ETSI TS 119 164-2 V1.1.1 (2012-03)

Technical Specification

Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC) Testing Compliance & Interoperability; Part 2: Test Suite for ASiC interoperability test events

Reference

DTS/ESI-000097

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

Important notice

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 (http://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. Full details of the entire series can be found in part 1 [i.2].

1 Scope

The present document defines a number of test suites that aim to assess the interoperability between implementations claiming conformance to ASiC [1].

ASiC containers are specified in TS 102 918 [1] where, for each different container form, a conformance clause is specified in clause 7. Implementations can claim conformance to ASiC by referencing at least one of the aforementioned conformance clauses. Interoperability can then be assessed for implementations claiming conformance to at least one common conformance clause.

This document starts from ASiC specification and specifies test assertions, derived from ASiC conformance clauses, and test suites, that allow to demonstrate that an implementation satisfies test assertions and, in consequence, the conformance clauses.

Clause 4 describes the overall approach followed in the present document: test assertions are derived from ASiC test clauses using a layered conformance model, addressing firstly the conformance of the container structure, then the syntactical conformance of ASiC specific data objects and, finally, the conformance of the electronic signature and/or time stamp format present in the container. From test assertions, are derived the test suites that reflects the same layered structure to address possible interoperability issues between implementations with a step by step approach.

Clause 5 is about conformance of Simple container forms (ASiC-S): all ASiC-S forms have a common structure and a common set of tests is defined for this conformance level; different tests are defined for syntactical and electronic signature conformance.

Clause 6 is about conformance of Extended container forms (ASiC-E): all three conformance levels are applied to each form.

2 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.

2.1 Normative references

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

[1] ETSI TS 102 918: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)".

[2] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[3] ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

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

2.2 Informative references

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", Committee Specification Draft 06 / Public Review Draft 03, 15 August 2011.

[i.2] ETSI TS 119 164-1: "Electronic Signatures and Infrastructures (ESI);Associated Signature Containers (ASiC) Testing Compliance & Interoperability".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ASiC [1] and [i.1] apply. In case of contrast the former prevails.

3.2 Abbreviations

For the purposes of the present document all the abbreviations defined in ASiC [1] and the following apply:

BES	Basic Electronic Signature
CS	Container Structure
EPES	Explicit Policy-based Electronic Signature
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 interoperability test specification overview

This clause describes the overall approach used throughout the present document to specify test suites for ASiC conformance testing.

TS 102 918 [1] defines different containers forms grouped in Simple (ASiC-S) and Extended (ASiC-E) and specifies conformance clauses for each specific form (ASiC [1], clause 7).

For ASiC-S three conformance clauses are specified for containers using CAdES to sign the associated data content; containers using XAdES to sign the associated data content and containers with time-stamp tokens applied to data content.

For ASiC-E, in a similar way, three conformance clauses are specified for containers associating a set of data object and related metadata to XAdES, CAdES or time-stamp tokens that apply to it. An additional conformance clause (ASiC [1], clause 7.2.4) specifies a minimum set of requirements for containers conformant to specifications external to ASiC but that allow to comply with the mentioned minimum set requirements.

The tests will be defined using recent developments in testing fields, based on test assertions work produced by OASIS in "Test Assertions Guidelines Version 1.0" [i.1], Committee Specification Draft 06 / Public Review Draft 03, 15 August 2011.

This methodology gives a better guarantee that the test suites cover all the relevant conformance clauses.

ASiC conformance clauses has been taken as the reference to derive and specify a set of test assertions for each conformance clause and test suites have been specified accordingly such as, applying the test suites to different implementations, it can be verified that test assertions are satisfied. As test assertions guarantee the conditions for conformance to the normative requirements of the ASiC specification, implementation interoperability can be ascertained.

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) **Predicate** fully and unambiguously defining the assertion to be tested by tools claiming conformance to the present document.

5) **Prescription level:** Three levels are defined: mandatory, recommended and optional.

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

For each ASiC form, test assertions, and derived test suites, are specified as belonging to one of three interoperability layers that allow to ascertain incrementally the interoperability of the implementations:

- The first layer is based on test assertions on the conformance of the container structure: the presence of certain data objects in the container with specific names. Entities testing interoperability can obtain specific information to identify potential container conformance problems.

- The second test layer is based on test assertions on the syntactical conformance and/or properties of data objects relevant to ASiC form under test: entities testing interoperability can obtain specific information to identify potential conformance and interoperability problems related to ASiC data object syntax or properties.

- The third layer is based on assertions on conformance of the specific security objects syntax (i.e. CAdES or XAdES signatures or time-stamp tokens) as applicable to the specific ASiC form under test: entities testing interoperability can obtain specific information to identify potential conformance and interoperability problems caused by lack of conformance in signatures or time-stamp tokens contained in ASiC.

All interoperability layer test **shall** be performed to complete interoperability testing.

Where necessary both positive and negative test cases have been defined and different PKI scenarios are available, as follows, to test ASiC in different conditions:

1) all the certificates managed during the generation and verification of the signature are valid. This is the default scenario when no specific PKI scenario is mentioned;

2) the signing certificate is revoked, and all the rest of certificates are valid. This scenario is identified as PKI_KO1;

3) the certificate of one of the CAs in the certification path is revoked. This scenario is identified as PKI_KO2.

5 Testing Simple Associated Signature Containers (ASiC-S)

This clause refers to Conformance Clauses specified in ASiC [1] clauses 7.1.1 (ASiC-S CAdES), 7.1.2 (ASiC-S XAdES) and 7.1.3 (ASiC-S Time-stamp) for ASiC forms defined in [1], clause 5.

5.1 Test Assertions for ASiC-S

5.1.1 ASiC-S test assertions for 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 at least one of the following Conformance Clauses in ASiC [1]: §7.1.1, §7.1.2 or §7.1.3
List Members: TA/ASiC-S/CS/1 ...

NOTE: Test Assertion part of this TA list are identified sequentially adding an integer starting by "1" to the base identifier "TA/ASiC-S/CS/" as TA-id.

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

TA id: TA/ASiC-S/CS/1
Normative Source: ASiC [1] – Clause 5.1 introductory part
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.1.1, §7.1.2 or §7.1.3
Predicate: The ZIP format **shall** be used to bind the contained objects into a single container
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 5.2.1 item 1
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.1.1, §7.1.2 or §7.1.3
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).
Prescription Level: recommended
Tag: conformance layer = 1 (container structure); Container type=Simple (ASiC-S)

TA id: TA/ASiC-S/CS/3
Normative Source: ASiC [1] – Clause 5.2.1 item 3
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.1.1, §7.1.2 or §7.1.3
Predicate: The comment field in the ZIP file header is set with “mimetype=” followed by the mime type of the data object held in the file.
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 5.2.2 item 1 and 5.2.1 item 2
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.1.1, §7.1.2 or §7.1.3
Predicate: mimetype is encoded as specified in ASiC [1] §A.1 and is set with the mime type specifically defined in ASiC [1] §5.2.1 item 2 if TA/ASiC-S/CS/2 fails; else any valid value.
Prescription Level: mandatory if ASiC-S/CS/2 fails; else recommended
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
Target: ASiC verifier claiming conformance to ASiC [1] §7.1.1, §7.1.2 or §7.1.3
Predicate: conformant implementations **shall** check that if TA/ASiC-S/CS/2 fails, then mimetype is set with the mime type specifically defined in ASiC [1] §5.2.1 item 2; else that it is set according to the mime type of the container content.
Prescription Level: mandatory
Tag: conformance layer = 1 (container structure); Container type=Extended (ASiC-S)

TA id: TA/ASiC-S/CS/6
Normative Source: ASiC [1] – Clause 5.2.2 item 3
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.1.1, §7.1.2 or §7.1.3
Predicate: META-INF folder is present and contains one file named timestamp.tst, signature.p7s or signatures.xml.
Prescription Level: mandatory
Tag: conformance layer = 1 (container structure); Container type=Simple (ASiC-S)

TA id: ASiC-S/CS/7
Normative Source: ASiC [1] – Clause 5.2.2 item 2
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.1.1, §7.1.2 or §7.1.3
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 ASiC-S test assertions for 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 syntactical conformance requirements for ASiC-S specific data objet to at least one of the following Conformance Clauses in ASiC [1]: §7.1.1, §7.1.2 or §7.1.3 as specified in the TA
List Members: TA/ASiC-S/SC/1 ...

NOTE: Test Assertion part of this TA list are identified sequentially adding an integer starting by "1" to the base identifier "TA/ASiC-S/SC/" as TA-id.

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

TA id: TA/ASiC-S/SC/1
Normative Source: ASiC [1] – Clause 5.2.2 item 3b
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.1.1
Prerequisite: the expected input is ASiC-S CAdES
Predicate: signature.p7s is present.
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 5.2.2 item 3c
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.1.2
Prerequisite: the expected input is ASiC-S XAdES
Predicate: signatures.xml is present and is conformant to the schema specified in ASiC [1] §A.5
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 5.2.2 item 3a
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.1.3
Prerequisite: the expected input is ASiC-S time-stamp token
Predicate: timestamp.tst is present
Prescription Level: mandatory
Tag: assertion layer = 2 (syntactical conformance); Container type=Simple (ASiC-S)

5.1.3 Test assertions for ASiC-S signature/time-stamp token 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/time-stamp token conformance requirements for ASiC-S to at least one of the following Conformance Clauses in ASiC [1]: §7.1.1, §7.1.2 or §7.1.3 as specified in the TA
List Members: TA/ASiC-S/STV/1 ...

NOTE: Test Assertion part of this TA list are identified sequentially adding an integer starting by "1" to the base identifier "TA/ASiC-S/STV/" as TA-id.

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

TA id: TA/ASiC-S/STV/1
Normative Source: ASiC [1] – Clause 5.2.2 item 3b
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.1.1
Prerequisite: the expected input is ASiC-S CAdES-BES or CAdES-EPES
Predicate: signature.p7s is conformant to CAdES-BES or CAdES-EPES form and calculated over the data object found in TA/ASiC-S/CS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (signature/time-stamp token conformance); Container type=Simple (ASiC-S)

TA id: TA/ASiC-S/STV/2
Normative Source: ASiC [1] – Clause 5.2.2 item 3c

Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.1.2
Prerequisite: the expected input is ASiC-S XAdES-BES or XAdES-EPES
Predicate: signatures.xml contain one or more signatures conformant to XAdES-BES or XAdES-EPES forms and calculated over the data object found in TA/ASiC-S/CS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (signature/time-stamp token conformance); Container type=Simple (ASiC-S)

TA id: TA/ASiC-S/STV/3
Normative Source: ASiC [1] – Clause 5.2.2 item 3a
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.1.3
Prerequisite: the expected input is ASiC-S time-stamp token
Predicate: timestamp.tst is conformant to RFC3161 and calculated over the data object found in TA/ASiC-S/CS/5
Prescription Level: mandatory
Tag: assertion layer = 3 (signature/time-stamp token conformance); Container type=Simple (ASiC-S)

5.2 ASiC-S test suites

A test suite is defined for each ASiC-S conformance clause, i.e. ASiC [1] clause 7.1.1, clause 7.1.2 and clause 7.1.3.

Each test suite is composed by:

- a set of test cases specified in clause 5.2.1 that are common to all ASiC-S forms;
- a set of test cases specified in clause 5.2.2 that are specific for implementations claiming conformance to ASiC-S with CAdES (ASiC [1] clause 7.1.1);
- a set of test cases specified in clause 5.2.3 that are specific for implementations claiming conformance to ASiC-S with XAdES (ASiC [1] clause 7.1.2);
- a set of test cases specified in clause 5.2.4 that are specific for implementations claiming conformance to ASiC-S with time-stamp token (ASiC [1] clause 7.1.3).

Each test suite is designed to verify all the test assertions associated with the applicable conformance clause.

5.2.1 Test cases common to all ASiC-S forms

The common test cases are specified in Table 1 and relates to test assertions in the test assertion list TAL/ASiC-S/CS (clause 5.1.1).

Table 1: Test cases common to all ASiC-S forms

TC ID	Description	Pass criteria	Interop. Level	Test Assertion
TC/ASiC-S/CS/1	This test case tests if the container has a ZIP format.	The container content is successfully extracted.	Container Structure	TA/ASiC-S/CS/1
TC/ASiC-S/CS/2	Verify if the container format is identifiable.	The container extension is "asics" or ".scs" or mimetype is present in the root folder, complies with ASiC [1] clause A.1 is set to "application/vnd.etsi.asic-s+zip".	Container Structure	TA/ASiC-S/CS/2 TA/ASiC-S/CS/4
TC/ASiC-S/CS/3	Verify if the ZIP comment, when used to identify the format, respect ASiC [1] clause 5.2.1 item 3.	If the ZIP comment field begins with the content "mimetype=" it is followed by a mime type value coherent with the signed object extension.	Container Structure	TA/ASiC-S/CS/3
TC/ASiC-S/CS/4	mimetype is set appropriately. Prerequisites: TC/ASiC-S/CS/2 passed Mimetype is present The container extension is "asics" or "scs".	mimetype value is set to "application/vnd.etsi.asic-s+zip" or is set coherently with the signed object extension.	Container Structure	TA/ASiC-S/CS/5
TC/ASiC-S/CS/6	This test case tests that container complies with ASiC [1] clause 5.2.2 - 3).	A META-INF folder in the root folder containing one of the following files: timestamp.tst; signature.p7s; signatures.xml.	Container Structure	TA/ASiC-S/CS/6
TC/ASiC-S/CS/7	Presence of the signed content.	A single data object, in addition to the optional mimetype, is present in the root folder.	Container Structure	TA/ASiC-S/CS/7

5.2.2 Test cases specific to ASiC-S CAdES form

This clause specify the test cases specific to ASiC-S CAdES form that, in addition to those specified in table 1, constitutes the test suite for ASiC-S CAdES form.

The minimum requirements specified for implementations in CAdES [2] applies also to ASiC-S CAdES that **shall** at least support CAdES-BES or CAdES-EPES forms.

The additional test cases specified in this clause include:

- the test cases specified in Table 2 that verify the test assertion TA/ASiC-S/SC/1 (clause 5.1.2);
- the test cases verifying the assertion TA/ASiC-S/STV/1 (clause 5.1.3) specified in Table 3 for implementations supporting CAdES.

Table 2: Test suite for ASiC-S with CAdES - syntactical conformance

TC ID	Description	Pass criteria	Interop. Level	Test Assertion
TC/ASiC-S/SC/C1	Test if ASiC-S with CAdES contains compliant signature metadata.	Data object signature.p7s is present in the META-INF folder.	Syntactical Conformance	TA/ASiC-S/SC/1

Table 3: Test suite for ASiC-S with CAdES signature verification

TC ID	Description	Pass criteria	Interop. Level	Test Assertion
TC/ASiC-S/STV/C1	Signature.p7s is CAdES-BES applied to the data object.	Signature.p7s contains a valid CAdES-BES signature that is verified correctly on the data object.	signature/time-stamp token conformance	TA/ASiC-S/STV/1
TC/ASiC-S/STV/C2	Signature.p7s is CAdES-EPES applied to the data object.	Signature.p7s contains an CAdES-EPES conformant signature that is verified correctly on the data object.	signature/time-stamp token conformance	TA/ASiC-S/STV/1
TC/ASiC-S/STV/C3	Signature.p7s contains 2 CAdES-BES or EPES signatures applied to the data object.	Signature.p7s contains 2 CAdES-BES or CAdES-EPES conformant signatures that are verified correctly on the data object.	signature/time-stamp token conformance	TA/ASiC-S/STV/1
TC/ASiC-S/STV/NC1	Signature.p7s contains a single CAdES-BES or EPES signature. The data object is modified after the signature calculation.	Signature.p7s contains an CAdES-BES or CAdES-EPES conformant signature that fails verification on the data object.	signature/time-stamp token conformance	TA/ASiC-S/STV/1
TC/ASiC-S/STV/NC2	Signature.p7s contains 2 CAdES-BES or EPES signatures applied to the data object. The second signature is generated in PKI_KO1 scenario.	Signature.p7s contains 2 CAdES-BES or CAdES-EPES conformant signatures and the first signature is verified correctly on the data object, the second one fails verification.	signature/time-stamp token conformance	TA/ASiC-S/STV/1
TC/ASiC-S/STV/NC3	Signature.p7s contains 2 CAdES-BES or EPES signatures applied to the data object. The second signature is generated in PKI_KO2 scenario.	Signature.p7s contains 2 CAdES-BES or CAdES-EPES conformant signatures and the first signature is verified correctly on the data object, the second one fails verification.	signature/time-stamp token conformance	TA/ASiC-S/STV/1

An implementation claiming conformance with ASiC [1] (clause 7.1.1) **shall** pass TC/ASiC-S/STV/C1 or TC/ASiC-S/STV/C2. A verifier **should** pass both. For all test cases the signature **shall** contain the minimum set of parameters that grant compliance with CAdES [2].

5.2.3 Test cases specific to ASiC-S XAdES form

This clause specify the test cases specific to ASiC-S CAdES form that, in addition to those specified in table 1, constitutes the test suite for ASiC-S CAdES form.

The minimum requirements specified for implementations in CAdES [2] applies also to ASiC-S CAdES that **shall** at least support CAdES-BES or CAdES-EPES form.

The additional test cases specified in this clause include:

- the test cases specified in Table 4 that verify the test assertion TA/ASiC-S/SC/2 (clause 5.1.2);
- the test cases verifying the assertion TA/ASiC-S/STV/2 (clause 5.1.3) specified in Table 5 for implementations supporting CAdES.

Table 4: Test suite for ASiC-S with XAdES - syntactical conformance

TC ID	Description	Pass criteria	Interop. Level	Test Assertion
TC/ASiC-S/SC/X1	Test if ASiC-S with XAdES contains compliant signature metadata.	Data object signatures.xml is present in the META-INF folder and its content is conformant with the schema specified in ASiC [1] clause A.5.	Syntactical Conformance	TA/ASiC-S/SC/2

Table 5: Test suite for ASiC-S with XAdES signature verification

TC ID	Description	Pass criteria	Interop. Level	Test Assertion
TC/ASiC-S/STV/X1	Signatures.xml contains a single XAdES-BES signature applied to the data object.	Signatures.xml contains an XAdES-BES conformant signature that is verified correctly on the data object.	signature/time-stamp token conformance	TA/ASiC-S/STV/2
TC/ASiC-S/STV/X2	Signatures.xml contains a single XAdES-EPES signature applied to the data object.	Signatures.xml contains an XAdES-EPES conformant signature that is verified correctly on the data object.	signature/time-stamp token conformance	TA/ASiC-S/STV/2
TC/ASiC-S/STV/X3	Signatures.xml contains 2 XAdES-BES or EPES signatures applied to the data object.	Signatures.xml contains 2 XAdES-BES or XAdES-EPES conformant signatures that are verified correctly on the data object.	signature/time-stamp token conformance	TA/ASiC-S/STV/2
TC/ASiC-S/STV/NX1	Signatures.xml contains a single XAdES-BES or EPES signature. The data object is modified after the signature calculation.	Signatures.xml contains an XAdES-BES or XAdES-EPES conformant signature that fails verification on the data object.	signature/time-stamp token conformance	TA/ASiC-S/STV/2
TC/ASiC-S/STV/NX2	Signatures.xml contains 2 XAdES signatures applied to the data object. The second signature is generated in PKI_KO1 scenario.	The first signature is verified correctly on the data object, the second fails verification.	signature/time-stamp token conformance	TA/ASiC-S/STV/2
TC/ASiC-S/STV/NX3	Signatures.xml contains 2 XAdES signatures applied to the data object. The second signature is generated in PKI_KO2 scenario.	The first signature is verified correctly on the data object, the second fails verification.	signature/time-stamp token conformance	TA/ASiC-S/STV/2

An implementation claiming conformance with ASiC [1] (clause 7.1.2) **shall** pass TC/ASiC-S/STV/X1 or TC/ASiC-S/STV/X2. A verifier **should** pass both. For both test cases the signature **shall** contain the minimum set of parameters that grant compliance with XAdES [3].

5.2.4 Test cases specific to ASiC-S Time-stamp token form

This clause specify the test cases specific to ASiC-S Time-stamp token form that, in addition to those specified in table 1, constitutes the test suite for ASiC-S Time-stamp token form.

The additional test cases specified in this clause include:

- the test cases specified in Table 6 that verify the test assertion TA/ASiC-S/SC/3 (clause 5.1.2);
- the test cases verifying the assertion TA/ASiC-S/STV/3 (clause 5.1.3) specified in Table 7 for applications supporting Time-stamp tokens.

Table 6: Test suite for ASiC-S with time-stamp token - syntactical conformance

TC ID	Description	Pass criteria	Interop. Level	Test Assertion
TC/ASiC-S/SC/T1	Test if ASiC-S with time-stamp token contains compliant time-stamp token metadata.	Data object timestamp.tst is present in the META-INF folder.	Syntactical Conformance	TA/ASiC-S/SC/3

Table 7: Test suite for ASiC-S with time-stamp token verification

TC ID	Description	Pass criteria	Interop. Level	Test Assertion
TC/ASiC-S/STV/T1	Timestamp.tst contains a time-stamp token conformant to RFC3161 [4] applied to the data object.	Timestamp.tst contains a valid RFC3161 time-stamp token that is verified correctly on the data object.	signature/time-stamp token conformance	TA/ASiC-S/STV/3
TC/ASiC-S/STV/NT1	Timestamp.tst contains a time-stamp token conformant to RFC3161 [4] applied to the data object. The data object is modified after the signature calculation.	Timestamp.tst contains a valid RFC3161 time-stamp token that fails verification on the data object.	signature/time-stamp token conformance	TA/ASiC-S/STV/3

An implementation claiming conformance with ASiC [1] (clause 7.13) **shall** pass TC/ASiC-S/STV/T1. The time-stamp token used in the context of TC/ASiC-S/STV/T1 **shall** contain the minimum set of parameters that grant compliance with RFC3161 [4].

6 Testing Extended Associated Signature Containers (ASiC-E)

This clause refers to Conformance Clauses specified in ASiC [1] clauses 7.2.1 (ASiC-E XAdES), 7.1.2 (ASiC-E CAdES), 7.2.3 (ASiC-E Time-stamp) and 7.2.4 (ASiC-E other container) for ASiC forms defined in [1], clause 6.

6.1 Test Assertions for ASiC-E

6.1.1 ASiC-E test assertions for 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-E/CS
List Description: all TAs describing container structure requirements for ASiC-E containers to at least one of the following Conformance Clauses in ASiC [1]: §7.2.1, §7.2.2, §7.2.3 or §7.2.4
List Members: TA/ASiC-E/CS/1 ...

NOTE: Test Assertion part of this TA list are identified sequentially adding an integer starting by "1" to the base identifier "TA/ASiC-E/CS/" as TA-id.

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

TA id: TA/ASiC-E/CS/1
Normative Source: ASiC [1] - Clause 6.1 introductory part
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.2.1, §7.2.2, §7.2.3 or §7.2.4
Predicate: The ZIP format **shall** be used to bind the contained objects into a single container
Prescription Level: mandatory
Tag: conformance layer = 1 (container structure); Container type=Extended (ASiC-E)

TA id: TA/ASiC-E/CS/2
Normative Source: ASiC [1] - Clause 6.2.1 item 1 or Clause 6.3.1 item 1 as applicable to the Target
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.2.1, §7.2.2, §7.2.3 or §7.2.4
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: recommended
Tag: conformance layer = 1 (container structure); Container type=Extended (ASiC-E)

TA id: TA/ASiC-E/CS/3
Normative Source: ASiC [1] - Clause 6.2.1 item 3 or Clause 6.3.1 item 3 as applicable to the Target
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.1.1, §7.1.2, §7.1.3 or §7.1.4
Predicate: The comment field in the ZIP file header is set with “mimetype=” followed by the mime type of the data object within the container
Prescription Level: optional

Tag: conformance layer = 1 (container structure); Container type= Extended (ASiC-E)

TA id: TA/ASiC-E/CS/4
Normative Source: ASiC [1] - Clause 6.2.2 item 1 and 6.2.1 item 2 or Clause 6.3.2 item 1 and 6.3.1 item 2 as applicable to the Target
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.2.1, §7.2.2 or §7.2.3
Predicate: mimetype contains the mime type defined in ASiC [1] §6.2.1 item 2 and is encoded as specified in ASiC [1] §A.1
Prescription Level: mandatory if ASiC-E/CS/2 fails; else recommended
Tag: conformance layer = 1 (container structure); Container type=Extended (ASiC-E)

TA id: TA/ASiC-E/CS/5
Normative Source: ASiC [1] - Clause 6.2.2 item 2
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.2.1
Prerequisite: the expected input is ASiC-E XAdES
Predicate: META-INF folder is present and contains one or more data objects whose name contains the word "signatures" and has the extension ".xml"
Prescription Level: mandatory
Tag: conformance layer = 1 (container structure); Container type=Extended (ASiC-E)

TA id: TA/ASiC-E/CS/6
Normative Source: ASiC [1] - Clause 6.3.2 item 4a
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.2.2
Prerequisite: the expected input is ASiC-E CAdES
Predicate: META-INF folder is present and contains one or more data objects whose name contains the word "signature" and has the extension ".p7s"
Prescription Level: mandatory
Tag: conformance layer = 1 (container structure); Container type=Extended (ASiC-E)

TA id: TA/ASiC-E/CS/7
Normative Source: ASiC [1] - Clause 6.3.2 item 4b
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.2.3
Prerequisite: the expected input is ASiC-E time-stamp token
Predicate: META-INF folder is present and contains one or more data objects whose name contains the word "timestamp" and has the extension ".tst"
Prescription Level: mandatory
Tag: conformance layer = 1 (container structure); Container type=Extended (ASiC-E)

TA id: TA/ASiC-E/CS/9
Normative Source: ASiC [1] - Clause 6.3.2 item 3
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.2.2 or §7.2.3
Prerequisite: the expected input is ASiC-E CAdES or ASiC-E time-stamp token
Predicate: META-INF folder is present and contains one or more files whose name begins with "ASiCManifest" and has the extension ".xml"
Prescription Level: mandatory
Tag: conformance layer = 1 (container structure); Container type=Extended (ASiC-E)

6.1.2 ASiC-E test assertions for 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-E/SC
List Description: all TAs describing syntactical conformance requirements for ASiC-E specific data objet to at least one of the following Conformance Clauses in ASiC [1]: §7.2.1, §7.2.2, §7.2.3 or §7.2.4 as specified in the TA
List Members: TA/ASiC-E/SC/1 ...

NOTE: Test Assertion part of this TA list are identified sequentially adding an integer starting by "1" to the base identifier "TA/ASiC-E/SC/" as TA-id.

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

TA id: TA/ASiC-E/SC/1
Normative Source: ASiC [1] - Clause 6.2.2 item 2 and item 3
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.2.1
Predicate: one or more *signatures*.xml are present and its content is compliant with one of the items 3a, 3b or 3c of 6.2.2.
Prescription Level: mandatory
Tag: assertion layer = 2 (syntactical conformance); Container type=Extended (ASiC-E)

TA id: TA/ASiC-E/SC/2
Normative Source: ASiC [1] - Clause 6.2.2 item 4a; specification of container.xml in OEBPS Container Format (OCF) §3.5.1
Target: ASiC verifier claiming conformance to ASiC [1] §7.2.1
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 OCF §3.5.1
Prescription Level: optional
Tag: conformance layer = 1 (container structure); Container type=Extended (ASiC-E)

TA id: TA/ASiC-E/SC/3
Normative Source: ASiC [1] – Clause 6.2.2 item 4b; specification of manifest.xml in OEBPS Container Format (OCF) §3.5.1
Target: ASiC verifier claiming conformance to ASiC [1] §7.2.1
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
Prescription Level: optional
Tag: conformance layer = 1 (container structure); Container type=Extended (ASiC-E)

TA id: TA/ASiC-E/SC/4
Normative Source: ASiC [1] – Clause 6.2.2 item 4c; specification of metadata.xml in OEBPS Container Format (OCF) §3.5.1
Target: ASiC verifier claiming conformance to ASiC [1] §7.2.1
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 OCF §3.5.1
Prescription Level: optional
Tag: conformance layer = 1 (container structure); Container type=Extended (ASiC-E)

TA id: TA/ASiC-E/SC/5
Normative Source: ASiC [1] – Clause A.6
Target: ASiC verifier claiming conformance to ASiC [1] §7.2.1
Predicate: all references present in signatures refer to data objects present in the container and use relative URIs that are relative to the root folder
Prescription Level: mandatory
Tag: conformance layer = 1 (container structure); Container type=Extended (ASiC-E)

TA id: TA/ASiC-E/SC/6
Normative Source: ASiC [1] – Clause 6.3.2 item 3
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.2.2 and §7.2.3
Predicate: at least a ASiCManifest*.xml is present and is conformant to the schema specified in ASiC [1] §A.4
Prescription Level: mandatory
Tag: assertion layer = 2 (syntactical conformance); Container type=Extended (ASiC-E)

TA id: TA/ASiC-E/SC/7
Normative Source: ASiC [1] – Clause 6.3.2 item 4a and 4b
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.2.2
Prerequisite: TA/ASiC-E/SC/6 does not fail
Predicate: for each ASiCManifest*.xml is present *signature*.p7s or *timestamp*.tst is present and is referenced by the corresponding ASiCManifest
Prescription Level: mandatory
Tag: assertion layer = 2 (syntactical conformance); Container type=Extended (ASiC-E)

TA id: TA/ASiC-E/SC/8
Normative Source: ASiC [1] – Clause 6.4
Target: ASiC verifier claiming conformance to ASiC [1] §7.2.1, §7.2.2, §7.2.3 or §7.2.4
Prerequisite: TA/ASiC-E/CS/4 does not fail
Predicate: conformant implementations **shall** check that if the META-INF includes manifest objects containing the mime type of the object referenced (e.g. ASiCManifest*.xml) implementations **shall** check that this is coherent with the object referenced.
Prescription Level: mandatory
Tag: conformance layer = 2 (syntactical conformance); Container type=Extended (ASiC-E)

6.1.3 Test assertions for ASiC-E signature/time-stamp token 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-E/STV
List Description: all TAs describing signature/time-stamp token conformance requirements for ASiC-E to at least one of the following Conformance Clauses in ASiC [1]: §7.2.1, §7.2.2, §7.2.3 or §7.2.4 as specified in the TA
List Members: TA/ASiC-E/STV/1 ...

NOTE: Test Assertion part of this TA list are identified sequentially adding an integer starting by "1" to the base identifier "TA/ASiC-E/STV/" as TA-id.

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

TA id: TA/ASiC-E/STV/1
Normative Source: ASiC [1] – Clause 6.2.2 item 2
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.2.1
Predicate: *signatures*.xml is conformant to XAdES
Prescription Level: mandatory
Tag: assertion layer = 3 (signature/time-stamp token conformance); Container type=Extended (ASiC-E)

TA id: TA/ASiC-E/STV/2
Normative Source: ASiC [1] – Clause 6.3.2 item 2 and item 4a
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.2.2
Predicate: *signature*.p7m is conformant to CAdES
Prescription Level: mandatory
Tag: assertion layer = 3 (signature/time-stamp token conformance); Container type=Extended (ASiC-E)

TA id: TA/ASiC-E/STV/3
Normative Source: ASiC [1] – Clause 6.3.2 item 2 and item 4b
Target: ASiC generator or verifier claiming conformance to ASiC [1] §7.2.2
Predicate: *timestamp*.tst is conformant to RFC3161
Prescription Level: mandatory
Tag: assertion layer = 3 (signature/time-stamp token conformance); Container type=Extended (ASiC-E)

6.2 ASiC-E test suites

A test suite is defined for each ASiC-E conformance clause, i.e. ASiC [1] clause 7.2.1, clause 7.2.2, clause 7.2.3 and clause 7.2.4.

Each test suite is composed by:

- a set of test cases specified in clause 6.2.1 that are common to all ASiC-S forms;
- a set of test cases specified in clause 6.2.2 that are specific for implementations claiming conformance to ASiC-S with CAdES (ASiC [1] clause 7.2.1);
- a set of test cases specified in clause 6.2.3 that are specific for implementations claiming conformance to ASiC-S with XAdES (ASiC [1] clause 7.2.2);
- a set of test cases specified in clause 6.2.4 that are specific for implementations claiming conformance to ASiC-S with time-stamp token (ASiC [1] clause 7.2.3);
- a set of test cases specified in clause 6.2.5 that are specific for implementations claiming conformance to ASiC-S with time-stamp token (ASiC [1] clause 7.2.4).

Each test suite is designed to verify all the test assertions associated with the applicable conformance clause.

6.2.1 Test cases common to all ASiC-E forms

The common test cases are specified in Table 8 and relates to test assertions in the test assertion list TAL/ASiC-E/CS (clause 6.1.1).

Table 8: Test cases for container structure conformance for ASiC-E forms

TC ID	Description	Pass criteria	Interop. Level	Test Assertion
TC/ASiC-E/CS/1	This test case tests if the container has a ZIP format.	The container content is successfully extracted.	Container Structure	TA/ASiC-E/CS/1
TC/ASiC-E/CS/2	Verify if the container format is identifiable.	The container extension is ".asice" or ".sce" or mimetype is present in the root folder, complies with ASiC [1] clause A.1 is set to "application/vnd.etsi.asic-e+zip".	Container Structure	TA/ASiC-E/CS/2 TA/ASiC-E/CS/4
TC/ASiC-E/CS/3	Verify if the ZIP comment, when used to identify the format, respect ASiC [1] clause 6.2.1 item 3.	If the ZIP comment field begins with the content "mimetype=" it is followed by a mime type value coherent with the container content.	Container Structure	TA/ASiC-E/CS/3
TC/ASiC-E/CS/4	Mimetype is set appropriately. Prerequisites: TC/ASiC-E/CS/2 passed Mimetype is present The container extension is ".asice" or ".sce".	Mimetype value is set to "application/vnd.etsi.asic-e+zip" or is set coherently with the container content.	Container Structure	TA/ASiC-E/CS/4
TC/ASiC-E/CS/5	Test if signature metadata is present.	META-INF folder in the root folder contains either: - one or more ASiCManifest*.xml and, for each one, a *signature*.p7m or a *timestamp*.tst metadata; or - one or more *signatures*.xml metadata.	Container Structure	TA/ASiC-E/CS/5 TA/ASiC-E/CS/6 TA/ASiC-E/CS/7

6.2.2 ASiC-E XAdES test suite

This clause specify the test cases specific to ASiC-E XAdES forms that, in addition to those specified in Table 8, constitutes the test suite for ASiC-E XAdES form (ASiC [1] clause 7.2.1) and, as applicable, for the ASiC-E other container (ASiC [1] clause 7.2.4).

The minimum requirements specified for implementations in XAdES [2] applies also to ASiC-E XAdES that **shall** at least support XAdES-BES or XAdES-EPES forms.

The additional test cases specified in this clause include:

- the test cases specified in table 9 that verify applicable test assertion in TAL/ASiC-E/SC (clause 6.1.2);
- the test cases verifying applicable test assertion in TAL/ASiC-E/STV (clause 6.1.3) specified in table 10.

Table 9: Test suite for ASiC-E with XAdES - syntactical conformance

TC ID	Description	Pass criteria	Interop. Level	Test Assertion
TC/ASiC-E/SC/X1	Test if XAdES signature metadata is present.	META-INF folder in the root folder contains one or more *signatures*.xml whose content is compliant with one of the items 3a, 3b or 3c of 6.2.2.	Syntactical Conformance	TA/ASiC-E/SC/1
TC/ASiC-E/SC/X2	Test if container.xml is conformant Prerequisite: container.xml is present.	META-INF/container.xml is well formed and compliant with OCF clause 3.5.1.	Syntactical Conformance	TA/ASiC-E/SC/2
TC/ASiC-E/SC/X3	Test if manifest.xml is conformant Prerequisite: manifest.xml is present.	META-INF/ manifest.xml is well formed and compliant with OASIS Open Document Format specifications.	Syntactical Conformance	TA/ASiC-E/SC/3
TC/ASiC-E/SC/X4	Test if container.xml is conformant Prerequisite: metadata.xml is present.	META-INF/ metadata.xml is well formed and compliant with OCF clause 3.5.1.	Syntactical Conformance	TA/ASiC-E/SC/4
TC/ASiC-E/SC/X5	Test if data objects referenced in XAdES signature metadata are present.	XAdES signature metadata reference data objects with URIs relative to the root folder and all referenced data object is present in the container.	Syntactical Conformance	TA/ASiC-E/SC/5
TC/ASiC-E/SC/X6	Test if mime types present in manifest.xml or container.xml metadata are coherent with referenced objects.	All mime types present in manifest.xml or container.xml metadata are coherent with referenced objects.	Container Structure	TA/ASiC-E/SC/8
Test TC/ASiC-E/ SC/X1 **shall** be repeated with different input containers, at least one with a single signature metadata and one with 2.				
At least one among TC/ASiC-E/ SC/X2 and TC/ASiC-E/ SC/X3 **shall** be supported by conformant implementation. Support for TC/ASiC-E/SC/X4 is optional.				

Table 10: Test suite for ASiC-E with XAdES signature verification

TC ID	Description	Pass criteria	Interop. Level	Test Assertion
TC/ASiC-E/STV/X1	A metadata whose name matches *signatures*.xml is present and contains a XAdES-BES signature applied to one or more data object.	The metadata whose name matches *signatures*.xml contains a valid XAdES-BES signature that is verified correctly on the referenced data object(s).	signature/time-stamp token conformance	TA/ASiC-E/STV/1
TC/ASiC-E/STV/X2	A metadata whose name matches *signatures*.xml is present and contains a XAdES-EPES signature applied to one or more data object.	The metadata whose name matches *signatures*.xml contains an XAdES-EPES conformant signature that is verified correctly on the referenced data object(s).	signature/time-stamp token conformance	TA/ASiC-E/STV/1
TC/ASiC-E/STV/X3	A metadata whose name matches *signatures*.xml contains 2 XAdES-BES or EPES signatures applied to one or more data object.	The metadata whose name matches *signatures*.xml contains 2 XAdES-BES or XAdES-EPES conformant signatures that are verified correctly on the referenced data object.	signature/time-stamp token conformance	TA/ASiC-E/STV/1
TC/ASiC-E/STV/NX1	A metadata whose name matches *signatures*.xml is present and contains a single XAdES-BES or EPES signature. One of the signed data object is modified after the signature calculation.	The metadata whose name matches *signatures*.xml contains an XAdES-BES or XAdES-EPES conformant signature that fails verification on the data object.	signature/time-stamp token conformance	TA/ASiC-E/STV/1
TC/ASiC-E/STV/NX2	A metadata whose name matches *signatures*.xml is present and contains 2 XAdES-BES or EPES signatures applied to the data object. The second signature is generated in PKI_KO1 scenario.	The metadata whose name matches *signatures*.xml contains 2 XAdES-BES or XAdES-EPES conformant signatures and the first signature is verified correctly on the data object, the second one fails verification.	signature/time-stamp token conformance	TA/ASiC-E/STV/1
TC/ASiC-E/STV/NX3	A metadata whose name matches *signatures*.xml is present and contains 2 XAdES-BES or EPES signatures applied to the data object. The second signature is generated in PKI_KO2 scenario.	The metadata whose name matches *signatures*.xml contains 2 XAdES-BES or XAdES-EPES conformant signatures and the first signature is verified correctly on the data object, the second one fails verification.	signature/time-stamp token conformance	TA/ASiC-E/STV/1

An implementation claiming conformance with ASiC [1] clause 7.2.2 or 7.2.4 **shall** pass TC/ASiC-E/STV/X1 or TC/ASiC-E/STV/X2. A verifier **should** pass both. For all test cases the signature **shall** contain the minimum set of parameters that grant compliance with XAdES [3].

6.2.3 ASiC-E CAdES and time-stamp token test suite

This clause specify the test cases specific to ASiC-E CAdES and time-stamp token forms that, in addition to those specified in Table 8, constitutes the test suite for ASiC-E CAdES and for ASiC-E time-stamp forms.

The minimum requirements specified for implementations in CAdES [2] applies also to ASiC-E CAdES that **shall** at least support CAdES-BES or CAdES-EPES forms.

The additional test cases specified in this clause include:

- the test cases specified in Table 11 that verify applicable test assertion in TAL/ASiC-E/SC (clause 6.1.2);
- the test cases verifying applicable test assertion in TAL/ASiC-E/STV (clause 6.1.3) specified in Table 12.

Table 11: Test suite for ASiC-E with CAdES and time-stamp token-syntactical conformance

TC ID	Description	Pass criteria	Interop. Level	Test Assertion
TC/ASiC-E/SC/CT1	Test if ASiCManifest metadata is present.	META-INF folder in the root folder contains one or more ASiCManifest*.xml that conforms to ASiC [1] clause A.4.	Container Structure	TA/ASiC-E/SC/6
TC/ASiC-E/SC/CT2	Test if CAdES signature and/or time-stamp token metadata is present.	For each ASiCManifest*.xml present in the META-INF folder the URI in the SigReference element point to an existent signature*.p7s or timestamp*.tst.	Container Structure	TA/ASiC-E/SC/7
TC/ASiC-E/SC/CT3	Test if mime types present in ASiCManifest metadata are coherent with referenced objects.	All mime types present in ASiCManifest metadata are coherent with referenced objects.	Container Structure	TA/ASiC-E/SC/8
As additional requirement for TC/ASiC-E/CS/2, the tests are repeated with different input containers: 1) for applications claiming conformance to ASiC [1] clause 7.2.2 at least a container with a single signature metadata and one with 2 **shall** be provided; 2) for applications claiming conformance to ASiC [1] clause 7.2.3 at least a container with a single signature metadata and one with 2 **shall** be provided; 3) for applications claiming conformance to both the conformance clauses above, in addition to requirements 1) and 2) at least a container with both a signature and a time-stamp token metadata **shall** be provided.				

Table 12: Test suite for ASiC-E with CAdES or time-stamp token signature verification

TC ID	Description	Pass criteria	Interop. Level	Test Assertion
TC/ASiC-E/STV/C1	A metadata whose name matches *signature*.p7s is present and contains a CAdES-BES signature applied to an ASiCManifest metadata that references it.	The metadata whose name matches *signature*.p7s contains a valid CAdES-BES conformant signature that is verified correctly on the related ASiCManifest metadata.	signature/time-stamp token conformance	TA/ASiC-E/STV/2
TC/ASiC-E/STV/C2	A metadata whose name matches *signature*.p7s is present and contains a CAdES-EPES signature applied to the related ASiCManifest metadata that references it and that references one or more data objects.	The metadata whose name matches *signature*.p7s contains an CAdES-EPES conformant signature that is verified correctly on the related ASiCManifest metadata. The references contained in ASiCManifest refer correctly to one or more data objects and their hashes.	signature/time-stamp token conformance	TA/ASiC-E/STV/2
TC/ASiC-E/STV/C3	A metadata whose name matches *signature*.p7s contains 2 CAdES-BES or EPES signatures applied to the related ASiCManifest metadata that references it and that references one or more data objects.	The metadata whose name matches *signature*.p7s contains 2 CAdES-BES or CAdES-EPES conformant signatures that are verified correctly on the ASiCManifest metadata. The references contained in ASiCManifest refer correctly to one or more data objects and their hashes.	signature/time-stamp token conformance	TA/ASiC-E/STV/2
TC/ASiC-E/STV/T1	A metadata whose name matches *timestamp*.tst contains a time-stamp token conformant to RFC3161 [4] applied to the related ASiCManifest metadata that references it and that references one or more data objects.	The metadata whose name matches *timestamp*.tst contains a valid RFC3161 time-stamp token that is verified correctly on the ASiCManifest metadata. The references contained in ASiCManifest refer correctly to one or more data objects and their hashes.	signature/time-stamp token conformance	TA/ASiC-S/STV/3
TC/ASiC-E/STV/NC1	A metadata whose name matches *signature*.p7s contains a single CAdES-BES or EPES signature. The ASiCManifest metadata is modified after the signature calculation.	The metadata whose name matches *signature.p7s contains an CAdES-BES or CAdES-EPES conformant signature that fails verification on the ASiCManifest metadata.	signature/time-stamp token conformance	TA/ASiC-E/STV/2
TC/ASiC-E/STV/NC2	A metadata whose name matches *signature*.p7s contains a single CAdES-BES or EPES signature. One of the data objects referenced by the related ASiCManifest metadata is modified after the signature calculation.	The metadata whose name matches *signature.p7s contains an CAdES-BES or CAdES-EPES conformant signature but the verification fails on the modified data object.	signature/time-stamp token conformance	TA/ASiC-E/STV/2
TC/ASiC-E/STV/NC3	A metadata whose name matches *signature.p7s contains 2 CAdES-BES or EPES signatures applied to the related ASiCManifest metadata. The second signature is generated in PKI_KO1 scenario.	The metadata whose name matches *signature.p7s contains 2 CAdES-BES or CAdES-EPES conformant signatures and the first signature is verified correctly on the data object, the second one fails verification.	signature/time-stamp token conformance	TA/ASiC-E/STV/2

TC ID	Description	Pass criteria	Interop. Level	Test Assertion
TC/ASiC-E/STV/NC4	A metadata whose name matches *signature.p7s contains 2 CAdES-BES or EPES signatures applied to the related ASiCManifest metadata. The second signature is generated in PKI_KO2 scenario.	The metadata whose name matches *signature.p7s contains 2 CAdES-BES or CAdES-EPES conformant signatures and the first signature is verified correctly on the data object, the second one fails verification.	signature/time-stamp token conformance	TA/ASiC-E/STV/2
TC/ASiC-S/STV/NT1	A metadata whose name matches *timestamp*.tst contains a time-stamp token conformant to RFC3161 [4] applied to the related ASiCManifest metadata. ASiCManifest is modified after the signature calculation.	The metadata whose name matches *timestamp.tst contains a valid RFC3161 time-stamp token that fails verification on the ASiCManifest metadata.	signature/time-stamp token conformance	TA/ASiC-S/STV/3
TC/ASiC-S/STV/NT2	A metadata whose name matches *timestamp*.tst contains a time-stamp token conformant to RFC3161 [4] applied to the related ASiCManifest metadata. One of the data objects referenced by the related ASiCManifest metadata is modified after the signature calculation.	The metadata whose name matches *timestamp.tst contains a valid RFC3161 time-stamp token but the verification fails on the modified data object.	signature/time-stamp token conformance	TA/ASiC-S/STV/3
All the tests are repeated for each input container user for the syntactical conformance test suite.				

An implementation claiming conformance with ASiC [1] clause 7.2.2 **shall** pass TC/ASiC-E/STV/C1 or TC/ASiC-E/STV/C2. A verifier **should** pass both. For all test cases the signature **shall** contain the minimum set of parameters that grant compliance with CAdES [2].

History

Document history		
V1.1.1	March 2012	Publication