ETSI TS 119 164-3 V1.1.1 (2016-06)

ETSI TS 119 164-3 V1.1.1 (2016-06)
STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/e21937a7-45c7-40e9-89de-904...-ts-119-164-3-v1.1.1-2016-06

Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC) - Testing Compliance and Interoperability; Part 3: Test suites for testing interoperability of ASiC containers other than baseline

Reference
DTS/ESI-0019164-3

Keywords
ASiC, e-commerce, electronic signature, interoperability, security, testing

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/e2f937a7-4537-400d-80de-9b452ef25ae9/etsi-ts-119164-3-v1.1.1-2016-06

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/e21937a7-25f7-40e8-8de4-0452925ac9/etsi-ts-119-164-3-v1.1.1-2016-06

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 3 of a multi-part deliverable covering Associated Signature Containers (ASiC) - Testing Conformance and Interoperability. Full details of the entire series can be found in part 1 [i.5].

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standards.iteh.ai/catalog/standards/sist/e21937a7-45c7-40e9-89de-90452ef25a19/etsi-ts-119-164-3-v1.1.1-2016-06

1 Scope

The present document defines a number of test suites to assess the interoperability between implementations claiming conformance to ASiC building blocks defined in ETSI EN 319 162-1 [1] and additional containers defined in ETSI EN 319 162-2 [2].

These test suites are agnostic of the PKI infrastructure. Any PKI infrastructure can be used including the one based on EU Member States Trusted Lists.

2 References

2.1 Normative references

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

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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

The following referenced documents are necessary for the application of the present document.

[1] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers".

[2] ETSI EN 319 162-2: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers".

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

[4] Application Note: "APPNOTE.TXT - .ZIP File Format Specification", PKWARE® Inc., September 2012.

[5] ETSI TS 119 124-3: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 3: Test suites for testing interoperability of extended CAdES signatures".

[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".

[7] 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".

[8] IETF RFC 4998: "Evidence Record Syntax (ERS)".

[9] IETF RFC 6283: "Extensible Markup Language Evidence Record Syntax (XMLERS)".

iTeh STANDARD PREVIEW
iTeh Standards (https://standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/e1937a7-4ec7-40e9-89de-10452f5bae9/etsi-ts-119-164-3-v1.1.1-2016-06

2.2 Informative references

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

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

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

[i.1] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.2] ETSI TS 119 164-2: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC) - Testing Compliance & Interoperability; Part 2: Test Suite for ASiC interoperability test events".

[i.3] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[i.4] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

[i.5] ETSI TR 119 164-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC) - Testing Conformance and Interoperability; Part 1: Overview".

[i.6] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/219374c7-45c7-40e9-89de-904522...5ae9/etsi-ts-119-164-3-v1.1.1-2016-06

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TR 119 001 [i.1] and the following apply:

negative test case: test case either for a container including signature(s) that are not extended CAdES signatures [i.3] or extended XAdES signatures [i.4] whose validation according to ETSI EN 319 102-1 [i.6] would not result in TOTAL_PASSED

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.1] and the following apply:

CS	Container Structure
SC	Syntactical Conformance
STV	Signature Time-stamp token Value
TC	Test Case

4 ASiC additional container interoperability test specification overview

The present document complements ETSI TS 119 164-2 [i.2] (interoperability testing of ASiC baseline containers) by specifying test suites for interoperability testing of ASiC containers supporting specific requirements not supported by ASiC baseline containers but still complying with the ASiC building blocks specified in ETSI EN 319 162-1 [1]. This clause describes the overall approach used to specify test suites for interoperability testing of these additional containers.

In particular, the following extensions of ASiC baseline containers are considered:

- extend ASiC baseline containers allowing use of extended XAdES signatures (ETSI EN 319 122-2 [i.3]) and extended CAdES signatures (ETSI EN 319 132-2 [i.4]);
- additional containers specified in ETSI EN 319 162-2 [2].

The test suites define:

- extending ETSI TS 119 164-2 [i.2] with test cases defined for extended CAdES digital signatures defined in ETSI TS 119 124-3 [5] and test cases defined for extended XAdES digital signatures defined in ETSI TS 119 134-3 [6]; and
- defining test cases considering the additional container types specified in ETSI EN 319 162-2 [2].

iTeh STANDARD PREVIEW (standards.iteh.ai) Full standard: https://standards.iteh.ai/catalog/standards/sist/e2f37a7-45c7-40e9-89de-90452f25ae9/etsi-ts-119-164-3-v1.1.1-2016-06

5 Test suite for testing interoperability of ASiC-S containers

5.1 Introduction to testing ASiC-S containers

The test suite for testing interoperability of ASiC-S containers is specified in the next clauses as follows:

- a set of test cases common to all ASiC-S forms is specified in clause 5.2;
- a set of test cases for ASiC-S with extended CAdES signature (ETSI EN 319 122-2 [i.3]) is specified in clause 5.3;
- a set of test cases for ASiC-S with extended XAdES signature (ETSI EN 319 132-2 [i.4]) is specified in clause 5.4;
- a set of test cases for ASiC-S with time assertion (ETSI EN 319 162-2 [2], clause 4.2.1) is specified in clause 5.5.

5.2 Test cases common to all ASiC-S forms

The test cases common to all ASiC-S container forms are specified in Table 1.

Table 1: Test cases common to all ASiC-S baseline containers

TC ID	Description	Pass criteria	Interop. Level
ASiC-S/CS/1	This test case tests if the container ZIP format is correct.	The container content shall comply with the ZIP file format specification [4] and be successfully extracted.	Container Structure
ASiC-S/CS/2	Verify if the container format is identifiable.	The container file extension shall be as specified in ASiC [1], clause 4.3.3.1 item 2)	Container Structure

TC ID	Description	Pass criteria	Interop. Level
ASiC-S/CS/3	mimetype is set appropriately. Prerequisites: • ASiC-S/BCS/1 and ASiC-S/BCS/2 passed; • mimetype is present	mimetype value shall comply with ASiC [1], clauses 4.3.3.1, item 1) and A.1.	Container Structure
ASiC-S/CS/4	This test case tests that one signature or one time assertion is present in the container.	A META-INF folder in the root folder shall be present and contain one file whose name shall comply with ASiC [1], clause 4.3.3.2 item 4.	Container Structure
ASiC-S/CS/5	Presence of the signed file.	A single file, in addition to the optional mimetype, shall be present in the root folder.	Container Structure

5.3 Test cases for ASiC-S containers with CAdES extended signatures

5.3.1 Positive test cases

The test cases for ASiC-S with CAdES containers shall be as specified in Table 2. The test cases specified in clause 5.2 and the presence of signature.p7s file ASiC [1], clause 4.3.3.2 item 3b) are a prerequisite.

A test suite for augmentation of extended CAdES signatures in an ASiC-S container can be defined by applying the augmentation test suites defined in ETSI TS 119 124-3 [5] as follows:

- a test suite for ASiC-S containers including a CAdES-E-BES or CAdES-E-T signature to be augmented to CAdES-E-C signature shall conform to ETSI TS 119 124-3 [5], clause 6.2;
- a test suite for ASiC-S containers including a CAdES-E-BES, CAdES-E-T or CAdES-E-C signature to be augmented to CAdES-E-X signatures shall conform to ETSI TS 119 124-3 [5], clause 6.3;
- a test suite for ASiC-S containers including a CAdES-E-BES, CAdES-E-T or CAdES-E-C signature to be augmented to CAdES-E-XL signatures shall conform to ETSI TS 119 124-3 [5], clause 6.4;
- a test suite for ASiC-S containers including a CAdES-E-BES, CAdES-E-T or CAdES-E-C signature to be augmented to CAdES-E-A signatures shall conform to ETSI TS 119 124-3 [5], clause 6.5.

The Test Case Identifier (TC-ID) for the augmentation of extended CAdES signatures shall be "ASiC-S/" followed by the TC-ID defined for the corresponding CAdES augmentation test case.

Table 2: Test cases for all ASiC-S container levels with extended CAdES signature

TC ID	Description	Pass criteria
ASiC-S/CAdES-E-BES	This group of test cases tests a set of ASiC-S container including each a signature created according to all the CAdES/BES/* test cases defined in the Test suites for testing interoperability of CAdES extended signatures ETSI TS 119 124-3 [5], clause 5.1.	All the CAdES/BES/* test cases in ASiC-S/CAdES-E-BES shall be passed according to the criteria specified in [5], clause 5.1.
ASiC-S/CAdES-E-EPES	This group of test cases tests a set of ASiC-S container including each a signature created according to all the CAdES/EPES/* test cases defined in the Test suites for testing interoperability of CAdES extended signatures ETSI TS 119 124-3 [5], clause 5.2.	All the CAdES/EPES/* test cases in ASiC-S/CAdES-E-EPES shall be passed according to the criteria specified in [5], clause 5.2.
ASiC-S/CAdES-E-T	This group of test cases tests a set of ASiC-S container including each a signature created according to all the CAdES/T/* test cases defined in the Test suites for testing interoperability of CAdES extended signatures ETSI TS 119 124-3 [5], clause 5.3.	All the CAdES/T/* test cases in ASiC-S/CAdES-E-T shall be passed according to the criteria specified in [5], clause 5.3.
ASiC-S/CAdES-E-C	This group of test cases tests a set of ASiC-S container including each a signature created according to all the CAdES/C/* test cases defined in the Test suites for testing interoperability of CAdES extended signatures ETSI TS 119 124-3 [5], clause 5.4.	All the CAdES/C/* test cases in ASiC-S/CAdES-E-C shall be passed according to the criteria specified in [5], clause 5.4.

TC ID	Description	Pass criteria
ASiC-S/CAdES-E-X	This group of test cases tests a set of ASiC-S container including each a signature created according to all the CAdES/X/* test cases defined in the Test suites for testing interoperability of CAdES extended signatures ETSI TS 119 124-3 [5], clause 5.5.	All the CAdES/X/* test cases in ASiC-S/CAdES-E-X shall be passed according to the criteria specified in [5], clause 5.5.
ASiC-S/CAdES-E-XL	This group of test cases tests a set of ASiC-S container including each a signature created according to all the CAdES/XL/* test cases defined in the Test suites for testing interoperability of CAdES extended signatures ETSI TS 119 124-3 [5], clause 5.6.	All the CAdES/XL/* test cases in ASiC-S/CAdES-E-XL shall be passed according to the criteria specified in [5], clause 5.6.
ASiC-S/CAdES-E-A	This group of test cases tests a set of ASiC-S container including each a signature created according to all the CAdES/A/* test cases defined in the Test suites for testing interoperability of CAdES extended signatures ETSI TS 119 124-3 [5], clause 5.7.	All the CAdES/A/* test cases in ASiC-S/CAdES-E-A shall be passed according to the criteria specified in [5], clause 5.7.

5.3.2 Negative test cases

The test cases in this clause are specified in table 3 and have been defined according to ETSI TS 119 124-3 [5], clause 7.

Table 3: Negative test cases for ASiC-S containers with extended CAdES signature

TC ID	Description	Pass criteria
ASiC-S/CAdES-E-BESN	This group of test cases tests a set of ASiC-S container including each a signature created according to all the CAdES/BESN/* test cases defined in the Test suites for testing interoperability of CAdES extended signatures ETSI TS 119 124-3 [5], clause 7.2.	All the CAdES/BESN/* test cases in ASiC-S/CAdES-E-BESN shall be passed according to the criteria specified in [5], clause 7.2.
ASiC-S/CAdES-E-EPESN	This group of test cases tests a set of ASiC-S container including each a signature created according to all the CAdES/EPESN/* test cases defined in the Test suites for testing interoperability of CAdES extended signatures ETSI TS 119 124-3 [5], clause 7.3.	All the CAdES/EPESN/* test cases in ASiC-S/CAdES-E-EPESN shall be passed according to the criteria specified in [5], clause 7.3.
ASiC-S/CAdES-E-TN	This group of test cases tests a set of ASiC-S container including each a signature created according to all the CAdES/TN/* test cases defined in the Test suites for testing interoperability of CAdES extended signatures ETSI TS 119 124-3 [5], clause 7.4.	All the CAdES/TN/* test cases in ASiC-S/CAdES-E-TN shall be passed according to the criteria specified in [5], clause 7.4.
ASiC-S/CAdES-E-AN	This group of test cases tests a set of ASiC-S container including each a signature created according to all the CAdES/AN/* test cases defined in the Test suites for testing interoperability of CAdES extended signatures ETSI TS 119 124-3 [5], clause 7.5.	All the CAdES/AN/* test cases in ASiC-S/CAdES-E-AN shall be passed according to the criteria specified in [5], clause 7.5.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 119 164-3 V1.1.1 (2016-06)
https://standards.iteh.ai/catalog/standards/sist/e219...

5.4 Test cases for ASiC-S containers with extended XAdES signature

5.4.1 Positive test cases

The test cases for ASiC-S containers with advanced XAdES signature shall be as specified in Table 4. The test cases specified in clause 5.2 and the presence of signatures.xml file ASiC [1], clause 4.3.3.2 item 3c) are a prerequisite.

A test suite for augmentation of extended XAdES signatures in an ASiC-S container can be defined by applying the augmentation test suites defined in ETSI TS 119 134-3 [6] as follows:

- a test suite for ASiC-S containers including a XAdES-E-BES or XAdES-E-T signature to be augmented to XAdES-E-C signature shall conform to ETSI TS 119 134-3 [6], clause 6.2;