ETSI TS 119 134-4 V1.1.1 (2016-06)

Electronic Signatures and Infrastructures (ESI);
XAdES digital signatures -
Testing Conformance and Interoperability;
Part 4: Testing Conformance of XAdES baseline signatures

Reference

DTS/ESI-0019134-4

Keywords

conformance, e-commerce, electronic signature, 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 4 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.2].

A tool implementing the present document has been developed and is accessible at http://signatures-conformance-checker.etsi.org/.

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 the set of checks to be performed for testing conformance of XAdES signatures against XAdES baseline signatures as specified ETSI EN 319 132-1 [1].

The present document does not specify checks leading to conclude whether a signature is technically valid or not (for instance, it does not specify checks for determining whether the cryptographic material present in the signature may be considered valid or not). In consequence no conclusion may be inferred regarding the technical validity of a signature that has been successfully tested by any tool conformant to the present document.

Checks specified by the present document are exclusively constrained to elements specified by XAdES [1] and to certain elements specified by XMLSig [3] that are re-used in XAdES schema definition (like `ds:DigestMethod`, `ds:DigestValue`).

Regarding XAdES properties, the present document explicitly differentiates between structural requirements that are defined by the XAdES XML Schema, and the rest of the requirements specified by XAdES [1]. Checks corresponding to the first set of requirements are specified in the normative annex A. Checks corresponding to the second set of requirements are specified in the body part of the present document.

The present document is intentionally not linked to any software development technology and is also intentionally agnostic on implementation strategies. This is one of the reasons why the test assertions set specified in the present document includes tests on the correctness of the structure of all the elements specified by XAdES [1].

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] W3C Recommendation (2008): "XML-Signature Syntax and Processing (Second Edition)".

[4] IETF RFC 3061 (2001): "A URN Namespace of Object Identifiers".

[5] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".

[6] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

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] OASIS Standard: "Test Assertions Model Version 1.0".

[i.2] ETSI TR 119 134-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview".

[i.3] ETSI TS 119 134-5: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 5: Testing Conformance of extended XAdES signatures".

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

BER	Basic Encoding Rules
CER	Canonical Encoding Rules
DER	Distinguished Encoding Rules
HTTP	Hyper Text Transfer Protocol
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
PER	Packed Encoding Rules
TSP	Trusted Service Providers
URI	Uniform Resource Identifier
URN	Uniform Resource Name
XER	XML Encoding Rules
XML	eXtensible Markup Language
XMLDSIG	eXtensible Markup Language Digital SIGnature

4 Overview

The present clause describes the main aspects of the technical approach used for specifying the whole set of tests to be performed for testing conformance to ETSI EN 319 132-1 [1].

In order to test conformance against the aforementioned specification, several types of tests are identified, namely:

1) Tests on the signature structure that are directly derived from the XML Schema specified in ETSI EN 319 132-1 [1]. These tests are specified in annex A.

2) Tests on the signature structure that are not defined by the XML schema of ETSI EN 319 132-1 [1] and that in consequence may not be tested by a XML Schema validator tool.

3) Tests on values of specific elements and/or attributes that cannot be tested by a XML Schema validator tool.

4) Tests on interrelationship between different elements present in the signature (URIs that point to certain elements, for instance).

5) Tests on computations reflected in the contents of the signatures (for instance message imprints for a time-stamping service, computed by digesting the concatenation of a number of elements of the signature).

No tests are included testing actual validity of the cryptographic material that might be present in the signature or to be used for its verification (for instance status of certificates).

Tests are defined as test assertions following the work produced by OASIS in "Test Assertions Model Version 1.0" [i.1].

For each XAdES qualifying property and for certain relevant elements specified in XMLDSIG [3], the present document defines a number of test assertions corresponding to the requirements specified in the aforementioned specifications.

ETSI EN 319 132-1 [1] defines requirements for building blocks and XAdES baseline signatures. For the purpose of identifying the whole set of test assertions required for testing conformance against XAdES baseline signatures as specified in ETSI EN 319 132-1 [1], the present document classifies the whole set of requirements specified in ETSI EN 319 132-1 [1] in three groups as follows:

1) Requirements "XAdES_BS" (after "XAdES baseline signatures"): requirements defined in clause 6 of ETSI EN 319 132-1 [1]. These are requirements specific to XAdES baseline signatures.

2) Requirements "XAdES_BB" (after "XAdES building blocks"): requirements defined in clauses 4 and 5, annexes A, C and D of ETSI EN 319 132-1 [1] applicable to both XAdES baseline signatures as specified in ETSI EN 319 132-1 [1] and XAdES extended signatures as specified in ETSI EN 319 132-2 [2].

3) Requirements "XAdES_SCH" (after "XAdES schema"): requirements defined in annex A. These are requirements directly derived from the XML Schema definitions in ETSI EN 319 132-1 [1].

The set of test assertions for XAdES baseline signatures as specified in ETSI EN 319 132-1 [1], shall be the addition of test assertions with code "XAdES_BB", and test assertions with code "XAdES_BS".

Each test assertion includes:

1) Unique identifier for further referencing. The identifiers of the assertions start with a code identifying the set of requirements the assertion corresponds to, namely: "XAdES_BB", and "XAdES_BS".

NOTE: The present document does not define test assertions for requirements "XAdES_BB_ES". These test assertions are defined in ETSI TS 119 134-5 [i.3].

2) Reference to the **Normative source** for the test.

3) The **Target** of the assertion. In the normative part, this field identifies ETSI EN 319 132-1 [1].

4) **Prerequisite** (**optional**) is, according to [i.1], "a logical expression (similar to a Predicate) which further qualifies the Target for undergoing the core test (expressed by the Predicate) that addresses the Normative Statement". It is used for building test assertions corresponding to requirements that are imposed under certain conditions.

5) **Predicate** fully and unambiguously defining the assertion to be tested.

6) **Prescription level:** three levels are defined: mandatory, preferred and permitted, whose semantics is to be interpreted as described in clause 3.1.2 of [i.1].

7) **Tag:** information on the element tested by the assertion. This indicates that XAdES [1] is the origin of the assertion.

Table 1 shows the prefixes used 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 Testing conformance to B-B level of XAdES signatures

5.1 General

The clause 5 specifies the whole set of assertions, not directly derived from XAdES XML schema, to be tested on applications claiming conformance to the XAdES-B-B signatures as specified in ETSI EN 319 132-1 [1]. As mentioned before the assertions derived from the XML Schema definition are specified in the normative annex A.

Clause 5.2 specifies the assertions for testing conformance on elements that are specified by the W3C XML Signature Recommendation [3] and further profiled by ETSI EN 319 132-1 [1], against ETSI EN 319 132-1 [1].

Clause 5.3 specifies the assertions for testing conformance on the qualifying properties that are relevant for the XAdES-B-B level.

According to ETSI EN 319 132-1 [1], XAdES-B-B signatures should not incorporate a number of qualifying properties. Nevertheless, a XAdES-B-B signature can incorporate them. The list below specifies how to test these properties in case they are present in a XAdES-B-B signature:

1) `xades:SignatureTimeStamp`, shall be tested as specified in clauses 6.2 and A.3.13.
2) `xadesv141:CompleteCertificateRefsV2`, shall be tested as specified in clauses 5.3.12 and A.3.14.
3) `xades:CompleteRevocationRefs`, shall be tested as specified in clauses 5.3.14 and A.3.15.
4) `xadesv141:AttributeCertificateRefsV2`, shall be tested as specified in clauses 5.3.13 and A.3.14.
5) `xades:AttributeRevocationRefs`, shall be tested as specified in clauses 5.3.15 and A.3.15.
6) `xadesv141:RefsOnlyTimeStampV2`, shall be tested as specified in clauses 5.3.17 and A.3.17.
7) `xadesv141:SigAndRefsTimeStampV2`, shall be tested as specified in clauses 5.3.16 and A.3.16.
8) `xades:CertificateValues`, shall be tested as specified in clauses 7.2 and A.3.18.
9) `xades:AttrAuthoritiesCertValues`, shall be tested as specified in clauses 7.4 and A.3.18.
10) `xades:RevocationValues`, shall be tested as specified in clauses 7.3 and A.3.19.
11) `xades:AttributeRevocationValues`, shall be tested as specified in clauses 7.5 and A.3.19.
12) `xadesv141:TimeStampValidationData`, shall be tested as specified in clauses 7.6 and A.3.20.
13) `xadesv141:ArchiveTimeStamp`, shall be tested as specified in clauses 8.2 and A.3.21.
14) `xadesv141:RenewedDigests`, shall be tested as specified in clauses 8.3 and A.3.22.

5.2 Testing XML Signature elements and containers of XAdES qualifying properties

5.2.1 Testing XML Signature elements

5.2.1.1 Testing ds:Signature element

TA id: XADES_BS/XMLSIG/DSSIG/1
Normative source: [1] – Clause 6.3
Target: XAdES signature generator claiming conformance to XAdES baseline signatures as specified in [1]
Predicate: The signature has one or more ds:Object children.
Prescription level: **mandatory**
Tag: XAdES baseline signatures.

5.2.1.2 Testing ds: Reference element

5.2.1.2.1 Test assertions common to XAdES baseline and extended signatures

This clause defines the test assertions for `ds:Reference` element.

TA id: XADES_BB/XMLSIG/REF/1
Normative source: [1] – Clause 4.4.2
Target: XAdES signature generator claiming conformance to XAdES baseline signatures as specified in [1] and to XAdES extended signatures as specified in [2]
Predicate: The value of the attribute Type of the ds:Reference element referencing the xades:SignedProperties element is "http://uri.etsi.org/01903#SignedProperties".
Prescription level: **mandatory**
Tag: XAdES baseline and extended signatures.

TA id: XADES_BB/XMLSIG/REF/2
Normative source: [1] – Clause 4.4.2
Target: XAdES signature generator claiming conformance to XAdES baseline signatures as specified in [1] and to XAdES extended signatures as specified in [2]
Predicate: The digest value appearing within the ds:Reference element is equal to the value computed after processing the ds:Reference according to XMLDSIG [3] clause 4.4.3.2.
Prescription level: **mandatory**
Tag: XAdES baseline and extended signatures.

5.2.1.2.2 Testing ds: Transforms element

This clause defines the test assertions for `ds:Reference`'s `ds:Transforms` child element.

TA id: XAdES_BS/XMLSIG/REF/TR/1
Normative source: [1] Clause 6.3
Target: XAdES signature generator claiming conformance to XAdES baseline signatures as specified in [1]
Predicate: The range of the Transformation algorithms used in new signatures, is the range identified in ETSI EN 319 132 Part 1 [1] clause 6.3.
Prescription level: **preferred**
Tag: XAdES baseline signatures.

5.2.1.3 Testing ds: Canonicalization element

This clause defines the test assertions for `ds:CanonicalizationMethod` element.

TA id: XADES_BS/XMLSIG/REF/CAN/1
Normative source: [1] Clause 6.3
Target: XAdES signature generator claiming conformance to XAdES baseline signatures as specified in [1]
Predicate: The value of the attribute Algorithm of ds:Canonicalization element for new signatures is one of the following three values: http://www.w3.org/2006/12/xml-c14n11, http://www.w3.org/2001/10/xml-exc-c14n#, http://www.w3.org/TR/2001/REC-xml-c14n-20010315.
Prescription level: **preferred**
Tag: XAdES baseline signatures.

TA id: XADES_BS/XMLSIG/REF/CAN/2
Normative source: [1] Clause 6.3
Target: XAdES signature generator claiming conformance to XAdES baseline signatures as specified in [1]
Predicate: The value of the attribute Algorithm of ds:Canonicalization element in legacy XAdES baseline signatures is one of the following six values: http://www.w3.org/2006/12/xml-c14n11, http://www.w3.org/2001/10/xml-exc-c14n#, http://www.w3.org/TR/2001/REC-xml-c14n-20010315, http://www.w3.org/2006/12/xml-c14n11#WithComments, http://www.w3.org/2001/10/xml-exc-c14n#WithComments, http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments.
Prescription level: **permitted**
Tag: XAdES baseline signatures.

5.2.1.4 Testing ds:SignatureValue element

5.2.1.4.1 Test assertions common to XAdES baseline and extended signatures

This clause defines the test assertions for `ds:SignatureValue` child element.

TA id: XAdES_BS/XMLSIG/SIGVAL/TR/1
Normative source: [3]
Target: XAdES signature generator claiming conformance to XAdES signatures either as specified in [1] or in [2]
Predicate: The value in ds:SignatureValue is cryptographically correct.
Prescription level: **mandatory**
Tag: XAdES baseline signatures and extended signatures.

5.2.1.5 Testing ds: KeyInfo element

5.2.1.5.1 Test assertions common to XAdES baseline and extended signatures

TA id: XADES_BB/XMLSIG/KEYINFO/1
Normative source: [3] – Clause 4.4.4
Target: XAdES signature generator claiming conformance to XAdES signatures either as specified in [1] or in [2]
Predicate: The content of any ds:X509Certificate descendant element within the ds:KeyInfo element is a base-64 encoding of a X509 certificate.
Prescription level: **mandatory**
Tag: XAdES baseline signatures and extended signatures.

5.2.1.5.2 Test assertions specific to XAdES baseline signatures

TA id: XADES_BS/XMLSIG/KEYINFO/1
Normative source: [1] Clause 6.3
Target: XAdES signature generator claiming conformance to XAdES baseline signatures as specified in [1]
Predicate: The ds:KeyInfo element is present within the XAdES baseline signatures as specified in [1]
Prescription level: **mandatory**
Tag: XAdES baseline signatures.

TA id: XADES_BS/XMLSIG/KEYINFO/2
Normative source: [1] Clause 6.3
Target: XAdES signature generator claiming conformance to XAdES baseline signatures as specified in [1]
Predicate: The ds:KeyInfo includes the signing certificate in one of its descendant X09Certificate elements
Prescription level: **mandatory**
Tag: XAdES baseline signatures.