Draft ETSI EN 319 162-1 V1.0.0 (2015-08)

Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers

Reference

DEN/ESI-0019162-1

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 1 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

When signing data, the resultant signature needs to be associated with the data to which it applies. This can be achieved either by creating a data set which combines the signature and the data that was signed (e.g. by enveloping the data with the signature or including a signature element in the data set) or placing the (detached) signature in a separate resource and have some external means for associating the signature with the data to which it applies. While there are some advantages to the use of detached signatures, most significantly their non-modification of the original data objects, there remains a risk that the signature becomes separated from the data to which it applies and so losing the association. Therefore, many application systems have developed their own technique for combining a detached signature with the signed object in some form of container so that they can be more easily distributed and guarantee that the correct signature and any relevant metadata is used when validating. The same requirements apply to associate time assertions (i.e. time-stamp tokens or evidence records) to their associated data.

The present document defines a standardized use of container types to establish a common way for associating files containing data objects with files containing digital signatures and/or time-assertions. Using a common container form and associated information will facilitate data interchange and interoperability among various signing and validation services.

Whilst ZIP [5] provides a basic container structure that can associate files containing data objects (file objects) and the signature(s) that apply to them, there is a recognized need for additional structure and metadata about the association, for example to link a particular signature with the file object to which it is applied. Other formats have already been specified for the use of ZIP based structures to bind together a number of file objects with related metadata. This includes OCF [4] which was originally designed for use by eBooks but has been adopted as the basis for other containers, for example ODF [6]. The present document builds on this work specifically addressing the requirements of associating a digital signature with any type of data, independent of the needs of any particular document or data type.

The present document is intended to cover containers including digital signatures and time-assertions supported by PKI and public key certificates, and aims to meet the general requirements of the international community to provide trust and confidence in electronic transactions, including, amongst other, applicable requirements from Regulation (EU) No 910/2014 [i.3].

The present document is part of a rationalized framework of standards (see ETSI TR 119 000 [i.9]). ETSI TR 119 100 [i.1] provides guidance on how to use the present document within the aforementioned framework.

1 Scope

The present document specifies Associated Signature Containers (ASiC) which bind together into one single digital container based on ZIP [5] either detached digital signatures or time-assertions, with a number of file objects (e.g. documents, XML structured data, spreadsheet, multimedia content) to which they apply.

The present document specifies general purpose ASiC containers building blocks and a limited set of baseline containers.

ASiC supports the following signature and time assertion formats:

- CAdES digital signatures (ETSI EN 319 122-1 [1] and ETSI EN 319 122-2 [11]);
- XAdES digital signatures (ETSI EN 319 132-1 [2] and ETSI EN 319 132-2 [12]);
- IETF RFC 3161 [3] and updated by IETF RFC 5816 [13] time-stamp tokens; and
- IETF RFC 4998 [8] or IETF RFC 6283 [9] evidence records.

NOTE: No restriction is placed on time assertions eventually used within CAdES/XAdES.

The building blocks defined in the present document support additional features not supported by the aforementioned formats, such as time-stamping and CAdES signing of multiple content and XAdES parallel signatures, that can be used in other contexts.

The present document defines baseline containers which provide 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.

The present document defines four levels of ASiC baseline containres addressing incremental requirements to maintain the validity of the containers over the long term, suitably profiled for reducing the optionality as much as possible, in a way that a certain level always addresses all the requirements addressed at levels that are below it.

ASiC containers specified in the two parts of this multipart deliverable aim at supporting containers in different regulatory frameworks.

The present document does not address the identification of the validation policy to be used for verifying a container that contains time-stamp assertions.

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 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

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

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

NOTE: Available at http://idpf.org/epub/30/spec/epub30-ocf.html.

[5] PKWARE® ".ZIP Application Note".

NOTE 1: If available in time a reference to ISO/IEC 21320-1 (now under development) will possibly be added.

NOTE 2: Available at http://www.pkware.com/support/zip-application-note.

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

[7] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

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

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

[10] IETF RFC 1951: "DEFLATE Compressed Data Format Specification version 1.3".

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

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

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

[14] W3C recommendation: "XML Signature Syntax and Processing".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Business Driven Guidance for Signature Creation and Validation".

[i.2] ISO 15489-1: "Information and documentation - Records management - Part 1: General".

[i.3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.4] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.5] IETF RFC 6838: "Media Type Specifications and Registration Procedures".

[i.6] IETF RFC 2045: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".

[i.7] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp profiles".

[i.8] ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management".

[i.9] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); Rationalized structure for Electronic Signature Standardization".

[i.10] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TR 119 001 [i.10] and the following apply:

ASiCArchiveManifest file: container file whose name matches "*ASiCArchiveManifest*.xml" containing one `ASiCManifest` element instance conforming to clause A.7

ASiCEvidenceRecordManifest file: container file used in ASiC-E to reference a set of files to which an ER applies whose name matches "META-INF/ASiCEvidenceRecordManifest*.xml" and containing one `ASiCManifest` element instance conformant to clause A.4

ASiCManifest file: file whose name matches "*ASiCManifest*.xml" containing one `ASiCManifest` element instance conformant to clause A.4

container: file created according to ZIP holding as internal elements files with related manifest, metadata and associated signature(s), under a folder hierarchy

media type: method to label arbitrary content, carried by MIME [i.6] or other protocols

NOTE: Refer to IETF RFC 6838 [i.5] clause 1.

metadata: data describing context, content and structure of data objects and their management over time

NOTE: Refer to ISO 15489-1: 2001, definition 3.12 with modifications [i.2].

time assertion: time-stamp token or evidence record

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in CAdES [1], XAdES [2] and the following apply:

ASiC Associated Signature Container
ER Evidence Record

NOTE: Refer to [8] and [9].

OCF Open Container Format, as specified in [4].

ODF Open Document Format

NOTE: Refer to [6].

OEBPS Open eBook Publication Structure
TST Time Stamp Token
ZIP Format specified in [5].

4 General Syntax

4.1 Description of main features of Associated Signature Containers

4.1.1 Basic container structure

The ASiC is a data container holding a set of file objects and associated digital signatures and/or time assertions using the ZIP [5] format.

Any ASiC container has an internal structure including:

- a root folder, for all the container content possibly including folders reflecting the content structure; and
- a "META-INF" folder, in the root folder, for files containing metadata about the content, including associated signature or time assertion files.

NOTE: The detached signatures or time assertions are applied in such a way that the integrity of the data is not broken when the files are extracted from the ZIP container. Hence, the signatures and time assertions used in ASiC can be verified against the file objects to which they apply when outside the container structure (for example when placed in local storage).

4.1.2 Container types

Signatures and time assertions within ASiC containers are present within signature or time assertion files.

A signature file can contain either:

- a detached CAdES signature instance, which contains one or more parallel signatures. Each CAdES signature can be individually counter-signed; or
- one or more XAdES signatures. Each XAdES signatures can be individually counter-signed.

A time assertion file can contain either:

- one time-stamp token conformant to IETF RFC 3161 [3] (which can be profiled as specified in ETSI EN 319 422 [i.7]); or
- one Evidence Record.

The present document defines two types of containers.

The first type is ASiC Simple (ASiC-S) that associates one single file object with either:

- one signature file; or
- one time assertion file.

This type of container can also include a file named "mimetype" specifying the media type.

This type of container allows to add at a later time additional signatures signing the aforementioned file object and additional ASiCArchiveManifest files to protect long term time-stamp tokens.

The second type is ASiC Extended (ASiC-E), a container that associates one or more file objects with either:

- one or more XAdES signatures present within one or more signature files and optionally one or more ERS within one or more time assertion files; or
- one or more CAdES signatures present within one or more signature files and/or one or more time assertions within one or more time assertion files.

Each signature is associated with all or part of the files in the container.

It is possible to add signature files, time assertion files and data files to an ASiC-E container. The additional signature and time assertion files can apply to the same set of files or a different set, without invalidating previously applied signatures or time assertions. Later signatures can also sign signatures applied previously.

NOTE: CAdES and XAdES Archive Time-stamp attributes do not guarantee long term validation of signer files referenced using `ASiCManifest` and `ds:Manifest`.

4.2 General requirements

1) The container format shall comply with the ZIP [5] specification.

2) ZIP [5] limitations:

   a) ASiC containers shall not use the multiple volumes split feature.

   b) File names and comments shall be UNICODE UTF-8 encoded.

   c) Only no compression or the Flate compression method specified in IETF RFC 1951 [10] based on the public-domain zlib/deflate compression method should be used; therefore, according to the ZIP specification [5] only 0 ("stored") or 8 ("deflated") values should be used as ZIP compression method.

3) At least one container type specified in clause 4.3 or 4.4 shall be supported.

4.3 Associated Signature Container Simple (ASiC-S)

4.3.1 Introduction

This clause defines the Associated Signature Container Simple (ASiC-S) that associates one data file with either:

- one signature file containaing one or more detached digital signature(s) that apply to it; or
- one time-assertion file containing a time assertion that apply to it.

Three ASiC-S container types are defined:

1) ASiC-S with XAdES: the data file is associated with signature(s) in XAdES format.

2) ASiC-E with CAdES: the data file is associated with signature(s) in CAdES format.

3) ASiC-E with time assertions: the data file is associated with a time assertion.

4.3.2 General Requirements for ASiC-S

The ASiC-S container shall comply with clause 4.2 and with the file structure specified in clause 4.3.3.2 to bind the constitutive files into a single container file.

The signed file object can be itself a container, for example ZIP, OCF, ODF or another ASiC. In this case the inner container is associated with one or more signatures or a time assertion that applies to it.

In case of signing a ZIP container, the file level comment may be used to specify the media type of each file with the value "mimetype= " followed by its media type.

Examples of the use of ASiC-S are given in clause B.1.

4.3.3 Detailed format for ASiC-S

4.3.3.1 Media type identification

1) In case the "mimetype" file defined in clause 4.3.3.2 point 1) is present, the media type shall be either:

   a) "application/vnd.etsi.asic-s+zip" if one of the following cases is verified:

      i) the file extension is as specified in item 2) c) of the present clause;

      ii) no specific media type is associated to the signed file object;

   b) the media type associated to the signed file object in all the other cases.

2) The container file extension shall be:

   a) ".asics";