Draft ETSI EN 319 162-2 V1.0.0 (2015-08)

Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers

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

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
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:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

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 combined Public Enquiry and Vote phase of the ETSI standards EN Approval Procedure.

The present document is part 2 of a multi-part deliverable specifying Associated Signature Containers (ASiC), as identified below:

Part 1: "Building blocks and ASiC baseline containers";

Part 2: "Additional ASiC containers".

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

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.

Introduction

Part 1 of the present multi-part deliverable, ETSI EN 319 162-1 [2] (ASiC part 1 henceforth) specifies the use of container structures for associating either detached CAdES [1] signatures or detached XAdES [i.7] signatures or time assertions, with one or more signed objects to which they apply and specifies a number of baseline containers that aim to fulfil the common use cases and allows a number of options.

1 Scope

Specific communities or use cases may have additional requirements that are not addressed by the baseline containers defined in ASiC part 1 [2] that can be built using the building blocks defined there or additional ones. The present document references such specific additional use of ASiC and aims to be used for containers that collects together electronic documents including those supported by OCF, ODF and UCF describing how these container formats can be used to associate digital signatures with any data objects in the container.

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 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[2] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and 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 reference 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] PKWARE®: ".ZIP Application Note".

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

[i.2] Universal Container Format (UCF).

NOTE: Available at https://wikidocs.adobe.com/wiki/display/PDFNAV/Universal+Container+Format.

[i.3] ISO/IEC TS 30135 (all parts): "Information technology -- Digital publishing -- EPUB3".

[i.4] OASIS: "Open Document Format for Office Applications (OpenDocument) Version 1.2; Part 3: Packages", 29 September 2011.

[i.5] IETF RFC 4998: "Evidence Record Syntax (ERS)".

[i.6] IETF RFC 6283: "Extensible Markup Language Evidence Record Syntax (XMLERS)".

[i.7] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in CAdES [1], XAdES [i.7] and ASiC part 1 [2] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in CAdES [1], XAdES [i.7] and ASiC part 1 [2] apply.

4 ASiC additional containers

4.1 Introduction

This clause defines ASiC additional containers designed to maximize interoperability for ASiC for use cases considered of general use not covered by baseline containers specified in ASiC part 1 [2] clause 5:

- ASiC-S with time assertion specified in clause 4.2.1;
- ASiC-E with CAdES specified in clause 4.3.1; and
- ASiC-E with time assertion specified in clause 4.3.2.

4.2 ASiC-S additional containers

4.2.1 ASiC-S Time assertion additional container

The present clause defines the ASiC-S Time assertion additional container. The requirement specified in ASiC part 1 [2] for ASiC-S shall apply with the following additional restrictions:

a) it shall comply with the specific provision given in ASiC part 1 [2], clause 4.3.3.1 item 2) a) and clause 4.3.3.2, item 4) a), 4) d) or 4) e);

b) it may contain additional elements in the META-INF folder as specified in ASiC part 1 [2], clause 4.3.3.2 item 5) a) and 5) b); and

c) it shall support ASiC part 1 [2], clause 4.3.3.2 item 2);

d) if one or more ASiCArchiveManifest files are present they shall comply with ASiC part 1 [2], clause A.7 with the additional restriction that only `SignedData` shall be used to include certificate and revocation information.

4.3 ASiC-E additional containers

4.3.1 ASiC-E CAdES additional container

The present clause defines the ASiC-E CAdES additional container. The requirement specified in ASiC part 1 [2] for ASiC-E shall apply with the following additional restrictions:

a) it shall comply with the specific provision given in ASiC part 1 [2], clause 4.4.4.1 item 1) a) and clause 4.4.4.2, item 3) a);

b) the CAdES signatures shall comply with CAdES [1] baseline profiles clause 6.3 B-B level, B-T level or B-LT level;

c) it shall support ASiC part 1 [2], clause 4.4.5 item 2).

4.3.2 ASiC-E Time assertion additional container

The present clause defines the ASiC-E time assertion additional container. The requirement specified in ASiC part 1 [2] for ASiC-E shall apply with the following additional restrictions:

a) it shall comply with the specific provision given in ASiC part 1 [2], clause 4.4.4.1 item 1) a) and clause 4.4.4.2, item 3) b) or 4) a) or 4) b); and

b) it shall support ASiC part 1 [2], clause 4.4.5 item 2).

Annex A (informative): Using ASiC with existing container specifications

The present annex specifies recommendations for the use of ASiC containers in a way which is compatible with existing container specifications that define a file structure with associated metadata and signatures.

The container may be realized either as a physical container based on ZIP [i.1] as required by ASiC part 1 [2], clause 4.4.2 item 1) or, when supported by the external specification, as an abstract container with a file system model supporting storage of files in a folder hierarchy.

NOTE: UCF [i.2] is an example of container formats supporting abstract containers.

ASiC part 1 [2], clause 4.4.2 item 3), clause 4.4.3.1 should apply.

Clause 4.4.3.2 should apply with the following additional requirements:

- "mimetype" may be present and should comply with ASiC part 1 [2] and contain the media type identifying the container type, if applicable.
- "META-INF/container.xml" may be present and should comply with OCF [i.3].
- "META-INF/manifest.xml" may be present and should comply with ODF [i.4].
- "META-INF/metadata.xml" may be present and should comply with ODF [i.4].
- "META-INF/signatures.xml" may be present and should comply with OCF [i.3] if "mimetype" is present and its value is "application/epub+zip".
- "META-INF/*signatures*.xml" may be present and should comply with ODF [i.4] if "mimetype" is present and its value is an ODF supported media type.

Other files defined in the OCF [i.3], UCF [i.2] and ODF [i.4] formats may be present and combined within ASiC as appropriate and should not violate the format implied by the "mimetype" file.

The following table specifies the general requirements that should apply for all ASiC-E containers.

Table A.1

Container files or properties	OCF	ODF	UCF	Additional requirements and notes
Mimetype	may be present	may be present	may be present	a
META-INF/manifest.xml	may be present	should be present	may be present	b
META-INF/container.xml	should be present	may be present	may be present	c
META-INF/metadata.xml	may be present	may be present	may be present	c
META-INF/ *signatures*.xml	should be present	should be present	should be present	d
Container filename extension	should be present	should be present	should be present	f, e
Archive level ZIP comment	may be present	may be present	may be present	g, e

Additional requirements:

a) If present the value should be conformant to the relevant container specification.

b) If present the content should be conformant to ODF [i.4].

c) If present the content should be conformant to OCF [i.3].

d) The filename should be conformant to the relevant container specification. The content root element should be compliant with ASiC part 1 [2], clause 4.4.3.2 item 3) b) for ODF [i.4], item 3) c) for OCF [i.3] and UCF [i.2].

e) If applicable (i.e. the container is a physical container).

f) The file extension should comply with the container media type associated to the container content or with ASiC part 1 [2], clause 4.4.3.1 item 2) b).

g) Presence and value should be as specified in ASiC part 1 [2], clause 4.4.3.1 item 3).