ETSI TS 119 164-5 V1.1.1 (2016-06)

TECHNICAL SPECIFICATION

Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC) - Testing Compliance and Interoperability; Part 5: Testing Conformance of additional ASiC containers

Reference

DTS/ESI-0019164-5

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 5 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 sets of checks required for testing conformance of ASiC containers against:

- ASiC containers conforming to building blocks defined in ETSI EN 319 162-1 [1] and containing extended CAdES [i.5] and extended XAdES [i.6] digital dignatures, expanding the scope of ASiC baseline containers also defined in ETSI EN 319 162-1 [1]; and
- additional containers defined in ETSI EN 319 162-2 [2]. The set of checks that are common with ASiC baseline containers, are defined in ETSI TS 119 164-4 [5] and referenced when needed.

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] ETSI TS 119 124-5: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 5: Testing conformance of extended CAdES signatures".

[4] ETSI TS 119 134-5: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Compliance & Interoperability; Part 5: Conformance Testing for XAdES Baseline Profile".

[5] ETSI TS 119 164-4: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC) - Testing Compliance and Interoperability; Part 4: Testing conformance of ASiC baseline containers".

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".

[i.4] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[i.5] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

[i.6] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[i.7] IETF RFC 5816: "ESSCertIDv2 Update for RFC 3161".

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

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

[i.10] OASIS: "Open Document Format for Office Applications (OpenDocument) Version 1.2; Part 3: Packages" 29 September 2011.

[i.11] ISO/IEC TS 30135 (all parts): "Information technology -- Digital publishing -- EPUB3".

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:

ACS	Additional Container Structure
PKI	Public Key Infrastructure
ACSC	Additional Container Syntactical Conformance
ACST	Additional Container Signature or Time-stamp token
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 additional container conformity test specification overview

The present document complements ETSI TS 119 164-4 [5] (conformance testing of ASiC baseline containers) by specifying tests to be performed for testing conformance 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 for testing conformance of these additional containers.

In particular **ASiC additional containers**, in scope of the present document, shall be:

1) ASiC additional containers obtained by expanding in scope ASiC baseline containers, in conformance to the ASiC building blocks specified in ETSI EN 319 162-1 [1] clause 4 and allowing use of extended CAdES signatures (ETSI EN 319 122-2 [i.4]) and extended CAdES signatures (ETSI EN 319 132-2 [i.5]); or

2) ASiC additional containers specified in ETSI EN 319 162-2 [2].

The conformance test are defined:

- extending ETSI TS 119 164-4 [5] with conformance tests defined for extended CAdES digital signatures in ETSI TS 119 124-5 [3] and conformance tests defined for extended XAdES digital signatures defined in ETSI TS 119 134-5 [4]; and

- defining conformance tests considering the additional container types specified in ETSI EN 319 162-2 [2].

The conformance 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 permitted, 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 Simple Associated Signature Containers (ASiC-S)

5.1 Test Assertions for ASiC-S

5.1.1 ASiC-S test assertions for Additional Container Structure

All the test assertions related to the first conformance layer, the Additional Container Structure (ACS), are grouped in a Test Assertion List defined as follows:

```
TA List id: TAL/ASiC-S/ACS
List Description: all TAs describing ACS requirements for ASiC-S additional containers
List Members: TA/ASiC-S/ACS/1 ... 6
```

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

TA id: TA/ASiC-S/ACS/1
Normative Source: ASiC ETSI EN 319 162-1 [1] clause 4.2 item 1 and 2
Target: ASiC generator claiming conformance to ASiC-S additional container
Predicate: The ZIP format, with the limitations specified in the Normative Source referred above, shall be used to bind the contained objects into a single container
Prescription Level: mandatory
Tag: conformance layer = 1 (ACS); Container type = ASiC-S additional container

TA id: TA/ASiC-S/ACS/2
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.1 item 2
Target: ASiC generator claiming conformance to ASiC-S additional container
Predicate: ASiC File extension is “.asics” or “.scs” if the operating systems and/or file systems do not allow more than 3 characters file extensions or “.zip”.
Prescription Level: mandatory
Tag: conformance layer = 1 (ACS); Container type = ASiC-S additional container

TA id: TA/ASiC-S/ACS/3
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.1 item 3
Target: ASiC generator claiming conformance to ASiC-S additional container
Predicate: The comment field in the ZIP file header is set with “mimetype=” followed by the media type of the data held in the file.
Prescription Level: permitted
Tag: conformance layer = 1 (ACS); Container type = ASiC-S additional container

TA id: TA/ASiC-S/ACS/4
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.1 item 1 and clause A.1
Target: ASiC generator claiming conformance to ASiC-S additional container
Predicate: mimetype is encoded as specified in ETSI EN 319 162-1 [1] clause A.1 and is set according to clause 4.3.3.1 item 1.
Prescription Level: mandatory if file extension is “.zip”; else recommended
Tag: conformance layer = 1 (ACS); Container type = ASiC-S additional container

TA id: TA/ASiC-S/ACS/5
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.3.2 item 3 and 4
Target: ASiC generator claiming conformance to ASiC-S additional container
Predicate: META-INF folder is present and contains one file named timestamp.tst, signature.p7s, signatures.xml, "evidencerecord.ers" or "evidencerecord.xml".
Prescription Level: mandatory
Tag: conformance layer = 1 (ACS); Container type = ASiC-S additional container

TA id: ASiC-S/ACS/6
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.3.2 item 2
Target: ASiC generator claiming conformance to ASiC-S additional container
Predicate: a single file object, in addition to the optional mimetype, is present in the root folder.
Prescription Level: mandatory
Tag: conformance layer = 1 (ACS); Container type = ASiC-S additional container

5.1.2 ASiC-S test assertions for Additional Container Syntactical Conformance

All the test assertions related to the second conformance layer, the Additional Container Syntactical Conformance (ACSC), are grouped in a Test Assertion List defined as follows:

TA List id: TAL/ASiC-S/ACSC
List Description: all TAs describing ACSC requirements for ASiC-S containers - see clause 4.3 of ETSI EN 319 162-1 [1]
List Members: TA/ASiC-S/ACSC/1 ... 8

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

TA id: TA/ASiC-S/ACSC/1
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.2 item 4b and ETSI TS 119 124-5 [3] clause 5
Target: ASiC generator claiming conformance to ASiC-S with CAdES additional container
Prerequisite: TAL/ASiC-S/ACS conformance verified and the expected input is ASiC-S CAdES.
Predicate: signature.p7s is present and fulfils the requirements specified in clause 5 of ETSI TS 119 124-5 [3].
Prescription Level: mandatory
Tag: assertion layer = 2 (ACSC); Container type = ASiC-S with CAdES additional container

TA id: TA/ASiC-S/ACSC/2
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.2 item 4c and ETSI TS 119 134-5 [4] clause 5
Target: ASiC generator claiming conformance to ASiC-S with XAdES additional container
Prerequisite: TAL/ASiC-S/ACS conformance verified and the expected input is ASiC-S XAdES.
Predicate: signatures.xml is present, conformant to the schema specified in ETSI EN 319 162-1 [1] §A.5 and each ds:Signature element that is present fulfils the requirements specified in clause 5 of ETSI TS 119 134-5 [4]
Prescription Level: mandatory
Tag: assertion layer = 2 (ACSC); Container type = ASiC-S with XAdES additional container

TA id: TA/ASiC-S/ACSC/3
Normative Source: ETSI EN 319 162-2 [2] clause 4.2.1 items a) and c)
Target: ASiC generator claiming conformance to ASiC-S Time assertion additional container
Prerequisite: TAL/ASiC-S/ACS conformance verified the expected input is ASiC-S Time assertion with a time-stamp token
Predicate: timestamp.tst compliant with IETF RFC 3161 [i.6] as updated by IETF RFC 5816 [i.7]
Prescription Level: mandatory
Tag: assertion layer = 2 (ACSC); Container type = ASiC-S Time assertion additional container

TA id: TA/ASiC-S/ACSC/4
Normative Source: ETSI EN 319 162-2 [2] clause 4.2.1 item d) and ETSI EN 319 162-1 [1] clause A.7
Target: ASiC generator claiming conformance to ASiC-S Time assertion additional container
Prerequisite: TAL/ASiC-S/ACS and TA/ASiC-S/ACSC/3 conformance verified the expected input is ASiC-S Time assertion with a time-stamp token and long term attributes
Predicate: one or more ASiCArchiveManifest files are present and conforms to comply with ASiC part 1 [2], clause A.7
Prescription Level: mandatory
Tag: assertion layer = 2 (ACSC); Container type = ASiC-S Time assertion additional container

TA id: TA/ASiC-S/ACSC/5
Normative Source: ETSI EN 319 162-2 [2] clause 4.2.1 item d)
Target: ASiC generator claiming conformance to ASiC-S Time assertion additional container
Prerequisite: TA/ASiC-S/ACSC/4 conformance verified the expected input is ASiC-S Time assertion with a time-stamp token and long term attributes
Predicate: one *timestamp*.tst for each ASiCArchiveManifest file is present whose actual file name matches the value of the URI attribute of the SigReference element.
Prescription Level: mandatory
Tag: assertion layer = 2 (ACSC); Container type = ASiC-S Time assertion additional container

TA id: TA/ASiC-S/ACSC/6
Normative Source: ETSI EN 319 162-2 [2] clause 4.2.1 item d)
Target: ASiC generator claiming conformance to ASiC-S Time assertion additional container
Prerequisite: TA/ASiC-S/ACSC/5 conformance verified the expected input is ASiC-S Time assertion with a time-stamp token and long term attributes
Predicate: each *timestamp*.tst is compliant with IETF RFC 3161 [i.6] as updated by IETF RFC 5816 [i.7]
Prescription Level: mandatory
Tag: assertion layer = 2 (ACSC); Container type = ASiC-S Time assertion additional container

TA id: TA/ASiC-S/ACSC/7
Normative Source: ETSI EN 319 162-2 [2] clause 4.2.1 items a) and c)
Target: ASiC generator claiming conformance to ASiC-S Time assertion additional container
Prerequisite: TAL/ASiC-S/ACS conformance verified the expected input is ASiC-S time assertion with evidencerecord.ers present
Predicate: evidencerecord.ers compliant with IETF RFC 4998 [i.8]
Prescription Level: mandatory
Tag: assertion layer = 2 (ACSC); Container type = ASiC-S Time assertion additional container

TA id: TA/ASiC-S/ACSC/8
Normative Source: ETSI EN 319 162-2 [2] clause 4.2.1 items a) and c)
Target: ASiC generator claiming conformance to ASiC-S Time assertion additional container
Prerequisite: TAL/ASiC-S/ACS conformance verified the expected input is ASiC-S time assertion with evidencerecord.xml present
Predicate: evidencerecord.xml compliant with IETF RFC 6283 [i.9]
Prescription Level: mandatory
Tag: assertion layer = 2 (ACSC); Container type = ASiC-S Time assertion additional container

5.1.3 Test assertions for ASiC-S ACST conformance

All the test assertions related to the third conformance layer, the Additional Container Signature or Timestamp token (ACST) conformance, are grouped in a Test Assertion List defined as follows:

TA List id: TAL/ASiC-S/ACST
List Description: all TAs describing ACST conformance requirements for ASiC-S additional containers
List Members: TA/ASiC-S/ACST/1 ... 16

The Test Assertions that belong to this Test Assertion List are specified as follows:
TA id: TA/ASiC-S/ACST/1
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.2 item 4b and ETSI TS 119 124-5 [3] clause 5
Target: ASiC generator claiming conformance to ASiC-S with CAdES additional container
Prerequisite: TA/ASiC-S/ACSC/1 conformance verified
Predicate: signature.p7s is conformant to CAdES-E-BES and the signature is cryptographically correct against the content of the file object found in TA/ASiC-S/ACS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-S with CAdES additional container

The Test Assertions that belong to this Test Assertion List are specified as follows:
TA id: TA/ASiC-S/ACST/2
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.2 item 4b and ETSI TS 119 124-5 [3] clause 6
Target: ASiC generator claiming conformance to ASiC-S with CAdES additional container
Prerequisite: TA/ASiC-S/ACSC/1 conformance verified
Predicate: signature.p7s is conformant to CAdES-E-EPES and the signature is cryptographically correct against the content of the file object found in TA/ASiC-S/ACS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-S with CAdES additional container

The Test Assertions that belong to this Test Assertion List are specified as follows:
TA id: TA/ASiC-S/ACST/3
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.2 item 4b and ETSI TS 119 124-5 [3] clause 7
Target: ASiC generator claiming conformance to ASiC-S with CAdES additional container
Prerequisite: TA/ASiC-S/ACSC/1 conformance verified
Predicate: signature.p7s is conformant to CAdES-E-T and the signature is cryptographically correct against the content of the file object found in TA/ASiC-S/ACS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-S with CAdES additional container

The Test Assertions that belong to this Test Assertion List are specified as follows:
TA id: TA/ASiC-S/ACST/4
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.2 item 4b and ETSI TS 119 124-5 [3] clause 8
Target: ASiC generator claiming conformance to ASiC-S with CAdES additional container
Prerequisite: TA/ASiC-S/ACSC/1 conformance verified
Predicate: signature.p7s is conformant to CAdES-E-A and the signature is cryptographically correct against the content of the file object found in TA/ASiC-S/ACS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-S with CAdES additional container

TA id: TA/ASiC-S/ACST/5
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.2 item 4c and ETSI TS 119 134-5 [4] clause 5
Target: ASiC generator claiming conformance to ASiC-S with XAdES additional container
Prerequisite: TA/ASiC-S/ACSC/2 conformance verified
Predicate: signatures.xml is conformant to XAdES-E-BES and the signature is cryptographically correct against the content of the file object found in TA/ASiC-S/ACS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-S with XAdES additional container

TA id: TA/ASiC-S/ACST/6
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.2 item 4c and ETSI TS 119 134-5 [4] clause 6
Target: ASiC generator claiming conformance to ASiC-S with XAdES additional container
Prerequisite: TA/ASiC-S/ACSC/2 conformance verified
Predicate: signatures.xml is conformant to XAdES-E-EPES and the signature is cryptographically correct against the content of the file object found in TA/ASiC-S/ACS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-S with XAdES additional container

TA id: TA/ASiC-S/ACST/7
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.2 item 4c and ETSI TS 119 134-5 [4] clause 7
Target: ASiC generator claiming conformance to ASiC-S with XAdES additional container
Prerequisite: TA/ASiC-S/ACSC/2 conformance verified
Predicate: signatures.xml is conformant to XAdES-E-T and the signature is cryptographically correct against the content of the file object found in TA/ASiC-S/ACS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-S with XAdES additional container

TA id: TA/ASiC-S/ACST/8
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.2 item 4c and ETSI TS 119 134-5 [4] clause 8
Target: ASiC generator claiming conformance to ASiC-S with XAdES additional container
Prerequisite: TA/ASiC-S/ACSC/2 conformance verified
Predicate: signatures.xml is conformant to XAdES-E-C and the signature is cryptographically correct against the content of the file object found in TA/ASiC-S/ACS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-S with XAdES additional container

TA id: TA/ASiC-S/ACST/9
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.2 item 4c and ETSI TS 119 134-5 [4] clause 9
Target: ASiC generator claiming conformance to ASiC-S with XAdES additional container
Prerequisite: TA/ASiC-S/ACSC/2 conformance verified
Predicate: signatures.xml is conformant to XAdES-E-X and the signature is cryptographically correct against the content of the file object found in TA/ASiC-S/ACS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-S with XAdES additional container

TA id: TA/ASiC-S/ACST/10
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.2 item 4c and ETSI TS 119 134-5 [4] clause 10
Target: ASiC generator claiming conformance to ASiC-S with XAdES additional container
Prerequisite: TA/ASiC-S/ACSC/2 conformance verified
Predicate: signatures.xml is conformant to XAdES-E-X-L and the signature is cryptographically correct against the content of the file object found in TA/ASiC-S/ACS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-S with XAdES additional container

TA id: TA/ASiC-S/ACST/11
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.2 item 4c and ETSI TS 119 134-5 [4] clause 11
Target: ASiC generator claiming conformance to ASiC-S with XAdES additional container
Prerequisite: TA/ASiC-S/ACSC/2 conformance verified
Predicate: signatures.xml is conformant to XAdES-E-X-Long and the signature is cryptographically correct against the content of the file object found in TA/ASiC-S/ACS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-S with XAdES additional container

TA id: TA/ASiC-S/ACST/12
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.2 item 4c and ETSI TS 119 134-5 [4] clause 12
Target: ASiC generator claiming conformance to ASiC-S with XAdES additional container
Prerequisite: TA/ASiC-S/ACSC/2 conformance verified
Predicate: signatures.xml is conformant to XAdES-E-A and the signature is cryptographically correct against the content of the file object found in TA/ASiC-S/ACS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-S with XAdES additional container

TA id: TA/ASiC-S/ACST/13
Normative Source: ETSI EN 319 162-2 [2] clause 4.2.1 items a) and c)
Target: ASiC generator claiming conformance to ASiC-S with Time Assertion additional container
Prerequisite: TA/ASiC-S/ACSC/3 conformance verified
Predicate: timestamp.tst is cryptographically correct against the content of the file object found in TA/ASiC-S/ACS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-S with Time Assertion additional container

TA id: TA/ASiC-S/ACST/14
Normative Source: ETSI EN 319 162-2 [2] clause 4.2.1 items d)
Target: ASiC generator claiming conformance to ASiC-S with Time Assertion additional container
Prerequisite: TA/ASiC-S/ACSC/6 conformance verified
Predicate: each *timestamp*.tst is cryptographically correct against the content of the ASiCArchiveManifest file that reference it with the URI attribute of the SigReference element
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-S with Time Assertion additional container

TA id: TA/ASiC-S/ACST/15
Normative Source: ETSI EN 319 162-2 [2] clause 4.2.1 items a) and c)
Target: ASiC generator claiming conformance to ASiC-S with Time Assertion additional container
Prerequisite: TA/ASiC-S/ACSC/7 conformance verified
Predicate: evidencerecord.ers is cryptographically correct against the content of the file object found in TA/ASiC-S/ACS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-S with Time Assertion additional container

TA id: TA/ASiC-S/ACST/16
Normative Source: ETSI EN 319 162-2 [2] clause 4.2.1 items a) and c)
Target: ASiC generator claiming conformance to ASiC-S with Time Assertion additional container
Prerequisite: TA/ASiC-S/ACSC/8 conformance verified
Predicate: evidencerecord.ers is cryptographically correct against the content of the file object found in TA/ASiC-S/ACS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-S with Time Assertion additional container

6 Testing Extended Associated Signature Containers (ASiC-E)

6.1 Test Assertions for ASiC-E

6.1.1 ASiC-E test assertions for Additional Container Structure

All the test assertions related to the first conformance layer, the Additional Container Structure (ACS), are grouped in a Test Assertion List defined as follows:

TA List id: TAL/ASiC-E/ACS
List Description: all TAs describing ACS requirements for ASiC-E additional containers
List Members: TA/ASiC-E/ACS/1 ... 5

The Test Assertions for this conformance layer are specified as follows.

TA id: TA/ASiC-E/ACS/1
Normative Source: ASiC ETSI EN 319 162-1 [1] clause 4.2 item 1 and 2
Target: ASiC generator claiming conformance to ASiC-E additional container
Predicate: The ZIP format, with the limitations specified in the Normative Source referred above, shall be used to bind the contained objects into a single container
Prescription Level: mandatory
Tag: conformance layer = 1 (ACS); Container type = ASiC-E additional container

TA id: TA/ASiC-E/ACS/2
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.3.1 item 1
Target: ASiC generator claiming conformance to ASiC-E additional container
Predicate: ASiC File extension is ".asice" (or ".sce" if the operating systems and/or file systems do not allow more than 3 characters file extensions)
Prescription Level: mandatory
Tag: conformance layer = 1 (ACS); Container type = ASiC-E additional container

TA id: TA/ASiC-E/ACS/3
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.3.1 item 3
Target: ASiC generator claiming conformance to ASiC-E additional container
Predicate: The comment field in the ZIP file header is set with "mimetype=" followed by the mime type of the file object within the container
Prescription Level: permitted
Tag: conformance layer = 1 (ACS); Container type = ASiC-E additional container

TA id: TA/ASiC-E/ACS/4
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.3.1 item 2 and clause A.1
Target: ASiC generator claiming conformance to ASiC-E additional container
Predicate: mimetype contains the media type defined in ETSI EN 319 162-1 [1] clause 4.4.3.1 item 2 and is encoded as specified in ETSI EN 319 162-1 [1] clause A.1
Prescription Level: mandatory
Tag: conformance layer = 1 (ACS); Container type = ASiC-E additional container

TA id: TA/ASiC-E/ACS/5
Normative Source: ETSI EN 319 162-1 [1] clause 6.2.2 item 2
Target: ASiC generator claiming conformance to ASiC-E additional container
Predicate: META-INF folder is present and contains either in an arbitrary path one or more file objects whose name contains the word "signatures" and has the extension ".xml"; or one or more file objects whose name contains the word "signature" and has the extension ".p7s"; or one or more file objects whose name contains the word "timestamp" and has the extension ".tst"; or zero or more ASiCManifest files; or zero or more ASiCEvidenceRecordManifest files
Prescription Level: mandatory
Tag: conformance layer = 1 (ACS); Container type = ASiC-E additional container

6.1.2 ASiC-E test assertions for Additional Container Syntactical Conformance

All the test assertions related to the second conformance layer, the Additional Container Syntactical Conformance (ACSC), are grouped in a Test Assertion List defined as follows:

TA List id: TAL/ASiC-E/ACSC
List Description: all TAs describing ACSC requirements for ASiC-E additional containers
List Members: TA/ASiC-E/ACSC/1 ... 11

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

TA id: TA/ASiC-E/ACSC/1
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.3.2 item 3 and ETSI TS 119 134-5 [4] clause 5
Target: ASiC generator claiming conformance to ASiC-E with XAdES additional container
Predicate: one or more *signatures*.xml files are present and their content is compliant with ETSI EN 319 162-1 [1] clause 4.4.3.2 items 3a, 3b, 3c, 3d or 3e; each ds:Signature element that is present in the *signatures*.xml files fulfils the requirements specified in clause 5 of ETSI TS 119 134-5 [4]
Prescription Level: mandatory
Tag: assertion layer = 2 (ACSC); Container type = ASiC-E with XAdES additional container

TA id: TA/ASiC-E/ACSC/2
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.3.2 item 5a
Target: ASiC generator claiming conformance to ASiC-E with XAdES additional container
Prerequisite: the expected input is ASiC-E XAdES that includes the META-INF/container.xml
Predicate: META-INF folder is present and contains a well formed container.xml, as defined in ISO/IEC TS 30135 [i.11] clause 3.5.1
Prescription Level: permitted
Tag: conformance layer = 2 (ACSC); Container type = ASiC-E with XAdES additional container

TA id: TA/ASiC-E/ACSC/3
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.3.2 item 5b
Target: ASiC generator claiming conformance to ASiC-E with XAdES additional container
Prerequisite: the expected input is ASiC-E XAdES that includes the META-INF/manifest.xml
Predicate: META-INF folder is present and contains a well formed manifest.xml, as defined in OASIS Open Document Format specifications [i.10]
Prescription Level: permitted
Tag: conformance layer = 2 (ACSC); Container type = ASiC-E with XAdES additional container

TA id: TA/ASiC-E/ACSC/4
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.3.2 item 5c
Target: ASiC generator claiming conformance to ASiC-E with XAdES additional container
Prerequisite: the expected input is ASiC-E XAdES that includes the META-INF/metadata.xml
Predicate: META-INF folder is present and contains a well formed metadata.xml, as defined in ISO/IEC TS 30135 [i.11] clause 3.5.1
Prescription Level: permitted
Tag: conformance layer = 2 (ACSC); Container type = ASiC-E with XAdES additional container

TA id: TA/ASiC-E/ACSC/5
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.4.2 item 2
Target: ASiC generator claiming conformance to ASiC-E with CAdES or Time Assertion additional container
Prerequisite: TAL/ASiC-E/ACS
Predicate: one or more ASiCManifest files are present, conformant to the schema specified in ETSI EN 319 162-1 [1] clause A.4
Prescription Level: mandatory
Tag: assertion layer = 2 (ACSC); Container type = ASiC-E with CAdES or Time Assertion additional container

TA id: TA/ASiC-E/ACSC/6
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.4.2 item 3a and 3b
Target: ASiC generator claiming conformance to ASiC-E with CAdES or Time Assertion additional container
Prerequisite: TA/ASiC-E/ACSC/5
Predicate: the URI attribute value of SigReference element in each ASiCManifest file refers to one *signature*.p7s or one *timestamp*.tst that is present in the container
Prescription Level: mandatory
Tag: assertion layer = 2 (ACSC); Container type = ASiC-E with CAdES or Time Assertion additional container

TA id: TA/ASiC-E/ACSC/7
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.5 item 2a and clause A.7
Target: ASiC generator claiming conformance to ASiC-E with CAdES or Time Assertion additional container
Prerequisite: TA/ASiC-E/ACSC/6 conformance verified the expected input is ASiC-E with CAdES or Time assertion with long term attributes
Predicate: one or more ASiCArchiveManifest files are present and conforms to ETSI EN 319 162-2 [2] clause A.7 item 1b
Prescription Level: mandatory
Tag: assertion layer = 2 (ACSC); Container type = ASiC-E with CAdES or Time Assertion additional container

TA id: TA/ASiC-E/ACSC/8
Normative Source: ETSI EN 319 162-2 [2] clause A.7 item 1c
Target: ASiC generator claiming conformance to ASiC-E with CAdES or Time Assertion additional container
Prerequisite: TA/ASiC-E/ACSC/7 conformance verified
Predicate: one *timestamp*.tst for each ASiCArchiveManifest file is present whose actual file name matches the value of the URI attribute of the SigReference element.
Prescription Level: mandatory
Tag: assertion layer = 2 (ACSC); Container type = ASiC-E with CAdES or Time Assertion additional container

TA id: TA/ASiC-E/ACSC/9
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.5 item 2a
Target: ASiC generator claiming conformance to ASiC-E with CAdES or Time Assertion additional container
Prerequisite: TA/ASiC-S/ACSC/8 conformance verified the expected input is ASiC-E with CAdES or Time Assertion with a time-stamp token and long term attributes
Predicate: each *timestamp*.tst is compliant with IETF RFC 3161 [i.6] as updated by IETF RFC 5816 [i.7]
Prescription Level: mandatory
Tag: assertion layer = 2 (ACSC); Container type = ASiC-E with CAdES or Time Assertion additional container

TA id: TA/ASiC-E/ACSC/10
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.5 item 2b
Target: ASiC generator claiming conformance to ASiC-E with CAdES or Time Assertion additional container
Prerequisite: TAL/ASiC-S/ACS conformance verified the expected input is ASiC-E with CAdES or Time Assertion with ASiCEvidenceRecordManifest and evidencerecord.ers present
Predicate: ASiCEvidenceRecordManifest is compliant with ETSI EN 319 162-1 [1] clause 4.4.5 item 2b and evidencerecord.ers compliant with IETF RFC 4998 [i.8]
Prescription Level: mandatory
Tag: assertion layer = 2 (ACSC); Container type = ASiC-E with CAdES or Time Assertion additional container

TA id: TA/ASiC-E/ACSC/11
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.5 item 2b
Target: ASiC generator claiming conformance to ASiC-E with CAdES or Time Assertion additional container
Prerequisite: TAL/ASiC-S/ACS conformance verified the expected input is ASiC-E with CAdES or Time Assertion with ASiCEvidenceRecordManifest and evidencerecord.xml present
Predicate: ASiCEvidenceRecordManifest is compliant with ETSI EN 319 162-1 [1] clause 4.4.5 item 2b and evidencerecord.xml compliant with IETF RFC 6283 [i.9]
Prescription Level: mandatory
Tag: assertion layer = 2 (ACSC); Container type = ASiC-E with CAdES or Time Assertion additional container

6.1.3 Test assertions for ASiC-E Additional Container Signature or Timestamp token conformance

All the test assertions related to the third conformance layer, the Additional Container Signature or Timestamp token (ACST) conformance, are grouped in a Test Assertion List defined as follows:

TA List id: TAL/ASiC-E/ACST
List Description: all TAs describing ACST conformance requirements for ASiC-E additional containers
List Members: TA/ASiC-E/ACST/1 ...

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

TA id: TA/ASiC-E/ACST/1
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.3.2 item 2 and ETSI TS 119 134-5 [4] clause 5
Target: ASiC generator claiming conformance to ASiC-E with XAdES additional container
Prerequisite: TA/ASiC-E/ACSC/1 conformance verified
Predicate: signatures.xml is conformant to XAdES-E-BES and the signature is cryptographically correct against the content of the data files either directly referenced by each signature with a set of ds:Reference elements or indirectly referenced using a signed ds:Manifest object that is pointed by a ds:Reference
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-E with XAdES additional container

TA id: TA/ASiC-E/ACST/2
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.3.2 item 2 and ETSI TS 119 134-5 [4] clause 6
Target: ASiC generator claiming conformance to ASiC-E with XAdES additional container
Prerequisite: TA/ASiC-E/ACSC/1 conformance verified
Predicate: signatures.xml is conformant to XAdES-E-EPES and the signature is cryptographically correct against the content of the data files either directly referenced by each signature with a set of ds:Reference elements or indirectly referenced using a signed ds:Manifest object that is pointed by a ds:Reference
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-E with XAdES additional container

TA id: TA/ASiC-E/ACST/3
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.3.2 item 2 and ETSI TS 119 134-5 [4] clause 7
Target: ASiC generator claiming conformance to ASiC-E with XAdES additional container
Prerequisite: TA/ASiC-E/ACSC/1 conformance verified
Predicate: signatures.xml is conformant to XAdES-E-T and the signature is cryptographically correct against the content of the data files either directly referenced by each signature with a set of ds:Reference elements or indirectly referenced using a signed ds:Manifest object that is pointed by a ds:Reference
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-E with XAdES additional container

TA id: TA/ASiC-E/ACST/4
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.3.2 item 2 and ETSI TS 119 134-5 [4] clause 8
Target: ASiC generator claiming conformance to ASiC-E with XAdES additional container
Prerequisite: TA/ASiC-E/ACSC/1 conformance verified
Predicate: signatures.xml is conformant to XAdES-E-C and the signature is cryptographically correct against the content of the data files either directly referenced by each signature with a set of ds:Reference elements or indirectly referenced using a signed ds:Manifest object that is pointed by a ds:Reference
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-E with XAdES additional container

TA id: TA/ASiC-E/ACST/5
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.2 item 4c and ETSI TS 119 134-5 [4] clause 9
Target: ASiC generator claiming conformance to ASiC-E with XAdES additional container
Prerequisite: TA/ASiC-E/ACSC/2 conformance verified
Predicate: signatures.xml is conformant to XAdES-E-X and the signature is cryptographically correct against the content of the data files either directly referenced by each signature with a set of ds:Reference elements or indirectly referenced using a signed ds:Manifest object that is pointed by a ds:Reference
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-E with XAdES additional container

TA id: TA/ASiC-E/ACST/6
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.2 item 4c and ETSI TS 119 134-5 [4] clause 10
Target: ASiC generator claiming conformance to ASiC-E with XAdES additional container
Prerequisite: TA/ASiC-S/ACSC/2 conformance verified
Predicate: signatures.xml is conformant to XAdES-E-X-L and the signature is cryptographically correct against the content of the data files either directly referenced by each signature with a set of ds:Reference elements or indirectly referenced using a signed ds:Manifest object that is pointed by a ds:Reference
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-E with XAdES additional container

TA id: TA/ASiC-E/ACST/7
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.2 item 4c and ETSI TS 119 134-5 [4] clause 11
Target: ASiC generator claiming conformance to ASiC-E with XAdES additional container
Prerequisite: TA/ASiC-S/ACSC/2 conformance verified
Predicate: signatures.xml is conformant to XAdES-E-X-Long and the signature is cryptographically correct against the content of the data files either directly referenced by each signature with a set of ds:Reference elements or indirectly referenced using a signed ds:Manifest object that is pointed by a ds:Reference
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-E with XAdES additional container

TA id: TA/ASiC-E/ACST/8
Normative Source: ETSI EN 319 162-1 [1] clause 4.3.3.2 item 4c and ETSI TS 119 134-5 [4] clause 12
Target: ASiC generator claiming conformance to ASiC-S with XAdES additional container
Prerequisite: TA/ASiC-S/ACSC/2 conformance verified
Predicate: signatures.xml is conformant to XAdES-E-A and the signature is cryptographically correct against the content of the data files either directly referenced by each signature with a set of ds:Reference elements or indirectly referenced using a signed ds:Manifest object that is pointed by a ds:Reference
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-S with XAdES additional container

TA id: TA/ASiC-E/ACST/9
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.3.2 item 2 and ETSI TS 119 134-5 [4] clause 5
Target: ASiC generator claiming conformance to ASiC-E with CAdES additional container
Prerequisite: TA/ASiC-E/ACSC/6 conformance verified and *signature*.p7s is present
Predicate: signatures.xml is conformant to CAdES-E-BES and the signature is cryptographically correct against the content of the data files referenced by the ASiCManifest file

Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-E with CAdES additional container

TA id: TA/ASiC-E/ACST/10
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.3.2 item 2 and ETSI TS 119 134-5 [4] clause 6
Target: ASiC generator claiming conformance to ASiC-E with CAdES additional container
Prerequisite: TA/ASiC-E/ACSC/6 conformance verified and *signature*.p7s is present
Predicate: signatures.xml is conformant to CAdES-E-EPES and the signature is cryptographically correct against the content of the data files referenced by the ASiCManifest file
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-E with CAdES additional container

TA id: TA/ASiC-E/ACST/11
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.3.2 item 2 and ETSI TS 119 134-5 [4] clause 7
Target: ASiC generator claiming conformance to ASiC-E with CAdES additional container
Prerequisite: TA/ASiC-E/ACSC/6 conformance verified and *signature*.p7s is present
Predicate: signatures.xml is conformant to CAdES-E-T and the signature is cryptographically correct against the content of the data files referenced by the ASiCManifest file
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-E with CAdES additional container

TA id: TA/ASiC-E/ACST/12
Normative Source: ETSI EN 319 162-1 [1] clause 4.4.3.2 item 2 and ETSI TS 119 134-5 [4] clause 8
Target: ASiC generator claiming conformance to ASiC-E with CAdES additional container
Prerequisite: TA/ASiC-E/ACSC/6 conformance verified and *signature*.p7s is present
Predicate: signatures.xml is conformant to CAdES-E-A and the signature is cryptographically correct against the content of the data files referenced by the ASiCManifest file
Prescription Level: mandatory
Tag: assertion layer = 3 (ACST); Container type = ASiC-E with CAdES additional container

History

Document history		
V1.1.1	June 2016	Publication