Draft ETSI EN 319 401 V3.1.0 (2024-03)

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/CommiteeSupportStaff.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

Contents

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 draft European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI EN Approval Procedure.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

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-Stamps".

[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".

3 Definition of terms, symbols, abbreviations and notation

3.1 Terms

For the purposes of the present document, the following terms apply:

access control: physical and logical access to assets that is authorized and/or restricted based on business and information security requirements

NOTE: Source: ISO/IEC 27002:2022 [i.11].

asset: anything that has value to the organization

NOTE: Source: ISO/IEC 27002:2022 [i.11].

attack: successful or unsuccessful unauthorized attempt to destroy, alter, disable, gain access to an asset or any attempt to expose, steal, or make unauthorized use of an asset

NOTE: Source: ISO/IEC 27002:2022 [i.11].

authentication: provision of assurance that a claimed characteristic of an entity is correct

NOTE: Source: ISO/IEC 27002:2022 [i.11].

authenticity: property that an entity is what it claims to be

NOTE: Source: ISO/IEC 27002:2022 [i.11].

Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-R TF.460-6 [i.4]

cybersecurity: activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats

cyber threat: potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons

impact: harm that may be suffered when a threat compromises an information asset

incident: any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems

NOTE: Source: NIS2 Directive [i.13].

incident handling: any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident

NOTE: Source: NIS2 Directive [i.13].

information security breach: compromise of information security that leads to the undesired destruction, loss, alteration, disclosure of, or access to, protected information transmitted, stored or otherwise processed

NOTE: Source: ISO/IEC 27002:2022 [i.11].

information security event: occurrence indicating a possible information security breach or failure of security controls

NOTE: Source: ISO/IEC 27002:2022 [i.11].

information security incident: one or multiple related and identified information security events that can harm an organization's assets or compromise its operations

NOTE: Source: ISO/IEC 27002:2022 [i.11].

information security incident management: exercise of a consistent and effective approach to the handling of information security incidents

NOTE: Source: ISO/IEC 27002:2022 [i.11].

information system: set of applications, services, information technology assets, or other information-handling components

NOTE: Source: ISO/IEC 27002:2022 [i.11].

large-scale cybersecurity incident: incident whose disruption exceeds a Member State's capacity to respond to it or with a significant impact on at least two Member States

NOTE: Source: NIS2 Directive [i.13].

multi-factor authentication: authentication mechanism consisting of two or more of the independent categories of credentials (knowledge, possession and inherence factor) to verify the user's identity for a login or other transaction

near miss: event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but was successfully prevented from transpiring or did not materialise

NOTE: Source: NIS2 Directive [i.13].

policy: intentions and direction of an organization, as formally expressed by its top management

NOTE: Source: ISO/IEC 27002:2022 [i.11].

procedure: specified way to carry out an activity or a process

NOTE: Source: ISO/IEC 27002:2022 [i.11].

process: set of interrelated or interacting activities that uses or transforms inputs to deliver a result

NOTE: Source: ISO/IEC 27002:2022 [i.11].

relying party: natural or legal person that relies upon an electronic identification or a trust service

NOTE: Relying parties include parties verifying a digital signature using a public key certificate.

risk: potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of that incident

risk analysis: process of estimating the likelihood that an event will create an impact and include as necessary components, the foreseeability of a threat, the expected effectiveness of Safeguards, and an evaluated result

risk assessment: Overall process of risk identification, risk analysis and risk evaluation

NOTE: Source: ISO Guide 73:2009 [i.20].

risk management: process for analysing, mitigating, overseeing, and reducing risk

risk treatment: process to modify risk

NOTE: Source: ISO Guide 73:2009 [i.20].

subscriber: legal or natural person bound by agreement with a trust service provider to any subscriber obligations

trust service: electronic service for:

- creation, verification, and validation of digital signatures and related certificates;
- creation, verification, and validation of time-stamps and related certificates;
- registered delivery and related certificates;
- creation, verification and validation of certificates for website authentication; or
- preservation of digital signatures or certificates related to those services.

trust service component: one part of the overall service of a TSP

EXAMPLE: Those identified in clause 4.4 of ETSI EN 319 411-1 [i.5]. Also, ETSI TS 119 431-1 [i.9] defines requirements for a Server Signing Application Service Component (SSASC) which can be implemented as part of TSP's service which also includes other service components.

NOTE: Other standards, including ETSI standards, can specify requirements for other service components which can form part of a wider TSP's service.

trust service policy: set of rules that indicates the applicability of a trust service to a particular community and/or class of application with common security requirements

NOTE: A trust service policy describes what is offered and provides information about the level of the service. It is defined independently of the specific details of the specific operating environment of a TSP; a trust service policy can apply to a community to which several TSPs belong that abide by the common set of rules specified in that policy. It can be defined for example by the TSP, by standards, by national (e.g. government) or international organizations, by the customers (subscribers) of the TSP and it is not necessarily part of the TSP's documentation.

trust service practice statement: statement of the practices that a TSP employs in providing a trust service

NOTE: See clause 6.2 for further information on practice statement.

Trust Service Provider (TSP): entity which provides one or more trust services

trust service token: physical or binary (logical) object generated or issued as a result of the use of a trust service

NOTE: Examples of trust service tokens are: certificates, CRLs, time-stamp tokens, OCSP responses.

vulnerability: weakness of an asset or control that can be exploited by one or more threats

NOTE: Source: ISO/IEC 27002:2022 [i.11].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CA	Certification Authority
CSIRT	Computer Security Incident Response Team
IP	Internet Protocol
IT	Information Technology
NIS2	Directive (EU) 2022/2555 [i.13]
SSASC	Server Signing Application Service Component
TSP	Trust Service Provider
UTC	Coordinated Universal Time

3.4 Notation

The requirements in the present document are identified as follows:

<the 3 letters REQ> **-** < the clause number> **-** <2 digit number - incremental> <change indicator / previous addition>

The management of the requirement identifiers throughout subsequent editions of the present document is as follows:

- When a requirement is inserted at the end of a clause, the 2 digit number above is incremented to the next available digit.
- Where a requirement has been renumbered, added, changed, renumbered or moved from latest version of this document (V2.3.1) to the present version of the present document a change indicator "X" is added.

NOTE: See Annex A for details of the mapping requirement numbers from latest version of this document (V2.3.1) with those of the present document. The current version does not explicitly identify requirements in previous versions of the present document considered as void.