Draft EN 319 162-2V 0.0.4 (2013-11)

Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Baseline Profile

STABLE DRAFT FOR PUBLIC REVIEW UNTIL 15 JANUARY 2014

Download the template for comments:

http://docbox.etsi.org/ESI/Open/Latest_Drafts/Template-for-comments.doc

Send comments to E-SIGNATURES_COMMENTS@LIST.ETSI.ORG

Reference
DEN/ESI-0019162-2

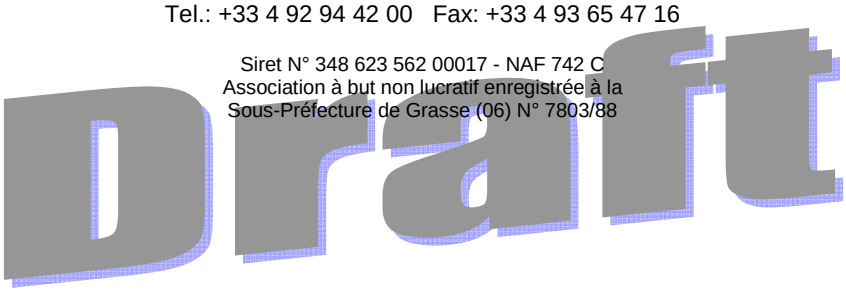
Keywords
ASiC, e-commerce, electronic signature, security

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

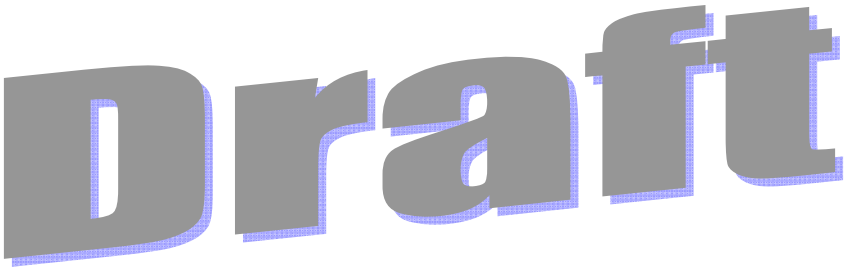
Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

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 draft European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI) and is now submitted for the Vote phase of the ETSI standards EN Approval Procedure.

The present document is part 2 of a multi-part deliverable.

The present document was previously published as TS 103 174 [i.9].

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

Introduction

Part 1 of the present multi-part document, EN 319 162-1 [5] (ASiC henceforth) specifies the use of container structures for associating either detached CAdES [1] signatures or detached XAdES [2] signatures or time-stamp tokens, with one or more signed objects to which they apply and allows a number of options.

In order to maximize interoperability in communities applying ASiC to particular environments it is necessary to identify a common set of options that are appropriate to that environment. Such a selection is commonly called a profile.

The present document is an ASiC baseline profile that provides the basic features necessary for a wide range of business and governmental use cases when there is a clear need for interoperability across borders. In particular it takes into account needs for interoperability of AdES signatures used in electronic documents issued by competent authorities to be interchanged across borders in the context of the EU Services Directive [i.3].

1 Scope

The present document defines a baseline profile for ASiC that provides the basic features necessary for a wide range of business and governmental use cases for electronic procedures and communications to be applicable to a wide range of communities when there is a clear need for interoperability of AdES signatures, on which ASiC is based, to be interchanged across borders. In particular it takes into account needs for interoperability of AdES signatures used in

electronic documents issued by competent authorities to be interchanged across borders in the context of the EU Services Directive [i.3].

The profile defines three different conformance levels addressing incremental requirements to maintain the validity of the container signatures over the long term based on the corresponding conformance levels specified in CAdES [3] and XAdES [4] profiles, in a way that all the requirements addressed at a certain level are always addressed also by the levels above. Each level requires the presence of certain attributes in the container signature, suitably profiled for reducing the optionality as much as possible and referring to the forms that are specified in CAdES [1] or XAdES [2] as applicable.

Clause 4 identifies the three conformance levels and shows how these levels might encompass the life cycle of the electronic signatures.

Clause 5 provides details on the way that the requirements on both signer and verifier will be presented throughout the present document.

Clauses 6, 7 and 8 specify the requirements for ASiC containers that are applicable to all the conformance levels specified in clause 4. Clause 6 specifies profiling requirements for elements common to all ASiC containers while clauses 7 and 8 specify profile requirements related to ASiC-S and ASiC-E respectively.

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 EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signature Formats (CAdES); Part 1: Core Specification".

[2] ETSI EN 319 132-1: " Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signature Formats (XAdES); Part 1: Core Specification".

[3] ETSI EN 319 122-2: " Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signature Formats (CAdES); Part 2: Baseline Profile".

[4] ETSI EN 319 132-2: " Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signature Formats (XAdES); Part 2: Baseline Profile ".

[5] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Mother Specification ".

[6] ETSI TS 101 861: "Electronic Signatures and Infrastructures (ESI); Time stamping profile".

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

[i.2] PKWARE: ".ZIP Application Note".

NOTE: Available at http://www.pkware.com/support/zip-application-note.

[i.3] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

[i.4] ECRYPT II (European Network of Excellence in Cryptology II): "ECRYPT II Yearly Report on Algorithms and Keysizes".

[i.5] ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management".

[i.6] ETSI TS 102 640-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture".

[i.7] Commission Decision 2011/130/EU of 25 February 2011; establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (notified under document C(2011) 1081).

[i.8] ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

[i.9] ETSI TS 103 174: "Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in CAdES [1], XAdES [2], ASiC [5] and the following apply:

generator: any party which creates, or adds attributes to, a signature

NOTE: This may be the signatory or any party which initially verifies or further maintains the signature.

protocol element: element of the protocol which may be including data elements and/or elements of procedure

service element: element of service that may be provided using one or more protocol elements

NOTE: All alternative protocol elements provide an equivalent service to the users of the protocol.

verifier: entity that validates or verifies an electronic signature

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in CAdES [1], XAdES [2] and ASiC [5] and TS 101 861 [6] apply.

4 Conformance Levels

This clause defines three conformance levels as indicated below for containers with CAdES or XAdES signatures and is not applicable to ASiC-S Time-stamp token (ASiC [6] clause 7.1.3) and ASiC-E Time-stamp token (ASiC [6] clause 7.2.3).

Applications managing containers that contain attributes for long term validation as specified in clause 7.6.4 points b) and c) of the present document may claim ASiC-S Time-stamp token long term compliance.

Applications managing containers that contain attributes for long term validation as specified in clause 8.5.2 points b) and c) of the present document may claim ASiC-E Time-stamp token long term compliance.

Applications managing containers that contain signatures conformant to requirements specified in clause 6 of [3] or clause 6 of [4] (as applicable, depending on the ASiC form) may claim **B-Level** (basic level) conformance.

Applications managing containers that contain signatures conformant to **B-Level** and signatures conformant to requirements specified in clause 7 of [3] or [4] (as applicable, depending on the ASiC form) may claim **T-Level** (Trusted time for signature existence) conformance.

Applications managing containers that contain signatures conformant to **T-Level** and signatures conformant to requirements specified in clause 8 of [3] or [4] (as applicable, depending on the ASiC form) may claim **LT-Level** (Long Term level) conformance.

Applications managing containers that contain signatures conformant to **LT-Level** and signatures conformant to one of the following requirements:

- in case of ASiC-S with CAdES form, the requirements specified in clause 9 of the CAdES baseline profile [3], or
- in case of ASiC-S with XAdES form, the requirements specified in clause 9 of the XAdES baseline profile [4], or
- in case of ASiC-E with CAdES form, the requirements specified in clause 8.4.2 points b(and c) of the present document, or
- in case of ASiC-E with XAdES form, the requirements specified in clause 9 of the XAdES baseline profile [4]

may claim **LTA-Level** (Long Term with Archive time-stamps) conformance.

These conformance levels are defined for encompassing the life cycle of electronic signature, namely:

a) B-Level profiles the incorporation of signed and some unsigned properties when the signature is actually generated.

NOTE 1: It is considered that this level is sufficient to conform to the Commission Decision 2011/130/EU [i.7].

b) T-Level profiles the generation, for an existing signature, of a trusted token proving that the signature itself actually existed at a certain date and time.

c) LT-Level profiles the incorporation of all the material required for validating the signature in the signature itself. This level is understood to tackle the long term availability of the validation material.

d) LTA-Level profiles the incorporation of time-stamp tokens that allow validation of the signature long time after its generation. This level is understood to tackle the long term availability and integrity of the validation material.

NOTE 2: The levels b) to d) are appropriate where the technical validity of signature needs to be preserved for a period of time after signature creation where certificate expiration, revocation and/or algorithm obsolescence is of concern. The specific level applicable depends on the context and use case.

All conformance levels up to LT use properties defined in CAdES [1] or XAdES [2] as applicable.

When signed data is exchanged between parties the sender should use at least signatures conforming to a level that allows the relying parties to trust the signature at the time the exchange takes place.

NOTE 3: Archiving or preservation of electronic signatures over long term requires in general conformance to LTA level. The use of LTA-level is considered an appropriate preservation and transmission technique for signed data. Conformance to lower level is sufficient when combined with appropriate additional protection techniques such as use of systems compliant to TS 101 533-1 [i.5].

NOTE 4: The assessment of the effectiveness of other preservation and transmission techniques for signed data is out of the scope of the present document. The reader is advised to consider legal instruments in force and related standards such as TS 101 533-1 [i.5] or TS 102 640-1 [i.6] to evaluate their appropriateness.

5 General requirements

5.1 Algorithm requirements

Generators are referred to applicable national laws regarding algorithms and key lengths.

Generators are also recommended to take into account the latest version of TS 102 176-1 [5] for guidelines purposes and the latest ECRYPT2 D.SPA.x [i.4] yearly report for further recommendations, when selecting algorithms and key lengths.

MD5 algorithm shall not be used as digest algorithm.

For CAdES and XAdES signatures present in the container the related profiles (respectively [3] and [4]) shall apply.

5.2 Compliance requirements

Profiles in the present document define requirements for generators of ASiC containers.

A verifier shall be able to accept ASiC containers with signatures containing any elements/properties conformant to XAdES [2] or CAdES [1], as applicable, but this profile does not specify any processing requirement on such elements/properties present in the signatures as it is meant to be used together with a specification describing processing during signature validation.

Requirements are grouped in two different categories, each one having its corresponding identifier. Table 1 defines these categories and their identifiers.

Table 1: Requirement categories

Identifier	Requirement on generator
M	Generator shall include the element in the signature.
O	Generator may include the element in the signature.

Optional elements defined in ASiC [6] but not specified in the present document are treated as "O" as above.

Any element present in CAdES [1] or XAdES [2] signatures included in ASiC containers and not specified in the present document shall be treated as specified in CAdES Baseline Profile [3] and XAdES Baseline Profile [4] as applicable.

Certain service elements may be provided by different protocol elements at user's choice. In these cases the semantics of M and O defined in table 1 depend on the requirement for the service element itself. Tables 2 and 3 (each one applies to a different requirement on the service element) define these semantics.

Table 2: Requirements for mandatory service with choices

Requirement Identifier for the Service/Protocol element	Requirement on generator
Service = M	Generator shall provide the service by including one protocol element chosen from the list of choices.
Protocol Choice = O	Generator may use this protocol element for providing the mandatory service elements.

Table 3: Requirements for optional service with choices

Requirement Identifier for the Service/Protocol element	Requirement on generator
Service = O	Generator may provide the service by including one protocol element chosen from the list of choices.
Protocol Choice = O	If the generator decides to provide the service, then she may use this protocol element.

The present document shows new requirements for each service and protocol element in tabular form. Below follows the structure of the table.

Table 4: Requirements for optional service with choices

Service/Protocol element	Reference	Requirement on generator	Additional requirements/notes
Service:			
Choice 1			
Choice 2			

Column **Service/Protocol element** will identify the service element or protocol element the requirement applies to. Service elements that may be implemented by different protocol elements (i.e. users may make a choice on several protocol elements) build tables with more than one row.

Column **Reference** will reference the relevant clause of the standard where the element is first defined. The reference is to ASiC [6], except where explicitly indicated otherwise.

Column **Requirement on generator** will contain an identifier of the requirement, as defined in table 1, bound to the corresponding protocol element for the generator.

Column **Notes/Additional requirements** will contain numbers referencing notes and/or letters referencing additional requirements. Both notes and additional requirements are listed below the table.

Profiles may be affected by applicable regulations; hence implementers should check any national regulation that may affect these profiles.

6 Requirements for ASiC formats

6.1 ASiC conformance

ASiC [6] specifies that a conformant implementation can support a single ASiC type.

Table 5

Service/Protocol element	ASiC [6] reference	Generator requirement	Additional requirements/notes
Service: ASiC		M	
ASiC-S CAdES	Clause 7.1.1	O	
ASiC-S CAdES long term	Clause 7.1.1.1	O	
ASiC-S XAdES	Clause 7.1.2	O	
ASiC-S XAdES long term	Clause 7.1.2.1	O	
ASiC-S Time-stamp token	Clause 7.1.3	O	
ASiC-S Time-stamp token long term	Clause 7.1.3.1	O	
ASiC-E XAdES	Clause 7.2.1	O	
ASiC-E XAdES long term	Clause 7.2.1.1	O	
ASiC-E CAdES	Clause 7.2.2	O	
ASiC-E CAdES long term	Clause 7.2.2.1	O	
ASiC-E Time-stamp	Clause 7.2.3	O	
ASiC-E Time-stamp long term	Clause 7.2.3.1	O	

NOTE: According to the requirements specified for this service, generator and verifier can implement one or more protocol options. Implementers are advised to detail in relevant documentation the implemented protocols by explicitly referencing all applicable ASiC [6] clause(s).

7 Requirements for ASiC-S

7.1 ASiC-S Media type identification

This clause specifies compliance requirements for any ASiC-S type as does not depend on the selected signature type.

Table 6

Service/Protocol element	ASiC [6] reference	Generator requirement	Additional requirements/notes
Service: ASiC-S Media type identification		M	
ASiC file extension is ".asics"	Clause 5.2.1	O	
ASiC file extension is ".scs"	Clause 5.2.1	O	
mimetype	Clauses 5.2.1 and A.1	O	

7.2 ASiC-S Signed or time-stamped data object

This clause specifies compliance requirements for any ASiC-S type as does not depend on specific signature type or time-stamp token.

Table 7

Service/Protocol element	ASiC [6] reference	Generator requirement	Additional requirements/notes
Signed data object	Clause 5.2.2 point 2	M	a

Additional requirement:

a) This protocol element shall be the only data element, with an arbitrary name, in the root container folder.

7.3 Requirements for ASiC-S format

7.3.1 General requirements for ASiC-S

The following table specify the requirements that shall apply for any ASiC-S form.

Table 8

Service/Protocol element	ASiC [6] reference	Generator requirement	Additional requirements/notes
Service: ASiC-S format		M	
META-INF/timestamp.tst	Clause 5.2.2 point 3a	O	Clause 7.3.2 shall apply
META-INF/signature.p7s	Clause 5.2.2 point 3b	O	Clause 7.3.3 shall apply
META-INF/signatures.xml	Clause 5.2.2 point 3c	O	Clause 7.3.4 shall apply

7.3.2 Requirements for ASiC-S CAdES signature format

The following table specify the requirements that shall apply for ASiC-S CAdES.

Table 9

Service/Protocol element	ASiC [6] reference	Generator requirement	Additional requirements/notes
META-INF/signature.p7m	Clause 5.2.2 point 3b	M	a, b, c

Additional requirement:

a) The CAdES [1] signature specified above shall conform to the CAdES baseline profiles [3] clause 6 to 8 according to the required conformance level (see clause 4) taking into account that only the detached signature shall be supported.

b) When conformance to ASiC-S CAdES long term is asserted, conformity to CAdES baseline profiles [3], clause 9 is required.

c) No other element is present in the container in addition to this element, mimetype (clause 7.1) and the signed data object (clause 7.2).

7.3.3 Requirements for ASiC-S XAdES signature format

The following table specify the requirements that shall apply for ASiC-S XAdES.

Table 10

Service/Protocol element	ASiC [6] reference	Generator requirement	Additional requirements/notes
META-INF/signatures.xml	Clause 5.2.2 point 3c	M	a, b, c, d

Additional requirements:

a) This protocol element shall contain a `<asic:XAdESSignatures>` root element as specified in ASiC [6], point 3a.

b) Each XAdES [2] element included in the root element specified in a) shall conform to the XAdES baseline profile [4] clause 6 to 8 according to the required conformance level (see clause 4) taking into account that only the detached signature shall be supported.

c) When conformance to ASiC-S XAdES long term is asserted, conformity to XAdES baseline profiles [4], clause 9 is required.

d) Each XAdES [2] element included in the root element specified in a) shall reference explicitly the signed data object using the `<ds:Reference>` element.

e) No other element shall be present in the container in addition to this element, mimetype (clause 7.1) and the signed data object (clause 7.2).

7.3.4 Requirements for ASiC-S Time stamp token format

The following table specify the requirements that shall apply for ASiC-S Time-stamp token

Table 11

Service/Protocol element	ASiC [6] reference	Generator requirement	Additional requirements/notes
META-INF/timestamp.tst	Clause 5.2.2 point 3a	M	a, d
META-INF/*ASiCArchiveManifest*	Clause 5.5 point 3	O	b, c, d
ASiC-E Time stamp token	Clause 6.3.2 point 4b	O	b, c, d

Additional requirement:

a) This protocol element shall conform to TS 101 861 [6].

b) To support ASiC-S Time-stamp token long term a single META-INF/ASiCArchiveManifest.xml element may be present and additional META-INF/*ASiCArchiveManifest* elements may be present

c) A time stamp token is present for each META-INF/*ASiCArchiveManifest* element and applies to it.

d) No other element is present in the container in addition to the elements specified in Table 11, mimetype (clause 7.1) and the signed data object (clause 7.2).

8 Requirements for ASiC-E

8.1 ASiC-E Media type identification

The following table specify the requirements that shall apply for any ASiC-E form.

Table 12

Service/Protocol element	ASiC [6] reference	Generator requirement	Additional requirements/notes
Service: ASiC-E Media type identification		M	
ASiC file extension is ".asice"	Clause 6.2.1	O	
ASiC file extension is ".sce"	Clause 6.2.1	O	
mimetype	Clause 6.2.1	O	

8.2 ASiC-E Signed data object

This clause specifies compliance requirements for any ASiC-E type as does not depend on the selected signature type.

Table 13

Service/Protocol element	ASiC [6] reference	Generator requirement	Additional requirements/notes
Signed data object	Clause 6.2.2	M	At least one signed data object shall be in the container outside the META-INF folder

8.3 Requirements for ASiC-E XAdES

This clause specifies additional compliance requirements specific for ASiC-E XAdES type.

8.3.1 ASiC-E XAdES signature

Table 14

Service/Protocol element	ASiC [6] reference	Generator requirement	Additional requirements/notes
ASiC-E XAdES signature	Clause 6.2.2 point 2	M	a, b, c

Additional requirements:

a) At least a signature shall be present in the META-INF folder conforming to ASiC [6], point 2.

b) The requirements stated in 7.3.3 points a), b) and c) shall apply.

c) Each XAdES [2] element included in the root element specified above shall reference directly all the signed data objects with a set of `<ds:Reference>` elements (see ASiC [6], point 2).

8.3.2 Requirements for the contents of Container

Table 15

Service/Protocol element	ASiC [6] reference	Generator requirement	Additional requirements/notes
META-INF/manifest.xml	Clause 6.2.2 point 4b	M	a

Additional requirements:

a) In META-INF folder shall not be present any additional data object in addition to what specified in this clause and in clause 8.3.1.

8.4 Requirements for ASiC-E CAdES

This clause specifies compliance requirements for ASiC-E CAdES.

8.4.1 ASiC-E CAdES signature

Table 16

Service/Protocol element	ASiC [6] reference	Generator requirement	Additional requirements/notes
ASiC-E CAdES signature	Clause 6.3.2 point 4a	M	a, b

Additional requirements:

a) At least a signature shall be present in the META-INF folder as specified in ASiC [6], clause 6.3.2, point 4a.

b) The requirement stated in clause 7.3.2 point a) shall apply.

8.4.2 Requirements for the contents of Container

Table 17

Service/Protocol element	ASiC [6] reference	Generator requirement	Additional requirements/notes
META-INF/ASiCManifest	Clause 6.3.2 point 3	M	a, d
META-INF/*ASiCArchiveManifest*	Clause 6.5 point 2	O	b, c, d
ASiC-E Time stamp token	Clause 6.3.2 point 4b	O	b, c, d

Additional requirements:

a) At least one ASiCManifest shall be present.

b) When conformance to ASiC-E CAdES long term is asserted, a single META-INF/ASiCArchiveManifest.xml element may be present and additional META-INF/*ASiCArchiveManifest* elements may be present.

c) A time stamp token is present for each META-INF/*ASiCArchiveManifest* element and applies to it.

d) In META-INF folder shall not be present any additional data object in addition to what specified in this clause and in clause 8.4.1.

8.5 Requirements for ASiC-E Time stamp token

This clause specifies compliance requirements for ASiC-E stamp token.

8.5.1 Requirements on Time stamp tokens

Table 18

Service/Protocol element	ASiC [6] reference	Generator requirement	Additional requirements/notes
ASiC-E Time stamp token	Clause 6.3.2 point 4b	M	a, b

Additional requirements:

a) At least a time stamp token shall be present in the META-INF folder as specified in ASiC [6], clause 6.3.2, point 4b.

b) Each Time stamp token specified above shall conform to TS 101 861 [7].

8.5.2 Requirements for the contents of Container

Table 19

Service/Protocol element	ASiC [6] reference	Generator requirement	Additional requirements/notes
META-INF/ASiCManifest	Clause 6.3.2 point 3	M	a, d
META-INF/*ASiCArchiveManifest*	Clause 6.5 point 2	O	b, c, d
ASiC-E Time stamp token	Clause 6.3.2 point 4b	O	b, c, d

Additional requirements:

a) At least one ASiCManifest shall be present.

b) When conformance to ASiC-E Time-stamp token long term is asserted, a single META-INF/ASiCArchiveManifest.xml element may be present and additional META-INF/*ASiCArchiveManifest* elements may be present.

c) A time stamp token is present for each META-INF/*ASiCArchiveManifest* element and applies to it.

d) In META-INF folder shall not be present any additional object in addition to what is specified in this clause and in clause 8.5.1.

Table 17

Service/Protocol element	ASiC [6] reference	Generator requirement	Additional requirements/notes
META-INF/*ASiCArchiveManifest*	Clause 6.5 point 2	M	a
ASiC-E Time stamp token	Clause 6.3.2 point 4b	M	b

Additional requirements:

a) A single META-INF/ASiCArchiveManifest.xml element is present and additional META-INF/*ASiCArchiveManifest* elements may be present.

History

Document history		
V0.0.1	July 2013	First draft
V0.0.2	November 2013	Stable draft
V0.0.4	November 2013	Deleted clause 9 and inserted long time attribute management in clauses 7 and 8 to improve document readability