



SLOVENSKI STANDARD
SIST EN 319 162-2 V1.1.1:2016
01-julij-2016

**Elektronski podpisi in infrastruktura (ESI) - Pripadajoči vsebniki podpisov (ASiC) -
2. del: Dodatni vsebniki ASiC**

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Ta slovenski standard je istoveten z: **ETSI EN 319 162-2 V1.1.1 (2016-04)**

SIST EN 319 162-2 V1.1.1:2016
<https://standards.iteh.ai/catalog/standards/sist/91a60012-0292-46a2-8db1-80a4453fb807/sist-en-319-162-2-v1-1-1-2016>

ICS:

35.040.01	Kodiranje informacij na splošno	Information coding in general
-----------	---------------------------------	-------------------------------

SIST EN 319 162-2 V1.1.1:2016	en
--------------------------------------	-----------

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 319 162-2 V1.1.1:2016

<https://standards.iteh.ai/catalog/standards/sist/9fa600f2-0292-46a2-8db1-80a4453fb807/sist-en-319-162-2-v1-1-1-2016>

ETSI EN 319 162-2 V1.1.1 (2016-04)



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

[SIST EN 319 162-2 V1.1.1:2016](https://standards.iteh.ai/catalog/standards/sist/9fa600f2-0292-46a2-8db1-80a4453fb807/sist-en-319-162-2-v1-1-1-2016)

<https://standards.iteh.ai/catalog/standards/sist/9fa600f2-0292-46a2-8db1-80a4453fb807/sist-en-319-162-2-v1-1-1-2016>

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 319 162-2 V1.1.1:2016

<https://standards.iteh.ai/catalog/standards/sist/9fa600f2-0292-46a2-8db1-80a4453fb807/sist-en-319-162-2-v1-1-1-2016>
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

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

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>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

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".

National transposition dates	
Date of adoption of this EN:	25 April 2016
Date of latest announcement of this EN (doa):	31 July 2016
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 January 2017
Date of withdrawal of any conflicting National Standard (dow):	31 January 2017

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 [1.7] 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 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.

- [i.1] Application Note: "APPNOTE.TXT - .ZIP File Format Specification", PKWARE® Inc., September 2012.

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

- [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);
- 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).

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN 319 162-2 V1.1.1:2016](https://standards.iteh.ai/catalog/standards/sist/9fa600f2-0292-46a2-8db1-80a4453fb807/sist-en-319-162-2-v1-1-1-2016)

<https://standards.iteh.ai/catalog/standards/sist/9fa600f2-0292-46a2-8db1-80a4453fb807/sist-en-319-162-2-v1-1-1-2016>