

STN	Elektronické podpisy a dôveryhodné infraštruktúry (ESI) Obecné požiadavky politiky pre poskytovateľov dôveryhodných služieb	STN EN 319 401 V3.1.1 87 9401
------------	--	---

Electronic Signatures and Trust 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. 10/24

Obsahuje: EN 319 401 V3.1.1:2024

ETSI EN 319 401 V3.1.1 (2024-06)



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

Reference

REN/ESI-0019401v311

Keywords

electronic 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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:

<https://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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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>

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

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.

© ETSI 2024.
All rights reserved.

Contents

Intellectual Property Rights	5
Foreword.....	5
Modal verbs terminology.....	5
Introduction	6
1 Scope	7
2 References	7
2.1 Normative references	7
2.2 Informative references.....	7
3 Definition of terms, symbols, abbreviations and notation.....	9
3.1 Terms.....	9
3.2 Symbols.....	11
3.3 Abbreviations	11
3.4 Notation.....	12
4 Overview	12
5 Risk Assessment.....	13
6 Policies and practices	13
6.1 Trust Service Practice statement	13
6.2 Terms and Conditions	14
6.3 Information security policy	14
7 TSP management and operation.....	15
7.1 Internal organization.....	15
7.1.1 Organization reliability	15
7.1.2 Segregation of duties	16
7.2 Human resources	16
7.3 Asset management.....	17
7.3.1 General requirements.....	17
7.3.2 Assets inventory and classification.....	17
7.3.3 Storage media handling	18
7.4 Access control	18
7.5 Cryptographic controls	19
7.6 Physical and environmental security	19
7.7 Operation security	20
7.8 Network security	21
7.9 Vulnerabilities and Incident management	22
7.9.1 Monitoring and logging	22
7.9.2 Incident response	22
7.9.3 Reporting	23
7.9.4 Event assessment and classification.....	24
7.9.5 Post-incident reviews.....	24
7.10 Collection of evidence.....	24
7.11 Business continuity management	25
7.11.1 General.....	25
7.11.2 Back up.....	25
7.11.3 Crisis management.....	25
7.12 TSP termination and termination plans	26
7.13 Compliance.....	26
7.14 Supply chain.....	27
7.14.1 Supply chain policy	27
7.14.2 Supply chain procedures and processes	27
7.14.3 Responsibility, third parties agreements and SLA	28

Annex A (normative): Mapping ETSI EN 319 401 V2.3.1 requirement numbers to Requirement numbers in the present document.....30

Annex B (informative): Mapping ETSI EN 319 401 requirements with eIDAS Regulation35

Annex C (informative): Change history37

History38

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

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:	30 May 2024
Date of latest announcement of this EN (doa):	31 August 2024
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	28 February 2025
Date of withdrawal of any conflicting National Standard (dow):	28 February 2025

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.

Further, the cybersecurity of all essential digital services is vital for digital transformation of Europe with digital services and electronic transactions. The provision of eIDAS trust services is identified as an essential element of Europe's digital infrastructure. The Directive (EU) 2022/2555 [i.13] of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive 2016/1148 (NIS2 Directive or NIS2) identifies in article 3 that requirements for cybersecurity risk management measures are applicable, as essential entities, to Qualified Trust Services Providers as per eIDAS Regulation. Furthermore, as eIDAS trust services are identified as fundamental element of Europe's digital infrastructure and NIS 2 is applicable to eIDAS trust services the present document also aims to meet the requirements of NIS2.

The present document specifies baseline policy requirements on the operation and management practices of TSP regardless the service they provide including cybersecurity requirements abiding NIS2. 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.1].

EXAMPLE: ETSI EN 319 411-2 [i.7], annex A describes the application of the present document to the requirements of Regulation (EU) No 910/2014 [i.1] 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.

The present document aims to support the requirements on NIS2 Directive [i.13] and addresses the general requirements for security management and cybersecurity of trust services (qualified and non-qualified).

NOTE: See ETSI EN 319 403-1 [i.2] for details about 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 referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <https://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 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 of 23 July 2014](#) on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- [i.2] ETSI EN 319 403-1: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers".
- [i.3] CA/Browser Forum: "Network and certificate system security requirements".
- [i.4] Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".
- [i.5] 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.6] ETSI EN 301 549: "Accessibility requirements for ICT products and services".
- [i.7] 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".
- [i.8] [Regulation \(EU\) 2016/679 of the European Parliament and of the Council of 27 April 2016](#) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- [i.9] ETSI TS 119 431-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev".
- [i.10] ISO/IEC 27701:2019: "Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines".
- [i.11] ISO/IEC 27002:2022: "Information security, cybersecurity and privacy protection - information security controls".
- [i.12] ISO/IEC 27005:2022: "Information security, cybersecurity and privacy protection - Guidance on managing information security risks".
- [i.13] [Directive \(EU\) 2022/2555](#) of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
- [i.14] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamp".
- [i.15] ETSI TS 119 441: "Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services".
- [i.16] ETSI TS 119 461: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects".
- [i.17] ETSI TS 119 511: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques".
- [i.18] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".
- [i.19] ETSI EN 319 531: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers".
- [i.20] ISO Guide 73:2009: "Risk management - Vocabulary".
- [i.21] [Regulation \(EU\) 2022/2554 of the European Parliament and of the Council of 14 December 2022](#) on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.
- [i.22] [Directive \(EU\) 2022/2557 of the European Parliament and of the Council of 14 December 2022](#) on the resilience of critical entities and repealing Council Directive 2008/114/EC.
- [i.23] Cyber Resilience Act (CRA), [Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation \(EU\) 2019/1020](#).
- [i.24] [Regulation \(EU\) 2022/2065 of the European Parliament and of the Council of 19 October 2022](#) on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).
- [i.25] [Regulation \(EU\) 2022/868 of the European Parliament and of the Council of 30 May 2022](#) on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

koniec náhľadu – text ďalej pokračuje v platenej verzii STN