



**Electronic Signatures and Infrastructures (ESI);
Associated Signature Containers (ASiC) -
Testing Conformance and Interoperability;
Part 2: Test suites for testing interoperability
of ASiC baseline containers**

PREVIEW
https://standards.itec.ai/en/standards/etv/00393185-08bd-44b3-b6c0-ef432016-0164-2-v2.1.1-08bd-44b3-b6c0-ef432016-0164-2-v2.1.1-

ReferenceRTS/ESI-0019164-2

KeywordsASiC, e-commerce, electronic signature,
interoperability, security, testing

ETSI650 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 |
| 1 Scope | 5 |
| 2 References | 5 |
| 2.1 Normative references | 5 |
| 2.2 Informative references..... | 6 |
| 3 Definitions and abbreviations..... | 6 |
| 3.1 Definitions..... | 6 |
| 3.2 Abbreviations | 6 |
| 4 ASiC baseline container interoperability test specification overview..... | 6 |
| 5 Test suite for testing interoperability of ASiC-S baseline containers | 7 |
| 5.1 Introduction to testing ASiC-S baseline containers..... | 7 |
| 5.2 Test cases common to all ASiC-S forms and levels..... | 7 |
| 5.3 Test cases for ASiC-S baseline containers with CADES signatures | 8 |
| 5.3.1 Positive test cases | 8 |
| 5.3.2 Negative test cases for ASiC-S baseline containers with CADES signatures | 8 |
| 5.4 Test cases for ASiC-S baseline containers with XAdES signatures..... | 9 |
| 5.4.1 Positive test cases | 9 |
| 5.4.2 Negative test cases for ASiC-S baseline containers with XAdES signatures | 9 |
| 6 Test suite for testing interoperability of ASiC-E baseline containers | 10 |
| 6.1 Introduction to testing ASiC-E baseline containers..... | 10 |
| 6.2 Test cases common to all ASiC-E forms and levels..... | 10 |
| 6.3 Test cases for ASiC-E baseline containers with XAdES signatures..... | 11 |
| 6.3.1 Positive test cases | 11 |
| 6.3.2 Negative test cases for ASiC-E baseline containers with XAdES signatures..... | 12 |
| 7 Test-suite for augmentation of ASiC baseline containers | 12 |
| Annex A (informative): Bibliography..... | 13 |
| History | 14 |

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 2 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.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 a number of test suites to assess the interoperability between implementations claiming conformance to ASiC baseline containers as specified in ETSI EN 319 162-1 [1].

The test suites are defined with four different layers reflecting the four different levels of ASiC baseline containers.

- Tests suite addressing interoperability between applications claiming B-B level conformance.
- Tests suite addressing interoperability between applications claiming B-T level conformance.
- Tests suite addressing interoperability between applications claiming B-LT level conformance.
- Tests suite addressing interoperability between applications claiming B-LTA level conformance.
- Test suites also cover augmentation of ASiC baseline containers and negative test cases.

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 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAAdES digital signatures; Part 1: Building blocks and CAAdES baseline signatures".
- [3] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".
- [4] ETSI TS 119 124-2: "Electronic Signatures and Infrastructures (ESI); CAAdES digital signatures - Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of CAAdES baseline signatures".
- [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".
- [6] ISO/IEC 21320-1: "Information technology -- Document Container File -- Part 1: Core".

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 TR 119 164-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC) - Testing Conformance and Interoperability; Part 1: Overview".
- [i.3] 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.4] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAAdES digital signatures; Part 1: Building blocks and CAAdES baseline signatures".
- [i.5] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

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 CAAdES baseline signatures [i.4] or XAdES baseline signatures [i.5], or for a signature whose validation according to ETSI EN 319 102-1 [i.3] 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:

| | |
|-----|----------------------------------|
| BCS | Baseline Container Structure |
| BSC | Baseline Syntactical Conformance |
| STV | Signature Time-stamp token Value |
| TC | Test Case |

4 ASiC baseline container interoperability test specification overview

This clause describes the overall approach used to specify test suites for ASiC baseline containers interoperability testing.

ETSI EN 319 162-1 [1] defines different forms and, for each, four levels of ASiC baseline containers.

The test suites are defined with different forms and layers reflecting the ASiC baseline containers specified in [1] and, for the signature test suites, reference to the appropriate CAdES test suites ETSI TS 119 124-2 [4] and XAdES test suites ETSI TS 119 134-2 [5] is made:

- Testing ASiC-S and ASiC-E containers interoperability between applications claiming B-B level conformance.
- Testing ASiC-S and ASiC-E containers interoperability between applications claiming B-T level conformance.
- Testing ASiC-S and ASiC-E containers interoperability between applications claiming B-LT level conformance.
- Testing ASiC-S and ASiC-E containers interoperability between applications claiming B-LTA level conformance.
- Testing augmentation of ASiC containers from B-T level to B-LTA level.
- Negative test cases for ASiC-S and ASiC-E baseline containers:
 - ASiC B-B level containers test cases.
 - ASiC B-T level containers test cases.
 - ASiC B-LTA level containers test cases.

5 Test suite for testing interoperability of ASiC-S baseline containers

5.1 Introduction to testing ASiC-S baseline containers

In clause 5 all the ASiC-S test cases necessary for testing conformance to each baseline level are specified.

In clause 5.2 the test cases common to all ASiC-S forms and levels are specified. In clauses 5.3 and 5.4 the test cases for each level are specified.

5.2 Test cases common to all ASiC-S forms and levels

The test cases common to all ASiC-S baseline containers 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/BCS/1 | This test case tests if the container ZIP format is correct. | The container content shall comply with ISO/IEC 21320-1 [6] and be successfully extracted. | Baseline Container Structure |
| ASiC-S/BCS/2 | Verify if the container format is identifiable. | The container extension shall be ".asics". | Baseline Container Structure |
| ASiC-S/BCS/3 | mimetype is set appropriately. Prerequisites: <ul style="list-style-type: none"> • 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, point 2) b) and A.1. | Baseline Container Structure |
| ASiC-S/BCS/4 | This test case tests that a signature is present in the container. | A META-INF folder in the root folder shall be present and contain one signature.p7s file (ASiC [1], clause 4.3.3.2 item 3b) or signatures.xml file (ASiC [1], clause 4.3.3.2, item 3c). | Baseline Container Structure |
| ASiC-S/BCS/5 | Presence of the signed file. | A single file, in addition to the optional mimetype, shall be present in the root folder. | Baseline Container Structure |

5.3 Test cases for ASiC-S baseline containers with CAdES 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 5.1 and the presence of signature.p7s file ASiC [1], clause 4.3.3.2 item 3b) are a prerequisite.

Table 2: Test cases for all ASiC-S baseline container levels with CAdES signatures

| TC ID | Description | Pass criteria |
|--------------|--|---|
| ASiC-S/CBB | This group of test cases tests a set of ASiC-S container including each a signature created according to all the CAdES/BB/* test cases defined in the Test suites for testing interoperability of CAdES baseline signatures ETSI TS 119 124-2 [4], clause 5. | All the CAdES/BB/* test cases in ASiC-S/CBB shall be passed according to the criteria specified in ETSI TS 119 124-2 [4], clause 5. |
| ASiC-S/CBT | This group of test cases tests a set of ASiC-S container including each a signature created according to all the CAdES/BT/* test cases defined in the Test suites for testing interoperability of CAdES baseline signatures ETSI TS 119 124-2 [4], clause 6. | All the CAdES/BT/* test cases in ASiC-S/CBT shall be passed according to the criteria specified in ETSI TS 119 124-2 [4], clause 6. |
| ASiC-S/CBLT | This group of test cases tests a set of ASiC-S container including each a signature created according to all the CAdES/BLT/* test cases defined in the Test suites for testing interoperability of CAdES baseline signatures ETSI TS 119 124-2 [4], clause 7. | All the CAdES/BLT/* test cases in ASiC-S/CBLT shall be passed according to the criteria specified in ETSI TS 119 124-2 [4], clause 7. |
| ASiC-S/CBLTA | This group of test cases tests a set of ASiC-S container including each a signature created according to all the CAdES/BLTA/* test cases defined in the Test suites for testing interoperability of CAdES baseline signatures ETSI TS 119 124-2 [4], clause 8. | All the CAdES/BLTA/* test cases in ASiC-S/CBLTA shall be passed according to the criteria specified in ETSI TS 119 124-2 [4], clause 8. |

5.3.2 Negative test cases for ASiC-S baseline containers with CAdES signatures

The test cases in this clause are specified in table 3 and have been defined according to ETSI TS 119 124-2 [4], clause 10.

Table 3: Negative test cases for all ASiC-S baseline container levels with CAdES signatures

| TC ID | Description | Pass criteria |
|---------------|---|--|
| ASiC-S/CBBN | This group of negative test cases tests a set of ASiC-S container including each a signature created according to all the CAdES/BBN/* test cases defined in the Test suites for testing interoperability of CAdES baseline signatures ETSI TS 119 124-2 [4], clause 10.2. | All the CAdES/BBN/* test cases in ASiC-S/CBBN shall be passed according to the criteria specified in ETSI TS 119 124-2 [4], clause 10.2. |
| ASiC-S/CBTN | This group of test cases tests a set of ASiC-S container including each a signature created according to all the CAdES/BTN/* test cases defined in the Test suites for testing interoperability of CAdES baseline signatures ETSI TS 119 124-2 [4], clause 10.3. | All the CAdES/BTN/* test cases in ASiC-S/CBTN shall be passed according to the criteria specified in ETSI TS 119 124-2 [4], clause 10.3. |
| ASiC-S/CBLTAN | This group of test cases tests a set of ASiC-S container including each a signature created according to all the CAdES/BLTAN/* test cases defined in the Test suites for testing interoperability of CAdES baseline signatures ETSI TS 119 124-2 [4], clause 10.4. | All the CAdES/BLTAN/* test cases in ASiC-S/CBLTAN shall be passed according to the criteria specified in ETSI TS 119 124-2 [4], clause 10.4. |

5.4 Test cases for ASiC-S baseline containers with XAdES signatures

5.4.1 Positive test cases

The test cases for ASiC-S with XAdES containers 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.

Table 4: Test cases for all ASiC-S baseline container levels with XAdES signatures

| TC ID | Description | Pass criteria |
|--------------|---|---|
| ASiC-S/XBB | This group of test cases tests a set of ASiC-S container including each a signature created according to all the XAdES/BB/* test cases defined in the Test suites for testing interoperability of XAdES baseline signatures ETSI TS 119 134-2 [5], clause 5 signing one data object. Test cases where more than one data object is signed shall not be included. | All the XAdES/BB/* test cases in ASiC-S/XBB shall be passed according to the criteria specified in ETSI TS 119 134-2 [5], clause 5. |
| ASiC-S/XBT | This group of test cases tests a set of ASiC-S container including each a signature created according to all the XAdES/BT/* test cases defined in the Test suites for testing interoperability of XAdES baseline signatures ETSI TS 119 134-2 [5], clause 6 signing one data object. Test cases where more than one data object is signed shall not be included. | All the XAdES/BT/* test cases in ASiC-S/XBT shall be passed according to the criteria specified in ETSI TS 119 134-2 [5], clause 6. |
| ASiC-S/XBLT | This group of test cases tests a set of ASiC-S container including each a signature created according to all the XAdES/BLT/* test cases defined in the Test suites for testing interoperability of XAdES baseline signatures ETSI TS 119 134-2 [5], clause 7 signing one data object. Test cases where more than one data object is signed shall not be included. | All the XAdES/BLT/* test cases in ASiC-S/XBLT shall be passed according to the criteria specified in ETSI TS 119 134-2 [5], clause 7. |
| ASiC-S/XBLTA | This group of test cases tests a set of ASiC-S container including each a signature created according to all the XAdES/BLTA/* test cases defined in the Test suites for testing interoperability of XAdES baseline signatures ETSI TS 119 134-2 [5], clause 8 signing one data object. Test cases where more than one data object is signed shall not be included. | All the XAdES/BLTA/* test cases in ASiC-S/XBLTA shall be passed according to the criteria specified in ETSI TS 119 134-2 [5], clause 8. |

5.4.2 Negative test cases for ASiC-S baseline containers with XAdES signatures

The test cases in this clause are specified in table 5 and have been defined according to ETSI TS 119 134-2 [5], clause 11.