationData` qualifying properties associated to different `xades:SignatureTimeStamp` qualifying properties	Positive validation	• `ds:KeyInfo with signing certificate of the signature` • `ds:KeyInfo is also signed by the signature` • `xades:SignatureTimeStamp (encapsulating one time-stamp token generated by one TSA1)` • `xades:SignatureTimeStamp (encapsulating one time-stamp token generated by a TSA2 different from the previous one, within a different trust hierarchy)`

TC ID	Description	Pass criteria	Signature qualifying properties
XAdES/ET/5	XAdES signature as specified in test case XAdES/EBES/3 with the incorporations mentioned below. Incorporates one `xades:SignatureTimeStamp` qualifying propertiy encapsulating one time-stamp token generated by a TSA that is within the same hierarchy as the signing certificate of the signature.	Positive validation	• `ds:KeyInfo` with signing certificate of the signature • `ds:KeyInfo` is also signed by the signature • `xades:SigningTime` • `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` • `xades:SignatureTimeStamp` (encapsulating one time-stamp token)