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

Intellectual Property Rights ................................................................................................................................ 4
Foreword ............................................................................................................................................................. 4
Modal verbs terminology .................................................................................................................................... 4
Introduction ........................................................................................................................................................ 4
1 Scope ........................................................................................................................................................... 6
2 References ................................................................................................................................................ 6
   2.1 Normative references ......................................................................................................................... 6
   2.2 Informative references ......................................................................................................................... 6
3 Definitions, abbreviations and terminology ............................................................................................. 7
   3.1 Definitions ............................................................................................................................................ 7
   3.2 Abbreviations ...................................................................................................................................... 7
   3.3 Terminology ......................................................................................................................................... 7
4 Additional XAdES levels without references to validation data .............................................................. 8
   4.1 Overview ............................................................................................................................................. 8
   4.2 General requirements ......................................................................................................................... 8
   4.3 XAdES-E-BES, XAdES-E-EPES, XAdES-E-T signatures, and XAdES-E-A signatures built on XAdES-E-T signatures ......................................................................................................................... 9
5 Legacy signatures ................................................................................................................................... 13

Annex A (normative): XAdES signature levels with references to validation data ....................................... 14
History .............................................................................................................................................................. 20
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].

<table>
<thead>
<tr>
<th>National transposition dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of adoption of this EN:</td>
</tr>
<tr>
<td>Date of latest announcement of this EN (doa):</td>
</tr>
<tr>
<td>Date of latest publication of new National Standard</td>
</tr>
<tr>
<td>or endorsement of this EN (dop/e):</td>
</tr>
<tr>
<td>Date of withdrawal of any conflicting National Standard</td>
</tr>
<tr>
<td>(dow):</td>
</tr>
</tbody>
</table>

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 [1.4], 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 [1.7]. 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 [1.6].

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


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.


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.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)”.

ETSI