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

- Intellectual Property Rights .................................................................................................................. 4
- Foreword .................................................................................................................................................. 4
- Modal verbs terminology ....................................................................................................................... 4
- Introduction ............................................................................................................................................... 4
  1 Scope .................................................................................................................................................. 5
  2 References ........................................................................................................................................... 5
    2.1 Normative references ....................................................................................................................... 5
    2.2 Informative references ..................................................................................................................... 5
- 3 Definitions and abbreviations ............................................................................................................ 6
  3.1 Definitions .......................................................................................................................................... 6
  3.2 Abbreviations .................................................................................................................................... 6
- 4 ASiC additional containers ................................................................................................................. 6
  4.1 Introduction ....................................................................................................................................... 6
  4.2 ASiC-S additional containers ............................................................................................................. 6
    4.2.1 ASiC-S Time assertion additional container ............................................................................. 6
  4.3 ASiC-E additional containers ............................................................................................................. 6
    4.3.1 ASiC-E CAdES additional container ....................................................................................... 6
    4.3.2 ASiC-E Time assertion additional container ............................................................................. 7
- Annex A (informative): Using ASiC with existing container specifications ........................................ 8
- Annex B (informative): ASiC application to archival systems using ER .............................................. 10
  B.1 Introduction ..................................................................................................................................... 10
  B.2 Extraction of one single signed data from the archive ................................................................. 10
  B.3 Extraction of multiple signed data from the archive ....................................................................... 10
- Annex C (informative): Example of ASiC-E with CAdES and time-stamp token ................................. 11
- History ..................................................................................................................................................... 13
Intellectual Property Rights

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

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

Foreword

This European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

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".

<table>
<thead>
<tr>
<th>National transposition dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of adoption of this EN:</td>
</tr>
<tr>
<td>Date of latest announcement of this EN (doa):</td>
</tr>
<tr>
<td>Date of latest publication of new National Standard or endorsement of this EN (dop/e):</td>
</tr>
<tr>
<td>Date of withdrawal of any conflicting National Standard (dow):</td>
</tr>
</tbody>
</table>

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 fulfill 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 collect 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.


NOTE: Available at http://www.pkware.com/documents/APPNOTE/APPNOTE-6.3.3.TXT.

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


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


[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);

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

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 requirements specified in ASiC part 1 [2] clause 4.4 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); and

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

NOTE: Implementations compliant with ASiC-E CAdES additional container requirements can support the same levels defined for baseline containers specified in ASiC part 1 [2], clause 5.
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, and 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>
<thead>
<tr>
<th>Container files or properties</th>
<th>OCF</th>
<th>ODF</th>
<th>UCF</th>
<th>Additional requirements and notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mimetype</td>
<td>may be present</td>
<td>may be present</td>
<td>may be present</td>
<td>a</td>
</tr>
<tr>
<td>META-INF/manifest.xml</td>
<td>may be present</td>
<td>should be present</td>
<td>may be present</td>
<td>b</td>
</tr>
<tr>
<td>META-INF/container.xml</td>
<td>should be present</td>
<td>may be present</td>
<td>may be present</td>
<td>c</td>
</tr>
<tr>
<td>META-INF/metadata.xml</td>
<td>may be present</td>
<td>may be present</td>
<td>may be present</td>
<td>c</td>
</tr>
<tr>
<td>META-INF/<em>/signatures</em>.xml</td>
<td>should be present</td>
<td>should be present</td>
<td>should be present</td>
<td>d</td>
</tr>
<tr>
<td>Container filename extension</td>
<td>should be present</td>
<td>should be present</td>
<td>should be present</td>
<td>f, e</td>
</tr>
<tr>
<td>Archive level ZIP comment</td>
<td>may be present</td>
<td>may be present</td>
<td>may be present</td>
<td>g, e</td>
</tr>
</tbody>
</table>

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).
Annex B (informative):
ASiC application to archival systems using ER

B.1 Introduction

The present annex specifies a possible way to support the extraction from an archival system of one or more signed data objects protected with one or more ERs.

B.2 Extraction of one single signed data from the archive

When one single signed data object protected with an ER is extracted from the archive, an ASiC-S container should be created. It should comply with ASiC part 1 [2], clauses 4.3.2, 4.3.3 and 4.3.4, according to the signed data format, and should include:

- a file containing the signed data object extracted from the archive in the root folder; and
- the extracted ER that applies to the signed data as a file that should be named according to ASiC part 1 [2], clause 4.3.3.2 item 4) d) in case the ER complies with IETF RFC 4998 [i.5] or item 4) e) in case the ER complies with IETF RFC 6283 [i.6].

NOTE: The ER hashtree can be reduced as specified in IETF RFC 4998 [i.5] and IETF RFC 6283 [i.6].

B.3 Extraction of multiple signed data from the archive

The present clause specifies how to support the extraction from an archival system of a set of digitally signed data objects protected by one or more ERs. When multiple signed data objects are extracted from the archive, an ASiC-E container should be created that should comply with ASiC part 1 [2], clause 4.4.2 and clause 4.4.3 or 4.4.4, according to the signed data format, and should include:

- a) one file for each extracted signed data object including, if applicable, detached signatures and/or ASiCManifest files that apply to the signed data;
- b) one file for each extracted ERs that apply to the data extracted from the archive renamed according to ASiC part 1 [2], clause 4.4.3.2 item 4) a) in case the ER complies with IETF RFC 4998 [i.5] or item 4) b) in case the ER complies with IETF RFC 6283 [i.6];
- c) an ASiCEvidenceRecordManifest file should be created and added for each ER extracted (as per item b)) referencing:
  - the ER using the SigReference element defined in clause A.4.2 of ASiC part 1 [2], and
  - the files extracted (as per item a)) using the DataObjectReference element defined in clause A.4.2 of ASiC part 1 [2].

NOTE: The ER hashtree can be reduced as specified in IETF RFC 4998 [i.5] and IETF RFC 6283 [i.6].
Annex C (informative):
Example of ASiC-E with CAdES and time-stamp token

In this example a set of file objects is digitally signed with a CAdES signature and an ASiC-E container is created. Later on a new set of file objects is added to the container and all the file objects are time-stamped.

The first version of the ASiC-E container includes:

- "mimetype", containing "application/vnd.etsi.asic-e+zip".
- "file1.xml", the first XML file object.
- "file2.xml", the second XML file object.
- "/META-INF/ ASiCManifest1.xml" containing the references to and the digests of file1.xml and file2.xml.
- "/META-INF/signatures1.p7s" containing the CAdES digital signature of "/META-INF/ ASiCManifest1.xml.

Subsequently the container content is updated as follows (added content in bold):

- "file1.xml", the first XML file object.
- "file2.xml", the second XML file object.
- "file1.pdf", the first PDF file object.
- "file2.pdf", the second PDF file object.
- "/META-INF/ ASiCManifest1.xml" containing the references to and the digests of "file1.xml" and "file2.xml".
- "/META-INF/signatures1.p7s" containing the CAdES digital signature of "/META-INF/ASiCmanifest1.xml".
- "/META-INF/ ASiCManifest2.xml" containing the references to and the digests of "file1.xml", "file2.xml", "file1.pdf", "file2.pdf".
- "/META-INF/timestamp.tst" containing the time-stamp token applied to "/META-INF/ ASiCManifest2.xml".

META-INF/ ASiCManifest1.xml

```xml
<?xml version="1.0" encoding="UTF-8"?>
<asic:ASiCManifest
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 xmlns:asic="http://uri.etsi.org/02918/v1.2.1#"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" >
 <asic:SigReference URI="META-INF/signature1.p7s"
  MimeType="application/x-pkcs7-signature"/>
 <asic:DataObjectReference URI="file1.xml" MimeType="application/xml">
   <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmlenc#sha256"/
   <ds:DigestValue>j61wx3SAvKTMUP4NbeZ1</ds:DigestValue>
 </asic:DataObjectReference>
 <asic:DataObjectReference URI="file2.xml" MimeType="application/xml">
   <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmlenc#sha256"/
   <ds:DigestValue>h3isbr37GE6Ek2wa</ds:DigestValue>
 </asic:DataObjectReference>
</asic:ASiCManifest>
```
META-INF/ ASiCManifest2.xml

<?xml version="1.0" encoding="UTF-8"?>
<asic:ASiCManifest
   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
   xmlns:asic="http://uri.etsi.org/02918/v1.2.1#"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <asic:SigReference URI="META-INF/timestamp.tst" MimeType="application/vnd.etsi.timestamp-token"/>
   <asic:DataObjectReference URI="file1.xml" MimeType="application/xml">
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmlenc#sha256"/>
      <ds:DigestValue>j6lwx3SAvKTMUP4NbeZ1</ds:DigestValue>
   </asic:DataObjectReference>
   <asic:DataObjectReference URI="file2.xml" MimeType="application/xml">
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmlenc#sha256"/>
      <ds:DigestValue>h3isbr37GE6Ek2wauT7J</ds:DigestValue>
   </asic:DataObjectReference>
   <asic:DataObjectReference URI="file1.pdf" MimeType="application/pdf">
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmlenc#sha256"/>
      <ds:DigestValue>7GE6Eek3SAvKT3isrvEPO</ds:DigestValue>
   </asic:DataObjectReference>
   <asic:DataObjectReference URI="file2.pdf" MimeType="application/pdf">
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmlenc#sha256"/>
      <ds:DigestValue>br37GTMU3SAvKT3sbr3I</ds:DigestValue>
   </asic:DataObjectReference>
</asic:ASiCManifest>
## History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Event</th>
<th>Approval/Vote</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0.0</td>
<td>August 2015</td>
<td>EN Approval Procedure</td>
<td>AP 20151211:</td>
<td>2015-08-13 to 2015-12-11</td>
</tr>
<tr>
<td>V1.0.1</td>
<td>August 2015</td>
<td>Publication as ETSI TS 119 162-2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>V1.1.0</td>
<td>February 2016</td>
<td>Vote</td>
<td>V 20160424:</td>
<td>2016-02-24 to 2016-04-25</td>
</tr>
<tr>
<td>V1.1.1</td>
<td>April 2016</td>
<td>Publication</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>