

STN	Elektronické podpisy a infraštruktúry (ESI). Všeobecné požiadavky politiky pre poskytovateľov dôveryhodných služieb.	STN EN 319 401 V2.1.1 87 9401
------------	---	---

Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

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 319 401 V2.1.1:2016

124181

Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, 2017
Podľa zákona č. 264/1999 Z. z. v znení neskorších predpisov sa môžu slovenské technické normy
rozmnžovať a rozširovať iba so súhlasom Úradu pre normalizáciu, metrológiu a skúšobníctvo SR.

ETSI EN 319 401 V2.1.1 (2016-02)



Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

Reference

REN/ESI-0019401V211

Keywordselectronic signature, provider, security,
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/CommitteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and
of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

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 and abbreviations.....	7
3.1 Definitions.....	7
3.2 Abbreviations	7
4 Overview	8
5 Risk Assessment	8
6 Policies and practices	8
6.1 Trust Service Practice statement	8
6.2 Terms and Conditions	9
6.3 Information security policy	9
7 TSP management and operation.....	10
7.1 Internal organization.....	10
7.1.1 Organization reliability	10
7.1.2 Segregation of duties	10
7.2 Human resources	10
7.3 Asset management.....	12
7.3.1 General requirements.....	12
7.3.2 Media handling	12
7.4 Access control	12
7.5 Cryptographic controls	12
7.6 Physical and environmental security	13
7.7 Operation security	13
7.8 Network security	14
7.9 Incident management	15
7.10 Collection of evidence	16
7.11 Business continuity management	16
7.12 TSP termination and termination plans	16
7.13 Compliance.....	17
Annex A (informative): Bibliography.....	18
History	19

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).

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

Building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of security, makes consumers, businesses and administrations hesitate to carry out transactions electronically and to adopt new services. Trust service providers are often an essential element to establish trust between parties transacting electronically, particularly in open public networks, and can be used, for example, to provide trusted identity information and help establish secure communications between transacting parties. Examples of such trust service providers are issuers of public key certificates, time-stamping service providers, providers of remote electronic signature generation or validation services.

For participants of electronic commerce to have confidence in the security of these trust services they need to have confidence that the trust service providers (TSPs) have established a set of procedures, processes and security measures in order to minimize the operational and financial threats and risks associated.

The present document specifies baseline policy requirements on the operation and management practices of TSP regardless the service they provide. Other standards, addressing particular type of trust service, can build on the present document to identify supplement requirements for particular type of trust service.

The present document is aiming to meet the general requirements to provide trust and confidence in electronic transactions including, amongst others, applicable requirements from Regulation (EU) No 910/2014 [i.2] and those from CA Browser Forum [i.4].

EXAMPLE: ETSI EN 319 411-2 [i.11] annex A describes the application of the present document to the requirements of Regulation No 910/2014 [i.2] requirements for TSPs issuing EU qualified certificates.

1 Scope

The present document specifies general policy requirements relating to trust service providers (TSPs) that are independent of the type of TSP. It defines policy requirements on the operation and management practices of TSPs.

Other specifications refine and extend these requirements as applicable to particular forms of TSP. The present document does not specify how the requirements identified can be assessed by an independent party, including requirements for information to be made available to such independent assessors, or requirements on such assessors.

NOTE: See ETSI EN 319 403 [i.6]: "Electronic Signatures and Infrastructures (ESI); Requirements for conformity assessment bodies assessing Trust Service Providers".

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 reference 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.

Not applicable.

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 reference 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] | Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. |
| [i.2] | Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. |
| [i.3] | ISO/IEC 27002:2013: "Information technology - Security techniques - Code of practice for information security management". |
| [i.4] | CA/Browser Forum: "Guidelines for the issuance and management of extended validation certificates". |
| [i.5] | ISO/IEC 27005:2011: "Information technology - Security techniques - Information security risk management". |
| [i.6] | ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers". |

- [i.7] CA/Browser Forum: "Network and certificate system security requirements".
 - [i.8] Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".
 - [i.9] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates; Part 1: General requirements".
 - [i.10] ETSI EN 301 549: "Accessibility requirements suitable for public procurement of ICT products and services in Europe".
 - [i.11] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".
-

koniec náhľadu – text ďalej pokračuje v platenej verzii STN