ETSI TS 119 134-5 V2.1.1 (2016-06)

Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 5: Testing Conformance of extended XAdES signatures

Reference
RTS/ESI-0019134-5

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

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 5 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].

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 sets of checks required for testing conformance of XAdES signatures against extended XAdES signatures as specified ETSI EN 319 132-2 [2]. It defines only the checks that are specific to extended XAdES signatures. The set of checks that are common to both extended and baseline XAdES signatures, are defined in ETSI TS 119 134-4 [4].

The complete set of checks to be performed by any tool on XAdES extended signatures is the union of the sets defined within the present document and the set of common checks for testing conformance against ETSI EN 319 132-1 [1] and ETSI EN 319 132-2 [2] defined in ETSI TS 119 134-4 [4], as indicated in the normative clauses of the present document.

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. The only possible inferences are the ones explicitly mentioned in the second paragraph of the present clause.

Checks specified by the present document are exclusively constrained to elements specified by ETSI EN 319 132-1 [1] and to certain elements specified by XMLSig [3] that are re-used in XAdES schema definition (like `ds:keyInfo`).

Regarding XAdES properties, the present document does not addresses the structural requirements that are defined by the XAdES XML Schema that are suitably addressed in ETSI TS 119 134-4 [4]. The present document does not address either requirements that are common to both XAdES signatures as specified in ETSI EN 319 132-1 [1] and ETSI EN 319 132-2 [2].

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] ETSI TS 119 134-4: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance of XAdES baseline signatures".

[5] IETF RFC 5035: "Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility".

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".

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 319 132-2 [2].

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 part of the XML Schema specified in ETSI EN 319 132-1 [1] that defines elements that are specific to extended XAdES signatures and not incorporated into XAdES baseline signatures. 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 at the signature or should 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]. The structure of the test assertions is defined in ETSI TS 119 134-4 [4].

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 319 132-2 [2] defines requirements for extended XAdES signatures, where the degree of optionality is higher than in XAdES baseline signatures. For the purpose of identifying the whole set of test assertions required for testing conformance against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], all the requirements defined within the present document are grouped in the group "XAdES_ES", after "XAdES extended signatures."

The set of test assertions to check when the conformance of a certain XAdES signature is tested against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], shall be the addition of the set of test assertions with code "XAdES_BB" in ETSI TS 119 134-4 [4], the set of test assertions with code "XAdES_SCH" in ETSI TS 119 134-4 [4], and the set of test assertions defined within the present document.

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 E-BES level of extended XAdES signatures

5.1 Introduction

The present clause specifies the set of assertions, not directly derived from XAdES XML schema and specific to only XAdES–E-BES signatures, to be tested on applications claiming conformance to the XAdES- E-BES signatures as specified in ETSI EN 319 132-2 [2].

Clause 5.2 specifies the assertions for testing conformance on elements that are specified by the W3C XML Signature Recommendation [3].

Clause 5.3 specifies the assertions for testing conformance on the XAdES qualifying properties.

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_ES/XMLSIG/DSIG/1
Normative source: [1] Clause 4.3, [2] – Clause 4.2
Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]
Predicate: The signature has 0 or more ds:Object children.
Prescription level: **mandatory**
Tag: extended XAdES signatures.

5.2.1.2 Testing ds:KeyInfo element

TA id: XADES_ES/XMLSIG/KEYINFO/1
Normative source: [1] Clause 4.3, [2] – Clause 4.2
Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]
Prerequisite: The signature does not incorporate the SigningCertificateV2 signed property.
Predicate: One of its ds:X509Certificate descendant elements contains the signing certificate of the XAdES signature AND this element is signed by the signature itself.
Prescription level: **mandatory**
Tag: extended XAdES signatures.

5.2.2 Testing containers of XAdES qualifying properties and references to containers of XAdES qualifying properties

5.2.2.1 Testing incorporation of XAdES qualifying properties to the signature

For testing that the incorporation of XAdES qualifying properties is conformant, the following test assertions shall apply:

TA id: XAdES_ES/PROPERTIES/INCORPORATION/1
Normative source: [1]- Clause 4.4.1
Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]
Predicate: The signature has 0 or more xades:QualifyingPropertyReferences descendant elements.
Prescription level: **mandatory**
Tag: extended XAdES signatures.

TA id: XAdES_ES/PROPERTIES/INCORPORATION/2
Normative source: [1]- Clause 4.4.1
Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]
Predicate: The signature contains 0 or one xades:QualifyingProperties descendant elements.
Prescription level: **mandatory**
Tag: extended XAdES signatures.

TA id: XAdES_ES/PROPERTIES/INCORPORATION/3
Normative source: [1]- Clause 4.4.1
Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]
Prerequisite: The XAdES signature contains 0 or more xades:QualifyingPropertyReferences descendant elements.
Predicate: All the xades:QualifyingPropertyReferences elements are children of the same ds:Object element.
Prescription level: **mandatory**
Tag: extended XAdES signatures.

TA id: XAdES_ES/PROPERTIES/INCORPORATION/3
Normative source: [1]- Clause 4.4.1
Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]
Prerequisite: The XAdES signature contains one xades:QualifyingProperties descendant element.
Predicate: The xades:QualifyingProperties element is child of one of the ds:Object element.
Prescription level: **mandatory**
Tag: extended XAdES signatures.

TA id: XAdES_ES/PROPERTIES/INCORPORATION/4
Normative source: [1]- Clause 4.4.1
Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]
Prerequisite: The XAdES signature contains some xades:QualifyingPropertyReferences descendant elements and one xades:QualifyingProperties descendant element.
Predicate: All the xades:QualifyingPropertyReferences elements and the xades:QualifyingProperties are children of the same ds:Object element.
Prescription level: **mandatory**
Tag: extended XAdES signatures.