ETSI TS 119 164-4 V1.1.1 (2016-06)

Electronic Signatures and Infrastructures (ESI);
Associated Signature Containers (ASiC) -
Testing Compliance and Interoperability;
Part 4: Testing Conformance of ASiC baseline containers

Reference
DTS/ESI-0019164-4

Keywords
ASiC, conformance, e-commerce, electronic signature, 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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

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

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

Foreword

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

The present document is part 4 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].

A tool implementing the present document has been developed and is accessible at http://signatures-conformance-checker.etsi.org/

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 set of checks to be performed for testing conformance of ASiC containers against ASiC baseline containers as specified in ETSI EN 319 162-1 [1].

The present document does not specify checks leading to conclude whether a container is technically valid or not (for instance, it does not specify checks for determining whether the cryptographic material present in signatures inside the container may be considered valid or not). In consequence, no conclusion may be inferred regarding the technical validity of a container that has been successfully tested by any tool conformant to the present document.

Checks are exclusively constrained to elements specified by ASiC [1].

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

[2] ETSI TS 119 124-4: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing conformance of CAdES baseline signatures".

[3] 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".

[4] 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] OASIS "Test Assertions Guidelines Version 1.0", 19 June 2013. OASIS Committee Note 02.

NOTE: Available at: http://docs.oasis-open.org/tag/guidelines/v1.0/cn02/guidelines-v1.0-cn02.html

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

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.3] and in the Test Assertions Guidelines [i.1] apply. In case of contrast the former prevails.

3.2 Abbreviations

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

CS Container Structure
PKI Public Key Infrastructure
SC Syntactical Conformance
STV Signature Time-stamp token Value
TA Test Assertion

NOTE: Refer to [i.1].

TAL Test Assertion List

NOTE: Refer to [i.1].

TC Test Case
URI Uniform Resource Identifier

4 ASiC baseline container conformity test specification overview

The present clause describes the main aspects of the technical approach used for specifying the whole set of checks to be performed for testing conformance to ASiC baseline containers [1].

ASiC [1] defines different containers forms grouped in Simple (ASiC-S) and Extended (ASiC-E).

In order to test conformity against ASiC [1], for each ASiC form, tests are specified as belonging to one of three layers:

- The first layer is based on test assertions on the conformance of the container structure: the presence of certain files in the container with specific names. Entities testing conformance can obtain specific information to identify potential container conformance problems.
- The second layer is based on test assertions on the syntactical conformance and/or properties of files relevant to ASiC form under test: specific information to identify potential conformance issues related to ASiC file syntax or properties can be obtained.
- The third layer is based on assertions on conformance of the CAdES or XAdES signatures contained in the specific ASiC form under test: specific information to identify potential conformance issues caused by lack of conformance in signatures contained in ASiC containers can be obtained.

All layer tests shall be performed to complete testing.

No tests are included testing the technical validity of the cryptographic material that might be present in the signature or to be used for its verification (status of certificates for instance).

The test definitions are based on test assertions work produced by OASIS in "Test Assertions Guidelines Version 1.0" [i.1].

Each test assertion includes the following information:

1) Unique identifier for further referencing.

2) Reference to the **Normative source** for the test.

3) The **Target** of the assertion.

4) The **Prerequisite** specifies the conditions under which the TA is applicable/can be performed

5) **Predicate** fully and unambiguously defining the assertion to be tested.

6) **Prescription level:** Three levels are defined: mandatory, recommended and optional, whose semantics is to be interpreted as described in clause 3.1.2 of [i.1].

7) **Tag:** information on the element tested by the assertion.

5 Testing conformance to ASiC-S baseline containers

5.1 Testing ASiC-S baseline containers

5.1.1 Test assertions for ASiC-S baseline container structure

All the test assertions related to the first conformance layer, the container structure, are grouped in a Test Assertion List defined as follows:

TA List id: TAL/ASiC-S/CS
List Description: all TAs describing container structure requirements for ASiC-S containers to the following Clauses in ASiC [1]: 5.3.1, 5.3.2.1, 5.3.2.2, 5.3.2.3
List Members: TA/ASiC-S/CS/1 ... 5

The Test Assertions that belong to this Test Assertion List are specified as follows:

TA id: TA/ASiC-S/CS/1
Normative Source: ASiC [1] – Clause 5.3.1
Target: ASiC generator claiming conformance to ASiC-S baseline containers [1]
Predicate: The container shall be compliant with ISO/IEC 21320-1 [6]
Prescription Level: mandatory
Tag: conformance layer = 1 (container structure); Container type=Simple (ASiC-S)

TA id: TA/ASiC-S/CS/2
Normative Source: ASiC [1] – Clause 5.3.2.1 Table 2 row 1
Target: ASiC generator claiming conformance to ASiC-S baseline containers [1]
Predicate: ASiC File extension is ".asics".
Prescription Level: mandatory
Tag: conformance layer = 1 (container structure); Container type=Simple (ASiC-S)

TA id: TA/ASiC-S/CS/3
Normative Source: ASiC [1] – Clause 5.3.2.1 Table 2 row 2
Target: ASiC generator claiming conformance to ASiC-S baseline containers [1]
Predicate: mimetype is encoded as specified in ASiC [1] Clauses 4.3.3.1, point 2) b) and A.1
Prescription Level: optional
Tag: conformance layer = 1 (container structure); Container type=Simple (ASiC-S)

TA id: TA/ASiC-S/CS/4
Normative Source: ASiC [1] – Clause 4.3.3.2 item 3 and either 4b or 4c
Target: ASiC generator claiming conformance to ASiC-S baseline containers [1]
Predicate: META-INF folder is present and contains one file named signature.p7s or signatures.xml.
Prescription Level: mandatory
Tag: conformance layer = 1 (container structure); Container type=Simple (ASiC-S)

TA id: TA/ASiC-S/CS/5
Normative Source: ASiC [1] – Clause 5.3.2.1 Table 2 row 3
Target: ASiC generator claiming conformance to ASiC-S baseline containers [1]
Predicate: a single data object, in addition to the optional mimetype, is present in the root folder.
Prescription Level: mandatory
Tag: conformance layer = 1 (container structure); Container type=Simple (ASiC-S)

5.1.2 Test assertions for ASiC-S baseline container syntactical conformance

All the test assertions related to the second conformance layer, the syntactical conformance, are grouped in a Test Assertion List defined as follows:

TA List id: TAL/ASiC-S/SC
List Description: all TAs describing container structure requirements for ASiC-S containers to the following Clauses in ASiC [1]: 5.3.1, 5.3.2.1, 5.3.2.2, 5.3.2.3
List Members: TA/ASiC-S/SC/1 ... 4

The Test Assertions that belong to this Test Assertion List are specified as follows:

TA id: TA/ASiC-S/SC/1
Normative Source: ASiC [1] – Clause 5.3.2.2 Table 3
Target: ASiC generator claiming conformance to ASiC-S with CAdES [1]
Prerequisite: the expected input is ASiC-S with CAdES.
Predicate: signature.p7s is present and contains a CAdES baseline signature whose conformance shall be tested according to Conformance Testing for CAdES baseline signatures specification [4], clause 5.2.
Prescription Level: mandatory
Tag: assertion layer = 2 (syntactical conformance); Container type=Simple (ASiC-S)

TA id: TA/ASiC-S/SC/2
Normative Source: ASiC [1] – Clause 5.3.2.3 Table 4
Target: ASiC generator claiming conformance to ASiC-S with XAdES [1]
Prerequisite: the expected input is ASiC-S XAdES.
Predicate: signatures.xml is present and contains asic:XAdESSignatures
Prescription Level: mandatory
Tag: assertion layer = 2 (syntactical conformance); Container type=Simple (ASiC-S)

TA id: TA/ASiC-S/SC/3
Normative Source: ASiC [1] – Clause 5.3.2.3 Table 4
Target: ASiC generator claiming conformance to ASiC-S with XAdES [1]
Prerequisite: TA/ASiC-S/SC/2 passed.
Predicate: signatures.xml contains a XAdES baseline signature whose conformance shall be tested according to Conformance Testing for XAdES core specification [5] clauses 5.2 and 5.3
Prescription Level: mandatory
Tag: assertion layer = 2 (syntactical conformance); Container type=Simple (ASiC-S)

TA id: TA/ASiC-S/SC/4
Normative Source: ASiC [1] – Clause 5.3.2.3 Table 4
Target: ASiC generator claiming conformance to ASiC-S with XAdES [1]
Prerequisite: TA/ASiC-S/SC/3 passed.
Predicate: Each XAdES signature child of the asic:XAdESSignatures element shall reference explicitly the signed file object using a ds:Reference child of the ds:SignedInfo element
Prescription Level: mandatory
Tag: assertion layer = 2 (syntactical conformance); Container type=Simple (ASiC-S)

5.1.3 Test assertions for ASiC-S signature conformance

All the test assertions related to the third conformance layer, the signature/time-stamp token conformance, are grouped in a Test Assertion List defined as follows:

TA List id: TAL/ASiC-S/STV
List Description: all TAs describing signature conformance requirements for ASiC-S to the following clauses in ASiC [1]: 5.3.1, 5.3.2.1, 5.3.2.2, 5.3.2.3
List Members: TA/ASiC-S/STV/1 ...

The Test Assertions that belong to this Test Assertion List are specified as follows:

TA id: TA/ASiC-S/STV/1
Normative Source: ASiC [1] – Clause 5.3.2.2 Table 3
Target: ASiC generator claiming conformance to ASiC-S with CAdES baseline container
Prerequisite: TAL/ASiC-S/CS and TA/ASiC-S/SC/1
Predicate: the signatures in signature.p7s apply to the data object in TA/ASiC-S/CS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (signature conformance); Container type=Simple (ASiC-S)

TA id: TA/ASiC-S/STV/2
Normative Source: ASiC [1] – Clause 5.3.2.3 Table 4
Target: ASiC generator claiming conformance to ASiC-S with XAdES baseline container
Prerequisite: TAL/ASiC-S/CS, TA/ASiC-S/SC/2, TA/ASiC-S/SC/3 and TA/ASiC-S/SC/4
Predicate: XAdES signatures in signatures.xml apply to the data object in TA/ASiC-S/CS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (signature conformance); Container type=Simple (ASiC-S)

TA id: TA/ASiC-S/STV/3
Normative Source: ASiC [1] – Clause 5.1 item a
Target: ASiC generator claiming conformance to ASiC-S B-B level with CAdES
Prerequisite: TA/ASiC-S/STV/1
Predicate: the signatures in signature.p7s are CAdES-B-B signatures whose conformance shall be tested according to Conformance Testing for CAdES baseline signatures specification [4] clause 5.
Prescription Level: mandatory
Tag: assertion layer = 3 (signature conformance); Container type=Simple (ASiC-S)

TA id: TA/ASiC-S/STV/4
Normative Source: ASiC [1] – Clause 5.1 item a
Target: ASiC generator claiming conformance to ASiC-S B-B level with XAdES
Prerequisite: TA/ASiC-S/STV/2
Predicate: the signatures in signatures.xml are XAdES-B-B signatures whose conformance shall be tested according to Conformance Testing for XAdES baseline signatures specification [5] clause 5.
Prescription Level: mandatory
Tag: assertion layer = 3 (signature conformance); Container type=Simple (ASiC-S)

TA id: TA/ASiC-S/STV/5
Normative Source: ASiC [1] – Clause 5.1 item b
Target: ASiC generator claiming conformance to ASiC-S B-T level with CAdES
Prerequisite: TA/ASiC-S/STV/1
Predicate: the signatures in signature.p7s are CAdES-B-T signatures whose conformance shall be tested according to Conformance Testing for CAdES baseline signatures specification [4] clause 6.
Prescription Level: mandatory
Tag: assertion layer = 3 (signature conformance); Container type=Simple (ASiC-S)

TA id: TA/ASiC-S/STV/6
Normative Source: ASiC [1] – Clause 5.1 item b
Target: ASiC generator claiming conformance to ASiC-S B-T level with XAdES
Prerequisite: TA/ASiC-S/STV/2
Predicate: the signatures in signatures.xml are XAdES-B-T signatures whose conformance shall be tested according to Conformance Testing for XAdES baseline signatures specification [5] clause 6.
Prescription Level: mandatory
Tag: assertion layer = 3 (signature conformance); Container type=Simple (ASiC-S)

TA id: TA/ASiC-S/STV/7
Normative Source: ASiC [1] – Clause 5.1 item c
Target: ASiC generator claiming conformance to ASiC-S B-LT level with CAdES
Prerequisite: TA/ASiC-S/STV/1
Predicate: the signatures in signature.p7s are CAdES-B-LT signatures whose conformance shall be tested according to Conformance Testing for CAdES baseline signatures specification [4] clause 7.
Prescription Level: mandatory
Tag: assertion layer = 3 (signature conformance); Container type=Simple (ASiC-S)

TA id: TA/ASiC-S/STV/8
Normative Source: ASiC [1] – Clause 5.1 item c
Target: ASiC generator claiming conformance to ASiC-S B-LT level with XAdES
Prerequisite: TA/ASiC-S/STV/2
Predicate: the signatures in signatures.xml are XAdES-B-LT signatures whose conformance shall be tested according to Conformance Testing for XAdES baseline signatures specification [5] clause 7.
Prescription Level: mandatory
Tag: assertion layer = 3 (signature conformance); Container type=Simple (ASiC-S)