



**Electronic Signatures and Infrastructures (ESI);
XAdES digital signatures -
Testing Conformance and Interoperability;
Part 1: Overview**

Reference

DTR/ESI-0019134-1

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	4
Foreword.....	4
Modal verbs terminology.....	4
Introduction	4
1 Scope	5
2 References	5
2.1 Normative references	5
2.2 Informative references.....	5
3 Definitions.....	6
4 Testing Conformance and Interoperability.....	6
4.1 Part 2: Test suites for testing interoperability of XAdES baseline signatures	6
4.2 Part 3: Test suites for testing interoperability of extended XAdES signatures.....	6
4.3 Part 4: Testing Conformance for XAdES baseline signatures.....	7
4.4 Part 5: Testing Conformance for extended XAdES signatures	7
History	8

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 Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 1 of a multi-part deliverable covering XAdES digital signatures - Testing Conformance and Interoperability, as identified below.

ETSI TR 119 134-1: "Overview";

ETSI TS 119 134-2: "Test suites for testing interoperability of XAdES baseline signatures";

ETSI TS 119 134-3: "Test suites for testing interoperability of extended XAdES signatures";

ETSI TS 119 134-4: "Testing Conformance of XAdES baseline signatures";

ETSI TS 119 134-5: "Testing Conformance of extended XAdES signatures".

Modal verbs terminology

In the present document "**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.

Introduction

This multi-part deliverable defines test suites for testing interoperability and conformance of XAdES signatures. The set of Technical Specifications consist of four documents.

The test suites for testing interoperability of XAdES baseline signatures (Part 2) and the specification required for building software tools for testing technical conformity of XAdES baseline signatures (Part 4) are defined against ETSI EN 319 132-1 [i.1]. The test suites for testing interoperability of extended XAdES signatures (Part 3) and the specification required for building software tools for testing technical conformity of extended XAdES signatures (Part 5) are defined against ETSI EN 319 132-2 [i.2].

1 Scope

The present document provides an overview of the set of test suites for testing interoperability and conformance of XAdES signatures.

The present document:

- a) provides a general description of the set of test suites for testing interoperability and conformance of XAdES signatures; and
- b) lists the features of every test suite for testing interoperability and conformance of XAdES signatures.

The present document is for information only. Normative requirements of each test suite are in other parts of this multi-part deliverable.

2 References

2.1 Normative references

As informative publications shall not contain normative references this clause shall remain empty.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".
- [i.2] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".
- [i.3] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".
- [i.4] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".
- [i.5] ETSI TS 119 134-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of XAdES baseline signatures".
- [i.6] ETSI TS 119 134-3: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 3: Test suites for testing interoperability of extended XAdES signatures".
- [i.7] 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".
- [i.8] 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 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TR 119 001 [i.3] apply.

4 Testing Conformance and Interoperability

4.1 Part 2: Test suites for testing interoperability of XAdES baseline signatures

ETSI TS 119 134-2 [i.5] specifies the test suites for testing interoperability of XAdES baseline signatures against ETSI EN 319 132-1 [i.1].

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

The test suites are defined with different layers reflecting the levels of XAdES baseline signatures specified in [i.1]:

- Testing XAdES signatures interoperability between applications claiming B-B level conformance.
- Testing XAdES signatures interoperability between applications claiming B-T level conformance.
- Testing XAdES signatures interoperability between applications claiming B-LT level conformance.
- Testing XAdES signatures interoperability between applications claiming B-LTA level conformance.
- Testing augmentation of XAdES signatures from B-T level to B-LTA level.
- Testing XAdES baseline signatures whose validation according to ETSI EN 319 102-1 [i.4] would not result in TOTAL_PASSED:
 - XAdES-B-B signatures test cases
 - XAdES-B-T signatures test cases
 - XAdES-B-LTA signatures test cases

4.2 Part 3: Test suites for testing interoperability of extended XAdES signatures

ETSI TS 119 134-3 [i.6] specifies the test suites for testing interoperability of extended XAdES signatures against ETSI EN 319 132-2 [i.2].

ETSI EN 319 132-2 [i.2] defines different signature levels.

The test suites are defined with different layers reflecting the levels of Extended XAdES signatures specified in [i.2].

Testing XAdES signatures:

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

- XAdES-E-X-L test cases;
- XAdES-E-A test cases.

Testing XAdES signatures whose validation according to ETSI EN 319 102-1 [i.4] would not result in TOTAL_PASSED:

- XAdES-E-BES test cases;
- XAdES-E-EPES test cases;
- XAdES-E-T test cases;
- XAdES-E-A test cases.

Testing augmentation of XAdES signatures:

- augmenting to XAdES-E-C level test cases;
- augmenting to XAdES-E-X level test cases;
- augmenting to XAdES-E-XL level test cases;
- augmenting to XAdES-E-A levels test cases.

4.3 Part 4: Testing Conformance for XAdES baseline signatures

ETSI TS 119 134-4 [i.7] defines the requirements for building software tools for testing technical conformity of XAdES baseline signatures against ETSI EN 319 132-1 [i.1].

ETSI EN 319 132-1 [i.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 [i.1], ETSI TS 119 134-4 [i.7] classifies the whole set of requirements specified in ETSI EN 319 132-1 [i.1] in two groups as follows:

- 1) Requirements specific to XAdES baseline signatures.
- 2) Requirements common to both XAdES baseline signatures as specified in ETSI EN 319 132-1 [i.1] and extended XAdES signatures as specified in ETSI EN 319 132-2 [i.2].

4.4 Part 5: Testing Conformance for extended XAdES signatures

ETSI TS 119 134-5 [i.8] defines the requirements for building software tools for testing technical conformance of extended XAdES signatures against ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures" [i.2].

ETSI EN 319 132-1 [i.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 extended XAdES signatures as specified in ETSI EN 319 132-2 [i.2], ETSI TS 119 134-5 [i.8] classifies the whole set of requirements specified in ETSI EN 319 132-1 [i.1] and in ETSI EN 319 132-2 [i.2] in two groups as follows:

- 1) Requirements common to both XAdES baseline signatures as specified in ETSI EN 319 132-1 [i.1] and extended XAdES signatures as specified in ETSI EN 319 132-2 [i.2].
- 2) Requirements specific to Extended XAdES signatures as specified in ETSI EN 319 132-2 [i.2].

History

Document history		
V1.1.1	June 2016	Publication