ETSI EN 319 422 V1.1.1 (2016-03)

EUROPEAN STANDARD

Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

Reference

DEN/ESI-0019422

Keywords

electronic signature, security, time-stamping,
trust services

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 was previously published as ETSI TS 101 861 [i.1].

National transposition dates	
Date of adoption of this EN:	22 February 2016
Date of latest announcement of this EN (doa):	31 May 2016
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	30 November 2016
Date of withdrawal of any conflicting National Standard (dow):	30 june 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

The present document is aiming to meet the general requirements of the international community to provide trust and confidence in electronic transactions including, amongst others, applicable requirements from Regulation (EU) No 910/2014 [i.2].

Time-stamping is critical for digital signatures in order to know whether the digital signature was affixed during the validity period of the certificate. One method of assuring the signing time is to affix a time-stamp bound to the signature as defined in IETF RFC 3161 [1].

IETF RFC 3161 [1] defines a time-stamp protocol and a time-stamp token format. The present document limits the number of options by placing some additional constraints.

1 Scope

The present document defines a profile for the time-stamping protocol and the time-stamp token defined in IETF RFC 3161 [1] including optional ESSCertIDv2 update in IETF RFC 5816 [4].

It defines what a time-stamping client supports and what a time-stamping server supports.

Time-stamp validation is out of scope and is defined in ETSI EN 319 102 [i.4].

Annex C defines media type and file-extension for time-stamp tokens.

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

[2] ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons".

[3] ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons".

[4] IETF RFC 5816: "ESSCertIDV2 update to RFC 3161".

[5] IETF RFC 7230 to RFC 7235: "Hypertext Transfer Protocol -- (HTTP/1.1)".

[6] IETF RFC 2818: "HTTP Over TLS".

[7] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

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] ETSI TS 101 861: "Electronic Signatures and Infrastructures (ESI); Time stamping profile".

[i.2] 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.

[i.3] IETF RFC 3739: "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile".