SLOVENSKI STANDARD
SIST EN 319 132-1 V1.1.1:2016

01-julij-2016

Elektronski podpisi in infrastruktura (ESI) - Digitalni podpisi XAdES - 1. del: Gradniki in izhodiščni podpisi XAdES

Electronic Signatures and Infrastructures (ESI) - XAdES digital signatures - Part 1: Building blocks and XAdES baseline signatures

Ta slovenski standard je istoveten z: ETSI EN 319 132-1 V1.1.1 (2016-04)

ICS:

35.040.01	Kodiranje informacij na splošno	Information coding in general

SIST EN 319 132-1 V1.1.1:2016 **en**

ETSI EN 319 132-1 V1.1.1 (2016-04)

Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures

Reference
DEN/ESI-0019132-1

Keywords
electronic signature, security, XAdES, XML

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
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

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 (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 1 of a multi-part deliverable covering XAdES digital signatures, as identified below:

Part 1: "Building blocks and XAdES baseline signatures";

Part 2: "Extended XAdES signatures".

Two .xsd files, whose locations are detailed in clauses C.1 and C.2, and which contain XML Schema definitions, are contained in archive en_31913201v010101p0.zip which accompanies the present document.

National transposition dates	
Date of adoption of this EN:	1 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

Electronic commerce has emerged as a frequent way of doing business between companies across local, wide area and global networks. Trust in this way of doing business is essential for the success and continued development of electronic commerce. It is therefore important that companies using this electronic means of doing business have suitable security controls and mechanisms in place to protect their transactions and to ensure trust and confidence with their business partners. In this respect digital signatures are an important security component that can be used to protect information and provide trust in electronic business.

The present document is intended to cover digital signatures 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.1].

The present document can be used for any transaction between an individual and a company, between two companies, between an individual and a governmental body, etc. The present document is independent of any environment. It can be applied to any environment e.g. smart cards, SIM cards, special programs for electronic signatures, etc.

The present document is part of a rationalized framework of standards (see ETSI TR 119 000 [i.10]). ETSI TR 119 100 [i.11] provides guidance on how to use the present document within the aforementioned framework.

1 Scope

The present document specifies XAdES digital signatures. XAdES signatures build on XML digital signatures [1], by incorporation of signed and unsigned qualifying properties, which fulfil certain common requirements (such as the long term validity of digital signatures, for instance) in a number of use cases.

The present document specifies XML Schema definitions for the aforementioned qualifying properties as well as mechanisms for incorporating them into XAdES signatures.

The present document specifies formats for XAdES baseline signatures, 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 of digital signatures used in electronic documents.

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

Procedures for creation, augmentation, and validation of XAdES digital signatures are out of scope and specified in ETSI EN 319 102-1 [i.6]. Guidance on creation, augmentation and validation of XAdES digital signatures including the usage of the different properties defined in the present document is provided in ETSI TR 119 100 [i.11].

The present document aims at supporting electronic signatures in different regulatory frameworks.

NOTE: Specifically but not exclusively, XAdES digital signatures specified in the present document aim at supporting electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, and qualified electronic seals as per Regulation (EU) No 910/2014 [i.1].

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] W3C Recommendation (11 April 2013): "XML Signature Syntax and Processing. Version 1.1".

[2] W3C Recommendation Part 1 (28 October 2004): "XML Schema Part 1: Structures Second Edition".

[3] W3C Recommendation Part 2 (28 October 2004): "XML Schema Part 2: Datatypes Second Edition".

[4] Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[5] W3C Recommendation (26 November 2008): "Extensible Markup Language (XML) 1.0".

[6] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

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

[8] IETF RFC 3061: "A URN Namespace of Object Identifiers".

[9] W3C Recommendation (15 March 2001): "Canonical XML Version 1.0".

[10] W3C Recommendation (18 July 2002): "Exclusive XML Canonicalization Version 1.0".

[11] W3C Recommendation (2 May 2008): "Canonical XML Version 1.1".

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

[13] W3C Recommendation (8 November 2002): "XML-Signature XPath Filter 2.0".

[14] ISO/IEC 29500-2:2012: "Information technology -- Document description and processing languages -- Office Open XML File Formats -- Part 2: Open Packaging Conventions".

[15] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

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

[17] IETF RFC 5035: "Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility".

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] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.08.2014, p. 73-114.

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

[i.3] ETSI TS 103 171: "Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile".

[i.4] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.5] Commission Decision 2009/767/EC of 16 October 2009 amended by CD 2010/425/EU of 28 July 2010, 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.

[i.6] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[i.7] ETSI TS 119 172-1: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents".

[i.8] IETF RFC 6931: "Additional XML Security Uniform Resource Identifiers (URIs)".

[i.9] OASIS Standard: "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0".

[i.10] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview".

[i.11] ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Business Driven Guidance for Signature Creation and Validation".

[i.12] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.13] ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management".

[i.14] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.15] IETF RFC 4998: "Evidence Record Syntax (ERS)".

[i.16] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

3 Definitions, abbreviations and terminology

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TR 119 001 [i.4] and the following apply:

attribute certificate: data structure, digitally signed by an attribute authority, that binds some attribute values with identification information about its holder

certificate revocation list: signed list indicating a set of certificates that are no longer considered valid by the certificate issuer

data object: actual binary/octet data being operated on (transformed, digested, or signed) by an application

NOTE: This definition is part of the definition of this term within XMLDSIG [1].

digital signature: data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

digital signature value: result of cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

electronic time-stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time

NOTE: In the case of IETF RFC 3161 [7] protocol, updated by IETF RFC 5816 [16], the electronic time-stamp is referring to the `timeStampToken` field within the `TimeStampResp` element (the TSA's response returned to the requesting client).

legacy XAdES 101 903 signature: digital signature generated according to ETSI TS 101 903 [i.2]

legacy XAdES baseline signature: digital signature generated according to ETSI TS 103 171 [i.3]

legacy XAdES signature: legacy XAdES 101 903 signature or legacy XAdES baseline signature

message imprint: digest value of the data that is going to be time-stamped

NOTE: In the case of electronic time-stamps compliant with IETF RFC 3161 [7], as updated by IETF RFC 5816 [16], it corresponds to the digest value incorporated into the `hashedMessage` field of `MessageImprint` type.

signature augmentation policy: set of rules, applicable to one or more digital signatures, that defines the technical and procedural requirements for their augmentation, in order to meet a particular business need, and under which the digital signature(s) can be determined to be conformant

NOTE: This covers collection of information and creation of new structures that allows performing, on the long term, validations of a signature.

signature creation policy: set of rules, applicable to one or more digital signatures, that defines the technical and procedural requirements for their creation, in order to meet a particular business need, and under which the digital signature(s) can be determined to be conformant

signature policy: signature creation policy, signature augmentation policy, signature validation policy or any combination thereof, applicable to the same signature or set of signatures

signature validation policy: set of rules, applicable to one or more digital signatures, that defines the technical and procedural requirements for their validation, in order to meet a particular business need, and under which the digital signature(s) can be determined to be valid

trust anchor: entity that is trusted by a relying party and used for validating certificates in certification paths

validation data: data that is used to validate a digital signature

XAdES signature: digital signature that satisfies the requirements specified within the present document or ETSI EN 319 132-2 [i.16]

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ASN.1	Abstract Syntax Notation 1
BER	Basic Encoding Rules
CA	Certification Authority
CD	European Commission Decission
CER	Canonical Encoding Rules
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
HTTP	Hyper Text Transfer Protocol
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
PER	Packed Encoding Rules
PKI	Public Key Infrastructure
SAML	Security Assertion Markup Language
SIM	Subscriber Identity Module
SPO	Service Provision Option
TSA	Time-Stamping Authorities
TSL	Trust-service Status List
TSP	Trusted Service Providers
TSU	Time-Stamping Unit
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UTC	Coordinated Universal Time
XER	XML Encoding Rules
XML	eXtensible Markup Language
XMLDSIG	eXtensible Markup Language Digital SIGnature
XSLT	eXtensible Stylesheet Language Transformations

3.3 Terminology

The present document uses the term "qualifying property" for denoting a XML element that qualifies the signature, the signed data objects, or the signer.

The present document uses the term "element" exclusively for denoting XML elements.

The present document defines new XML elements that are containers of qualifying properties (for instance `QualifyingProperties`, `SignedProperties`, or `UnsignedProperties`). The present document uses the terms "element" or "container" when refers to them.

The present document uses the term "attribute" for denoting either XML attributes of XML elements or for denoting attributes owned by the signer (as in clause 5.2.6 for instance). Consequently, a qualifying property, being a XML element, can have (XML) attributes.

The present document uses the term "child element" exclusively in the context of XML content, for denoting an XML element that is a child element of another XML element.

The present document uses the term "XAdES components" for denoting any XAdES signature's element, and any XAdES qualifying property incorporated into the XAdES signature.

4 General Syntax

4.1 General requirements

XAdES signatures shall build on XMLDSIG as specified in [1] by incorporation of XML [5] signed and unsigned qualifying properties. These qualifying properties shall be instances of XML types using the XML Schema syntax and structures specified in [2] and [3].

The present clause defines the namespaces used in the aforementioned XML schema definitions.

The present clause also defines the types for the containers of the qualifying properties, and specifies the mechanisms for incorporating them into the XAdES signature.

4.2 XML Namespaces

The present document uses the URI namespaces listed below:

- http://uri.etsi.org/01903/v1.3.2#
- http://uri.etsi.org/01903/v1.4.1#
- http://www.w3.org/2000/09/xmldsig#
- http://www.w3.org/2001/XMLSchema

ETSI defines two XML Schema files for the present specification, namely: "XAdES01903v132-201601.xsd", and "XAdES01903v141-201601.xsd". See annex C for details on their locations.

Table 1 shows two prefixes that refer to the same namespaces in the two XML Schema files. These prefixes are used throughout the present document to refer to specific elements in the XAdES signature.

Table 1: Namespaces with constant prefixes

XML Namespace URI	Prefix
http://www.w3.org/2000/09/xmldsig#	ds
http://www.w3.org/2001/XMLSchema	xsd

NOTE 1: The present document uses other prefixes in the excerpts of the XML Schema files for referencing XML elements. The preambles of the corresponding XML Schema files clearly identify the namespace corresponding to each prefix.

Below follows a copy of the `xsd:schema` element of the XML Schema file "XAdES01903v132-201601.xsd", whose location is detailed in clause C.1, and that defines the namespace whose URI is http://uri.etsi.org/01903/v1.3.2#.

```
<xsd:schema targetNamespace="http://uri.etsi.org/01903/v1.3.2#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns="http://uri.etsi.org/01903/v1.3.2#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
```

Below follows a copy of the `xsd:schema` element of the XML Schema file "XAdES01903v141-201601.xsd", whose location is detailed in clause C.2, and that defines the namespace whose URI is http://uri.etsi.org/01903/v1.4.1#.

```
<xsd:schema targetNamespace="http://uri.etsi.org/01903/v1.4.1#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns="http://uri.etsi.org/01903/v1.4.1#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xades="http://uri.etsi.org/01903/v1.3.2#"
elementFormDefault="qualified">
```

NOTE 2: The http://uri.etsi.org/01903/v1.3.2# URI was defined by ETSI TS 101 903 (V1.3.2) [i.2]. Most of the XML elements and types used by XAdES signatures were defined in this namespace. The present document adds new types and elements to this namespace. Additionally, ETSI TS 101 903 (V1.4.1) [i.2] defined http://uri.etsi.org/01903/v1.4.1# URI, where new types and elements were defined. The present document also adds new types and elements to this namespace.

NOTE 3: The present document is accompanied by two xml schema files, whose access details are given in annex C.

In case of discrepancies between the xml schema excerpts provided in the present document and the XML Schema files, the XML Schema files shall take precedence.

4.3 The `QualifyingProperties` container

4.3.1 Semantics and syntax

Semantics

The `QualifyingProperties` element shall act as a container element for all the qualifying information that is added to an XML signature.

The qualifying properties shall be split into qualifying properties that are cryptographically bound to (i.e. signed by) the XML signature, and qualifying properties that are not cryptographically bound to (i.e. not signed by) the XML signature.

Syntax

The `QualifyingProperties` element shall be defined as in XML Schema file "XAdES01903v132-201601.xsd", whose location is detailed in clause C.1, and is copied below for information.


```
<!-- targetNamespace="http://uri.etsi.org/01903/v1.3.2#" -->

<xsd:element name="QualifyingProperties" type="QualifyingPropertiesType"/>

<xsd:complexType name="QualifyingPropertiesType">
    <xsd:sequence>
        <xsd:element ref="SignedProperties" minOccurs="0"/>
        <xsd:element ref="UnsignedProperties" minOccurs="0"/>
    </xsd:sequence>
    <xsd:attribute name="Target" type="xsd:anyURI" use="required"/>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

The `Target` attribute shall refer to the `Id` attribute of the corresponding `ds:Signature`.

The value of `Target` attribute shall be a URI [12] with a bare-name XPointer fragment. If the XAdES signature envelops the `QualifyingProperties` element, its not-fragment part shall be empty. Otherwise, its not-fragment part needs not be empty.

The `Id` attribute shall be used to reference the `QualifyingProperties` container.

A XAdES signature shall not incorporate empty `QualifyingProperties` elements.

4.3.2 The `SignedProperties` container

Semantics

The `SignedProperties` element shall contain qualifying properties that are collectively signed by the XML signature. In consequence one of the `ds:Reference` children of `ds:SignedInfo` element in the XAdES signature shall be generated in a way that ensures that the `SignedProperties` element contributes to the digital signature value computation.

The SignedProperties element may contain qualifying properties that qualify the XML signature itself, the signer, or some of the signed data objects.

Syntax

The SignedProperties element shall be defined as in XML Schema file "XAdES01903v132-201601.xsd", whose location is detailed in clause C.1, and is copied below for information.

```
<!-- targetNamespace="http://uri.etsi.org/01903/v1.3.2#" -->

<xsd:element name="SignedProperties" type="SignedPropertiesType" />

<xsd:complexType name="SignedPropertiesType">
    <xsd:sequence>
        <xsd:element ref="SignedSignatureProperties"  minOccurs="0"/>
        <xsd:element ref="SignedDataObjectProperties"  minOccurs="0"/>
    </xsd:sequence>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

The SignedSignatureProperties element shall contain qualifying properties that qualify the XML signature itself or the signer. This element is specified in clause 4.3.4.

The SignedDataObjectProperties element shall contain qualifying properties that qualify some of the signed data objects. This element is specified in clause 4.3.5.

The Id attribute shall be used to reference the SignedProperties element.

A XAdES signature shall not incorporate empty SignedProperties element.

4.3.3 The UnsignedProperties container

Semantics

The UnsignedProperties element shall contain qualifying properties that are not signed by the XML signature.

The UnsignedProperties element may contain qualifying properties that qualify the XML signature itself, the signer, or some of the signed data objects.

Syntax

The UnsignedProperties element shall be defined as in XML Schema file "XAdES01903v132-201601.xsd", whose location is detailed in clause C.1, and is copied below for information.

```
<!-- targetNamespace="http://uri.etsi.org/01903/v1.3.2#" -->

<xsd:element name="UnsignedProperties" type="UnsignedPropertiesType" />

<xsd:complexType name="UnsignedPropertiesType">
    <xsd:sequence>
        <xsd:element ref="UnsignedSignatureProperties"  minOccurs="0"/>
        <xsd:element ref="UnsignedDataObjectProperties"  minOccurs="0"/>
    </xsd:sequence>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

The UnsignedSignatureProperties element shall contain qualifying properties that qualify the XML signature itself or the signer. This element is specified in clause 4.3.6.

The UnsignedDataObjectProperties element shall contain qualifying properties that qualify some of the signed data objects. This element is specified in clause 4.3.7.

The Id attribute shall be used to reference the UnsignedProperties element.

A XAdES signature shall not incorporate empty UnsignedProperties elements.