ETSI TS 103 174 V1.2.1 (2012-01)

Technical Specification

Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile

Reference

RTS/ESI-00122

Keywords

ASiC, electronic signature, profile, 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 Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Introduction

TS 102 918 [6] (ASiC henceforth) specifies the use of container structures to bind together one or more signed objects with either advanced electronic signatures or time-stamp tokens into one single digital container. It uses package formats based on ZIP [i.2] and supports the following signature and time-stamp token formats:

- CAdES [1] detached signature(s);
- XAdES [2] detached signature(s);
- RFC 3161 [i.1] time-stamp tokens.

In order to maximise 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 profiles the use of TS 102 918 [6] containers for its use in the context of the "Directive 2006/123/EC [i.3] of the European Parliament and of the Council of 12 December 2006 on services in the internal market" (EU Services Directive henceforth) and any applicable context where qualified signatures are used.

1 Scope

The present document defines a baseline profile for ASiC which corresponds to the minimum basic requirements in the context of the EU Services Directive, and provides the same basic features necessary in this context with the minimal number of options. This is required because there is a clear need for interoperability of AdES signatures, on which ASiC is based, used in electronic documents issued by competent authorities to be interchanged across borders in the context of the EU Services Directive.

The present document defines a profile that specifies elements and properties requirements for an ASiC container.

Clause 2 in the present document contains references to the relevant documents and standards.

Clause 3 includes definitions of relevant terms and abbreviations used in the present document.

Clause 4 provides details on the way that the requirements on both signer and verifier will be presented throughout the present document.

Clauses 5, 6 and 7 specify the requirements for the short-term electronic signatures, that is, requirements for ASiC containers based on BES and EPES forms of XAdES and CAdES. Clause 5 specifies profiling requirements for elements common to all ASiC containers while clauses 6 and 7 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 TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[2] ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[3] ETSI TS 103 173: "Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile".

[4] ETSI TS 103 171: "Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile".

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

[6] ETSI TS 102 918: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)".

[7] 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".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 101 733 [1], TS 101 903 [2], TS 102 918 [6] 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.

long term signatures: signatures that are expected to be verified beyond the signers' certificate expiration date and, possibly, even after the expiration date of the certificate of the signers' certificate-issuing CA

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.

short term signatures: signatures that are to be verified for a period of time that does not go beyond the signers' certificate expiration date

verifier: entity that validates or verifies an electronic signature

The present document makes use of certain key words to signify requirements. Below follows their definitions:

may: Means that a course of action is permissible within the limits of the present document.

shall: Means that the definition is an absolute requirement of the present document. It has to strictly be followed in order to conform to the present document.

should: Means that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required. Implementers may know valid reasons in particular circumstances to ignore this recommendation, but the full implications must be understood and carefully weighed before choosing a different course.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TS 101 733 [1], TS 101 903 [2] and TS 102 918 [6] apply.

4 General requirements

4.1 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.

4.2 Compliance requirements

Profiles in the present document define requirements generator 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 verification.

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 or XAdES 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	Notes / Additional requirements
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.

5 Requirements for ASiC formats

5.1 ASiC conformance

TS 102 918 [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 XAdES	Clause 7.1.2	O	
ASiC-S Time-stamp token	Clause 7.1.3	O	
ASiC-E XAdES	Clause 7.2.1	O	
ASiC-E CAdES	Clause 7.2.2	O	
ASiC-E Time-stamp	Clause 7.2.3	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 TS 102 918 [6] clause(s).

6 Requirements for ASiC-S

6.1 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	

6.2 ASiC-S Signed data object

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

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 requirements:

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

6.3 Requirements for ASiC-S format

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 6.3.1 **shall** apply
META-INF/signature.p7s	Clause 5.2.2 point 3b	O	Clause 6.3.2 **shall** apply
META-INF/signatures.xml	Clause 5.2.2 point 3c	O	Clause 6.3.3 **shall** apply

6.3.1 Requirements for ASiC-S CAdES signature format

Table 9

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

6.3.2 Requirements for ASiC-S XAdES signature format

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

Additional requirements:

a) This protocol element **shall** contain a `<asic:XAdESSignatures>` element as specified in TS 102 918 [6], point 3a.

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

6.3.3 Requirements for ASiC-S Time stamp token format

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

Additional requirements:

a) This protocol element **shall** conform to TS 101 861 [7].

7 Requirements for ASiC-E

7.1 ASiC-E Media type identification

This clause specifies compliance requirements for any ASiC-E type.

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	

7.2 ASiC-E Signed data object

This clause specifies a 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

7.3 Requirements for ASiC-E XAdES

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

7.3.1 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 TS 102 918 [6], point 2.

b) The root element in each signature **shall** contain a `<asic:XAdESSignatures>` element conforming to TS 102 918 [6], clause 6.2.2, point 3a.

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 TS 102 918 [6], point 2).

7.3.2 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, b

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 7.3.1.

b) Manifest.xml **shall** be signed by at least one of the signatures present in the container.

7.4 Requirements for ASiC-E CAdES

This clause specifies a compliance requirements for ASiC-E CAdES.

7.4.1 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 TS 102 918 [6], clause 6.3.2 point 4a.

b) Each CAdES [1] signature specified above **shall** conform to the CAdES baseline profiles [3], clause 5 and all subclauses, except tor clause 5.1.1 where only the detached signature service **shall** be supported.

7.4.2 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

Additional requirements:

a) At least one ASiCManifest **shall** be present.

b) In META-INF folder **shall not** be present any additional data object in addition to what specified in this clause and in clause 7.4.1.

7.5 Requirements for ASiC-E Time stamp token

This clause specifies a compliance requirements for ASiC-E CAdES.

7.5.1 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 TS 102 918 [6], clause 6.3.2, point 4b.

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

7.5.2 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

Additional requirements:

a) At least one ASiCManifest **shall** be present.

b) In META-INF folder **shall not** be present any additional object in addition to what specified in this clause and in clause 7.5.1.

History

Document history		
V1.1.1	September 2011	Publication
V1.2.1	January 2012	Publication