ICS 35.240.30 SLOVENSKÁ TECHNICKÁ NORMA Február 2017

STN	**Elektronické podpisy a infraštruktúry (ESI). Digitálne podpisy vo formáte XAdES. Časť 1: Stavebné bloky a základné podpisy vo formáte XAdES.**	**STN EN 319 132-1 V1.1.1** 87 9132

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

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 01/17

Obsahuje: EN 319 132-1 V1.1.1:2016

124089

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

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".