SLOVENSKI STANDARD
SIST EN 319 132-2 V1.1.1:2016

01-julij-2016

Elektronski podpisi in infrastruktura (ESI) - Digitalni podpisi XAdES - 2. del: Razširjeni podpisi XAdES

Electronic Signatures and Infrastructures (ESI) - XAdES digital signatures - Part 2: Extended XAdES signatures

Ta slovenski standard je istoveten z: ETSI EN 319 132-2 V1.1.1 (2016-04)

ICS:

35.040.01	Kodiranje informacij na splošno	Information coding in general

SIST EN 319 132-2 V1.1.1:2016 **en**

ETSI EN 319 132-2 V1.1.1 (2016-04)

Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures

Reference
DEN/ESI-0019132-2

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 2 of a multi-part deliverable covering XAdES digital signatures. Full details of the entire series can be found in part 1 [1].

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, GSM 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.5]). See ETSI TR 119 100 [i.6] for getting guidance on how to use the present document within the aforementioned framework.

1 Scope

The present document specifies XAdES digital signatures. XAdES signatures are built on XML digital signatures [i.4], 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 a number of XAdES signature levels, 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. These XAdES extended signatures offer a higher degree of optionality than the XAdES baseline signatures specified ETSI EN 319 132-1 [1].

Procedures for creation, augmentation, and validation of XAdES digital signatures are out of scope and specified in ETSI EN 319 102-1 [i.7]. Guidance on creation, augmentation and validation of XAdES digital signatures is provided including the usage of the different properties is provided in ETSI TR 119 100 [i.6].

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

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

[i.3] ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[i.4] W3C Recommendation: "XML-Signature Syntax and Processing. Version 1.1".

[i.5] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview".

[i.6] ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Business Driven Guidance for Signature Creation and Validation".

[i.7] 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.8] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.9] IETF RFC 6931: "Additional XML Security Uniform Resource Identifiers (URIs)".

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.2] and ETSI EN 319 132-1 [1] apply.

3.2 Abbreviations

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

EU	European Union
GSM	Global System for Mobile communications
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
SIM	Subscriber Identity Module
SPO	Service Provision Option
TSA	Time-Stamping Authorities
URI	Uniform Resource Identifier
XML	eXtensible Markup Language

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 uses the terms "container" or "element" for denoting XML elements that are containers of qualifying properties (for instance `QualifyingProperties`, `SignedProperties`, or `UnsignedProperties`).

The present document uses the term "attribute" exclusively for denoting XML attributes of XML elements. 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.

4 Additional XAdES levels without references to validation data

4.1 Overview

The present document specifies a number of additional levels for XAdES.

Each level is generated by a different combination of the XAdES qualifying properties specified in ETSI EN 319 132-1 [1], and incorporated to the XAdES signatures using one of the two mechanisms (direct or indirect incorporation) described in clause 4.4 of ETSI EN 319 132-1 [1].

NOTE 1: ETSI TR 119 100 [i.6] provides a description on the life-cycle of a signature and the rationales on which level is suitable in which situation.

NOTE 2: Clause 4.3 defines four XAdES levels namely the XAdES-E-BES, XAdES-E-EPES, XAdES-E-T, and XAdES-E-A built on XAdES-E-T. Normative Annex A defines levels of XAdES signatures incorporating qualifying properties that encapsulate references to validation data and qualifying properties that encapsulate time-stamp tokens on them.

NOTE 3: Names of XML elements in the namespace whose URI is http://www.w3.org/2000/09/xmldsig# will be preceded in the present document by prefix `ds`. No other prefixes will be used in the present document for identifying XAdES containers and/or XAdES qualifying properties, as their usage is not required for unambiguously identifying the referenced XAdES container or XAdES qualifying property, regardless of the namespace where they have been defined.

NOTE 4: The requirements on the presence and cardinality of the attributes for each XAdES signature level are expressed in tables whose formats and semantics are as specified in clause 6.2.2 of ETSI EN 319 132-1 [1].

4.2 General requirements

XAdES qualifying properties deprecated by ETSI EN 319 132-1 [1] (see Annex D) do not appear in the tables. Their cardinality shall be 0 and consequently, they shall not be incorporated in the signature.

Any XAdES signature of any of the levels specified in the present document shall contain at least one of the following components with the specified contents:

- The `SigningCertificateV2` signed qualifying property.
- The `ds:KeyInfo` element. If the `SigningCertificateV2` qualifying property is incorporated to the signature, no restrictions apply to this element. Otherwise, then the following restrictions apply:
  - the `ds:KeyInfo` element shall include a `ds:X509Data` containing the signing certificate;
  - the `ds:KeyInfo` element may also contain other certificates;
  - the `ds:SignedInfo` element shall contain a `ds:Reference` element that ensures that the signing certificate is actually signed.

NOTE 1: Signing the whole `ds:KeyInfo` locks the element: any addition of a certificate or validation data would make signature validation fail. Applications can, alternatively, use XPath transforms for signing at least the signing certificate, leaving the `ds:KeyInfo` element open for addition of new data after signing.

The algorithms and key lengths used to generate and augment digital signatures should be as specified in ETSI TS 119 312 [i.8].

NOTE 2: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.8] can be superseded by national recommendations.

NOTE 3: IETF RFC 6931 [i.9]defines a set of additional XML security URIs, which complement those ones defined in XMLDSIG [i.4].

4.3 XAdES-E-BES, XAdES-E-EPES, XAdES-E-T signatures, and XAdES-E-A signatures built on XAdES-E-T signatures

XAdES-E-BES, XAdES-E-EPES, XAdES-E-T, and XAdES-E-A built on XAdES-E-T signatures shall be XAdES signatures whose qualifying properties satisfy the requirements specified in the present clause.

XAdES-E-EPES signatures are built on XAdES-E-BES signatures by adding one `SignaturePolicyIdentifier` qualifying property.

XAdES-E-T signatures are built on XAdES-E-BES and XAdES-E-EPES signatures by adding one or more `SignatureTimeStamp` qualifying properties.

XAdES-E-A signatures are built on XAdES-E-T, XAdES-E-C, XAdES-E-X (of Type 1 and of Type 2), XAdES-E-X-Long, and XAdES-E-X-L (of Type 1 and of Type 2) signatures.

Annex A specifies XAdES-E-C, XAdES-E-X (of Type 1 and of Type 2), XAdES-E-X-Long, and XAdES-E-X-L (of Type 1 and of Type 2) signatures, and XAdES-E-A signatures built on them.