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

EUROPEAN STANDARD

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 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-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".

[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).

[i.26]   Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

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
CER   Critical Entities Resilience

NOTE: Directive on the resilience of critical entities, see [i.22].

CRA   Cyber Resilience Act

NOTE: See [i.23].

CSIRT   Computer Security Incident Response Team
DGA   Data Governance Act

NOTE: See [i.25].

DORA Digital Operational Resilience Act

NOTE: See [i.21].

DSA Digital Services Act

NOTE: See [i.24].

eIDAS electronic IDentification, Authentication and trust Services

NOTE: Informal name for Regulation (EU) No 910/2014 [i.1].

eIDAS2 Regulation (EU) 2024/1183 amending eIDAS

NOTE: See [i.26].

```
ICT      Information & Communication Technology
IP       Internet Protocol
IT       Information Technology
NIS2     Directive (EU) 2022/2555 [i.13]
SLA      Service-Level Agreement
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 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.

4 Overview

Trust services can encompass but is not limited to the issuance of public key certificates, provision of registration services, time-stamping services, long term preservation services, e-delivery services and/or signature validation services.

These policy requirements are not meant to imply any restrictions on charging for TSP's services.

The requirements are indicated in terms of the security objectives followed by more specific requirements for controls to meet those objectives where considered necessary to provide the necessary confidence that those objectives will be met.

When implementing controls of clause 7, guidance given in ISO/IEC 27002:2022 [i.11] should be applied as appropriate.

NOTE: The details of controls required to meet an objective is a balance between achieving the necessary confidence whilst minimizing the restrictions on the techniques that a TSP can employ in providing services.

5 Risk Assessment

REQ-5-01: The TSP shall carry out a risk assessment to identify, analyse and evaluate trust service risks taking into account business and technical issues.

REQ-5-02: The TSP shall select the appropriate risk treatment measures, taking account of the risk assessment results. The risk treatment measures shall ensure that the level of security is commensurate to the degree of risk.

   NOTE: See ISO/IEC 27005:2022 [i.12] for guidance on information security risk management as part of an information security management system.

REQ-5-03: The TSP shall determine all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the information security policy and the trust service practice statement (see clause 6).

REQ-5-04: The risk assessment shall be regularly reviewed and revised.

REQ-5-05: The TSP's management shall approve the risk assessment and accept the residual risk identified.

6 Policies and practices

6.1 Trust Service Practice statement

REQ-6.1-01: The TSP shall specify the set of policies and practices appropriate for the trust services it is providing.

REQ-6.1-02: The set of policies and practices shall be approved by management, published and communicated to employees and external parties as relevant.

In particular:

- **REQ-6.1-03X:** The TSP shall have a statement of the practices and procedures used to address all the requirements of the applicable trust service policy as identified by the TSP.

   NOTE 1: The present document makes no requirement as to the structure of the trust service practice statement.

- **REQ-6.1-04:** The TSP's trust service practice statement shall identify the obligations of all external organizations supporting the TSP's services including the applicable policies and practices.

- **REQ-6.1-05X:** The TSP shall make available to subscribers and relying parties its practice statement, and other relevant documentation, as necessary to demonstrate conformance to the trust service policy.

   NOTE 2: The TSP need not disclose any aspects containing sensitive information in the documentation that is made available to subscribers and relying parties.

- **REQ-6.1-06:** The TSP shall have a management body with overall responsibility for the TSP with final authority for approving the TSP's practice statement.

- **REQ-6.1-07:** The TSP's management shall implement the practices.

- **REQ-6.1-08:** The TSP shall define a review process for the practices including responsibilities for maintaining the TSP's practice statement.

- **REQ-6.1-09X [CONDITIONAL]:** When the TSP intends to make changes in its practice statement that might affect the acceptance of the service by the subject, subscriber or relying parties, it shall give due notice of changes to subscribers and relying parties.

   NOTE 3: The due notice does not need to provide the details of the changes. The due notice can be published on the TSP's repository.

- **REQ-6.1-10:** The TSP shall, following approval as in **REQ-6.1-06** above, make the revised TSP's practice statement immediately available as required under **REQ-6.1-05** above.

- **REQ-6.1-11:** The TSP shall state in its practices the provisions made for termination of service (see clause 7.12).

6.2 Terms and Conditions

REQ-6.2-01: TSP shall make the terms and conditions regarding its services available to all subscribers and relying parties.

REQ-6.2-02: The terms and conditions shall at least specify for each trust service policy supported by the TSP the following:

    a)   the trust service policy being applied;

    b)   any limitations on the use of the service provided including the limitation for damages arising from the use of services exceeding such limitations;

EXAMPLE 1:   The expected life-time of public key certificates.

    c)   the subscriber's obligations, if any;

    d)   information for parties relying on the trust service;

EXAMPLE 2:   How to verify the trust service token, any possible limitations on the validity period associated with the trust service token.

    e)   the period of time during which TSP's event logs are retained;

    f)   limitations of liability;

    g)   the applicable legal system;

    h)   procedures for complaints and dispute settlement;

    i)   whether the TSP's trust service has been assessed to be conformant with the trust service policy, and if so through which conformity assessment scheme;

    j)   the TSP's contact information; and

    k)   any undertaking regarding availability.

REQ-6.2-03: Subscribers and parties relying on the trust service shall be informed of precise terms and conditions, including the items listed above, before entering into a contractual relationship.

REQ-6.2-04: Terms and conditions shall be made available through a durable means of communication.

REQ-6.2-05: Terms and conditions shall be available in a readily understandable language.

REQ-6.2-06: Terms and conditions may be transmitted electronically.

6.3 Information security policy

REQ-6.3-01: The TSP shall define an information security policy which is approved by management and which sets out the organization's approach to managing its information security.

REQ-6.3-02: Changes to the information security policy shall be communicated to third parties, where applicable. This includes subscribers, relying parties, assessment bodies, supervisory or other regulatory bodies.

In particular:

- **REQ-6.3-03:** A TSP's information security policy shall be documented, implemented and maintained including the security controls and operating procedures for TSP's facilities, systems and information assets providing the services.

- **REQ-6.3-04X:** The TSP shall establish procedures to notify of important changes in the provision of the trust service to the appropriate parties in accordance with business requirements and relevant laws and regulations, including changes in the provision of trust services and the intention to cease on its provision.

NOTE 1: Trust service providers qualified according to Regulation (EU) 2014/910 [i.1] are required to inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities.

- **REQ-6.3-05X:** The TSP shall publish and communicate the information security policy to all employees who are impacted by it.

NOTE 2: See clause 5.1 of ISO/IEC 27002:2022 [i.11] for guidance.

- **REQ-6.3-06X:** The TSP's information security policy and inventory of assets for information security (see clause 7.3) shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

- **REQ-6.3-07X:** Any changes that will impact on the level of security provided shall be approved by the management body referred to in **REQ-6.1-07**.

- **REQ-6.3-08X:** The configuration of the TSPs systems shall be regularly checked for changes which violate the TSPs security policies.

- **REQ-6.3-09X:** The maximum interval between two checks shall be documented in the trust service practice statement.

NOTE 3: Further recommendations are given in the CA/Browser Forum network security guide [i.3], item 1.

7 TSP management and operation

7.1 Internal organization

7.1.1 Organization reliability

REQ-7.1.1-01: The TSP organization shall be reliable.

In particular:

- **REQ-7.1.1-02:** Trust service practices under which the TSP operates shall be non-discriminatory.

- **REQ-7.1.1-03:** The TSP should make its services accessible to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in the TSP's terms and conditions.

- **REQ-7.1.1-04:** The TSP shall maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with applicable law, to cover liabilities arising from its operations and/or activities.

NOTE: For liability of TSPs operating in EU, see article 13 of the Regulation (EU) No 910/2014 [i.1].

- **REQ-7.1.1-05:** The TSP shall have the financial stability and resources required to operate in conformity with this policy.

- **REQ-7.1.1-06:** The TSP shall have policies and procedures for the resolution of complaints and disputes received from customers or other relying parties about the provisioning of the services or any other related matters.

7.1.2 Segregation of duties

REQ-7.1.2-01: Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the TSP's assets.

NOTE: See clause 5.3 of ISO/IEC 27002:2022 [i.11] for guidance.

7.2 Human resources

REQ-7.2-01X: The TSP shall ensure that all personnel and contractors apply information security in accordance with the established information security policy, topic-specific policies and procedures of the TSP.

NOTE 1: See clause 5.4 of ISO/IEC 27002:2022 [i.11] for guidance.

In particular:

- **REQ-7.2-02:** The TSP shall employ staff and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications and who have received training regarding cybersecurity and personal data protection rules as appropriate for the offered services and the job function.

- **REQ-7.2-03X:** The TSP shall identify at least one person responsible for network and information security and reporting to top management.

- **REQ-7.2-04X:** TSP's personnel should be able to fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, or actual experience, or a combination of the two.

- **REQ-7.2-05X:** This should include regular (at least every 12 months) updates on new threats and current security practices.

NOTE 2: Personnel employed by a TSP include individual personnel contractually engaged in performing functions in support of the TSP's services. Personnel who can be involved in monitoring the TSP's services need not be TSP's personnel.

- **REQ-7.2-06X:** Appropriate disciplinary sanctions shall be applied to personnel violating TSP's policies or procedures.

NOTE 3: See clause 6.4 of ISO/IEC 27002:2022 [i.11] for guidance.

- **REQ-7.2-07X:** Information security roles and responsibilities, as specified in the TSP's information security policy, shall be documented in job descriptions or in documents available to all concerned personnel and allocated accordingly.

- **REQ-7.2-08X:** Trusted roles, on which the TSP's operation is dependent, shall be clearly identified.

NOTE 4: See clause 5.2 of ISO/IEC 27002:2022 [i.11] for guidance.

NOTE 5: See clause 5.4 of ISO/IEC 27002:2022 [i.11] for further guidance on management responsibilities.

- **REQ-7.2-09X:** TSP's personnel (both temporary and permanent) shall have job descriptions defined from the view point of roles fulfilled with segregation of duties and least privilege (see clause 7.1.2), determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.

NOTE 6: See clause 6.1 of ISO/IEC 27002:2022 [i.11] for further guidance on screening, and clause 6.2 for further guidance on terms and conditions on employment.

- **REQ-7.2-10X:** Where appropriate, job descriptions shall differentiate between general functions and TSP's specific functions. These should include skills and experience requirements.

- **REQ-7.2-11X:** Personnel shall exercise administrative and management procedures and processes that are in line with the TSP's information security management procedures.

- **REQ-7.2-12X:** Managerial personnel shall possess experience or training with respect to the trust service that is provided, familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

- **REQ-7.2-13X:** All TSP's personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the TSP's operations.

- **REQ-7.2-14X:** Trusted roles shall include roles that involve the following responsibilities:

    a) Security Officers: Overall responsibility for administering the implementation of the security practices.

    b) System Administrators: Authorized to install, configure and maintain the TSP's trustworthy systems for service management.

NOTE 7: This includes recovery of the system.

    c) System Operators: Responsible for operating the TSP's trustworthy systems on a day-to-day basis. Authorized to perform system backup.

    d) System Auditors: Authorized to view archives and audit logs of the TSP's trustworthy systems.

NOTE 8: Additional application specific roles can be required for particular trust services.

- **REQ-7.2-15X:** TSP's personnel shall be formally appointed to trusted roles by senior management responsible for security.

- **REQ-7.2-16X:** Trusted roles shall be accepted by the appointed person to fulfil the role.

- **REQ-7.2-17:** Personnel shall not have access to the trusted functions until the necessary checks are completed.

NOTE 9: In some countries it is not possible for TSP to obtain information on past convictions without the collaboration of the candidate employee.

NOTE 10: See clause 6.1 of ISO/IEC 27002:2022 [i.11] for further guidance on screening.

- **REQ-7.2-18X:** [CONDITIONAL] When personnel are working remotely, TSP shall implement cybersecurity measures to protect information accessed, processed or stored outside the TSP's premises.

In particular:

- **REQ-7.2-19X:** TSPs allowing remote working activities shall issue a topic-specific policy on remote working that defines the relevant cybersecurity conditions and restrictions.

NOTE 11: See clause 6.7 of ISO/IEC 27002:2022 [i.11] for further guidance on remote working.

7.3 Asset management

7.3.1 General requirements

REQ-7.3.1-01: The TSP shall ensure an appropriate level of protection of its assets including information assets.

REQ-7.3.1-02X: The assets provided through a supply chain shall be protected as specified in clause 7.14.

NOTE: Asset Management is a requirement which is incorporated in all ETSI EN 319 411-1 [i.5] (clause 6.4.1), ETSI EN 319 421 [i.14] (clause 7.4), ETSI TS 119 431-1 [i.9] (clause 6.4.1), ETSI TS 119 441 [i.15] (clause 7.3), ETSI TS 119 461 [i.16] (clause 7.3), ETSI TS 119 511 [i.17] (clause 7.3), ETSI EN 319 521 [i.18] (clause 7.3.1), ETSI EN 319 531 [i.19] (clause 7.3.1).

7.3.2 Assets inventory and classification

REQ-7.3.2.01X: The TSP shall maintain an accurate inventory of assets as a prerequisite for effective technical vulnerability management and shall assign a classification consistent with the risk assessment.

REQ-7.3.2-02X: For asset, or group of assets, the inventory shall contain, when applicable:

a)   a unique asset ID;

b)   an asset description;

c)   the asset owner;

d)   the asset location;

e)   the asset type (e.g. software, hardware, services, facilities, HVAC systems, personnel, physical records);

f)   the type of information processed or/stored in the asset and its information classification;

g)   the date and version of the asset's last update or patch;

h)   the classification level of the asset; and

i)   the asset's end of life.

- **REQ-7.3.2-03X:** The TSP shall assign a classification level to each asset, or group of assets, based on requirements for protecting confidentiality, integrity, authenticity and availability, and in accordance to its risk assessment and business value.

- **REQ-7.3.2-04X:** The TSP shall assure that the availability requirements of each asset, or group of assets, classified are aligned with the delivery and recovery objectives as described in the business and disaster recovery plan.

- **REQ-7.3. 2-05X:** The TSP shall conduct periodic reviews of the classification levels of the assets.

NOTE 1:   See clauses 5.9 and 8.8 of ISO/IEC 27002:2022 [i.11] for guidance.

- **REQ-7.3.2-06X:** The TSP shall identify, document and implement rules for the acceptable use of and procedures for handling information and other associated assets.

NOTE 2:   See clause 5.10 of ISO/IEC 27002:2022 [i.11] for guidance.

- **REQ-7.3.2-07X:** The TSP shall implement and document procedures in case of change or termination process of, internal and external personnel, contractors or other third parties in order to include the return of all previously issued physical and electronic assets owned by or entrusted to the TSP.

NOTE 3:   See clause 5.11 of ISO/IEC 27002:2022 [i.11] for guidance.

7.3.3   Storage media handling

REQ-7.3.3-01X: All storage media shall be managed through its life cycle of acquisition, use, transportation and disposal in accordance with the TSP's classification scheme and handling requirements.

REQ-7.3.3-02X: Storage media used within the TSP's systems shall be securely handled to protect storage media from damage, theft, unauthorized access and obsolescence.

REQ-7.3.3-03X: Storage media management procedures shall protect against obsolescence and deterioration of storage media within the period of time that records are required to be retained.

NOTE: See clause 7.10 of ISO/IEC 27002:2022 [i.11] for guidance.

7.4   Access control

REQ-7.4-01: The TSP's system access shall be limited to authorized individuals.

In particular:

- **REQ-7.4-02X:** The TSP shall administer user access of operators, administrators and other privileged accounts and system auditors applying the principle of "least privileges" when configuring access privileges. In particular:

- **REQ-7.4-03X:** The TSP shall provide setting up specific accounts to be used for administrative purposes like installation, configuration, management or maintenance.

- **REQ-7.4-04X:** Privileged accounts shall be used only if the privileges are necessary for the specific activity.

- **REQ-7.4-05X:** Strong identification, authentication and authorisation procedures shall be used for privileged accounts.

NOTE 1:   This generally applies to personnel appointed to trusted roles as per **REQ-7.2-14X.**

- **REQ-7.4-06X [CONDITIONAL]:** Where appropriate, the TSP shall ensure that users and devices are authenticated by multi-factor or continuous authentication mechanisms, such as secure voice, video and text, before accessing the TSP's network and ITS information systems, depending on the classification of the systems to be accessed.

NOTE 2:   See clauses 8.5 of ISO/IEC 27002:2022 [i.11] for guidance.

- **REQ-7.4-07X:** The TSP shall review access rights to privileged and administrator accounts at planned intervals, and access rights shall be modified based on organisational changes. The result of the review, including the necessary changes of access rights, shall be documented.

- **REQ-7.4-08X:** The TSP shall ensure that access permissions are modified accordingly upon termination of employment or change of function.

- **REQ-7.4-09X:** Access to information and application system functions shall be restricted in accordance with the access control policy.

- **REQ-7.4-10X:** The TSP's system shall provide sufficient computer security controls for the separation of trusted roles identified in TSP's practices, including the separation of security administration and operation functions. Particularly, use of system utility programs shall be restricted and controlled.

- **REQ-7.4-11X:** TSP's personnel shall be identified and authenticated before using critical applications related to the service.

- **REQ-7.4-12X:** TSP's personnel shall be accountable for their activities.

EXAMPLE: By retaining event logs.

- **REQ-7.4-13X:** Sensitive data shall be protected against being revealed through re-used storage objects (e.g. deleted files) or storage media (see clause 7.3.2) being accessible to unauthorized users.

NOTE 3:   See clauses 5.15, 5.16, 5.17, 5.18, 8.2, 8.3, 8.4, 8.5 and 8.18 of ISO/IEC 27002:2022 [i.11] for guidance.

NOTE 4:   Further recommendations regarding authentication are given in the CA/Browser Forum network security guide [i.3], clause 2.

7.5   Cryptographic controls

REQ-7.5-01X: Appropriate security controls shall be in place for the management of any cryptographic keys, cryptographic algorithms, and cryptographic devices throughout their lifecycle.

NOTE: See clause 8.24 of ISO/IEC 27002:2022 [i.11] for guidance.

7.6   Physical and environmental security

REQ-7.6-01: The TSP shall control physical access to components of the TSP's system whose security is critical to the provision of its trust services and minimize risks related to physical security.

NOTE 1:   See clauses 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 and 8.1 of ISO/IEC 27002:2022 [i.11] for guidance.

In particular:

- **REQ-7.6-02:** Physical access to components of the TSP's system whose security is critical to the provision of its trust services shall be limited to authorized individuals.

NOTE 2: Criticality is identified through risk assessment, or through application security requirements, as requiring a security protection.

- **REQ-7.6-03:** Controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities.

- **REQ-7.6-04:** Controls shall be implemented to avoid compromise or theft of information and information processing facilities.

- **REQ-7.6-05:** Components that are critical for the secure operation of the trust service shall be located in a protected security perimeter with physical protection against intrusion, controls on access through the security perimeter and alarms to detect intrusion.

7.7   Operation security

REQ-7.7-01: The TSP shall use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

In particular:

- **REQ-7.7-02:** An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the TSP or on behalf of the TSP to ensure that security is built into IT systems.

- **REQ-7.7-03:** Change control procedures shall be applied for releases, modifications and emergency software fixes of any operational software and changes to the configuration which applies the TSP's security policy.

- **REQ-7.7-04:** The procedures shall include documentation of the changes.

NOTE 1: See clauses 5.37, 8.6, 8.31 and 8.32 of ISO/IEC 27002:2022 [i.11] for guidance.

- **REQ-7.7-05:** The integrity of TSP's systems and information shall be protected against viruses, malicious and unauthorized software.

NOTE 2: See clause 8.7 of ISO/IEC 27002:2022 [i.11] for guidance.

- **REQ-7.7-06X:** Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of services.

- **REQ-7.7-07X:** The TSP shall specify and apply procedures for ensuring that:

    a)   security patches are applied within a reasonable time after they come available;

    b)   security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and

    c)   the reasons for not applying any security patches are documented.

REQ-7.7-08X: The TSP shall establish, document, implement, monitor, and review configurations, including security configurations, of hardware, software, services and networks.

REQ-7.7-09X: The TSP shall monitor configurations with a comprehensive set of system management tools.

EXAMPLE: Examples of system management tools are: maintenance utilities, remote support, enterprise management tools, backup and restore software, or change detection mechanisms, such as file integrity monitoring solutions

REQ-7.7.10X: The TSP shall review configurations on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed.

NOTE 3: See clause 8.9 of ISO/IEC 27002:2022 [i.11] for guidance.

NOTE 4: Further recommendations are given in the CA/Browser Forum network security guide [i.3], item 1.

7.8   Network security

REQ-7.8-01: The TSP shall protect its network and systems from attacks.

NOTE 1: See clauses 8.20, 8.21, 8.22 and 8.23 of ISO/IEC 27002:2022 [i.11] for guidance.

In particular:

- **REQ-7.8-02:** The TSP shall segment its systems into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationship between trustworthy systems and services.

- **REQ-7.8-03:** The TSP shall apply the same security controls to all systems co-located in the same zone.

- **REQ-7.8-04:** The TSP shall restrict access and communications between zones to those necessary for the operation of the TSP.

- **REQ-7.8-05:** The TSP shall explicitly forbid or deactivate not needed connections and services.

- **REQ-7.8-06:** The TSP shall review the established rule set on a regular basis.

- **REQ-7.8-07:** The TSP shall keep all systems that are critical to the TSP's operation in one or more secured zone(s) (e.g. Root CA systems see ETSI EN 319 411-1 [i.5]).

- **REQ-7.8-08:** The TSP shall separate dedicated network for administration of IT systems and TSP's operational network.

- **REQ-7.8-09X:** The TSP shall logically separate administration systems and networks from other information systems and networks.

- **REQ-7.8-10:** The TSP shall separate the production systems for the TSP's services from systems used in development and testing (e.g. development, test and staging systems).

- **REQ-7.8-11X:** The TSP shall establish communication between distinct trustworthy systems only through trusted channels that are isolated using logical, cryptographic or physical separation from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.

- **REQ-7.8-12:** If a high level of availability of external access to the trust service is required, the external network connection shall be redundant to ensure availability of the services in case of a single failure.

- **REQ-7.8-13:** The TSP shall undergo or perform a regular vulnerability scan on public and private IP addresses identified by the TSP and record evidence that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

- **REQ-7.8-14X:** The vulnerability scan requested by **REQ-7.8-13** should be performed once per quarter.

- **REQ-7.8-15X:** The TSP shall protect its network and information systems against malicious and unauthorised software by means of malware detection and removal software, which is updated at least on a daily basis.

NOTE 2:   See clause 8.7 of ISO/IEC 27002:2022 [i.11] for guidance.

- **REQ-7.8-16X:** The TSP shall regularly update its malware detection and repair software.

- **REQ-7.8-17X:** The TSP shall undergo a penetration test on the TSP's systems at set up and after infrastructure or application upgrades or modifications that the TSP determines are significant.

- **REQ-7.8-18X:** The penetration test requested by **REQ-7.8-17X** should be performed at least once per year.

- **REQ-7.8-19X:** The TSP shall record evidence that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

- **REQ-7.8-20X:** Controls (e.g. firewalls) shall protect the TSP's internal network domains from unauthorized access including access by subscribers and third parties.

- **REQ-7.8-21X:** Firewalls should also be configured to prevent all protocols and accesses not required for the operation of the TSP.

7.9 Vulnerabilities and Incident management

7.9.1 Monitoring and logging

REQ-7.9.1-01X: The TSP shall establish mechanisms to detect potential security incidents and to respond accordingly by implementing tools and processes to enable continuous monitoring and logging of activities on the entity's network and information systems.

NOTE 1: See clauses 8.16, 5.24, 5.25, 5.26, 5.27, 5.28 and 6.8 of ISO/IEC 27002:2022 [i.11] for guidance.

In particular:

- **REQ-7.9.1-02X:** Monitoring activities should take account of the sensitivity of any information collected or analysed.

- **REQ-7.9.1-03X:** Abnormal system activities that indicate a potential security violation, including intrusion into the TSP's network, shall be detected and reported as alarms.

NOTE 2: Abnormal network system activities can comprise (external) network scans or packet drops.

- **REQ-7.9.1-04X:** The TSP shall maintain, document and regularly review logs which shall include:

a) outbound and inbound network traffic;

b) activities regarding user administration and permission management, access (including privileged access) to systems and applications;

c) activities performed with administrator accounts;

d) assess or changes to critical configuration files and backups;

e) security relevant logs;

f) use and performance of system resources;

g) physical access to facilities, where appropriate;

h) access and use of network equipment and devices; and

i) environmental events, where appropriate.

- **REQ-7.9.1-05X:** The TSP's systems shall be monitored including the monitoring or regular review of audit logs to identify evidence of malicious activity implementing automatic mechanisms to process the audit logs and alert personnel of possible critical security events.

7.9.2 Incident response

- **REQ-7.9.2-01X:** The TSP shall establish incident response procedures including containment, eradication and recovery.

- **REQ-7.9.2-02X:** The TSP shall comply with reporting obligations as mandated by relevant legislative frameworks for network and information security incidents, including supervisory authorities and CSIRTs.

EXAMPLE 1:   Relevant legislative frameworks such as DORA [i.21], CER [i.22], eIDAS [i.1], eIDAS2 [i.26], CRA [i.23], DSA [i.24], DGA [i.25], etc.

- **REQ-7.9.2-03X:** TSPs shall inform stakeholders about incidents according to agreed communication plans.

- **REQ-7.9.2-04X:** The TSP shall establish and maintain effective communication plans that include incident categorisation, well-defined escalation procedures, and standardised reporting protocols.

- **REQ-7.9.2-05X:** The TSP shall ensure that personnel possess the necessary competencies to proficiently detect and respond to security incidents.

- **REQ-7.9.2-06X:** The TSP shall create and maintain comprehensive documentation throughout the incident detection and response process.

- **REQ-7.9.2-07X:** The TSP shall establish clear interfaces between the incident handling and business continuity management functions to ensure a coordinated and cohesive response during incidents.

- **REQ-7.9.2-08X:** The TSP shall test and review regularly and after incidents roles, responsibilities and appropriate procedures.

- **REQ-7.9.2-09X:** The TSP shall address any critical vulnerability not previously addressed by the TSP, within a period of 48 hours after its discovery.

- **REQ-7.9.2-10X:** For any vulnerability, given the potential impact, the TSP shall [CHOICE]:

  - create and implement a plan to mitigate the vulnerability; or

  - document the factual basis for the TSP's determination that the vulnerability does not require remediation.

EXAMPLE 2:   The TSP can determine that the vulnerability does not require remediation when the cost of the potential impact does not warrant the cost of mitigation.

NOTE 1: Further recommendations are given in the CA/Browser Forum network security guide [i.3] item 4 f).

- **REQ-7.9.2-11X:** Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized.

- **REQ-7.9.2-12X:** The TSP shall appoint trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the TSP's procedures.

7.9.3   Reporting

- **REQ-7.9.3-01X:** The TSP shall establish procedures to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein within 24 hours of the breach being identified.

NOTE: TSPs operating within the European Union can contact the appropriate supervisory body and/or other competent authorities for further guidance on implementing notification procedures as per article 19.2 of Regulation (EU) No 910/2014 [i.1].

- **REQ-7.9.3-02X:** Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the TSP shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

- **REQ-7.9.3-03X:** The TSP shall establish a simple procedure allowing its staff, contractors and customers to report possible network and information security incidents.

- **REQ-7.9.3-04X:** The TSP shall communicate the reporting procedure to its contractors and customers and shall train its staff to follow the reporting procedure and to address the appropriate point of contact.

7.9.4 Event assessment and classification

- **REQ-7.9.4-01X:** The TSP shall analyse the reported events and assess their severity.

- **REQ-7.9.4-02X:** The TSP shall be capable to reassess and reclassify events based on new inputs.

7.9.5 Post-incident reviews

- **REQ-7.9.5-01X:** The TSP shall keep itself informed about technical vulnerabilities of all information systems it uses.

- **REQ-7.9.5-02X:** The TSP shall evaluate the TSP's exposure to such vulnerabilities and take appropriate measures.

  NOTE: See clause 8.8 of ISO/IEC 27002:2022 [i.11] for guidance.

- **REQ-7.9.5-03X:** The TSP shall identify the root cause of an incident and shall conduct a post-incident review possibly resulting in measures mitigating the risk of the recurrence of similar incidents.

- **REQ-7.9.5-04X:** The TSP shall ensure that each past incident led to a post-incident review.

7.10 Collection of evidence

REQ-7.10-01: The TSP shall record and keep accessible for an appropriate period of time, including after the activities of the TSP have ceased, all relevant information concerning data issued and received by the TSP, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service.

  NOTE 1: See requirement **REQ-7.13-05.**

  NOTE 2: See clauses 5.28 and 8.15 of ISO/IEC 27002:2022 [i.11] for guidance.

In particular:

- **REQ-7.10-02:** The confidentiality and integrity of current and archived records concerning operation of services shall be maintained.

- **REQ-7.10-03:** Records concerning the operation of services shall be completely and confidentially archived in accordance with disclosed business practices.

- **REQ-7.10-04:** Records concerning the operation of services shall be made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.

- **REQ-7.10-05:** The precise time of significant TSP's environmental, key management and clock synchronization events shall be recorded.

- **REQ-7.10-06:** The time used to record events as required in the audit log shall be synchronized with UTC at least once a day.

- **REQ-7.10-07:** Records concerning services shall be held for a period of time as appropriate for providing necessary legal evidence and as notified in the TSP's terms and conditions (see clause 6.2).

- **REQ-7.10-08:** The events shall be logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held.

  EXAMPLE: This can be achieved, for example, through the use of write-only media, a record of each removable storage media used and the use of off-site backup or by parallel storage of the information at several (e.g. 2 or 3) independent sites.

7.11   Business continuity management

7.11.1   General

REQ-7.11.1-01X: The TSP shall define and maintain a continuity plan to enact in case of a disaster.

REQ-7.11-1-02X: In the event of a disaster, including compromise of a private signing key or compromise of some other credential of the TSP, operations shall be restored within the delay established in the continuity plan, having addressed any cause for the disaster which may recur (e.g. a security vulnerability) with appropriate remediation measures.

> NOTE 1:   See clauses 8.13, 5.29, 5.29 and 5.30 of ISO/IEC 27002:2022 [i.11] for guidance in the event of a disaster.

> NOTE 2:   Other disaster situations include failure of critical components of a TSP's trustworthy system, including hardware and software.

7.11.2   Back up

REQ-7.11.2-01X: The TSP shall maintain backup copies of information and sufficient resources, including facilities, network and information systems as well as personnel in accordance with risk assessment and business continuity plan.

REQ-7.11.2-02X: The TSP shall define backup plans taking into account at least the following:

a)   recovery times;

b)   assurance of the backup copies' completeness and accuracy (including configuration data and information stored in cloud service environment);

c)   storage of backup copies at a safe location or locations which are outside the network of the system backed up and are at sufficient distance to escape any damage from a disaster at the main site;

d)   physical/environmental and logical controls for backup copies in accordance with their information classification level; and

e)   processes for restoring information from backup copies (including approval processes).

REQ-7.11.2-03X: The TSP shall perform integrity check on the backup copies.

REQ-7.11.2-04X: The TSP shall test at planed intervals the recovery of backup copies and redundancies and shall take corrective actions in case of findings. The results of these tests shall be documented.

> NOTE: See clauses 8.3 and 8.13 of ISO/IEC 27002:2022 [i.11] for guidance.

7.11.3   Crisis management

REQ-7.11.3.-01X: The TSP shall establish processes for crisis management addressing at least:

a)   roles and responsibilities in crisis situations;

b)   mandatory and voluntary communications between the TSP and relevant competent authorities, and

c)   appropriate controls for maintaining network and information security in crisis situations.

REQ-7.11.3-02X: The TSP shall implement a process for managing and making use of information received from National CSIRT or, where applicable, competent authorities useful for crisis management.

REQ-7.11.3-03X: The TSP shall test and review, at planned intervals or in the post-incident review process, its crisis management plan.

7.12 TSP termination and termination plans

REQ-7.12-01: Potential disruptions to subscribers and relying parties shall be minimized as a result of the cessation of the TSP's services, and in particular continued maintenance of information required to verify the correctness of trust services shall be provided.

In particular:

- **REQ-7.12-02:** The TSP shall have an up-to-date termination plan.

Before the TSP terminates its services at least the following procedures apply:

- **REQ-7.12-03:** Before the TSP terminates its services, the TSP shall inform the following of the termination: all subscribers and other entities with which the TSP has agreements or other form of established relations, among which relying parties, TSPs and relevant authorities such as supervisory bodies.

- **REQ-7.12-04:** Before the TSP terminates its services, the TSP shall make the information of the termination available to other relying parties.

- **REQ-7.12-05:** Before the TSP terminates its services, the TSP shall terminate authorization of all subcontractors to act on behalf of the TSP in carrying out any functions relating to the process of issuing trust service tokens.

- **REQ-7.12-06:** Before the TSP terminates its services, the TSP shall transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period, unless it can be demonstrated that the TSP does not hold any such information.

- **REQ-7.12-07:** Before the TSP terminates its services, the TSP's private keys, including backup copies, shall be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.

- **REQ-7.12-08:** Before the TSP terminates its services, where possible TSP should make arrangements to transfer provision of trust services for its existing customers to another TSP.

- **REQ-7.12-09:** The TSP shall have an arrangement to cover the costs to fulfil these minimum requirements in case the TSP becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.

- **REQ-7.12-10:** The TSP shall state in its practices the provisions made for termination of service. This shall include:

  a) notification of affected entities; and

  b) where applicable, transferring the TSP's obligations to other parties.

- **REQ-7.12-11:** The TSP shall maintain or transfer to a reliable party its obligations to make available its public key or its trust service tokens to relying parties for a reasonable period.

7.13 Compliance

REQ-7.13-01: The TSP shall ensure that it operates in a legal and trustworthy manner.

In particular:

- **REQ-7.13-02:** The TSP shall provide evidence on how it meets the applicable legal requirements.

- **REQ-7.13-03:** Trust services provided and end user products used in the provision of those services shall be made accessible for persons with disabilities, where feasible.

- **REQ-7.13-04:** Applicable standards on accessibility such as ETSI EN 301 549 [i.6] should be taken into account.

- **REQ-7.13-05:** Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

NOTE 1: TSPs operating in Europe are required to ensure that personal data is processed in accordance with Regulation (EU) 2016/679 [i.8]. In this respect, authentication for a service online concerns processing of only those identification data which are adequate, relevant and not excessive to grant access to that service online.

NOTE 2: See ISO/IEC 27701:2019 [i.10] for requirements and guidance on the extension to ISO/IEC 27002:2022 [i.11] for privacy information management.

NOTE 3: See clauses 5.31, 5.32, 5.33, 5.34 and 5.35 of ISO/IEC 27002:2022 [i.11] for guidance.

7.14 Supply chain

7.14.1 Supply chain policy

REQ-7.14.1-01X: The TSP shall identify and implement processes and procedures to address security risks associated with the use of products and services provided by suppliers, including the ICT supply chain.

REQ-7.14.1-02X: The TSP shall define, document and implement processes and procedures to manage the information security risks associated with the use of supplier's products or services.

In particular,

- **REQ-7.14-03X:** The supply chain policy shall identify and communicate the TSP's role in the supply chain.

- **REQ-7.14-04X:** The supply chain policy shall define criteria for selecting and contracting suppliers or service providers. Criteria shall include:

a) the ability of the supplier or service provider to meet the cybersecurity specifications, risks and classification levels of the TSP's services, systems or products delivered by the supplier or service provider;

b) the ability of the TSP to diversify sources of supply and to limit vendor lock-in; and

c) the results of the coordinated security risk assessments of critical supply chains.

7.14.2 Supply chain procedures and processes

REQ-7.14.2-01X: Processes and procedures shall be defined and implemented to manage information security risks associated with the information and communication technologies products and services supply chain.

In particular:

- **REQ-7.14.2-02X:** TSP shall define information security requirements to apply to ICT product or service acquisition.

- **REQ-7.14.2-03X:** TSP shall require that ICT services suppliers propagate the TSP's security requirements throughout the supply chain if they sub-contract for parts of the ICT service provided to the TSP.

- **REQ-7.14.2-04X:** TSP shall require that ICT products suppliers propagate appropriate security practices throughout the supply chain if these products include components purchased or acquired from other suppliers or other entities.

- **REQ-7.14.2-05X:** TSP shall request that ICT products suppliers provide information describing the software components used in products.

- **REQ-7.14.2-06X:** TSP shall request that ICT products suppliers provide information describing the implemented security functions of their product and the configuration required for its secure operation.

- **REQ-7.14.2-07X:** TSP shall implement a monitoring process and acceptable methods for validating ICT products and services conform to stated cybersecurity requirements.

- **REQ-7.14.2-08X:** TSP shall implement a process for identifying and documenting product or service components that are critical for maintaining functionality.

- **REQ-7.14.2-09X:** TSP shall obtain assurance that critical components and their origin can be traced throughout the supply chain.

- **REQ-7.14.2-10X:** TSP shall obtain assurance that the delivered ICT products are functioning as expected without any unexpected or unwanted features.

- **REQ-7.14.2-11X:** TSP shall implement processes to ensure that components from suppliers are genuine and unaltered from their specification.

- **REQ-7.14.2-12X:** TSP shall define rules for sharing of information regarding the supply chain and any potential issues and compromises among the TSP and its suppliers.

- **REQ-7.14.2-13X:** TSP shall implement specific processes for managing ICT component life cycle and availability and associated security risks.

NOTE 1: See clause 5.21 of ISO/IEC 27002:2022 [i.11] for guidance on managing information security in the ICT supply chain.

REQ-7.14.2-14X: TSP shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.

NOTE 2: See clause 5.22 of ISO/IEC 27002:2022 [i.11] for guidance on Monitoring, review and change management of supplier services.

REQ-7.14.2-15X: The TSP shall define, implement and communicate to all relevant interested parties topic-specific policies on the use of cloud services and on how the TSP intends to manage information security risks associated with them.

NOTE 3: See clause 5.23 of ISO/IEC 27002:2022 [i.11] for guidance on Information security for use of cloud services.

NOTE 4: The use of cloud services involves, as per contract, shared responsibility for information security and collaborative effort between the cloud service provider and the TSP acting as the cloud service provider customer. It is essential that the responsibilities for both the cloud service provider and the organization, acting as the cloud service customer, are defined and implemented appropriately.

7.14.3 Responsibility, third parties agreements and SLA

REQ-7.14.3-01X [CONDITIONAL]: When the TSP makes use of other parties, including trust service component providers, to provide parts of its service through subcontracting, outsourcing or other third party arrangements, it shall maintain overall responsibility for conformance with the supply chain policy, its information security policy and the requirements defined in the trust service policy.

REQ-7.14.3-02X: The TSP shall define the outsourcers' liability and ensure that outsourcers are bound to implement any controls required by the TSP.

In particular:

- **REQ-7.14.3-03X:** These processes and procedures shall include:

    a) those to be implemented by the TSP;

    b) those the TSP requires the supplier to implement for the commencement of use of a supplier's products or services; and

    c) those the TSP requires the supplier to implement for the termination of use of a supplier's products and services.

NOTE 1: This applies to TSP's use of resources of cloud service providers.

NOTE 2: See clause 5.19 of ISO/IEC 27002:2022 [i.11] for guidance on information security in supplier relationships.

REQ-7.14.3-04X: The TSP shall have a documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements to ensure that there is clear understanding between the TSP and the supplier regarding both parties' obligations to fulfil relevant information security requirements.

REQ-7.14.3-05X [CONDITIONAL]: When the TSP makes use of a trust service component provided by another party it shall ensure that the use of the component interface meets the requirements as specified by the trust service component provider.

REQ-7.14.3-06X [CONDITIONAL]: When the TSP makes use of a trust service component provided by another party it shall ensure that the security and functionality required by the trust service component meet the appropriate requirements of the applicable policy and practices.

REQ-7.14.3-07X: The TSP shall include in their services agreements "Service level agreements" and/or auditing mechanisms ensuring that direct suppliers and service providers, including cloud computing providers, take appropriate security measures addressing the TSP's security requirements aligned with the TSP's risk assessment.

In particular:

- **REQ-7.14.3-08X:** Compliance with TSPs security policies and requirements shall be considered in the selection process of any direct supplier or service provider as part of the procurement process.

- **REQ-7.14.3-09X:** Applicable TSPs security policies and requirements and shall be included in contracts with direct suppliers or service providers.

REQ-7.14.3-10X: The TSP shall review the supply chain policy and monitor, review, evaluate and manage changes in the cybersecurity practices of direct suppliers or service providers at planned intervals or after an incident related to the provision of services from direct suppliers or service providers.

NOTE 3: See clauses 5.19 to 5.23 of ISO/IEC 27002:2022 [i.11] for guidance on supplier relationships.

REQ-7.14.3-11X: The TSP shall establish and maintain a register of suppliers and their agreements to track where the TSP information is managed and/or archived.

EXAMPLE: This can help identify where information is exchanged.

REQ-7.14.3-12X: The TSP shall regularly review, validate and update its registry of suppliers and their agreements to ensure that they are still valid, fit for purpose, and include the relevant information security clauses.

NOTE 4: See clause 5.20 of ISO/IEC 27002:2022 [i.11] for guidance on addressing information security within supplier agreements.

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

The following mapping table shall be used for standards referencing ETSI EN 319 401 which were published prior to the present version (i.e. before February 2024) as some of the requirement numbers have changed from previous version.

Former requirement	Status* • **No changes: Idem** • **Partially changed: PC** • **New content: NCT** • **New requirement: NR** • **Moved to another clause: M** • **Renumbered: R** • **Previously Void: V** • **Deleted: D**	Current number (if changed) and/or new content
	Clause 5 Risk Assessment	
REQ-5-01	Idem	
REQ-5-02	Idem	
REQ-5-03	Idem	
REQ-5-04	Idem	
REQ-5-05	Idem	
	Clause 6.1 Trust Service Practice statement	
REQ-6.1-01	Idem	
REQ-6.1-02	Idem	
REQ-6.1-03	V	removed
REQ-6.1-03A	R	REQ-6.1-03X
REQ-6.1-04	Idem	
REQ-6.1-05	V	removed
REQ-6.1-05A	R	REQ-6.1-05X
REQ-6.1-06	Idem	
REQ-6.1-07	Idem	
REQ-6.1-08	Idem	
REQ-6.1-09	V	removed
REQ-6.1-09A	R	REQ-6.1-09X
REQ-6.1-10	Idem	
REQ-6.1-11	Idem	
	Clause 6.2 Terms and Conditions	
REQ-6.2-01	Idem	
REQ-6.2-02	Idem	
REQ-6.2-03	Idem	
REQ-6.2-04	Idem	
REQ-6.2-05	Idem	
REQ-6.2-06	Idem	
	Clause 6.3 Information security policy	
REQ-6.3-01	Idem	
REQ-6.3-02	Idem	
REQ-6.3-03	Idem	
	NR	REQ-6.3-04X
REQ-6.3-04	R	REQ-6.3-05X
REQ-6.3-05	M, NCT	REQ-7.14.3-01X combines former REQ-6.3-05 and REQ-7.1.1-08
REQ-6.3-06	M	REQ-7.14.3-02X
REQ-6.3-07	R	REQ-6.3-06X
REQ-6.3-08	R	REQ-6.3-07X
REQ-6.3-09	R	REQ-6.3-08X
REQ-6.3-10	R	REQ-6.3-09X

	Clause 7 TSP management and operation	
	Clause 7.1 Internal organization	
	Clause 7.1.1 Organization reliability	
REQ-7.1.1-01	Idem	
REQ-7.1.1-02	Idem	
REQ-7.1.1-03	Idem	
REQ-7.1.1-04	Idem	
REQ-7.1.1-05	Idem	
REQ-7.1.1-06	Idem	
REQ-7.1.1-07	M, NCT	REQ-7.14.3-04X
REQ-7.1.1-08	M	REQ-7.14.3-01X combines former REQ-6.3-05 and REQ-7.1.1-08
REQ-7.1.1-09	M	REQ-7.14.3-05X
REQ-7.1.1-10	M	REQ-7.14.3-06X
	Clause 7.1.2 Segregation of duties	
REQ-7.1.2-01	Idem	
	Clause 7.2 Human resources	
REQ-7.2-01	PC	REQ-7.2-01X
REQ-7.2-02	Idem	
	NR	REQ-7.2-03X
REQ-7.2-03	R	REQ-7.2-04X
REQ-7.2-04	R	REQ-7.2-05X
REQ-7.2-05	R	REQ-7.2-06X
REQ-7.2-06	R, PC	REQ-7.2-07X
REQ-7.2-07	R, PC	REQ-7.2-08X
REQ-7.2-08	V	removed
REQ-7.2-09	V	removed
REQ-7.2-10	R	REQ-7.2-09X
REQ-7.2-11	R	REQ-7.2-10X. Note deleted
REQ-7.2-12	R	REQ-7.2-11X. Note deleted
REQ-7.2-13	R	REQ-7.2-12X
REQ-7.2-14	R	REQ-7.2-13X. Note deleted
REQ-7.2-15	R	REQ-7.2-14X
REQ-7.2-16	V	removed
REQ-7.2-16A	R	REQ-7.2-15X
REQ-7.2-16B	R	REQ-7.2-16X
REQ-7.2-17	Idem	
	NR	REQ-7.2-18X
	NR	REQ-7.2-19X
	Clause 7.3 Asset management	
	Clause 7.3.1 General requirements	
REQ-7.3.1-01	Idem.	Note deleted
	NR	REQ-7.3.1-02X
	Clause 7.3.2 Assets inventory and classification	
REQ-7.3.1-02	M, PC	REQ-7.3.2-01X
	NR	REQ-7.3.2-02X
	NR	REQ-7.3.2-03X
	NR	REQ-7.3.2-04X
	NR	REQ-7.3.2-05X
	NR	REQ-7.3.2-06X
	NR	REQ-7.3.2-07X
	Clause 7.3.3 Title Changed: Storage media handling	
REQ-7.3.2-01	M, PC	REQ-7.3.3-01X
REQ-7.3.2-02	M, PC	REQ-7.3.3-02X
REQ-7.3.2-03	M, PC	REQ-7.3.3-03X

	Clause 7.4	Access Control	
REQ-7.4-01	Idem		
REQ-7.4-02	V	removed	
REQ-7.4-03	V	removed	
REQ-7.4-04	V	removed	
REQ-7.4-04A	PC	REQ-7.4-02X	
REQ-7.4-05	D	Deleted	
	NR	REQ-7.4-03X	
	NR	REQ-7.4-04X	
	NR	REQ-7.4-05X	
	NR	REQ-7.4-06X	
	NR	REQ-7.4-07X	
	NR	REQ-7.4-08X	
REQ-7.4-06	R	REQ-7.4-09X	
REQ-7.4-07	R	REQ-7.4-10X	
REQ-7.4-08	R	REQ-7.4-11X	
REQ-7.4-09	R	REQ-7.4-12X	
REQ-7.4-10	R, PC	REQ-7.4-13X	
	Clause 7.5	Cryptographic controls	
REQ-7.5-01	PC	REQ-7.5-01X	
	Clause 7.6	Physical and environmental security	
REQ-7.6-01	Idem	Note updated	
REQ-7.6-02	Idem		
REQ-7.6-03	Idem		
REQ-7.6-04	Idem		
REQ-7.6-05	Idem	Deleted note	
	Clause 7.7	Operation security	
REQ-7.7-01	Idem	Notes deleted	
REQ-7.7-02	Idem		
REQ-7.7-03	Idem		
REQ-7.7-04	Idem	Note updated	
REQ-7.7-05	Idem	Note added	
REQ-7.7-06	V	removed	
REQ-7.7-07	V	removed	
REQ-7.7-08	R	REQ-7.7-06X	
REQ-7.7-09	R	REQ-7.7-07X	
	NR	REQ-7.7-08X	
	NR	REQ-7.7-09X	
	NR	REQ-7.7-10X	
	Clause 7.8	Network security	
REQ-7.8-01	Idem		
REQ-7.8-02	Idem		
REQ-7.8-03	Idem		
REQ-7.8-04	Idem		
REQ-7.8-05	Idem		
REQ-7.8-06	Idem		
REQ-7.8-07	Idem		
REQ-7.8-08	Idem		
REQ-7.8-09	NCT	REQ-7.8-09X	
REQ-7.8-10	Idem		
REQ-7.8-11	V	removed	
REQ-7.8-11A	R	REQ-7.8-11X	
REQ-7.8-12	Idem		
REQ-7.8-13	Idem		
REQ-7.8-13A	R	REQ-7.8-14X	
	NR	REQ-7.8-15X	
	NR	REQ-7.8-16X	
REQ-7.8-14	R	REQ-7.8-17X	
REQ-7.8-14A	R	REQ-7.8-18X	
REQ-7.8-15	R	REQ-7.8-19X	
REQ-7.8-16	R	REQ-7.8-20X	
REQ-7.8-17	R	REQ-7.8-21X	

	Clause 7.9	Vulnerabilities and Incident management	
	Clause 7.9.1	Monitoring and logging	
REQ-7.9.01	NCT		REQ-7.9.1-01X
REQ-7.9.02	R		REQ-7.9.1-02X
REQ-7.9.03	R		REQ-7.9.1-03X
REQ-7.9.04	NCT		REQ-7.9.1-04X
	Clause 7.9.2	Incident response	
REQ-7.9-05	R, NCT		REQ-7.9.2-01X
	NR		REQ-7.9.2-02X
	NR		REQ-7.9.2-03X
	NR		REQ-7.9.2-04X
	NR		REQ-7.9.2-05X
	NR		REQ-7.9.2-06X
	NR		REQ-7.9.2-07X
	NR		REQ-7.9.2-08X
REQ-7.9.06	R, M		REQ-7.9.2-12X
REQ-7.9-07	R, M		REQ-7.9.3-01X
REQ-7.9-08	R, M		REQ-7.9.3-02X
REQ-7.9-09	R, M		REQ-7.9.1-05X
REQ-7.9-10	R, M		REQ-7.9.2-09X
REQ-7.9-11	R, M		REQ-7.9.2-10X
REQ-7.9-12	R, M		REQ-7.9.2-11X
	Clause 7.9.3	Reporting	
	NR		REQ-7.9.3-03X
	NR		REQ-7.9.3-04X
	Clause 7.9.4	Event assessment and classification	
	NR		REQ-7.9.4-01X
	NR		REQ-7.9.4-02X
	Clause 7.9.5	Post-incident reviews	
	NR		REQ-7.9.5-01X
	NR		REQ-7.9.5-02X
	NR		REQ-7.9.5-03X
	NR		REQ-7.9.5-04X
	Clause 7.10	Collection of evidence	
REQ-7.10-01	Idem		New Note 2
REQ-7.10-02	Idem		
REQ-7.10-03	Idem		
REQ-7.10-04	Idem		
REQ-7.10-05	Idem		
REQ-7.10-06	Idem		
REQ-7.10-07	Idem		
REQ-7.10-08	Idem		In note: Change "media" to "storage media"
	Clause 7.11	Business continuity management	
	Clause 7.11.1	General	
REQ-7.11-01	R		REQ-7.11.1-01X
REQ-7.11-02	R		REQ-7.11.1-02X
	Clause 7.11.2	Back Up	
	NR		REQ-7.11.2-01X
	NR		REQ-7.11.2-02X
	NR		REQ-7.11.2-03X
	NR		REQ-7.11.2-04X
	Clause 7.11.3	Crisis Management	
	NR		REQ-7.11.3-01X
	NR		REQ-7.11.3-02X
	NR		REQ-7.11.3-03X

	Clause 7.12	TSP termination and termination plans	
REQ-7.12-01	Idem		
REQ-7.12-02	Idem		
REQ-7.12-03	Idem		
REQ-7.12-04	Idem		
REQ-7.12-05	Idem		
REQ-7.12-06	Idem		
REQ-7.12-07	Idem		
REQ-7.12-08	Idem		
REQ-7.12-09	Idem		
REQ-7.12-10	Idem		
REQ-7.12-11	Idem		
	Clause 7.13	Compliance	
REQ-7.13-01	Idem		
REQ-7.13-02	Idem		
REQ-7.13-03	Idem		
REQ-7.13-04	Idem		
REQ-7.13-05	Idem		
	Clause 7.14	Supply chain	
	Clause 7.14.1	Supply chain policy	
		NR	REQ-7.14.1-01X
		NR	REQ-7.14.1-02X
		NR	REQ-7.14.1-03X
		NR	REQ-7.14.1-04X
	Clause 7.14.2	Supply chain procedures and processes	
		NR	REQ-7.14.2-01X
		NR	REQ-7.14.2-02X
		NR	REQ-7.14.2-03X
		NR	REQ-7.14.2-04X
		NR	REQ-7.14.2-05X
		NR	REQ-7.14.2-06X
		NR	REQ-7.14.2-07X
		NR	REQ-7.14.2-08X
		NR	REQ-7.14.2-09X
		NR	REQ-7.14.2-10X
		NR	REQ-7.14.2-11X
		NR	REQ-7.14.2-12X
		NR	REQ-7.14.2-13X
		NR	REQ-7.14.2-14X
		NR	REQ-7.14.2-15X
	Clause 7.14.3	Responsibility, third parties agreements and SLA	
		M, NCT	REQ-7.14.3-01X (combines former REQ-6.3-05 and REQ-7.1.1-08)
		M	REQ-7.14.3-02X (former REQ-6.3-06)
		NR	REQ-7.14.3-03X
		M, NCT	REQ-7.14.3-04X (former REQ-7.1.1-07)
		M	REQ-7.14.3-05X (former REQ-7.1.1-09)
		M	REQ-7.14.3-06X (former REQ-7.1.1-10)
		NR	REQ-7.14.3-07X
		NR	REQ-7.14.3-08X
		NR	REQ-7.14.3-09X
		NR	REQ-7.14.3-10X
		NR	REQ-7.14.3-11X
		NR	REQ-7.14.3-12X

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

Regulation (EU) No 910/2014 [i.1]	ETSI EN 319 401
Regulation article 5.1 Data protection	**EU qualified certificate policy reference**
"5 1. Processing of personal data shall be carried out in accordance with Directive 95/46/EC."	REQ-7.13-05 and note
Regulation article 13.2 Liability and burden of proof	**EU qualified certificate policy reference**
"13 2. Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations."	REQ-6.2-02 items f) and g)
Regulation article 15 Accessibility for persons with disabilities	**EU qualified certificate policy reference**
"Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities."	REQ-7.13-03 and REQ-7.13-04
Regulation article 19 **Security requirements applicable to trust service providers**	**EU qualified certificate policy reference**
"19 1. Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk."	Clauses 5, 6.3, 7.2 to 7.12
"In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents."	Clauses 7.9 and 7.11
"19. 2. Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein. Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay."	Clauses 7.9 and 7.11
Regulation article 24 **Requirements for qualified trust service providers**	**EU qualified certificate policy reference**
"24.2 (a) inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities"	REQ-6.3-04X
"24.2 (b) employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards."	Clause 7.2
"24.2 (c) with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law;"	REQ-7.1.1-04
"24.2 (d) before entering into a contractual relationship, inform, in a clear and comprehensive manner, any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use;"	Clause 6.2
"24.2 (e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them;"	REQ-7.4-13X, REQ-7.8-20X and REQ-7.8-21X Clauses 7.5 to 7.8

Regulation (EU) No 910/2014 [i.1]	ETSI EN 319 401

"24.2 (f) use trustworthy systems to store data provided to them, in a verifiable form so that:
    (i)   they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,
    (ii)   only authorised persons can make entries and changes to the stored data,
    (iii)   the data can be checked for authenticity;"
	REQ-7.4-13X, REQ-7.8-20X and REQ-7.8-21X
	Clauses 7.5 to 7.8

Regulation article 24 **Requirements for qualified trust service providers**	**EU qualified certificate policy reference**
"24.2 (g) take appropriate measures against forgery and theft of data;"	Clauses 5, 6.3, 7.2 to 7.12 REQ-7.4-13X, REQ-7.8-20X and REQ-7.8-21X
"24.2 (h) record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;"	Clause 7.12 REQ-7.3.3-02X
"24.2 (i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body."	Clause 7.12
"24.2 (j) ensure lawful processing of personal data in accordance with Directive 95/46/EC."	REQ-7.13-05

Annex C (informative):
Change history

Date	Version	Information about changes
February 2016	2.1.1	Publication.
June 2017	2.2.0	All requirements numbered as per clause 3.3. **REQ-7.1.1-04:** "national law" replaced with "applicable law". Clause 7.8: several requirement rephrased to use active verbal form, with no technical change. **REQ-7.9-1:** reformulated. **REQ-7.12-10:** "where applicable" added before "transferring the TSP obligations to other parties". **REQ-7.13-03:** "where feasible" added at the end of the sentence. Clause 7.13: note updated to include Regulation (EU) 2016/679. **REQ-7.9-11:** the text "*the TSP can determine that the vulnerability does not require remediation when the cost of the potential impact does not warrant the cost of mitigation*" is turned into a note.
January 2018	2.2.1	Following ENAP public enquiry, the following changes were made: • Deletion of REQ-6.1-03 that was replicated. • Deletion of REQ-6.2-02 g) that was replicated. • Addition of REQ-6.3-10 to document the maximum interval between two checks. • Correction of requirement numbering in clause 7.8 (REQ-7.8-04 was used twice).
September 2020	2.2.2	CR#1 Trust service policy definition and use in clauses 6.1-03. CR#2 Policy for separate components provided by third parties in clause 7.1.1. CR#3 Deviation between the note 2 in OVR 5.2-05 in 319 411-1 and REQ-6.1-05 - REQ-6.1-03 in ETSI EN 319 401. CR#4 Editorial cleaning on Void items. CR#5 Explain "notify notice of changes" in REQ-6.1-09. CR#6 REQ-7.2-08 duplicates REQ-7.2-16. CR#7 Redundant requirement REQ-7.2-09 covered by REQ-7.2-16. CR#8 Use of least privilege in clause 7.2.16. CR#9 Move requirements in clauses 7.4 & 7.7 to 7.8. CR#10 REQ-7.8-11 overcautious. CR#11 Time period in REQ-7.8-13. CR#12 Time period in REQ-7.8-14. CR#13 General correct use of term TSP or Trust service component provider. CR#14 REQ-7.13-05 reference ISO/IEC 27701:2019 for guidance.
April 2023		Updates to take into account NIS2 Directive Updates to take into account revision to ISO/IEC 27002:2022
December 2023		Renumbered all new, changed or moved requirements. Removing "void" requirements

History

Document history			
V1.1.1	January 2013	Publication	
V2.0.1	July 2015	Publication as ETSI TS 119 401 (withdrawn)	
V2.1.1	February 2016	Publication	
V2.2.1	April 2018	Publication	
V2.3.1	May 2021	Publication	
V3.1.0	March 2024	EN Approval Procedure	AP 20240530: 2024-03-01 to 2024-05-30
V3.1.1	June 2024	Publication	