



TECHNICAL SPECIFICATION

**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

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	6
Foreword.....	6
Modal verbs terminology.....	6
1 Scope	7
2 References	7
2.1 Normative references	7
2.2 Informative references.....	8
3 Abbreviations	8
4 Overview	8
5 Testing conformance to E-BES level of extended XAdES signatures.....	9
5.1 Introduction	9
5.2 Testing XML Signature elements and containers of XAdES qualifying properties.....	9
5.2.1 Testing XML Signature elements	9
5.2.1.1 Testing ds:Signature element	9
5.2.1.2 Testing ds:KeyInfo element	10
5.2.2 Testing containers of XAdES qualifying properties and references to containers of XAdES qualifying properties	10
5.2.2.1 Testing incorporation of XAdES qualifying properties to the signature	10
5.2.2.2 Testing xades:QualifyingPropertiesReference	11
5.2.2.3 Testing xades:QualifyingProperties	11
5.2.2.4 Testing xades:SignedProperties	11
5.2.2.5 Testing xades:SignedSignatureProperties	12
5.2.2.6 Testing xades:SignedDataObjectProperties	12
5.2.2.7 Testing xades:UnsignedProperties	12
5.2.2.8 Testing xades:UnsignedSignatureProperties	12
5.2.2.9 Testing xades:UnsignedDataObjectProperties	13
5.3 Testing XAdES qualifying properties	13
5.3.1 Testing xades:SigningTime element.....	13
5.3.2 Testing xades:SigningCertificateV2 element.....	13
5.3.3 Testing xades:CommitmentTypeIndication element	13
5.3.4 Testing xades:DataObjectFormat element	13
5.3.5 Testing xades:SignatureProductionPlaceV2 element	14
5.3.6 Testing xades:SignerRoleV2 element.....	14
5.3.7 Testing xades:CounterSignature element.....	14
5.3.8 Testing xades:AllDataObjectsTimeStamp element	14
5.3.9 Testing xades:IndividualDataObjectsTimeStamp element	14
5.3.10 Testing properties from upper levels	14
6 Testing conformance to E-EPES level of extended XAdES signatures.....	16
6.1 Introduction	16
6.2 Testing xades:SignaturePolicyIdentifier element	16
6.2.1 General requirements.....	16
6.2.2 Test assertions specific to E-EPES level.....	16
6.2.3 Testing xades:SPURI signature policy qualifier	16
6.2.4 Testing xades:SPUserNotice signature policy qualifier.....	16
6.2.5 Testing xadesv141:SPDocSpecification signature policy qualifier	16
6.3 Testing xadesv141:SignaturePolicyStore element	16
6.4 Testing properties of upper levels	17
7 Testing conformance to E-T level of extended XAdES signatures.....	17
7.1 Introduction	17
7.2 Testing xades:SignatureTimeStamp element	17
7.2.1 General requirements.....	17
7.2.2 Test assertions specific to E-T level	17

7.3	Testing properties from upper levels	17
8	Testing conformance to E-C level of extended XAdES signatures.....	18
8.1	Introduction	18
8.2	Testing xadesv141:CompleteCertificateRefsV2 element	18
8.2.1	General requirements.....	18
8.2.2	Test assertions specific to E-C level	18
8.2.3	Test assertions no specific to E-C level	18
8.3	Testing xadesv141:AttributeCertificateRefsV2 element	19
8.4	Testing xades:CompleteRevocationRefs element	19
8.4.1	General requirements.....	19
8.4.2	Test assertions specific to E-C level	19
8.4.3	Test assertions no specific to E-C level	19
8.5	Testing xades:AttributeRevocationRefs element	20
8.6	Testing properties from upper levels	20
9	Testing conformance to E-X level of extended XAdES signatures	20
9.1	Introduction	20
9.2	Testing xadesv141:SigAndRefsTimeStampV2 element	20
9.2.1	General requirements.....	20
9.2.2	Test assertions specific to E-X level	21
9.2.3	Test assertions no specific to E-X level.....	21
9.3	Testing xadesv141:RefsOnlyTimeStampV2 element.....	21
9.3.1	General requirements.....	21
9.3.2	Test assertions specific to E-X level	21
9.3.3	Test assertions no specific to E-X level.....	21
9.4	Testing properties from upper levels	22
10	Testing conformance to E-X-L level of extended XAdES signatures.....	22
10.1	Introduction	22
10.2	Testing xades:CertificateValues element	22
10.3	Testing xades:RevocationValues element	23
10.4	Testing xades:AttrAuthoritiesCertValues element	23
10.4.1	General requirements.....	23
10.4.2	Test assertions specific to the E-X-L and E-X-Long levels.....	23
10.4.3	Test assertions no specific to the E-X-L and E-X-Long levels.....	23
10.5	Testing xades:AttributeRevocationValues element.....	24
10.5.1	General requirements.....	24
10.5.2	Test assertions specific to the E-X-L and E-X-Long levels.....	24
10.5.3	Test assertions no specific to the E-X-L and E-X-Long levels.....	24
10.6	Testing properties from upper levels	24
11	Testing conformance to E-X-Long level of extended XAdES signatures.....	24
11.1	General requirements	24
11.2	Test assertions for qualifying properties specific of the level	25
11.3	Testing properties from upper levels	25
12	Testing conformance to E-A level of extended XAdES signatures	25
12.1	Introduction	25
12.2	Testing xadesv141:TimeStampValidationData element	25
12.2.1	General requirements.....	25
12.2.2	Test assertions specific to E-A level	26
12.3	Testing xadesv141:ArchiveTimeStamp element.....	26
12.3.1	General requirements.....	26
12.3.2	Test assertions specific to E-A level	26
12.3.3	Test assertions no specific to E-A level	26
12.4	Testing xadesv141:RenewedDigests element.....	26
12.4.1	General requirements.....	26
12.4.2	Test assertions specific to E-A level	26
Annex A (normative):	Test assertions derived from XML Schema	27
A.1	Introduction	27

A.2 Testing xades:QualifyingPropertiesReference27

History28

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 address 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/xmlsig#	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.

5.2.2.2 Testing xades:QualifyingPropertiesReference

For testing conformance of `xades:QualifyingPropertiesReference` element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions specified in clause A.2 of the present document, and the following test assertions shall apply:

TA id: XAdES_ES/QPREFS/1

Normative source: [1]- Clause 4.4.1

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: The URI attribute of `xades:QualifyingPropertiesReference` element contains a bare-name XPointer fragment AND references an external `xades:QualifyingProperties` element.

Prescription level: mandatory

Tag: extended XAdES signatures.

TA id: XAdES_ES/QPREFS/2

Normative source: [1]- Clause 4.4.1

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: In the value of the URI attribute of `xades:QualifyingPropertiesReference` element, the not-fragment part identifies the enclosing document, and the bare-name XPointer fragment identifies the `xades:QualifyingProperties` element.

Prescription level: mandatory

Tag: extended XAdES signatures.

5.2.2.3 Testing xades:QualifyingProperties

For testing conformance of `xades:QualifyingProperties` element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4], clauses 5.2.2.2.1 and A.2.1.1 test assertions shall apply.

5.2.2.4 Testing xades:SignedProperties

For testing conformance of `xades:SignedProperties` element against extended XAdES signatures, the test assertions defined in ETSI TS 119 134-4 [4], clause A.2.1.2, and the following test assertions shall apply:

TA id: XAdES_ES/SIGPROP/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 `ds:KeyInfo` does not contain the signing certificate of the signature.

Predicate: A XAdES signature incorporates one `xades:SignedProperties` container element.

Prescription level: mandatory

Tag: extended XAdES signatures.

TA id: XAdES_ES/SIGPROP/2

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 `ds:KeyInfo` contains the signing certificate of the signature within one of its `ds:X509Certificate` descendants AND this element IS NOT signed by the signature itself.

Predicate: A XAdES signature incorporates one `xades:SignedProperties` container element.

Prescription level: mandatory

Tag: extended XAdES signatures.

TA id: XAdES_ES/SIGPROP/3

Normative source: [1]- Clause 4.3.2

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: The `xades:SignedProperties` element is not an empty element.

Prescription level: mandatory

Tag: extended XAdES signatures.

TA id: XAdES_ES/SIGPROP/4

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 `ds:KeyInfo` does not contain the signing certificate of the signature.

Predicate: The `xades:SignedProperties` element contains one `xades:SignedSignatureProperties` container element.

Prescription level: mandatory

Tag: extended XAdES signatures.

TA id: XADES_ES/SIGSIGPROP/5

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 ds:KeyInfo contains the signing certificate of the signature within one of its ds:X509Certificate descendants AND this element IS NOT signed by the signature itself.

Predicate: The xades:SignedProperties element contains one xades:SignedSignatureProperties container element.

Prescription level: mandatory

Tag: extended XAdES signatures.

5.2.2.5 Testing xades:SignedSignatureProperties

For testing conformance of xades:SignedSignatureProperties element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4], clause A.2.1.2.2, and the following test assertions shall apply:

TA id: XADES_ES/SIGSIGPROP/1

Normative source: [1] - Clause 4.3.4

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: The xades:SignedSignatureProperties element is not an empty element.

Prescription level: mandatory

Tag: extended XAdES signatures.

TA id: XADES_ES/SIGSIGPROP/2

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 ds:KeyInfo does not contain the signing certificate of the signature.

Predicate: The xades:SignedSignatureProperties element contains one xades:SigningCertificateV2 qualifying property.

Prescription level: mandatory

Tag: extended XAdES signatures.

TA id: XADES_ES/SIGSIGPROP/3

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 ds:KeyInfo contains the signing certificate of the signature within one of its ds:X509Certificate descendants AND this element IS NOT signed by the signature itself.

Predicate: The xades:SignedSignatureProperties element contains one xades:SigningCertificateV2 qualifying property.

Prescription level: mandatory

Tag: extended XAdES signatures.

5.2.2.6 Testing xades:SignedDataObjectProperties

For testing conformance of xades:SignedDataObjectProperties element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.2.2.5.1 and A.2.1.2.3 shall apply.

5.2.2.7 Testing xades:UnsignedProperties

For testing conformance of xades:UnsignedProperties element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.2.2.6.1 and A.2.1.3.1 shall apply.

5.2.2.8 Testing xades:UnsignedSignatureProperties

For testing conformance of xades:UnsignedSignatureProperties element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.2.2.7.1 and A.2.1.3.2 test assertions shall apply.

5.2.2.9 Testing xades:UnsignedDataObjectProperties

For testing conformance of `xades:UnsignedSignatureProperties` element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.2.2.8.1 and A.2.1.3.3 shall apply.

NOTE : So far no property of this type has been specified within XAdES framework. It is out of the scope of the present document to specify any conformance assertion for this property or their potential children other than the assertion above.

5.3 Testing XAdES qualifying properties

5.3.1 Testing xades:SigningTime element

For testing conformance of `xades:SigningTime` element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clause A.3.2 test assertions shall apply.

5.3.2 Testing xades:SigningCertificateV2 element

For testing conformance of `xades:SigningCertificateV2` element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.2.1 and A.3.3, and the following test assertions shall apply:

TA id: XADES_ES/SIGCERTV2/1

Normative source: [2] - Clause 4.3

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: The `xades:Cert` children do not contain the `IssuerSerialV2` child.

Prescription level: preferred

Tag: extended XAdES signatures

TA id: XADES_ES/SIGCERTV2/2

Normative source: [2] - Clause 4.3

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: The content of `IssuerSerialV2` child element of `xades:Cert` is the base-64 encoding of one DER-encoded instance of type `IssuerSerial` type defined in IETF RFC 5035 [5].

Prescription level: mandatory

Tag: extended XAdES signatures

TA id: XADES_ES/SIGCERTV2/3

Normative source: [1] - Clause 5.2.2

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: The URI attribute value references a place containing the X509 certificate referenced by its `xades:Cert` parent element.

Prescription level: mandatory

Tag: extended XAdES signatures

5.3.3 Testing xades:CommitmentTypeIndication element

For testing conformance of `xades:CommitmentTypeIndication` element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.3.1 and A.3.4 shall apply.

5.3.4 Testing xades:DataObjectFormat element

For testing conformance of `xades:DataObjectFormat` element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.4.1 and A.3.5 shall apply.

5.3.5 Testing `xades:SignatureProductionPlaceV2` element

For testing conformance of `xades:SignatureProductionPlaceV2` element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.5.1 and A.3.6 shall apply.

5.3.6 Testing `xades:SignerRoleV2` element

For testing conformance of `xades:SignerRoleV2` element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.6.1 and A.3.7 shall apply.

5.3.7 Testing `xades:CounterSignature` element

For testing conformance of `xades:CounterSignature` element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.7.1 and A.3.8, and the following requirements shall apply.

For testing conformance of the countersignature itself against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], its components shall be checked as specified in the present document.

NOTE: ETSI TS 119 134-4 [4] provides details on how to proceed for testing conformance of the countersignature against XAdES extended signatures as specified in ETSI EN 319 132-1 [1].

5.3.8 Testing `xades:AllDataObjectsTimeStamp` element

For testing conformance of `xades:AllDataObjectsTimeStamp` element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.8.1 and A.3.9 shall apply.

5.3.9 Testing `xades:IndividualDataObjectsTimeStamp` element

For testing conformance of `xades:IndividualDataObjectsTimeStamp` element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.9.1 and A.3.10 shall apply.

5.3.10 Testing properties from upper levels

According to ETSI EN 319 132-2 [2], XAdES-E-BES extended signatures should not incorporate the following qualifying properties: `xades:SignaturePolicyIdentifier`, `xadesv141:SignaturePolicyStore`, `xades:SignatureTimeStamp`, `xadesv141:CompleteCertificateRefsV2`, `xadesv141:AttributeCertificateRefsV2`, `xades:CompleteRevocationRefs`, `xades:AttributeRevocationRefs`, `xadesv141:RefsOnlyTimeStampV2`, `xadesv141:SigAndRefsTimeStampV2`, `xades:CertificateValues`, `xades:AttrAuthoritiesCertValues`, `xades:RevocationValues`, `xades:AttributeRevocationValues`, `xadesv141:TimeStampValidationData`, `xadesv141:ArchiveTimeStamp`, and `xadesv141:RenewedDigests`.

Nevertheless, a XAdES-E-BES extended signature can incorporate any of them. The list below specifies how to test these properties in case they are present:

- 1) For testing conformance of `xades:SignaturePolicyIdentifier` qualifying property against XAdES-E-BES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.10.1 and A.3.11, and the test assertions defined in clauses 6.2.3, 6.2.4, and 6.2.5 of the present document shall apply.
- 2) For testing conformance of `xadesv141:SignaturePolicyStore` qualifying property against XAdES-E-BES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.11.1 and A.3.12, and the test assertions defined in clause 6.3 of the present document shall apply.

- 3) For testing conformance of `xades:SignatureTimeStamp` qualifying property against XAdES-E-BES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 6.2.1 and A.3.13 shall apply.
- 4) For testing conformance of `xadesv141:CompleteCertificateRefsV2` element against XAdES-E-BES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.12.1 and A.3.14, and clause 8.2.3 of the present document shall apply.
- 5) For testing conformance of `xadesv141:AttributeCertificateRefsV2` element against XAdES-E-BES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.13.1 and A.3.14, and clause 8.3 of the present document shall apply.
- 6) For testing conformance of `xades:CompleteRevocationRefs` element against XAdES-E-BES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.14.1 and A.3.15, and clause 8.4.3 of the present document shall apply.
- 7) For testing conformance of `xades:AttributeRevocationRefs` element against XAdES-E-BES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.15.1 and A.3.15, and clause 8.5 of the present document shall apply.
- 8) For testing conformance of `xadesv141:SigAndRefsTimeStampV2` element against XAdES-E-BES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.16.1 and A.3.16, and clause 9.2.3 of the present document shall apply.
- 9) For testing conformance of `xadesv141:RefsOnlyTimeStampV2` element against XAdES-E-BES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.17.1 and A.3.17, and clause 9.3.3 of the present document shall apply.
- 10) For testing conformance of `xades:CertificateValues` element against XAdES-E-BES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 7.2.1 and A.3.18, and clause 10.2 of the present document shall apply.
- 11) For testing conformance of `xades:RevocationValues` element against XAdES-E-BES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 7.3.1 and A.3.19, and clause 10.3 of the present document shall apply.
- 12) For testing conformance of `xades:AttrAuthoritiesCertValues` element against XAdES-E-BES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 7.4.1 and A.3.18, and clause 10.4.3 of the present document shall apply.
- 13) For testing conformance of `xades:AttributeRevocationValues` element against XAdES-E-BES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 7.5.1 and A.3.19, and clause 10.5.3 of the present document shall apply.
- 14) For testing conformance of `xadesv141:TimeStampValidationData` element against XAdES-E-BES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 7.6.1 and A.3.20 shall apply.
- 15) For testing conformance of `xadesv141:ArchiveTimeStamp` element against XAdES-E-BES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 8.2.1 and A.3.21, and clause 12.3.3 shall apply.
- 16) For testing conformance of `xadesv141:RenewedDigests` element against XAdES-E-BES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 8.3.1 and A.3.22 shall apply.

6 Testing conformance to E-EPES level of extended XAdES signatures

6.1 Introduction

The clause 6 specifies the set of assertions not directly derived from XAdES XML schema to be tested on XAdES qualifying properties corresponding to XAdES-E-EPES level as specified in ETSI EN 319 132-2 [2], which should not be present in lower levels of extended XAdES signatures, namely: `xades:SignaturePolicyIdentifier`, and `xadesv141:SignaturePolicyStore`.

6.2 Testing `xades:SignaturePolicyIdentifier` element

6.2.1 General requirements

For testing conformance of `xades:SignaturePolicyIdentifier` element against XAdES-E-EPES extended signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.10.1 and A.3.11, and clauses 6.2.2, 6.2.3, 6.2.4, and 6.2.5 of the present document shall apply.

6.2.2 Test assertions specific to E-EPES level

TA id: XADES_ES/E_EPES/SIGPOLID/1

Normative source: [2] - clause 4.3

Target: XAdES signature generator claiming conformance to XAdES baseline signatures as specified in [1]

Predicate: The `xades:SignaturePolicyIdentifier` property is present in the signature.

Prescription level: mandatory

Tag: extended XAdES signatures

6.2.3 Testing `xades:SPURI` signature policy qualifier

For testing conformance of `xades:SPURI` signature policy qualifier against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.10.2.1 and A.3.11.2 shall apply.

6.2.4 Testing `xades:SPUserNotice` signature policy qualifier

For testing conformance of `xades:SPUserNotice` signature policy qualifier against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clause A.3.11.3 shall apply.

6.2.5 Testing `xadesv141:SPDocSpecification` signature policy qualifier

For testing conformance of `xadesv141:SPDocSpecification` signature policy qualifier against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.10.3.1 and A.3.11.4 shall apply.

6.3 Testing `xadesv141:SignaturePolicyStore` element

For testing conformance of `xadesv141:SignaturePolicyStore` element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.11.1 and A.3.12 shall apply.

6.4 Testing properties of upper levels

According ETSI EN 319 132-2 [2], XAdES-E-EPES extended signatures should not incorporate the following qualifying properties: `xades:SignatureTimeStamp`, `xadesv141:CompleteCertificateRefsV2`, `xadesv141:AttributeCertificateRefsV2`, `xades:CompleteRevocationRefs`, `xades:AttributeRevocationRefs`, `xadesv141:RefsOnlyTimeStampV2`, `xadesv141:SigAndRefsTimeStampV2`, `xades:CertificateValues`, `xades:AttrAuthoritiesCertValues`, `xades:RevocationValues`, `xades:AttributeRevocationValues`, `xadesv141:TimeStampValidationData`, `xadesv141:ArchiveTimeStamp`, and `xadesv141:RenewedDigests`.

Nevertheless, a XAdES-E-EPES extended signature can incorporate any of them. If any of the aforementioned qualifying properties is incorporated into a XAdES-E-EPES signature, it shall be tested as indicated in clause 5.3.10.

7 Testing conformance to E-T level of extended XAdES signatures

7.1 Introduction

The present clause specifies the set of assertions not directly derived from XAdES XML schema to be tested on the XAdES qualifying property corresponding to XAdES-E-T level as specified in ETSI EN 319 132-2 [2], which should not be present in lower levels of extended XAdES signatures, namely: `xades:SignatureTimeStamp`.

7.2 Testing `xades:SignatureTimeStamp` element

7.2.1 General requirements

For testing conformance of `xades:SignatureTimeStamp` element against XAdES-E-T extended signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 6.2.1 and A.3.13, and the test assertions defined in clause 7.2.2 of the present document shall apply.

7.2.2 Test assertions specific to E-T level

TA id: XADES_ES/E_T/SIGTST/1

Normative source: [2] – clause 4.3

Target: XAdES signature generator claiming conformance to XAdES baseline signatures as specified in [1]

Predicate: The `xades:SignatureTimeStamp` property is present in the signature.

Prescription level: mandatory

Tag: extended XAdES signatures

7.3 Testing properties from upper levels

According ETSI EN 319 132-2 [2], XAdES-E-T extended signatures should not incorporate the following qualifying properties: `xadesv141:CompleteCertificateRefsV2`, `xadesv141:AttributeCertificateRefsV2`, `xades:CompleteRevocationRefs`, `xades:AttributeRevocationRefs`, `xadesv141:RefsOnlyTimeStampV2`, `xadesv141:SigAndRefsTimeStampV2`, `xades:CertificateValues`, `xades:AttrAuthoritiesCertValues`, `xades:RevocationValues`, `xades:AttributeRevocationValues`, `xadesv141:TimeStampValidationData`, `xadesv141:ArchiveTimeStamp`, and `xadesv141:RenewedDigests`.

Nevertheless, a XAdES-E-T extended signature can incorporate any of them. If any of the aforementioned qualifying properties is incorporated into a XAdES-E-T signature, it shall be tested as indicated in clause 5.3.10.

8 Testing conformance to E-C level of extended XAdES signatures

8.1 Introduction

The present clause specifies the set of assertions not directly derived from XAdES XML schema to be tested on the XAdES qualifying properties corresponding to XAdES-E-C level as specified in ETSI EN 319 132-2 [2], which should not be present in lower levels of extended XAdES signatures, namely:

`xadesv141:CompleteCertificateRefsV2`, `xadesv141:AttributeCertificateRefsV2`, `xades:CompleteRevocationRefs`, and `xades:AttributeRevocationRefs`.

8.2 Testing `xadesv141:CompleteCertificateRefsV2` element

8.2.1 General requirements

For testing conformance of `xadesv141:CompleteCertificateRefsV2` element against XAdES-E-C extended signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.12.1 and A.3.14, and the test assertions defined in clauses 8.2.2 and 8.2.3 of the present document shall apply.

8.2.2 Test assertions specific to E-C level

TA id: XADES_ES/E_C/CCERTREFSV2/1

Normative source: [2] - Clause 4.3

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: The `xadesv141:CompleteCertificateRefsV2` property is present in the signature.

Prescription level: **mandatory**

Tag: extended XAdES signatures

8.2.3 Test assertions no specific to E-C level

TA id: XADES_ES/CCERTREFSV2/1

Normative source: [2] - Clause 4.3

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: At most one instance of `xadesv141:CompleteCertificateRefsV2` property is incorporated into the signature.

Prescription level: **mandatory**

Tag: extended XAdES signatures

TA id: XADES_ES/CCERTREFSV2/2

Normative source: [2] - Clause 4.3

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: The `xades:Cert` children do not contain the `IssuerSerialV2` child.

Prescription level: **preferred**

Tag: extended XAdES signatures

TA id: XADES_ES/CCERTREFSV2/3

Normative source: [1]- Clause A.1.1

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: The content of `IssuerSerialV2` element is the base-64 encoding of one DER-encoded instance of type `IssuerSerial` type defined in IETF RFC 5035 [5].

Prescription level: **mandatory**

Tag: extended XAdES signatures

8.3 Testing xadesv141:AttributeCertificateRefsV2 element

For testing conformance of xadesv141:AttributeCertificateRefsV2 element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.13.1 and A.3.14, and the following test assertions shall apply:

TA id: XADES_ES/ATTCERTREFSV2/1

Normative source: [2] - Clause 4.3

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: At most one instance of xadesv141:AttributeCertificateRefsV2 property is incorporated into the signature.

Prescription level: **mandatory**

Tag: extended XAdES signatures

TA id: XADES_ES/ATTCERTREFSV2/2

Normative source: [2] - Clause 4.3

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: The xades:Cert children do not contain the IssuerSerialV2 child.

Prescription level: **preferred**

Tag: extended XAdES signatures

TA id: XADES_ES/ATTCERTREFSV2/3

Normative source: [1]- Clause A.1.3

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: The content of IssuerSerialV2 element is the base-64 encoding of one DER-encoded instance of type IssuerSerial type defined in IETF RFC 5035 [5].

Prescription level: **mandatory**

Tag: extended XAdES signatures

8.4 Testing xades:CompleteRevocationRefs element

8.4.1 General requirements

For testing conformance of xades:CompleteRevocationRefs element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.14.1 and A.3.15, and the test assertions defined in clauses 8.4.2 and 8.4.3 of the present document shall apply.

8.4.2 Test assertions specific to E-C level

TA id: XADES_ES/E_C/CREVREFS/1

Normative source: [2] - Clause 4.3

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: The xadesv141: CompleteRevocationRefs property is present in the signature.

Prescription level: **mandatory**

Tag: extended XAdES signatures

8.4.3 Test assertions no specific to E-C level

TA id: XADES_ES/CREVREFS/1

Normative source: [2] - Clause 4.3

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: At most one instance of xades:CompleteRevocationRefs property is incorporated into the signature.

Prescription level: **mandatory**

Tag: extended XAdES signatures

8.5 Testing xades:AttributeRevocationRefs element

For testing conformance of `xades:AttributeRevocationRefs` element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.15.1 and A.3.15, and the following test assertions shall apply:

TA id: XADES_ES/ATTREVREFS/1

Normative source: [2] - Clause 4.3

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: The `xades:AttributeRevocationRefs` property is not present in the signature.

Prescription level: preferred

Tag: extended XAdES signatures

TA id: XADES_BS/ATTREVREFS/2

Normative source: [2] - Clause 4.3

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: At most one instance of `xades:AttributeRevocationRefs` property is incorporated into the signature.

Prescription level: mandatory

Tag: extended XAdES signatures

8.6 Testing properties from upper levels

According ETSI EN 319 132-2 [2], XAdES-E-C extended signatures should not incorporate the following qualifying properties: `xadesv141:RefsOnlyTimeStampV2`, `xadesv141:SigAndRefsTimeStampV2`, `xades:CertificateValues`, `xades:AttrAuthoritiesCertValues`, `xades:RevocationValues`, `xades:AttributeRevocationValues`, `xadesv141:TimeStampValidationData`, `xadesv141:ArchiveTimeStamp`, and `xadesv141:RenewedDigests`.

Nevertheless, a XAdES-E-C extended signature can incorporate any of them. If any of the aforementioned qualifying properties is incorporated into a XAdES-E-C signature, it shall be tested as indicated in clause 5.3.10.

9 Testing conformance to E-X level of extended XAdES signatures

9.1 Introduction

The present clause specifies the set of assertions not directly derived from XAdES XML schema to be tested on the XAdES qualifying properties corresponding to XAdES-E-X level as specified in ETSI EN 319 132-2 [2], which should not be present in lower levels of extended XAdES signatures, namely: `xadesv141:SigAndRefsTimeStampV2`, `xadesv141:RefsOnlyTimeStampV2`.

9.2 Testing xadesv141:SigAndRefsTimeStampV2 element

9.2.1 General requirements

For testing conformance of `xadesv141:SigAndRefsTimeStampV2` element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.16.1 and A.3.16, and the test defined in clauses 9.2.2 and 9.2.3 assertions shall apply.

9.2.2 Test assertions specific to E-X level

TA id: XADES_ES/SIGREFSTSTV2/1

Normative source: [2] - Clause A.1

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Prerequisite: The XAdES signature does not incorporate any xadesv141:RefsOnlyTimeStampV2 element.

Predicate: XAdES-E-X signatures contain one or more xades:SigAndRefsTimeStamp.

Prescription level: **mandatory**

Tag: extended XAdES signatures

9.2.3 Test assertions no specific to E-X level

TA id: XADES_ES/SIGREFSTSTV2/2

Normative source: [2] - Clause A.1

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Prerequisite: The XAdES signature incorporates one or more xadesv141:RefsOnlyTimeStampV2 element contains some xades:Include children elements.

Predicate: XAdES-E-X signatures contain one or more xades:SigAndRefsTimeStamp.

Prescription level: **permitted**

Tag: extended XAdES signatures

TA id: XADES_ES/SIGREFSTSTV2/3

Normative source: [1] - Clause A.1.5.1.3

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Prerequisite: The xadesv141:SigAndRefsTimeStampV2 element contains some xades:Include children elements.

Predicate: The message imprint computation input of any time-stamp token encapsulated by xadesv141:SigAndRefsTimeStamp is the concatenation of the objects obtained as specified in ETSI EN 319 132-1 [1] clause A.1.5.1.3.

Prescription level: **mandatory**

Tag: extended XAdES signatures

9.3 Testing xadesv141:RefsOnlyTimeStampV2 element

9.3.1 General requirements

For testing conformance of xadesv141:RefsOnlyTimeStampV2 element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 5.3.17.1 and A.3.17 and the test assertions defined in clauses 9.3.2 and 9.3.3 shall apply.

9.3.2 Test assertions specific to E-X level

TA id: XADES_ES/REFSONTSTV2/1

Normative source: [2] - Clause A.1

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Prerequisite: The XAdES signature does not incorporate any xadesv141:SigAndRefsTimeStamp.

Predicate: XAdES-E-X signatures contain one or more xades:RefsOnlyTimeStampV2.

Prescription level: **mandatory**

Tag: extended XAdES signatures

9.3.3 Test assertions no specific to E-X level

TA id: XADES_ES/REFSONTSTV2/2

Normative source: [2] - Clause A.1

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Prerequisite: The XAdES signature incorporates one or more xadesv141:SigAndRefsTimeStamp element.

Predicate: XAdES-E-X signatures contain one or more xades:RefsOnlyTimeStampV2.

Prescription level: **permitted**

Tag: extended XAdES signatures

TA id: XAdES_ES/REFSONTSTV2/3

Normative source: [1] – Clause A.1.5.2.3

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Prerequisite: The `xadesv141:RefsOnlyTimeStampV2` element contains some `xades:IncludeChildren` elements.

Predicate: The message imprint computation input of any time-stamp token encapsulated by `xadesv141:RefsOnlyTimeStamp` is the concatenation of the objects obtained as specified in ETSI EN 319 132-1 [1] clause A.1.5.2.3.

Prescription level: mandatory

Tag: extended XAdES signatures

9.4 Testing properties from upper levels

According ETSI EN 319 132-2 [2], XAdES-E-X extended signatures should not incorporate the following qualifying properties: `xades:CertificateValues`, `xades:AttrAuthoritiesCertValues`, `xades:RevocationValues`, `xades:AttributeRevocationValues`, `xadesv141:TimeStampValidationData`, `xadesv141:ArchiveTimeStamp`, and `xadesv141:RenewedDigests`.

Nevertheless, a XAdES-E-X-L extended signature can incorporate any of them. The list below specifies how to test these properties in case they are present. If any of the aforementioned qualifying properties is incorporated into a XAdES-E-X signature, it shall be tested as indicated in clause 5.3.10.

10 Testing conformance to E-X-L level of extended XAdES signatures

10.1 Introduction

The present clause specifies the set of assertions not directly derived from XAdES XML schema to be tested on the XAdES qualifying properties corresponding to XAdES-E-X-L level as specified in ETSI EN 319 132-2 [2], which should not be present in lower levels of extended XAdES signatures, namely: `xades:CertificateValues`, `xades:RevocationValue`, `xades:AttrAuthoritiesCertValues`, and `xades:AttributeRevocationValues`.

10.2 Testing `xades:CertificateValues` element

For testing conformance of `xades:CertificateValues` element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 7.2.1 and A.3.18, and the following test assertions shall apply:

TA id: XAdES_ES/CERTVALS/1

Normative source: [2] – Clause A.1

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: A XAdES signature contains at most one `xades:CertificateValues` qualifying property.

Prescription level: mandatory

Tag: extended XAdES signatures

TA id: XAdES_ES/CERTVALS/2

Normative source: [2] – Clause A.1

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: The `xades:CertificateValues` property does not include certificates that are present elsewhere in the XAdES signature.

Prescription level: preferred

Tag: extended XAdES signatures

10.3 Testing xades:RevocationValues element

For testing conformance of xades:RevocationValues element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 7.3.1 and A.3.19, and the following test assertions shall apply:

TA id: XAdES_ES/REVVALS/1

Normative source: [2] - Clause A.1

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: A XAdES signature contains at most one xades:RevocationValues qualifying property.

Prescription level: mandatory

Tag: extended XAdES signatures

TA id: XAdES_ES/REVVALS/2

Normative source: [2] - Clauses A.1, A.2

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: The xades:RevocationValues property does not include revocation values that are present elsewhere in the XAdES signature.

Prescription level: preferred

Tag: extended XAdES signatures

10.4 Testing xades:AttrAuthoritiesCertValues element

10.4.1 General requirements

For testing conformance of xades:AttrAuthoritiesCertValues element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 7.4.1 and A.3.18, and the test assertions defined in clauses 10.4.2 and 10.4.3 of the present document shall apply.

10.4.2 Test assertions specific to the E-X-L and E-X-Long levels

TA id: XAdES_ES/E-X-LONG/ATTCERTVALS/1

Normative source: [2] - Clause A.1

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Prerequisite: The signature incorporates attribute certificate(s) and/or signed assertion(s) AND the rest of elements and properties miss some of the certificates required for their validation.

Predicate: The xades:AttrAuthoritiesCertValues property is present in the signature.

Prescription level: mandatory

Tag: extended XAdES signatures

10.4.3 Test assertions no specific to the E-X-L and E-X-Long levels

TA id: XAdES_ES/ATTCERTVALS/1

Normative source: [2] - Clause A.1

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: A XAdES-E-X-Long contains at most one xades:AttrAuthoritiesCertValues qualifying property.

Prescription level: mandatory

Tag: extended XAdES signatures

TA id: XAdES_ES/ATTCERTVALS/2

Normative source: [2] - Clause A.1

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: The xades:AttrAuthoritiesCertValues property does not include certificates that are present elsewhere in the XAdES signature.

Prescription level: preferred

Tag: extended XAdES signatures

10.5 Testing xades:AttributeRevocationValues element

10.5.1 General requirements

For testing conformance of `xades:AttributeRevocationValues` element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 7.5.1 and A.3.19, and the test assertions defined clauses 10.5.2 and 10.5.3 of the present document shall apply.

10.5.2 Test assertions specific to the E-X-L and E-X-Long levels

TA id: XAdES_ES/E-X-LONG/ATTREVVALS/1

Normative source: [2] - Clause A.1

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Prerequisite: The signature incorporates attribute certificate(s) and/or signed assertion(s) AND the rest of elements and properties miss some of the revocation values required for their validation.

Predicate: The `xades:AttributeRevocationValues` property is present in the signature.

Prescription level: **mandatory**

Tag: extended XAdES signatures

10.5.3 Test assertions no specific to the E-X-L and E-X-Long levels

TA id: XAdES_ES/ATTREVVALS/1

Normative source: [2] - Clause A.1

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: A XAdES-E-X-Long contains at most one `xades:AttributeRevocationValues` qualifying property.

Prescription level: **mandatory**

Tag: extended XAdES signatures

TA id: XAdES_ES/ATTREVVALS/2

Normative source: [2] - Clause A.1

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: The `xades:AttributeRevocationValues` property does not include revocation values that are present elsewhere in the XAdES signature.

Prescription level: **preferred**

Tag: extended XAdES signatures

10.6 Testing properties from upper levels

According ETSI EN 319 132-2 [2], XAdES-E-X-L extended signatures should not incorporate the following qualifying properties: `xadesv141:TimeStampValidationData`, `xadesv141:ArchiveTimeStamp`, and `xadesv141:RenewedDigests`.

Nevertheless, a XAdES-E-X extended signature can incorporate any of them. The list below specifies how to test these properties in case they are present. If any of the aforementioned qualifying properties is incorporated into a XAdES-E-X-L signature, it shall be tested as indicated in clause 5.3.10.

11 Testing conformance to E-X-Long level of extended XAdES signatures

11.1 General requirements

The present clause specifies the set of assertions not directly derived from XAdES XML schema to be tested on the XAdES qualifying properties corresponding to XAdES-E-X-Long level as specified in ETSI EN 319 132-2 [2], which should not be present in lower levels of extended XAdES signatures, namely: `xades:CertificateValues`, `xades:RevocationValue`, `xades:AttrAuthoritiesCertValues`, and `xades:AttributeRevocationValues`.

In addition to that the following qualifying properties from E-X-Long level should not be present: `xadesv141:SigAndRefsTimeStampV2`, and `xadesv141:RefsOnlyTimeStampV2`. Nevertheless, a XAdES-E-X-Long extended signature can incorporate any of them. If any of the aforementioned qualifying properties is incorporated into a XAdES-E-X-Long signature, it shall be tested as indicated in clause 5.3.10.

11.2 Test assertions for qualifying properties specific of the level

For testing conformance of `xades:CertificateValues` element against XAdES-E-X-Long signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in clause 10.2 of the present document shall apply.

For testing conformance of `xades:RevocationValues` element against XAdES-E-X-Long signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in clause 10.3 of the present document shall apply.

For testing conformance of `xades:AttrAuthoritiesCertValues` element against XAdES-E-X-Long signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in clause 10.4 of the present document shall apply.

For testing conformance of `xades:AttributeRevocationValues` element against XAdES-E-X-Long signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in clause 10.5 of the present document shall apply.

11.3 Testing properties from upper levels

According ETSI EN 319 132-2 [2], XAdES-E-X-Long extended signatures should not incorporate the following qualifying properties: `xadesv141:TimeStampValidationData`, `xadesv141:ArchiveTimeStamp`, and `xadesv141:RenewedDigests`.

Nevertheless, a XAdES-E-X-Long extended signature can incorporate any of them. If any of the aforementioned qualifying properties is incorporated into a XAdES-E-X-Long signature, it shall be tested as indicated in clause 5.3.10.

12 Testing conformance to E-A level of extended XAdES signatures

12.1 Introduction

The present clause specifies the set of assertions not directly derived from XAdES XML schema to be tested on the XAdES qualifying properties corresponding to XAdES-E-A level as specified in ETSI EN 319 132-2 [2], which should not be present in lower levels of extended XAdES signatures, namely: `xadesv141:ArchiveTimeStamp`, `xadesv141:TimeStampValidationData`, and `xadesv141:RenewedDigests`.

12.2 Testing `xadesv141:TimeStampValidationData` element

12.2.1 General requirements

For testing conformance of `xadesv141:TimeStampValidationData` element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 7.6.1 and A.3.20, and the test assertions defined in clause 12.2.2 of the present document shall apply.

12.2.2 Test assertions specific to E-A level

TA id: XAdES_ES/E_A/TSTVALDAT/1

Normative source: [2] - Clauses 4.3, A.1, A.2

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Prerequisite: The XAdES-A signature incorporates a xadesv141:ArchiveTimeStamp that time-stamps one or more XAdES qualifying properties that are containers of time-stamp tokens.

Predicate: The XAdES signature incorporates one xadesv141:TimeStampValidation qualifying property for each time-stamp token incorporated before the last archive time-stamp for which the XAdES signature did not incorporate all the validation data required for its validation.

Prescription level: preferred

Tag: extended XAdES signatures

12.3 Testing xadesv141:ArchiveTimeStamp element

12.3.1 General requirements

For testing conformance of xadesv141:ArchiveTimeStamp element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 8.2.1 and A.3.21, and the test assertions defined in clauses 12.3.2 and 12.3.3 of the present document shall apply.

12.3.2 Test assertions specific to E-A level

TA id: XAdES_ES/E_A/ATSTV141/1

Normative source: [2] - Clauses 4.3, A.1, A.2

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: The XAdES-E-A signature incorporates one or more xadesv141:ArchiveTimeStamp qualifying properties.

Prescription level: mandatory

Tag: extended XAdES signatures

12.3.3 Test assertions no specific to E-A level

TA id: XAdES_ES/ATSTV141/1

Normative source: [1] - Clause 5.5.2.3

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Prerequisite: The xadesv141:ArchiveTimeStamp contains some xades:Include children elements.

Predicate: The message imprint computation input of any time-stamp token encapsulated by xadesv141:ArchiveTimeStamp is the concatenation of the objects obtained as specified in ETSI EN 319 132-1 [1] clause 5.5.2.3.

Prescription level: mandatory

Tag: extended XAdES signatures

12.4 Testing xadesv141:RenewedDigests element

12.4.1 General requirements

For testing conformance of xadesv141:RenewedDigests element against extended XAdES signatures as specified in ETSI EN 319 132-2 [2], the test assertions defined in ETSI TS 119 134-4 [4] clauses 8.3.1 and A.3.22, and the test assertions defined in clause 12.4.2 of the present document shall apply.

12.4.2 Test assertions specific to E-A level

TA id: XAdES_ES/E_A/RENDIG /1

Normative source: [2] - Clauses 4.3, A.1, A.2

Target: XAdES signature generator claiming conformance to XAdES extended signatures as specified in [2]

Predicate: The XAdES-E-A signature incorporates one or more xadesv141:RenewedDigests qualifying properties.

Prescription level: permitted

Tag: extended XAdES signatures

Annex A (normative): Test assertions derived from XML Schema

A.1 Introduction

This annex specifies test assertions focussed on testing the structure of the elements specified by XAdES [1] according to its XML Schema. The notation used is the same as the one detailed and used in annex A of ETSI TS 119 134-4 [4].

A.2 Testing xades:QualifyingPropertiesReference

Below follow the test assertions on xades:QualifyingPropertiesReference element.

TA id: XADES_SCH/SCHEMA/QPREF/1

Normative source: [1]- Clause 5.2

Target: XAdES signature generator claiming conformance to extended XAdES signatures as specified in [2]

Predicate: The xades:QualifyingPropertiesReference element does not have any child element.

Prescription level: mandatory

Tag: extended XAdES signatures

TA id: XADES_SCH/SCHEMA/QPREF/2

Normative source: [1]- Clause 5.2

Target: XAdES signature generator claiming conformance to extended XAdES signatures as specified in [2]

Predicate: The set of attributes (leaving apart the attributes declaring namespaces) of one instance of xades:QualifyingPropertiesReference is as follows: noOrder(URI,Id?).

Prescription level: mandatory

Tag: extended XAdES signatures

TA id: XADES_SCH/SCHEMA/QPREF/3

Normative source: [1]- Clause 5.2

Target: XAdES signature generator claiming conformance to extended XAdES signatures as specified in [2]

Predicate: The value of the attribute URI is a URI reference.

Prescription level: mandatory

Tag: extended XAdES signatures

History

Document history		
V1.1.1	April 2012	Publication
V2.1.1	June 2016	Publication