ETSI TS 103 171 V1.1.1 (2011-09)

Technical Specification

**Electronic Signatures and Infrastructures (ESI);
XAdES Baseline Profile**

Reference

DTS/ESI-000091

Keywords

electronic signature, security, profile, XAdES

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

ETSI

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 101 903 [1] (XAdES henceforth) specifies formats for Advanced Electronic Signatures built on XML SIG [2]. That document defines a number of signed and unsigned optional signature properties, resulting in support for a number of variations in the signature contents and powerful processing requirements.

In order to maximise interoperability in communities applying XAdES 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 101 903 [1] signatures for its use in the context of the "Directive 2006/123/EC [i.1] 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 XAdES, 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 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 a XAdES Signature.

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.

Clause 5 specifies the requirements for the short-term electronic signatures, that is, requirements for XAdES-BES and XAdES-EPES forms.

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 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[2] W3C Recommendation W3C-IETF (June 2008): "XML-Signature Syntax and Processing (Second Edition)".

[3] W3C Recommendation W3C-IETF (March 2001): "Canonical XML Version 1.0".

[4] W3C Recommendation W3C-IETF (July 2002): "Exclusive XML Canonicalization".

[5] W3C Recommendation W3C-IETF (May 2008): "Canonical XML Version 1.1".

[6] W3C Recommendation W3C-IETF (November 1999): "XSL Transformations (XSLT) Version 1.0".

[7] W3C Recommendation W3C-IETF (November 2002): "XML-Signature XPath Filter 2.0".

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

[9] ECRYPT II (European Network of Excellence in Cryptology II): "ECRYPT II Yearly Report on Algorithms and Keysizes".

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] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

[i.2] Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

generator: any party which creates, or adds attributes to, a signature

NOTE: This may be the signatory or any party that 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 XAdES [1] and the following apply:

TSL   Trust Status List

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 [8] for guidelines purposes and the latest ECRYPT2 D.SPA.x [9] yearly report for further recommendations, when selecting algorithms and key lengths.

MD5 algorithm **shall not** be used as digest algorithm.

4.2 Compliance requirements

Profiles in the present document define requirements for generators of XAdES signatures [1].

A verifier **shall** be able to accept a XAdES signature containing any elements/properties conformant to XAdES [1], but this profile does not specify any processing requirement on such elements/properties present in the signature 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 XAdES [1] **but not specified in the present document are treated as "O" as above**.

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 the table above 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 it **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 XAdES [1], 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 short-term Electronic Signatures

The present clause specifies compliance requirements for short-term electronic signatures. In consequence it includes requirements for the following forms: XAdES-BES and XAdES-EPES.

Clause 5.1 provides an overview of the XAdES forms profiled in this clause.

Clause 5.2 specifies the method selected for incorporating the qualifying properties to a XAdES signatures conformant with the present document.

Clause 5.3 profiles certain elements defined in XMLSig [2].

Clauses 5.4 and 5.5 profile XAdES-BES and XAdES-EPES forms respectively.

5.1 Profiled XAdES Forms

The present clause provides an overview of the XAdES forms profiled in the present clause.

Table 5

Service / Protocol element	XAdES Reference	Generator requirement	Additional requirements / notes
Service: signature		M	
XAdES-BES	Clause 4.4.1	O	1
XAdES-EPES	Clause 4.4.2	O	2

NOTE 1: Properties leading to XAdES-BES signatures are profiled in clause 5.4.

NOTE 2: Properties leading to XAdES-EPES signatures are profiled in clause 5.5.

5.2   Incorporation of XAdES qualifying properties to the signature

XAdES qualifying properties incorporation to the signature **shall** be direct as specified in [1], clause 6.3.

> NOTE: This means that all the XAdES qualifying properties will remain within one single
> `xades:QualifyingProperties` element, which in turn will be the child of one `ds:Object`
> element within the signature; and that in consequence no
> `xades:QualifyingPropertiesReference` elements will be present.

5.3   Profile of elements defined in XML Signature

5.3.1   Placement of the signing certificate

Table 6

Service / Protocol element	XML SIG [2] Reference	Generator requirement	Additional requirements / notes
`ds:KeyInfo/X509Data/X509Certificate`	Clause 4.4.4	M	a, b

Additional requirement:

a)   The generator **shall** include the signing certificate as content of `ds:KeyInfo/X509Data/X509Certificate` element.

b)   In order to facilitate path building, generators should include in the SignedData.certificate field all certificates not available to verifiers that can be used during path building. In the case of signature based on qualified certificates and whose verification is expected to be based on TSLs, (in conformance with Decision 2009/767/EC [i.2]), the generator **should** include all intermediary certificates forming a chain between the signer certificate and a CA present in the TSL which are not available to verifiers.

> NOTE 1:   A certificate is considered available to the verifier if reliable information about its location is known and allows automated retrieval of the certificate (for instance through an Authority Info Access Extension or equivalent information present in a TSL).

> NOTE 2:   In the general case, different verifiers can have different trust parameters and can validate the signer certificate through different chains. Therefore, generators may not know which certificates will be relevant for path building. However, in practice, such certificates can often clearly be identified. In this case, it is advised that generators include them unless they can be automatically retrieved by verifiers. In the specific case of a signature meant to be validated through TSL, it is advised to include at least the unavailable intermediary certificates up to but not including the CAs present in the TSLs, since the TSL is information that is shared globally by all verifiers.

5.3.2 Canonicalization of `ds:SignedInfo` element

Table 7

Service / Protocol element	Reference	Generator requirement	Additional requirements / notes
Service: canonicalization of `ds:SignedInfo` element		M	a
`ds:CanonicalizationMethod's` Algorithm attribute set to: "http://www.w3.org/2006/12/xml-c14n11"	XML Sig [2] Clause 4.3.1 Can. XML V1.1 [5]	O	1
`ds:CanonicalizationMethod's` Algorithm attribute set to: "http://www.w3.org/2001/10/xml-exc-c14n#"	XML Sig [2] Clause 4.3.1 Ex. Canon. [4]	O	2
`ds:CanonicalizationMethod's` Algorithm attribute set to: "http://www.w3.org/TR/2001/REC-xml-c14n-20010315"	XML Sig [2] Clause 4.3.1 Can. XML V1.0 [3]	O	3
`ds:CanonicalizationMethod's` Algorithm attribute set to: "http://www.w3.org/2006/12/xml-c14n11#WithComments"	XML Sig [2] Clause 4.3.1 Can. XML V1.1 [5]		a, 4, 7
`ds:CanonicalizationMethod's` Algorithm attribute set to: "http://www.w3.org/2001/10/xml-exc-c14n#WithComments"	XML Sig [2] Clause 4.3.1 Ex. Canon. [4]		a, 5, 7
`ds:CanonicalizationMethod's` Algorithm attribute set to: "http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"	XML Sig [2] Clause 4.3.1 Can. XML V1.0 [3]		a, 6, 7

Additional requirement:

   a) The generator **should not** use canonicalization algorithms "with comments".

   NOTE 1: This URI value corresponds to Canonical XML v1.1 (omits comments).

   NOTE 2: This URI value corresponds to Exclusive Canonicalization (omits comments).

   NOTE 3: This URI value corresponds to Canonical XML v1.0 (omits comments).

   NOTE 4: This URI value corresponds to Canonical XML v1.1 (with comments).

   NOTE 5: This URI value corresponds to Exclusive Canonicalization (with comments).

   NOTE 6: This URI value corresponds to Canonical XML v1.0 (with comments).

   NOTE 7: Support of canonicalization algorithms "with comments" is for residual interoperability in the signature verification process.

5.3.3 Profile of `ds:Reference` element

Table 8

Service / Protocol element	XML Sig Reference	Generator requirement	Additional requirements / notes
`ds:Reference`	Clause 4.3.3	M	a, b

Additional requirements:

a) The generator **shall** create as many `ds:Reference` element as signed data objects (each one referencing one of them) plus one `ds:Reference` element referencing xades:SignedProperties element.

b) The `ds:Reference`'s URI attribute referencing signed data objects **may** have as values references that are or are not 'same-document' references as defined in [9], section 4.4.

5.3.4 Transforms within `ds:Reference` element

Table 9

Service / Protocol element	Reference	Generator requirement	Additional requirements / notes
Service: Transforms applicable within `ds:Reference` element		O	a, b
`ds:Transform`'s Algorithm attribute set to: "http://www.w3.org/2000/09/xmldsig#base64"	XML Sig [2] Clause 6.6.2	O	
`ds:Transform`'s Algorithm attribute set to: "http://www.w3.org/TR/1999/REC-xpath-19991116"	XML Sig [2] Clause 6.6.3	O	
`ds:Transform`'s Algorithm attribute set to: "http://www.w3.org/2000/09/xmldsig#enveloped-signature"	XML Sig [2] Clause 6.6.4	O	
`ds:Transform`'s Algorithm attribute set to: "http://www.w3.org/TR/1999/REC-xslt-19991116"	XML Sig [2] Clause 6.6.5 XSLT [6]	O	
`ds:Transform`'s Algorithm attribute set to: "http://www.w3.org/2002/06/xmldsig-filter2"	XPathFilter 2 [7]	O	

Additional requirement:

a) Generator **should** limit the range of transforms used in the signatures to the ones identified in table 9 of the present document.

b) Requirements defined in clause 5.1.3 of the present documentt **shall** apply when `ds:Transform`'s `Algorithm` attribute is set to any of the canonicalization algorithms identifiers mentioned in that clause.

5.4 Profile of elements in Basic XAdES form (XAdES-BES)

5.4.1 Profile of `xades:SigningCertificate` element

Table 10

Service / Protocol element	XAdES Reference	Generator requirement	Additional requirements / notes
`xades:SigningCertificate`	Clause 7.2.2	M	a, 1
`xades:SigningCertificate/CertDigest`	Clause 7.2.2	M	b
`xades:SigningCertificate/IssuerSerial`	Clause 7.2.2	M	c

Additional requirements:

a) The generator **shall not** generate `xades:SigningCertificate`'s URI optional attribute.

b) `xades:SigningCertificate/CertDigest` element **shall** contain the digest value of the signing certificate present within `ds:KeyInfo` element and the identifier of the corresponding digest algorithm.

c) `xades:SigningCertificate/IssuerSerial` element **shall** contain the IssuerSerial of the signing certificate present within `ds:KeyInfo` element.

NOTE: The presence of the signing certificate within ds:KeyInfo ensures a way to locate it (on the basis of digest equality with the value within ds:SigningCertificate/CertDigest) within the signature.

5.4.2   Profile of `xades:SigningTime` element

Table 11

Service / Protocol element	XAdES Reference	Generator requirement	Additional requirements / notes
`xades:SigningTime`	Clause 7.2.1	M	a

Additional requirements:

a) The generator **shall** include the UTC time when the signature was generated as content of this element.

5.4.3   Profile of `xades:DataObjectFormat` element

Table 12

Service / Protocol element	XAdES Reference	Generator requirement	Additional requirements / notes
`xades:DataObjectFormat`	Clause 7.2.5	M	
`xades:DataObjectFormat/Description`	Clause 7.2.5	O	
`xades:DataObjectFormat/ObjectIdentifier`	Clause 7.2.5	O	
`xades:DataObjectFormat/MimeType`	Clause 7.2.5	M	
`xades:DataObjectFormat/Encoding`	Clause 7.2.5	O	
`xades:DataObjectFormat`'s `ObjectReference` attribute	Clause 7.2.5	M	

5.5   Profile of elements in Explicit Policy based Electronic Signature XAdES form (XAdES-EPES)

Table 13

Service / Protocol element	XAdES Reference	Generator requirement	Additional requirements / notes
`xades:SignaturePolicyIdentifier`	Clause 7.2.3	M	

History

Document history		
V1.1.1	September 2011	Publication