

White Paper of the European Signature Dialog

DORA Requirements

Regulatory eco-system of a trusted service provider

Contents

Introduction	2
The Specialty of the provision of Qualified Trust Services	3
Conclusion	5
About European Signature Dialog (ESD)	6
Legal notice	6
Requirements for a trust service	7

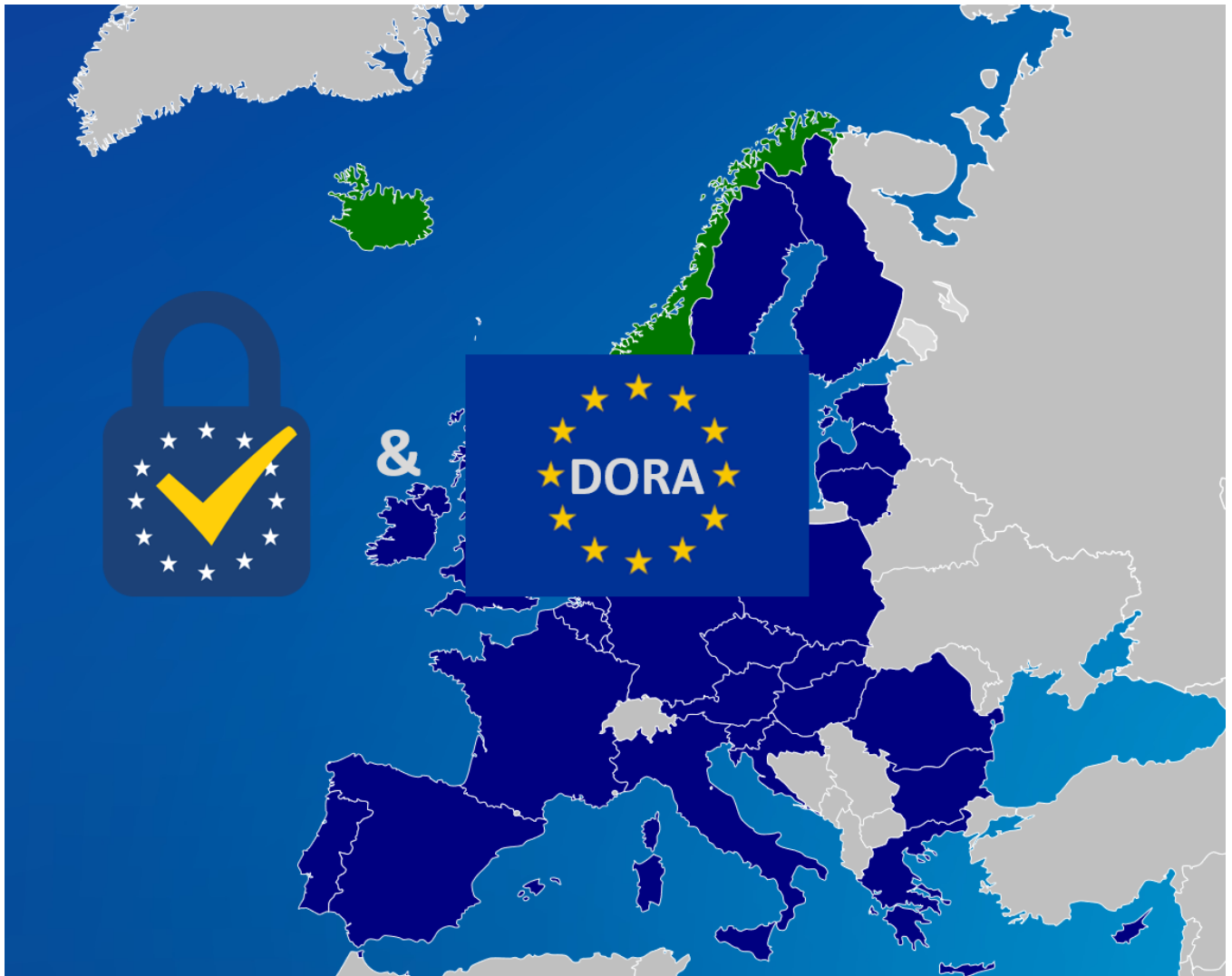
Introduction

With the introduction of DORA (Digital Operational Resilience Act), financial service providers must adhere to a framework for limiting ICT risks. They also oblige their sub-service providers/suppliers to be cyber-resilient.

Qualified trust service providers (QTSPs) are often used by DORA-obliged entities as a service provider for identification, authentication, authenticity assurance, encryption and similar applications with the qualified trust services they provide.

This is where QTSPs differ from most other ICT service providers. They act under their own responsibility and are subject to a very tight regulatory regime with Regulation (EU) 2014/910, amended in May 2024 (eIDAS), including strict regular certification requirements, which in particular also contain the requirements for the NIS2 Directive including the implementing regulation (EU) C(2024) 7151.

This paper is intended to develop a practical recommendation on how DORA obligated parties can deal with QTSPs as ICT service providers so that both DORA obligated parties and QTSPs can fulfil their respective regulatory obligations.



The Specialty of the provision of Qualified Trust Services

In today's digital landscape, trust and security are paramount. Qualified trust services, such as qualified electronic signatures, website certificates, seals, and delivery services, play a crucial role in ensuring the integrity and authenticity of electronic transactions. These services are particularly important for regulated industries, where compliance with stringent standards is essential.

The European Union's eIDAS Regulation sets the framework for qualified trust services, ensuring that these services meet the highest standards of security and reliability. To provide qualified trust services, organizations must obtain prior authorization from their national supervisory authority for each service and any subsequent modifications. This process involves successful certification by an independent conformity assessment body, which must be renewed periodically to maintain qualification status.

Qualified Trust Service Providers (QTSPs) undergo rigorous certification by accredited conformity assessment bodies, with audits repeated every two years. This certification is communicated to the supervisory authority, ensuring that QTSPs adhere to stringent security and quality requirements, many of which are outlined by the European Telecommunications Standards Institute (ETSI).

Once conformity is established and confirmed by the supervisory authority, the trust service provider is included in the EU Trusted List. This comprehensive list validates the conformity of specific services, such as qualified electronic signature services, and affirms that these services have passed rigorous controls. You can access the EU Trusted List via the eIDAS Dashboard: <https://eid.as.ec.europa.eu/efda/tl-browser/#/screen/home>.

Qualified Trust Service Providers generally operate under their own regulatory responsibility without any influence of operation from outside and maintain direct contractual relationships with trust service users, such as signatories. This ensures that services are delivered with the highest level of accountability and compliance.

The certified eIDAS requirements cover the following aspects in particular and not conclusively:

Information security and risk management

- Qualified Trust Service Providers (QTSPs) are subject to strict security requirements and regular audits. They are essential companies, regardless of size, as defined by the NIS2 Directive. In addition to the NIS2 requirements, the implementing act for NIS2 provides detailed requirements for information security, risk management, and related areas, as outlined in the annex. The NIS2 requirements offer a comparable level of protection to the DORA requirements. For informational purposes, a mapping of the requirements from NIS2 and DORA can be found in the annex of this document, which also fulfills the DORA requirements for ICT risk management.
- Furthermore, strict IT security measures must be implemented by Trust Services Providers, such as encryption and access controls.

Auditing and control

- The annual external conformity assessments of Trust Services are carried out by an independent authorised conformity assessment body.
- The audit reports can prove compliance with all applicable eIDAS and NIS2-requirements.

Incident management and reporting

- The NIS2 requirements also mandate that Qualified Trust Service Providers have robust processes in place for identifying and reporting security incidents. Notably, the incident reporting thresholds for trust services are set at a very low level, with a 24-hour timeframe. These requirements extend beyond data breaches and cybersecurity incidents to include service unavailability, ensuring a comparable level of protection aligned with DORA requirements. This supports the DORA incident reporting requirements, emphasizing the importance of timely and comprehensive incident management.

Third-party risk management

- As audited service providers, Trust Services are also subject to strict requirements for managing third-party ICT providers.

Business continuity and resilience

- The high availability requirements for trust services support the DORA specifications for operational resilience.

Nonetheless, leveraging audited trust services can also significantly support DORA compliance and reduce the need for verification and auditing. This is also an advantage of using qualified trust services that the DORA assessment could also be limited to the assessment of the external certification required by the eIDAS Regulation.

Conclusion

Qualified trust service providers are to be afforded special and privileged treatment as ICT service providers under DORA due to the regulatory framework to which they are subject under the eIDAS Regulation. This is due to the closed requirements and certification regime of eIDAS, which make the provision of qualified trust services possible in the first place. This rigid and strict certification regime also makes QTSPs stand out from other NIS2 obligated parties, which are regularly not subject to such strict certification requirements. QTSPs can best be compared with providers of notified electronic identities (eID). These are also subject to a rigid and strict assessment scheme. Here too, special, privileged treatment as an ICT service provider by DORA obligated parties can be assumed on a regular basis. Therefore, complex questionnaires by DORA obliged entities and their analyses can be omitted by limiting the audit of the DORA requirement for ICT service providers to checking the eIDAS certification, which includes fulfilment of the requirements from the NIS2 directive. Furthermore, publicly available mandatory information on the qualified trust services provided, such as the Trust Service Practice Statement (TSPS), can be used for simplified ICT supplier verification by entities subject to DORA. These documents can of course also be provided by the relevant QTSP on request.

Qualified Trust Service Providers (QTSPs) are entitled to privileged treatment as ICT service providers under the DORA framework due to the stringent regulatory requirements they must meet under the eIDAS Regulation. The eIDAS framework's rigorous certification regime, which enables the provision of qualified trust services, distinguishes QTSPs from other entities subject to NIS2. Unlike many NIS2-obligated parties, QTSPs are subject to strict certification requirements, similar to providers of notified electronic identities (eID), who also undergo a rigorous assessment process. Consequently, QTSPs can typically expect privileged treatment as ICT service providers by DORA-obligated entities.

Given this context, complex questionnaires and analyses by DORA-obliged entities can be streamlined by focusing audits on verifying eIDAS certification, which inherently includes compliance with NIS2 requirements. Additionally, publicly available documents such as the Trust Service Practice Statement (CP and CPS) can be used to simplify ICT supplier verification for entities subject to DORA. These documents can also be provided by the relevant QTSP upon request, further facilitating compliance checks.

On the other side, the use of a qualified trust service as a fully externally certified supplier simplifies compliance requirements, particularly in DORA, but also in other cybersecurity or risk management requirements, such as NIS2.

About European Signature Dialog (ESD)

The European Signature Dialog (ESD) is the foremost consortium of leading European Qualified Trust Service Providers (QTSPs), dedicated to enabling secure and trustworthy digital interactions across Europe. Founded in 2017, ESD unites 18 prominent Trust Service Providers (TSPs) from 16 European countries, creating a unified voice to address the evolving challenges and opportunities in the digital trust ecosystem.

Mission and Commitment

ESD's mission is to foster trust, transparency, security, and consumer protection in digital interactions, ensuring adherence to the highest EU standards. By connecting public entities, businesses, and individuals, ESD members work tirelessly to build a secure digital environment where trust is the foundation of every interaction.

Expertise and Influence

With extensive, hands-on experience, ESD members have played a pivotal role in advising European institutions - including the European Commission, Parliament, and Council - since the inception of eIDAS. ESD serves as the primary interlocutor and go-to authority for trust services across the EU, leveraging its deep insights and expertise to drive impactful change.

Global Ambassadors

While rooted in Europe, ESD's influence extends globally. Many member companies actively promote trust services worldwide, including in Africa, China, Ukraine, and beyond, serving as ambassadors of European excellence in digital security.

By uniting expertise, driving collaboration, and amplifying the voice of trust service providers, ESD is paving the way for a secure and trusted digital future for Europe and beyond.

<https://www.european-signature-dialog.eu/>

Legal notice

The information provided in this White Paper is for informational purposes only and does not constitute a binding offer. It is subject to potential errors and changes.

The European Signature Dialog presents the views and opinions of its experts in this document, including on legal judgments such as the DORA and NIS2 regulations. However, no guarantees or liabilities are assumed.

All parties are advised to thoroughly examine their specific circumstances and reach their own informed conclusions. Where necessary, the European Signature Dialog strongly recommends consulting with qualified experts to address specific legal or regulatory issues, particularly in specialized areas of legislation.

Annex: Comparison of eIDAS and NIS2 requirements (ETSI standards) and DORA requirements

Example of reference of ETSI standards in a TSP certificate for the trust service

The certificate includes a list of essential ICT standards established by ETSI, which can serve financial institutions as credible evidence of compliance with the requirements outlined in DORA.

Requirements for a trust service

A trust service has not only to fulfill the eIDAS regulation 910/2014 and the amendment made in eIDAS regulation 2024/1183 but has to follow a lot of detailed regulatory specifications issued by ETSI. Those standards can be found on every certificate of a trusted service provider:

for the following services:

Qualified trust services provided	ETSI AUDIT CRITERIA (name and version)
Qualified certificate for electronic signature (Art. 28 of the eIDAS Regulation)	ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412-2, ETSI EN 319 412-5.
Qualified certificate for electronic seal (Art. 38 of the eIDAS Regulation)	ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412-3.
Qualified certificate for website authentication (Art. 45 of the eIDAS Regulation)	ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412-4.
Qualified validation service for qualified electronic signatures (Art. 33 of the eIDAS Regulation)	ETSI EN 319 401, ETSI TS 119 441, ETSI TS 119 442, ETSI EN 319 102-1, ETSI TS 119 102-2.
Qualified validation service for qualified electronic seals (Art. 40 of the eIDAS Regulation)	ETSI EN 319 401, ETSI TS 119 441. ETSI TS 119 442.

ETSI TR 119 400 (2016-03)
ETSI EN 319 401 (2021-05)
ETSI EN 319 411-1 (2021-05)
ETSI EN 319 411-2 (2021-11)
ETSI EN 319 412-1 (2021-05)

ETSI EN 319 412-2 (2020-07)
ETSI EN 319 412-3 (2020-07)
ETSI EN 319 412-5 (2020-04)
ETSI EN 319 421 (2016-03)
ETSI EN 319 422 (2016-03)

- [ETSI EN 319 401 V3.1.1 \(2024-06\)](#)
Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- [ETSI EN 319 411-1 V1.5.0 \(2024-12\)](#)
Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- [ETSI EN 319 411-2 V2.6.0 \(2024-12\)](#)
Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- [ETSI TS 119 461 V2.1.1 \(2025-02\)](#)
Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
- [ETSI EN 319 421 V1.3.0 \(2025-01\)](#)
Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

Trust Service Providers are also under

- NIS2 directive 2022/2555 and its NIS2 implementing regulation as essential entity
- Cyber Resilience Act
- Critical Entity Resilience Act

The correspondent eIDAS conformity assessment bodies have to follow the following standards:

- [ETSI EN 319 403-1 V2.3.1 \(2020-06\)](#)
Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers
- [ETSI TS 119 403-2 V1.3.1 \(2023-03\)](#)
Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates
- [ETSI TS 119 403-3 V1.1.1 \(2019-03\)](#)
Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers

In the following, we discuss important aspects related to implementing DORA (Digital Operational Resilience Act) article 30 with ICT service providers and integrating it within the auditing of trust services. In particular, eIDAS regulation, NIS2 directive and implementing regulation, ETSI EN 319 401 and EN 319 411-X standards regulate the requirements for risk minimization and cyber resilience. This examination is based on the fundamental obligations that all financial institutions should incorporate into their ICT contracts with suppliers.

DORA Article 30 requirements

Art. 30 (2) (a) a clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider, indicating whether subcontracting of an ICT service supporting a critical or important function, or material parts thereof, is permitted and, when that is the case, the conditions applying to such subcontracting;

Corresponding requirements in regulations and laws for Trust Services

A Trust Service Provider (TSP) must furnish a clear and comprehensive description of all functions and services it provides. This includes indicating to a customer whether the TSP subcontracts any trust service that supports a critical or important function.

Several requirements support the need for a TSP to provide transparency regarding its operations, including the use of subcontractors:

Overall responsibility: A TSP may use other parties to provide parts of the certification service, but the TSP always maintains overall responsibility and ensures that policy requirements are met.

ETSI EN 319 411-01, clause 5.4.1:

OVR-5.4.1-01: The TSP may make use of other parties to provide parts of the certification service.

NOTE: However, the TSP always maintains overall responsibility and ensures that the policy requirements identified in the present document are met (ETSI EN 319 401 [9], requirements REQ-6.3-05 and REQ-6.3-06).

EXAMPLE: A TSP can sub-contract all the component services, including the certificate generation service (referred to as the CA in the present document). However, the key used to sign the certificates is identified as belonging to the CA, and the TSP maintains overall responsibility for meeting the requirements defined in the present document.

ETSI EN 319 421, clause 3.1:

TSA Disclosure statement: set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements

TSA Disclosure statement: set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements

TSA practice statement: statement of the practices that a TSA employs in issuing time-stamp

NOTE: This is a specific type of trust service practice statement as defined in ETSI EN 319 401.

TSA system: composition of IT products and components organized to support the provision of time-stamping services

(...) Clause 4.4:

4.5 Time-stamp policy and TSA practice statement This clause explains the relative roles of time-stamp policy and TSA practice statement. It places no restriction on the form of a time-stamp policy or practice statement specification.

A time-stamp policy is a form of Trust Service Policy as specified in ETSI EN 319 401 [4] applicable to trust service providers issuing time-stamps.

Practise Statement: A trust service 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.

ETSI EN 319 401:

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.

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.

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.

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-7.14.1-01X: 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.

Third-party services: Qualified TSPs can use third parties to operate part or all of the service components of the qualified trust services they provide. The QTSP remains the final entity responsible and liable for the QTS it provides and needs to document and ensure correct implementation of those service components against its declared practices and policies as well as against Regulation (EU) No 910/2014.

ETSI TS 119 403-3:

NOTE 2: QTSPs can make use of third parties, whether (Q)TSPs or not, to operate part or all of the service components of the QTS they provide. In this situation, the QTSP remains the final entity responsible and liable for the QTS it provides and needs to document and ensure correct implementation of those service components against its declared practices and policies as well as against Regulation (EU) No 910/2014 [i.1].

CAR-4.2-09: The CAR shall identify, in accordance with clause 5.5.3 of ETSI TS 119 612 (V2.1.1) [2], the service digital identity(ies) per type of QTS for which the CAR confirms the conformity with the requirements of Regulation (EU) No 910/2014 [i.1] providing at least:

In summary, a TSP has to provide a **clear and complete** description of all its functions and services, making it clear to the customer if any critical or important functions are subcontracted. The TSP remains responsible for all services, whether directly provided or subcontracted.

*DORA Article 30
requirements*

Art. 30 (2) (b) the locations, namely the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed, including the storage location, and the requirement for the ICT third- party service provider to notify the financial entity in advance if it envisages changing such locations;

*Corresponding requirements in regulations and laws for
Trust Services*

Information about the **locations where trust services are provided and where data is processed, including storage locations**, as well as the requirement for advance notification of changes to these locations, can be found in several areas:

Terms and conditions: The Trust Service Provider (TSP) must make available to relying parties the terms and conditions regarding the use of the certificate. The applicable **terms and conditions should be readily identifiable for a given certificate**. These terms and conditions should be communicated through a durable means of communication in a human-readable form before the agreement.

ETSI 319 411-1:

DIS-6.1-04: The TSP shall make available to relying parties the terms and conditions regarding the use of the certificate (see clause 6.9.4).

7.3.4 Dissemination of terms and conditions

ETSI 319 411-3, clause 7.3.4:

The general obligations specified in EN 319 401 [10] clause 6.2 shall apply. In addition the CA shall ensure that the terms and conditions are made available to subscribers and relying parties.

Certificate Policy (CP) and Certification Practice Statement (CPS):

The information about service locations should be available as specified in the TSP's CPS. If the TSP has a **Normalised Certificate Profile (NCP)**, information should be available 24/7, and the TSP should apply best efforts to ensure the service is not unavailable for longer than a maximum period denoted in the CPS. The CP(s) identified by the TSP's documentation should specify the requirements on certificate profiles to be used.

ETSI 319 411-3, clause 7.3.5:

c) The CA shall make available to relying parties the terms and conditions regarding the use of the certificate (see clause 7.3.4).

d) The applicable terms and conditions shall be readily identifiable for a given certificate.(...)

ii) [NCP] the information identified in b) and c) above shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the CA, the CA shall apply best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the certification practice statement.

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

ETSI EN 319 401:

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.

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.

Trusted Lists: The website with specific information about the trust services (e.g., Certificate Policy and Certification Practice Statement) needs to be included in the trusted list.

EU implementing decision (EU) 2015/1505, Annex 1, Chapter 4:

SPECIFICATIONS FOR THE HUMAN READABLE FORM OF THE TRUSTED LIST

When a human readable form of the trusted list is established and published, it shall be provided in the form of a Portable Document Format (PDF) document according to ISO 32000 (3) that shall be formatted according to the profile PDF/A (ISO 19005 (4)).

The content of the PDF/A based human readable form of the trusted list shall comply with the following requirements:

The structure of the human readable form shall reflect the logical model described in TS 119 612;

Every present field shall be displayed and provide:

The title of the field (e.g. 'Service type identifier');

The value of the field (e.g. 'http://uri.etsi.org/TrstSvc/Svctype/CA/QC');

The meaning (description) of the value of the field, when applicable (e.g. 'A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.');

Multiple natural language versions as provided in the trusted list, when applicable.

The following fields and corresponding values of the digital certificates (5), if present in the 'Service digital identity' field shall, as a minimum, be displayed in the human readable form:

Version

Certificate serial number

Signature algorithm

Issuer — all relevant distinguished name fields

Validity period

Subject — all relevant distinguished name fields

Public key

Authority Key Identifier

Subject Key Identifier

Key Usage

Extended key usage

Certificate Policies — all policy identifiers and policy qualifiers

Policy mappings

Subject alternative name

Subject directory attributes

Basic constraints

Policy constraints

CRL Distribution Points (6)

Authority Information Access

Subject Information Access

Qualified Certificate Statements (7)

Hash algorithm

Hash value of certificate

The human readable form shall be easily printable

The human readable form shall be signed or sealed by the Scheme Operator according to PDF advanced signature specified in Articles 1 and 3 of the Commission Implementing Decision (EU) 2015/1505.

Audit reports: The audit attestation shall list the city, state/province (if applicable), and country of all relevant physical locations used in Certification Authority operations.

ETSI 119 403-2:

PTA-4.3-14: The Audit Attestation shall list the city, state/province (if applicable), and country of all relevant physical locations used in Certification Authority operations.

PTA-4.3-15: The Audit Attestation should cover all Root CAs in scope of the audit in one document.

PTA-4.3-15a: In exceptional cases more than one Audit Attestation may be issued per TSP.

NOTE 3: Root programs relying on audits based on ETSI EN 319 403-1 [1] and the present document may place additional mandatory requirements on the audit attestations for TSPs issuing Publicly-Trusted certificates, e. g. the use of one of the Audit Attestation Letter templates provided by the Accredited Conformity Assessment Bodies' Council (ACAB's, see <https://www.acab-c.com/>).

Registry of entities: ENISA shall create and maintain a registry of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, on the basis of the information received from the single points of contact. The registry will contain the Member States where the entity provides services.

NIS2 Directive 2022/2555:**Registry of entities**

1. ENISA shall create and maintain a registry of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, on the basis of the information received from the single points of contact in accordance with paragraph 4. Upon request, ENISA shall allow the competent authorities access to that registry, while ensuring that the confidentiality of information is protected where applicable.

Changes in locations: The TSP must inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities.

eIDAS regulation 910/2014:

2. A qualified trust service provider providing qualified trust services shall:

(a) inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities;

Directory of suppliers and service providers: The relevant entities shall maintain and keep up to date a registry of their direct suppliers and service providers.

NIS2 directive 2022/2555:

5.2. Directory of suppliers and service providers

The relevant entities shall maintain and keep up to date a registry of their direct suppliers and service providers, including:

(a) contact points for each direct supplier and service provider;

(b) a list of ICT products, ICT services, and ICT processes provided by the direct suppliers and service provider to the relevant entity.

Overall, a customer should consult the TSP's terms and conditions, certificate policy, certification practice statement, and trusted lists for details on service locations and data processing locations. Furthermore, the TSP is obligated to inform customers of changes to these locations in advance. The TSP keeps responsibility about any third party processing and has to track the information where the data is processed.

*DORA Article 30
requirements*

Art. 30 (2) c)

(c) provisions on
availability, authenticity,
integrity and
confidentiality in
relation to the
protection of data,
including personal data;

*Corresponding requirements in regulations and laws for
Trust Services*

The following requirements are defined by the regulation:

General Security Measures: Both qualified and non-qualified trust service providers are required to implement appropriate technical and organizational measures to manage risks to the security of their trust services. These measures must ensure a level of security that is commensurate with the degree of risk, considering the latest technological developments.

Article 19 eIDAS regulation, 910/2014:

"Security requirements applicable to trust service providers

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. 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."

ETSI EN 319 411-2 Clause 6.4

ETSI EN 319 411-1, clause 6.4

ETSI EN 319 401, clauses 5, 6.3 and 7.3

ETSI EN 319 401, clause 7.6

ETSI EN 319 401, REQ-7.4-04A to REQ-7.4-09

ETSI EN 319 401, clause 7.2

ETSI EN 319 401, clause 7.10

ETSI EN 319 401, clauses 7.9 and 7.11

ETSI EN 319 401, clause 7.12 (termination)

ETSI EN 319 411-2 Clause 6.5

ETSI EN 319 411-1, clause 6.5

ETSI EN 319 401, clause 7.5

ETSI EN 319 401, REQ-7.4-10, REQ-7.8-16 and REQ-7.8-17

ETSI EN 319 401, clause 7.7

ETSI EN 319 401, clause 7.8

ETSI EN 319 411-1, clause 6.4.8

ETSI EN 319 411-1, clause 6.4.8

ETSI EN 319 401, clauses 7.9 and 7.11

Prevention and Minimization of Impact: Measures should be in place to prevent and minimize the impact of security incidents and to inform stakeholders of any adverse effects.

ETSI EN 319 411-1, clause 6.4.8

ETSI EN 319 411-1, clause 6.4.8

ETSI EN 319 401, clauses 7.9 and 7.11

Notification of Breaches: TSPs are obligated to notify the supervisory body (and other relevant bodies like national bodies for information security or data protection authorities) of any security breach or loss of integrity that has a significant impact on the trust service or personal data. This notification should occur without undue delay and, in any event, within 24 hours of becoming aware of the issue. If the breach is likely to adversely affect a natural or legal person, they must also be notified without undue delay.

Article 19.2 eIDAS regulation 910/2014:

"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."

ETSI EN 319 411-2, clause 6.4.8

ETSI EN 319 411-1, clause 6.4.8

ETSI EN 319 401, clauses 7.9 and 7.11

Specific Requirements for Qualified TSPs: Qualified TSPs have additional requirements to ensure data protection:

Data Storage: They must use trustworthy systems to store data in a verifiable form, ensuring that access is restricted to authorized personnel, data can be checked for authenticity, and data is publicly available only with the consent of the person to whom it relates.

eIDAS regulation 910/2014, art. 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;

ETSI EN 319 411-1, DIS-6.1-04 to DIS-6.1-09
ETSI EN 319 411-1, REG-6.3.4-02 to REG-6.3.4-03 and
OVR-6.3.4-04 to OVR-6.3.4-06
ETSI EN 319 411-2, clause 6.9.4
ETSI EN 319 411-1, clause 6.9.4
ETSI EN 319 401 clause 6.2

(e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them;

ETSI EN 319 411-2, clause 6.5
ETSI EN 319 411-1, clause 6.5
ETSI EN 319 401, clause 7.5
ETSI EN 319 401, clause 7.6
ETSI EN 319 401, REQ-7.4-10, REQ-7.8-16 and REQ-7.8-17
ETSI EN 319 401, clause 7.7
ETSI EN 319 401, clause 7.8

(f) use trustworthy systems to store data provided to it, 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

ETSI EN 319 411-2, clause 6.4.3
ETSI EN 319 411-1, clause 6.4.3
ETSI EN 319 411-2, clause 6.4.6
ETSI EN 319 411-1, clause 6.4.6
ETSI EN 319 411-2, clause 6.5
ETSI EN 319 411-1, clause 6.5
ETSI EN 319 401, clause 7.5
ETSI EN 319 401, clause 7.6
ETSI EN 319 401, REQ-7.4-10, REQ-7.8-16 and REQ-7.8-17
ETSI EN 319 401, clause 7.7
ETSI EN 319 401, clause 7.8

Protection Against Forgery and Theft: Qualified TSPs need to take appropriate measures against forgery and theft of data.

eIDAS regulation 910/2014, art. 24 (2):

(g) take appropriate measures against forgery and theft of data;

ETSI EN 319 411-2, clause 6.4

ETSI EN 319 411-1, clause 6.4

ETSI EN 319 401, clauses 5, 6.3 and 7.3

ETSI EN 319 401, clause 7.6

ETSI EN 319 401, REQ-7.4-04A to REQ-7.4-09 ETSI EN 319 401, clause 7.2

ETSI EN 319 401, clause 7.10

ETSI EN 319 401, clauses 7.9 and 7.11

ETSI EN 319 401, clause 7.12 (termination)

ETSI EN 319 411-2, clause 6.5

ETSI EN 319 411-1, clause 6.5

ETSI EN 319 401, clause 7.5

ETSI EN 319 401, REQ-7.4-10, REQ-7.8-16 and REQ-7.8-17

ETSI EN 319 401, clause 7.7

ETSI EN 319 401 [1], clause 7.8

Recording and Accessibility of Information: They must record and keep accessible all relevant information concerning data issued and received, including after the TSP ceases operations. This is particularly important for providing evidence in legal proceedings and ensuring service continuity.

(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;

ETSI EN 319 411-1, REG-6.2.2-18

ETSI EN 319 411-1, REG-6.3.4-07, REG-6.3.4-08, and REG-6.3.4-17

ETSI EN 319 411-1, REG-6.3.8-02

ETSI EN 319 411-1, REG-6.4.5-04

ETSI EN 319 411-2, clause 6.4.6

ETSI EN 319 411-1, clause 6.4.6

ETSI EN 319 411-2, clause 6.4.9

ETSI EN 319 411-1, clause 6.4.9

ETSI EN 319 401, clause 7.12

ETSI EN 319 401, REQ-7.3.2-02

Termination Plan: Qualified TSPs should have an up-to-date termination plan to ensure service continuity, as verified by the supervisory body.

(i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article 17(4);

ETSI EN 319 411-2, clause 6.4.9

ETSI EN 319 411-1, clause 6.4.9

ETSI EN 319 401, clause 7.12

Lawful Processing of Personal Data: They must ensure the lawful processing of personal data.

(i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article 17(4);

ETSI EN 319 411-2, clause 6.4.9

ETSI EN 319 411-1, clause 6.4.9

ETSI EN 319 401, clause 7.12

Certificate Database: Qualified TSPs issuing qualified certificates must establish and maintain an updated certificate database.

(k) in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database.

ETSI EN 319 411-2, clause 6.1

ETSI EN 319 411-1, clause 6.1

Pseudonyms: The use of pseudonyms in electronic transactions should not be prohibited. If a pseudonym is used, it shall be clearly indicated in qualified certificates.

eIDAS regulation 910/2014 Article 5:

Article 5

Data processing and protection

1. Processing of personal data shall be carried out in accordance with Directive 95/46/EC.

2. Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.

and Annex 1 b), c), d):

(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and:

- for a legal person: the name and, where applicable, registration number as stated in the official records,
- for a natural person: the person's name;

(c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;

(d) electronic signature validation data that corresponds to the electronic signature creation data;

Data Minimization: Authentication for an online service should only process identification data that is adequate, relevant, and not excessive to grant access to that service online.

eIDAS regulation 910/2014 recital 11:

(11) This Regulation should be applied in full compliance with the principles relating to the protection of personal data provided for in Directive 95/46/EC of the European Parliament and of the Council (4). In this respect, having regard to the principle of mutual recognition established by this Regulation, authentication for an online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online. Furthermore, requirements under Directive 95/46/EC concerning confidentiality and security of processing should be respected by trust service providers and supervisory bodies.

Risk Management: TSPs' information security risk assessment and risk treatment should properly reflect its activities and extend to the boundaries of activities concerning trust services. Interfaces with services or activities that are not completely within the scope of the trust services are to be included in the TSP's information security risk assessment.

ETSI EN 319 403-1 V2.3.1:

7.4.1.0 (...) NOTE: The following requirements are considered particularly relevant to separately assessed providers of component services: obligations of external organizations; subcontracting, outsourcing or other third party arrangements and termination. The Conformity Assessment Body shall ensure that the scope and boundaries of the trust services of the TSP are clearly defined in terms of the characteristics of the business, the organization, facilities, assets and technology.

The Conformity Assessment Body shall ensure that the TSP's information security risk assessment and risk treatment properly reflect its activities and extend to the boundaries of activities concerning trust services.

The Conformity Assessment Body shall ensure that interfaces with services or activities that are not completely within the scope of the trust services are included in the TSP's information security risk assessment.

Audits: Supervisory bodies should cooperate with data protection authorities, for example, by informing them about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached.

eIDAS regulation 910/2014, recital 31:

(31) Supervisory bodies should cooperate with data protection authorities, for example, by informing them about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached. The provision of information should in particular cover security incidents and personal data breaches.

Logging: The TSP shall log all events relating to the life-cycle of CA keys and certificates.

ETSI EN 319 411-1 (V1.4.1):

REG-6.4.5-04: All registration information including the following shall be recorded:

- a) type of document(s) presented by the applicant to support registration;
- b) record of unique identification data, numbers, or a combination thereof (e.g. applicant's identity card or passport) of identification documents, if applicable;
- c) storage location of copies of applications and identification documents, including the subscriber agreement (see requirement REG-6.3.4-07);
- d) any specific choices in the subscriber agreement (e.g. consent to publication of certificate, see requirement REG-6.3.4-07);
- e) identity of entity accepting the application;
- f) method used to validate identification documents, if any; and
- g) name of receiving TSP and/or submitting Registration Authority, if applicable.

OVR-6.4.5-04A: The TSP shall document how the information recorded as per REG-6.4.5-04 is accessible.

REG-6.4.5-05: The TSP shall maintain the privacy of subject information.

GEN-6.4.5-06: The TSP shall log all events relating to the life-cycle of CA keys.

GEN-6.4.5-07: Void.

OVR-6.4.5-07A: The TSP shall log all events relating to the life-cycle of certificates as requested by REV-6.3.9-18, REG-6.4.5-03, GEN-6.4.5-08, REV-6.4.5-09, SDP-6.4.5-10 as well as all events relating to certificates generation and dissemination.

Backups: Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure. Back-up arrangements should be regularly tested to ensure that they meet the requirements of business continuity plans.

ETSI EN 319 411-1 (V1.4.1):

OVR-6.4.8-04: Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

OVR-6.4.8-05: Back-up arrangements should be regularly tested to ensure that they meet the requirements of business continuity plans.

OVR-6.4.8-06: Backup and restore functions shall be performed by the relevant trusted roles specified in clause 6.4.4.

OVR-6.4.8-07 [CONDITIONAL]: If risk analysis identifies information requiring dual control for management, for example keys, then dual control should be applied to recovery.

Multi-Factor Authentication: The TSP shall enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

ETSI EN 319 411-1 (V1.4.1):

NOTE 2: With regards general to requirement REQ-7.4-10 "Sensitive data shall be protected" in ETSI EN 319 401 [9], Sensitive data includes registration information.

In addition the following particular requirements apply:

GEN-6.5.5-02: Local network components (e.g. routers) shall be kept in a physically and logically secure environment.

GEN-6.5.5-03: Local network components (e.g. routers) configurations shall be periodically checked for compliance with the requirements specified by the TSP.

GEN-6.5.5-04: The TSP shall enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

Confidentiality and Integrity: The confidentiality and integrity of registration data shall be protected, especially when exchanged with the subscriber/subject or between distributed TSP's system components.

ETSI EN 319 411-1 (V1.4.1):

6.8.4 Privacy of personal information

OVR-6.8.4-01: The requirement REQ 7.13-05 identified in ETSI EN 319 401 [9], shall apply.

In addition the following particular requirements apply:

OVR-6.8.4-02: The confidentiality and integrity of registration data shall be protected, especially when exchanged with the subscriber/subject or between distributed TSP's system components.

OVR-6.8.4-03: Some records may need to be securely retained to meet statutory requirements, as well as to support essential business activities (see clauses 6.4.5 and 6.4.6).

Access to Data: On request by courts or other authorities, a qualified TSP has to grant access to the documentation according to Art. 24 Abs. 2 lit. h eIDAS-VO.

eIDAS VO 910/2014, §24 (2) h:

"... to record and keep accessible for as long as necessary 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, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service."

Identity Proofing: Policy and security requirements for trust service components providing identity proofing of trust service subjects are specified in ETSI TS 119 461 V2.1.1.

These provisions collectively aim to ensure that trust services are provided with appropriate safeguards for data protection, maintaining availability, authenticity, integrity, and confidentiality.

*DORA Article 30
requirements*

Art. 30 (2) (d) provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the financial entity in the event of the insolvency, resolution or discontinuation of the business operations of the ICT third-party service provider, or in the event of the termination of the contractual arrangements;

*Corresponding requirements in regulations and laws for
Trust Services*

Termination Plans: Qualified trust service providers must have up-to-date termination plans to ensure continuity of service, verified by the supervisory body. These plans should address how information is kept accessible.

eIDAS regulation 910/2014 Article 17:

(i) to verify the existence and correct application of provisions on termination plans in cases where the qualified trust service provider ceases its activities, including how information is kept accessible in accordance with point (h) of Article 24(2);

(j) to require that trust service providers remedy any failure to fulfil the requirements laid down in this Regulation.

5. Member States may require the supervisory body to establish, maintain and update a trust infrastructure in accordance with the conditions under national law.

eIDAS regulation 910/2014 Article 24 (2):

(i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article 17(4);

ETSI EN 319 411-2, clause 6.4.9

ETSI EN 319 411-1, clause 6.4.9

ETSI EN 319 401, clause 7.12

Recording and Accessibility of Information: Qualified trust service providers are required to record and keep accessible, for an appropriate period of time, all relevant information concerning data issued and received. This applies even after the trust service provider ceases its activities. The purpose is to provide evidence in legal proceedings and ensure service continuity. Such recording may be done electronically.

eIDAS regulation 910/2014 Article 24 (2):

(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;

(g) take appropriate measures against forgery and theft of data;

(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;

ETSI EN 319 411-1, REG-6.2.2-18
ETSI EN 319 411-1, REG-6.3.4-07, REG-6.3.4-08, and REG-6.3.4-17
ETSI EN 319 411-1, REG-6.3.8-02
ETSI EN 319 411-1, REG-6.4.5-04
ETSI EN 319 411-2, clause 6.4.6
ETSI EN 319 411-1, clause 6.4.6
ETSI EN 319 411-2, clause 6.4.9
ETSI EN 319 411-1, clause 6.4.9
ETSI EN 319 401, clause 7.12
ETSI EN 319 401, REQ-7.3.2-02

Data Retention: The TSP shall document precisely the period of retention of the information in its practices statements and shall indicate which information is subject to be handed over through its termination plan.

ETSI EN 319 411-1 (V1.4.1):

GEN-6.4.5-08: The TSP shall log all events relating to the life cycle of keys managed by the CA, including any subject keys generated by the CA.

REV-6.4.5-09: The TSP shall log all requests and reports relating to revocation, as well as the resulting action.

SDP-6.4.5-10 [NCP+]: The TSP shall log all events relating to the preparation of the subject's device.

OVR-6.4.5-11: The TSP shall document precisely the period of retention of the information mentioned above in its practices statements and shall indicate which information is subject to be handed-over through its termination plan.

Certificate Database: Qualified trust service providers issuing qualified certificates must establish and keep updated a certificate database.... The formats of the certificate database must be suitable for continuation by the supervisory body and must allow determination of whether a certificate was revoked at a specific time. The certificate database must be generally freely accessible, and its queries must be possible free of charge and without identification.

eIDAS regulation 910/2014, Article 24:

"24.2 (k) in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database."

ETSI EN 319 411-2, clause 6.8.4

ETSI EN 319 411-1, clause 6.8.4

ETSI EN 319 401, REQ-7.13-05

Handling of Revocation Status: The TSP's provisions for termination of service shall include the handling of the revocation status for unexpired certificates that have been issued.

ETSI EN 319 411-3 (V1.1.1):

b) Regarding the requirement "The TSP shall state in its practices the provisions made for termination of service" this shall also include the handling of the revocation status for unexpired certificates that have been issued.

7.4.10 Compliance with legal requirements

The requirements identified in EN 319 401 [10], clause 6.4.10 shall apply. In addition the following particular requirements apply:

a) Some records may need to be securely retained to meet statutory requirements, as well as to support essential business activities (see clause 7.4.11).

TSPs' system data backup and recovery: TSP's systems data necessary to resume CA operations shall be backed up and stored in safe places, preferably also remote, suitable to allow the TSP to timely go back to operations in case of incident/disasters.

ETSI EN 319 411-1 (V1.4.1):

6.4.8 Compromise and disaster recovery

OVR-6.4.8-01: The requirements identified in ETSI EN 319 401 [9], clauses 7.9 and 7.11, shall apply.

In addition the following particular requirements apply:

TSP systems data backup and recovery:

OVR-6.4.8-02: TSP's systems data necessary to resume CA operations shall be backed up and stored in safe places, preferably also remote, suitable to allow the TSP to timely go back to operations in case of incident/disasters.

OVR-6.4.8-03: In line with ISO/IEC 27002 [i.7], clause 12.3: Back-up copies of essential information and software should be taken regularly.

Anzeigepflicht (Notification Duty): The Supervisory Body must be promptly notified of any information that needs to be examined for supervisory measures. In the event of insolvency proceedings, the Supervisory Body must react quickly and ensure that the trust services are discontinued in an orderly fashion or continued by another Trust Service Provider.

Obligation of the Supervisory Body

Cooperation in Insolvency: In the event of insolvency, the Supervisory Body must react particularly fast. If necessary, it must ensure that the trust services are discontinued in an orderly manner or continued by another trust service provider.

Obligation of the Supervisory Body

Data Portability: Data subjects have the right to receive personal data concerning them in a structured, commonly used, machine-readable, and interoperable format, and to transmit it to another controller.

GDPR regulation 2016/679, recital 68:

(68) To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

Data Erasure: Data subjects have the right to have their personal data erased under certain conditions, such as when the data is no longer necessary for the purposes for which it was collected, or when the data subject withdraws consent¹².

GDPR regulation 2016/679, recital 64, 65:

(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

(65) A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given.

*DORA Article 30
requirements*

Art. 30 (2) (e) service level descriptions, including updates and revisions thereof

*Corresponding requirements in regulations and laws for
Trust Services*

TSP (Trust Service Provider) duties for service level descriptions, including updates and revisions, involve several key aspects related to their Certificate Policy (CP) and Certification Practice Statement (CPS). These duties ensure transparency, reliability, and adherence to established standards.

Certificate Policy and Practice Statements: TSPs must have a Certificate Policy (CP) and a Certification Practice Statement (CPS). The CP outlines the requirements for the use of certificate profiles. The CPS details the practices the TSP employs in issuing, managing, revoking, and renewing certificates.

ETSI 319 411-1, Clause 4.2.1

The CPS describes how the TSP operates its service and is owned by the TSP: it is tailored to the organizational structure, operating procedures, facilities, and computing environment of the TSP. The CPS defines how the TSP meets the technical, organizational and procedural requirements identified in a Certificate Policy (CP) (see clause 4.2.2). For example, where the CP requires secure management of the private key(s), the CPS can describe the dual-control, secure storage practices, and so on, relying on operational procedures that in turn can provide the details with locations, access lists and access procedures.

ETSI 319 411-3, Clause 3.1

Certification Practice Statement (CPS): statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates

NOTE: See RFC 3647 [i.3].

ETSI 319 411-1, clause 5.2

Content and Structure of CPS: The TSP's CPS should be structured in accordance with IETF RFC 3647. It shall include the signature algorithms and parameters employed.

ETSI 319 411-1, clause 5.2:

OVR-5.2-02: The TSP's CPS should be structured in accordance with IETF RFC 3647 [i.3].

OVR-5.2-03: Void.

OVR-5.2-03A: The CP(s) identified by the TSP's documentation should specify the requirements on certificate profiles to be used.

OVR-5.2-04: The TSP's CPS shall include the signature algorithms and parameters employed.

Public Disclosure: TSPs are required to publicly disclose their CPS through an online means that is available 24 hours a day, 7 days a week. While sensitive information need not be disclosed, the CPS should provide comprehensive details about the TSP's operations.

ETSI 319 411-1, clause 5.2:

OVR-5.2-05: The TSP shall publicly disclose its CPS through an online means that is available on a 24x7 basis.

NOTE 2: The TSP is not obliged to disclose any aspects containing sensitive information.

Terms and Conditions: A TSP is required to issue terms and conditions, which can be part of the CPS or CP, or a standalone document. The target audience of the terms and conditions can be the subscribers, the subjects and the relying parties. The TSP shall communicate the terms and conditions through a durable means of communication, and in a human readable form before the agreement.

ETSI 319 411-1, clause 4.2.3:

4.2.3 Terms and conditions and PKI disclosure statement

A TSP is required to issue terms and conditions (see clause 6.9.4).

This can be as part of the CPS or the CP if issued by the TSP.

Alternatively, this can be a standalone document. The terms and conditions are specific to a TSP. The target audience of the terms and conditions can be the subscribers, the subjects and the relying parties.

Availability of Information: Information outlined in DIS-6.1-01A, DIS-6.1-01B, and DIS-6.1-04 (certificate information and terms of use) should be available as specified in the TSP's CPS. For Network Certificate Policy (NCP), this information should be available 24/7, with best efforts to minimize unavailability due to system failures or other factors.

ETSI 319 411-1:

DIS-6.1-06A [LCP]: The information identified in DIS-6.1-01A, DIS-6.1-01B and DIS-6.1-04 above shall be available as specified in the TSP's CPS.

ETSI EN 319 411-1 V1.4.1 (2023-10) 22

DIS-6.1-07: Void.

DIS-6.1-07A [NCP]: The information identified in DIS-6.1-01A, DIS-6.1-01B and DIS-6.1-04 above shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the TSP, the TSP shall apply best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the CPS.

Updates and Revisions: Revisions to CPs supported by the TSP should be made available to subscribers and relying parties.

ETSI 319 401

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

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

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

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

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-7.14.3-10X: 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.

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.

ETSI 319 411-1

OVR-7.1-07: The TSP should make available the CPs supported by the TSP to its user community.

NOTE: The TSP's user community includes the subscribers/subjects eligible to hold certificates issued under the policy and any parties which rely on those certificates.

OVR-7.1-08: Revisions to CPs supported by the TSP should be made available to subscribers and relying parties.

Framework for Other Certificate Policies: If a TSP issues CPs other than those defined in clause 5, it must demonstrate the effectiveness of these CPs. The CP shall identify which of the certificate policies defined in the present document it adopts as the basis, plus any variances it chooses to apply.

ETSI 319 411-1:

7 Framework for the definition of other certificate policies

7.1 Certificate policy management

OVR-7.1-01: The authority issuing a CP other than the ones defined in clause 5 shall demonstrate that the CP is effective.

In particular, when the TSP issues other CPs:

OVR-7.1-02: The CP shall identify which of the certificate policies defined in the present document it adopts as the basis, plus any variances it chooses to apply.

Service Availability: The TSA should include in its time-stamping disclosure statement availability of its service. For example, expected mean time between failure of the time-stamping service, expected mean time to recovery following a failure and provisions made for disaster recovery including back-up services.

ETSI 319 421:

OVR-6.2-03: The TSA should include in its time-stamping disclosure statement availability of its service.

EXAMPLE: Expected mean time between failure of the time-stamping service, expected mean time to recovery following a failure and provisions made for disaster recovery including back-up services.

In summary, TSPs must maintain and ~~make~~ accessible, up-to-date service level descriptions through their CP and CPS, ensuring that subscribers and relying parties are well-informed about the TSP's practices, policies, and service availability.

*DORA Article 30
requirements*

Art. 30 (2) (f) the obligation of the ICT third-party service provider to provide assistance to the financial entity at no additional cost, or at a cost that is determined ex-ante, when an ICT incident that is related to the ICT service provided to the financial entity occurs;

*Corresponding requirements in regulations and laws for
Trust Services*

Trust Service Provider (TSP) could and should provide assistance to the customer, the cost proposition must be determined in a mutual contract. Here are some points concerning this issue:

Incident response and assistance: Since trust services are NIS2 regulated CSIRTs (Computer Security Incident Response Teams) should be able to respond to incidents and provide assistance to essential and important entities.

NIS2 directive 2022/2555:

3. The CSIRTs shall have the following tasks:

- (a) monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, providing assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems;
- (b) providing early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant stakeholders on cyber threats, vulnerabilities and incidents, if possible in near real-time;
- (c) responding to incidents and providing assistance to the essential and important entities concerned, where applicable;
- (d) collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;
- (e) providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;

Communication: If a significant cyber threat occurs, essential and important entities should communicate, without undue delay, any measures or remedies that service recipients can take to mitigate resulting risks. They should also inform service recipients of the threat itself, especially if it is likely to materialize. This information should be provided free of charge and in easily understandable language.

NIS2 directive 2022/2555:

In the event of an ongoing incident at the time of the submission of the final report, Member States should ensure that entities concerned provide a progress report at that time, and a final report within one month of their handling of the significant incident.

(103) Where applicable, essential and important entities should communicate, without undue delay, to their service recipients any measures or remedies that they can take to mitigate the resulting risks from a significant cyber threat. Those entities should, where appropriate and in particular where the significant cyber threat is likely to materialise, also inform their service recipients of the threat itself. The requirement to inform those recipients of significant cyber threats should be met on a best efforts basis but should not discharge those entities from the obligation to take, at their own expense, appropriate and immediate measures to prevent or remedy any such threats and restore the normal security level of the service. The provision of such information about significant cyber threats to the service recipients should be free of charge and drafted in easily comprehensible language.

Article 23:

Where the entities concerned notify the competent authority of a significant incident under the first subparagraph, the Member State shall ensure that that competent authority forwards the notification to the CSIRT upon receipt.

In the case of a cross-border or cross-sectoral significant incident, Member States shall ensure that their single points of contact are provided in due time with relevant information notified in accordance with paragraph 4.

2. Where applicable, Member States shall ensure that essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself.

Reporting: Essential and important entities must provide progress reports at the time of submitting the final report for ongoing incidents and a final report within one month of handling the significant incident. If a significant incident affects two or more Member States, the CSIRT, competent authority, or single point of contact should inform the other affected Member States and ENISA (European Union Agency for Cybersecurity) without undue delay, while preserving the entity's security and commercial interests and the confidentiality of the information.

NIS2 directive 2022/2555, article 23:

(e) in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident.

By way of derogation from the first subparagraph, point (b), a trust service provider shall, with regard to significant incidents that have an impact on the provision of its trust services, notify the CSIRT or, where applicable, the competent authority, without undue delay and in any event within 24 hours of becoming aware of the significant incident. (...)

6. Where appropriate, and in particular where the significant incident concerns two or more Member States, the CSIRT, the competent authority or the single point of contact shall inform, without undue delay, the other affected Member States and ENISA of the significant incident. Such information shall include the type of information received in accordance with paragraph 4. In so doing, the CSIRT, the competent authority or the single point of contact shall, in accordance with Union or national law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.

Mutual assistance: Supervisory authorities should provide each other with relevant information and mutual assistance to consistently implement and apply regulations, including information requests and supervisory measures like consultations, inspections, and investigations. Requested supervisory authorities should generally supply information by electronic means using a standardized format and should not charge a fee for actions taken in response to a mutual assistance request.

NIS2 directive 2022/2555, article 60:

Mutual assistance

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations. (...)

6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

8. Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).

Incident notification: Qualified and non-qualified trust service providers must notify the supervisory body and other relevant bodies, such as the national body for information security or the data protection authority, of any security breach or loss of integrity that significantly impacts the trust service or personal data within 24 hours of becoming aware of it. If the breach is likely to adversely affect a natural or legal person, they should also be notified without undue delay.

eIDAS regulation 910/2014, article 19(1):

"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."

ETSI EN 319 411-1, clause 6.4.8

ETSI EN 319 411-1, clause 6.4.8

ETSI EN 319 401, clauses 7.9 and 7.1

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.

ETSI EN 319 411-2, clause 6.4.8

ETSI EN 319 411-1, clause 6.4.8

ETSI EN 319 401, clauses 7.9 and 7.11

ETSI EN 319 401, clauses 7.9

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.

Contractual agreements: Conclude contracts for emergency supply with corresponding services, such as for the fuel for emergency power supply. Ensure continuous effectiveness, monitor, maintain, and test the supply of the network and information systems necessary for the operation of the service offered, in particular the electricity, temperature and humidity control, telecommunications and Internet connection.

NIS2 implementing regulation (EU) 2022/2555, clause 13

(e) conclude contracts for the emergency supply with corresponding services, such as for the fuel for emergency power supply;

(f) ensure continuous effectiveness, monitor, maintain and test the supply of the network and information systems necessary for the operation of the service offered, in particular the electricity, temperature and humidity control, telecommunications and Internet connection.

13.1.3. The relevant entities shall test, review and, where appropriate, update the protection measures on a regular basis or following significant incidents or significant changes to operations or risks.

Service Level Agreements (SLAs): Regularly monitor reports on the implementation of service level agreements, where applicable.

NIS2 implementing regulation (EU) 2022/2555, clause 5:

- 5.1.7. For the purpose of point 5.1.6., the relevant entities shall:
- (a) regularly monitor reports on the implementation of the service level agreements, where applicable;
 - (b) review incidents related to ICT products and ICT services from suppliers and service providers;
 - (c) assess the need for unscheduled reviews and document the findings in a comprehensible manner;

The **specific costs** associated with incident assistance may be determined ex-ante through contractual agreements or service level agreements.

*DORA Article 30
requirements*

Art. 30 (2) (g) the obligation of the ICT third-party service provider to fully cooperate with the competent authorities and the resolution authorities of the financial entity, including persons appointed by them;

*Corresponding requirements in regulations and laws for
Trust Services*

Trust Service Providers (TSPs) have a strong obligation to cooperate with competent authorities and supervisory bodies.

While the sources do not explicitly mention "resolution authorities of the financial entity," the broad requirements for cooperation would likely extend to them, especially concerning security breaches, compliance audits, and ensuring the safety and continuity of trust services.

Here's a breakdown of the relevant points:

Cooperation with Supervisory Authorities: TSPs must cooperate with supervisory authorities upon request in the performance of their tasks.

ETSI EN 319 401, clauses 7.9

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.

Example GDPR regulation 2016/679, Article 31:

Cooperation with the supervisory authority

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

Mutual Assistance: Supervisory authorities are expected to provide each other with assistance and cooperate to implement regulations consistently.

eIDAS regulation 910/2014, Article 17(4):

- (a) to cooperate with other supervisory bodies and provide them with assistance in accordance with Article 18;
- (b) to analyse the conformity assessment reports referred to in Articles 20(1) and 21(1);
- (c) to inform other supervisory bodies and the public about breaches of security or loss of integrity in accordance with Article 19(2);
- (d) to report to the Commission about its main activities in accordance with paragraph 6 of this Article;
- (e) to carry out audits or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers in accordance with Article 20(2);

Information Sharing: TSPs must inform supervisory bodies about breaches of security or loss of integrity.

Compliance Audits: TSPs are subject to compliance audits to ensure they meet regulatory requirements.

Cooperation with other Authorities: Competent authorities should ensure appropriate cooperation between law enforcement authorities, data protection authorities, supervisory bodies under Regulation (EU) No 910/2014 and competent authorities under Regulation (EU) 2022/2554.

NIS2 Directive

4. In order to ensure that the tasks and obligations of the competent authorities, the single points of contact and the CSIRTs are carried out effectively, Member States shall, to the extent possible, ensure appropriate cooperation between those bodies and law enforcement authorities, data protection authorities, the national authorities under Regulations (EC) No 300/2008 and (EU) 2018/1139, the supervisory bodies under Regulation (EU) No 910/2014, the competent authorities under Regulation (EU) 2022/2554, the national regulatory authorities under Directive (EU) 2018/1972, the competent authorities under Directive (EU) 2022/2557, as well as the competent authorities under other sector-specific Union legal acts, within that Member State

Although the term "resolution authorities of the financial entity" isn't explicitly used, the general spirit and requirements of the regulations suggest that TSPs would need to cooperate with such authorities, particularly in situations involving financial entities and the need to maintain data security, privacy, and service continuity.

*DORA Article 30
requirements*

Art. 30 (2) (h)
termination rights and
related minimum notice
periods for the
termination of the
contractual
arrangements, in
accordance with the
expectations of
competent authorities
and resolution
authorities;

*Corresponding requirements in regulations and laws for
Trust Services*

The sources discuss termination of Trust Service Providers (TSPs) and related requirements, but they **do not explicitly detail TSP termination rights or minimum notice periods for terminating contractual arrangements** in accordance with the expectations of competent and resolution authorities.

However, the sources do provide relevant information regarding termination plans and related obligations:

Termination Plans: Qualified TSPs must have up-to-date termination plans to ensure service continuity. These plans are verified by a supervisory body.

eIDAS regulation 910/2014, article 24:

24.2 (i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body.²

ETSI EN 319 411-2, clause 6.4.9

ETSI EN 319 411-1, clause 6.4.9

ETSI EN 319 401, clause 7.12

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.

Obligations During Termination: TSPs have several obligations during termination to ensure data and service continuity. These include notifying affected entities, transferring obligations to a reliable party for maintaining necessary information, and handling revocation status for unexpired certificates.

ETSI 319 411-3:

7.4.9 CA termination

The requirements identified in EN 319 401 [10], clause 6.4.9 shall apply. In addition the following particular requirements apply:

- a) Regarding the requirement "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" this shall apply to registration information (see clause 7.3.1), revocation status information (see clause 7.3.6) and event log archives (see clause 7.4.11) for their respective period of time as indicated to the subscriber and relying party (see clause 7.3.4).

ETSI 319 411-1:

6.4.9 Certification Authority or Registration Authority termination
OVR-6.4.9-01: The requirements identified in ETSI EN 319 401 [9], clause 7.12, shall apply.

In addition the following particular requirements apply:

OVR-6.4.9-02: Requirement REQ-7.12-06 of ETSI EN 319 401 [9], shall apply to the following information for their respective period of time as indicated to the subscriber and relying party (see in particular REG-6.3.4-17 and CSS-6.3.10-02):

- a) registration information (see clauses 6.2.2, 6.3.1 and 6.3.4);
- b) revocation status information (see clause 6.3.10);
- c) event log archives (see clauses 6.4.5 and 6.4.6).

(...)

NOTE: Affected entities to be informed of termination under ETSI EN 319 401 [9], REQ-7.12-10 include cross certified TSP.

Data Retention: TSPs must retain registration information, revocation status information, and event log archives for a period of time that is indicated to the subscriber and relying party.

Cooperation: TSPs are required to cooperate with supervisory authorities. Although "resolution authorities" are not explicitly mentioned, the requirements for cooperation likely extend to them.

eIDAS regulation 910/2014, article 19(1):

"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."

ETSI EN 319 411-1, clause 6.4.8

ETSI EN 319 411-1, clause 6.4.8

ETSI EN 319 401, clauses 7.9 and 7.1

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.

ETSI EN 319 411-2, clause 6.4.8

ETSI EN 319 411-1, clause 6.4.8

ETSI EN 319 401, clauses 7.9 and 7.11

TSA Termination: When a Time-Stamping Authority (TSA) terminates its services, it must revoke all non-expired Time-Stamping Unit's (TSU) certificates.

ETSI EN 319 421:

OVR-7.14-02 [CONDITIONAL]: When the TSA terminates its services, the TSA shall revoke all non-expired TSU's certificates.

7.15 Compliance OVR-7.15-01: The requirements identified in ETSI EN 319 401 [4], clause 7.13 shall apply.

While the sources do not specify the rights or minimum notice periods for contractual termination, they emphasize the responsibilities of the TSP to maintain service and data availability. The specific terms for termination rights and notice periods would likely be detailed in the individual contracts between the TSP and its clients, and potentially subject to national laws.

*DORA Article 30
requirements*

Art. 30 (2) (i) the conditions for the participation of ICT third-party service providers in the financial entities' ICT security awareness programmes and digital operational resilience training

*Corresponding requirements in regulations and laws for
Trust Services*

A Trust Service Provider (TSP) is required to undergo ICT security awareness programs and digital operational resilience training. Here's a detailed breakdown:

Training obligations for trust services: TSP staff must show expertise and undergo the necessary trainings.

ETSI EN 319 401:

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-7.2-04X: 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.

Data Protection Training: Appropriate data protection training must be provided to personnel with permanent or regular access to personal data.

GDPR regulation 2016/679, article 47:

(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

Training for Management Bodies: Member States should ensure that the members of the management bodies of essential and important entities are required to follow training. This training should provide them with sufficient knowledge and skills to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

NIS2 directive:

2. Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

Regular Training for Employees: Essential and important entities should be encouraged to offer similar training to their employees on a regular basis.

Basic Cyber Hygiene and Security Training: Relevant entities should adopt a wide range of basic cyber hygiene practices, organize training for their staff, and raise awareness concerning cyber threats, phishing, or social engineering techniques.

NIS2 directive, recital 89:

(89) Essential and important entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness, organise training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques. Furthermore, those entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine-learning systems to enhance their capabilities and the security of network and information systems.

Awareness and Cyber Hygiene: Relevant entities must ensure that their employees, including members of management bodies, as well as direct suppliers and service providers, are aware of risks, are informed of the importance of cybersecurity, and apply cyber hygiene practices.

NIS2 implementing regulation, :

8.1. Awareness raising and basic cyber hygiene practices

8.1.1. For the purpose of Article 21(2), point (g) of Directive (EU) 2022/2555, the relevant entities shall ensure that their employees, including members of management bodies, as well as direct suppliers and service providers are aware of risks, are informed of the importance of cybersecurity and apply cyber hygiene practices.

8.1.2. For the purpose of point 8.1.1., the relevant entities shall offer to their employees, including members of management bodies, as well as to direct suppliers and service providers where appropriate in accordance with point 5.1.4., an awareness raising programme, which shall: (...)

Awareness Raising Programs: Relevant entities should offer their employees an awareness raising program:

- Scheduled over time, repeated, and covering new employees.
- Aligned with network and information security policy and relevant procedures.
- Covering relevant cyber threats, cybersecurity risk-management measures, contact points, resources, and cyber hygiene practices.
- Tested for effectiveness and updated at planned intervals, considering changes in cyber hygiene practices and the current threat landscape.

NIS2 implementing regulation:

(a) be scheduled over time, so that the activities are repeated and cover new employees;

(b) be established in line with the network and information security policy, topic-specific policies and relevant procedures on network and information security;

(c) cover relevant cyber threats, the cybersecurity risk-management measures in place, contact points and resources for additional information and advice on cybersecurity matters, as well as cyber hygiene practices for users.

(...). The awareness raising programme shall be updated and offered at planned intervals taking into account changes in cyber hygiene practices, and the current threat landscape and risks posed to the relevant entities.

Regular Training for Employees with Security Responsibilities:

Relevant entities must identify employees whose roles require security-relevant skill sets and expertise and ensure that they receive regular training on network and information system security. The training should be relevant to the employee's job function and its effectiveness should be assessed.

NIS2 implementing regulation, 8.2.3:

8.2. Security training

8.2.1. The relevant entities shall identify employees, whose roles require security relevant skill sets and expertise, and ensure that they receive regular training on network and information system security.

Training Content: Training should include:

- Instructions regarding the secure configuration and operation of network and information systems, including mobile devices.
- Briefings on known cyber threats.
- Training on behavior when security-relevant events occur.

NIS2 implementing regulation, 8.2.3:

- (a) instructions regarding the secure configuration and operation of the network and information systems, including mobile devices;
- (b) briefing on known cyber threats;
- (c) training of the behaviour when security-relevant events occur.

Training for New Roles: Staff members who transfer to new positions or roles requiring security relevant skill sets and expertise should receive training.

NIS2 implementing regulation, 8.2.4:

8.2.4. The relevant entities shall apply training to staff members who transfer to new positions or roles which require security relevant skill sets and expertise.

Program Updates: The training program should be updated and run periodically, considering applicable policies and rules, assigned roles, responsibilities, as well as known cyber threats and technological developments.

NIS2 implementing regulation, 8.2.5

8.2.5. The program shall be updated and run periodically taking into account applicable policies and rules, assigned roles, responsibilities, as well as known cyber threats and technological developments.

In summary, TSPs are obligated to implement comprehensive ICT security awareness programs and digital operational resilience training to ensure their personnel, including management, employees, and relevant suppliers, are equipped to handle cyber threats and maintain a high level of security.

*DORA Article 30
requirements*

Art. 30 (3)

(a) full service level descriptions, including updates and revisions thereof with precise quantitative and qualitative performance targets within the agreed service levels to allow effective monitoring by the financial entity of ICT services and enable appropriate corrective actions to be taken, without undue delay, when agreed service levels are not met;

*Corresponding requirements in regulations and laws for
Trust Services*

Trust Service Providers (TSPs) are generally required to supply service level descriptions, including updates and revisions, with performance targets to enable effective monitoring and corrective actions.

Here's a breakdown of the requirements:

Service Level Agreements (SLAs): TSPs should include "Service Level Agreements" and/or auditing mechanisms in their service agreements to ensure 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.

ETSI EN 319 401:

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.

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-6.1-09X [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.

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.

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.

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-7.14.2-10X: 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-7.14.2-14X: TSP shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.

Monitoring Reports: Relevant entities should regularly monitor reports on the implementation of the service level agreements, where applicable.

NIS2 implementing regulation 2025/2555:

5.1.7. For the purpose of point 5.1.6., the relevant entities shall:

- (a) regularly monitor reports on the implementation of the service level agreements, where applicable;
- (b) review incidents related to ICT products and ICT services from suppliers and service providers;
- (c) assess the need for unscheduled reviews and document the findings in a comprehensible manner;

Corrective Actions: It's necessary to take mitigating measures in a timely manner, where appropriate. The TSP shall ensure that access permissions are modified accordingly upon termination of employment or change of function. The supervisory body may require that trust service providers remedy any failure to fulfil the requirements laid down in the relevant regulations.

ETSI EN 319 401:

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.

eIDAS regulation 910/2014, article 17:

(j) to require that trust service providers remedy any failure to fulfil the requirements laid down in this Regulation.

Notification of Changes: 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.

ETSI EN 319 401:

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.

Terms and Conditions: Terms and conditions should specify any undertaking regarding availability. Subscribers and parties relying on the trust service shall be informed of precise terms and conditions before entering into a contractual relationship.

ETSI EN 319 401:

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.

Incident Management: The TSP shall establish incident response procedures including containment, eradication and recovery. The TSP shall establish and maintain effective communication plans that include incident categorisation, well-defined escalation procedures, and standardised reporting protocols. The TSP shall test and review regularly and after incidents roles, responsibilities and appropriate procedures. The TSP shall address any critical vulnerability not previously addressed by the TSP, within a period of 48 hours after its discovery. Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized.

ETSI EN 319 401:

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

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-7.9.2-07X: 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-7.9.2-11X: 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.

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.

Review of ICT incidents: Incidents related to ICT products and ICT services from suppliers and service providers should be reviewed.

NIS2 implementing regulation 2025/2555:

5.1.7. For the purpose of point 5.1.6., the relevant entities shall:

- (a) regularly monitor reports on the implementation of the service level agreements, where applicable;
- (b) review incidents related to ICT products and ICT services from suppliers and service providers;
- (c) assess the need for unscheduled reviews and document the findings in a comprehensible manner;

TSA obligations toward subscribers: The terms and conditions made available to relying parties shall include an obligation on the relying party, when relying on a time-stamp.

ETSI EN 319 421:

6.6 Information for relying parties OVR-6.6-01: The terms and conditions made available to relying parties (see clause 6.3) shall include an obligation on the relying party, when relying on a time-stamp,

TSA practice statement: Subscribers and relying parties are expected to consult the TSA's practice statement to obtain further details of precisely how this time-stamp policy is implemented by the particular TSA.

ETSI EN 319 421, clause 4.1:

Subscriber and relying parties are expected to consult the TSA's practice statement to obtain further details of precisely how this time-stamp policy is implemented by the particular TSA (e.g. protocols used in providing this service).

Reporting obligations: The TSP shall comply with reporting obligations as mandated by relevant legislative frameworks for network and information security incidents, including supervisory authorities and CSIRTs. 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.

ETSI EN 319 401:

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-7.9.3-01X: 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.

These measures collectively ensure that customers can effectively monitor ICT services, and that TSPs take appropriate corrective actions without undue delay when service levels are not met.

*DORA Article 30
requirements*

Art. 30 (3)

(b) notice periods and reporting obligations of the ICT third-party service provider to the financial entity, including notification of any development that might have a material impact on the ICT third-party service provider's ability to effectively provide the ICT services supporting critical or important functions in line with agreed service levels;

*Corresponding requirements in regulations and laws for
Trust Services*

Trust Service Providers (TSPs) have specific notice periods and reporting obligations to their customers, particularly concerning developments that could materially impact their ability to deliver ICT services in line with agreed service levels.

Here's a breakdown of these obligations:

Notification of Changes: TSPs must establish procedures to notify relevant parties of significant changes in their service provision, including any intention to cease providing trust services. Trust service providers qualified according to Regulation (EU) 2014/910 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.

ETSI EN 319 401:

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.

Changes to Practice Statement: When TSPs intend 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. The revised TSP's practice statement shall be made immediately available.

ETSI EN 319 401:

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.

Terms and Conditions: TSPs must make the terms and conditions regarding their services available to all subscribers and relying parties. Subscribers and relying parties must be informed of the precise terms and conditions before entering into a contractual relationship.

ETSI EN 319 401:

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-6.2-03: 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.

Incident Reporting:

TSPs must establish procedures to notify the appropriate parties of any breach of security or loss of integrity that has a significant impact on the trust service and personal data within 24 hours of identifying the breach.

If the breach is likely to adversely affect a natural or legal person, that person must also be notified without undue delay.

ETSI EN 319 401:

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..

Incident Response: TSPs shall comply with reporting obligations as mandated by relevant legislative frameworks for network and information security incidents, including supervisory authorities and CSIRTs.

ETSI EN 319 401:

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

Communication Plans: TSPs must establish and maintain effective communication plans that include incident categorization, well-defined escalation procedures, and standardized reporting protocols.

ETSI EN 319 401:

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

Termination of Services:

TSPs must minimize potential disruptions to subscribers and relying parties if services cease.

Before terminating services, the TSP must inform all subscribers, entities with agreements, relying parties, other TSPs, and relevant authorities, such as supervisory bodies.

Information about the termination must be made available to other relying parties.

ETSI EN 319 401:

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.

In addition to these general obligations, essential and important entities are required to adhere to specific timelines for reporting incidents under the NIS2 Directive:

- **Early Warning:** Within 24 hours of becoming aware of a significant incident.
- **Incident Notification:** Within 72 hours of becoming aware of a significant incident, including an initial assessment of the incident's severity and impact.
- **Final Report:** Not later than one month after the incident notification, including a detailed description of the incident, its causes, and mitigation measures.

TSPs must also establish a process for managing information received from CSIRTs or competent authorities regarding incidents, vulnerabilities, and possible mitigation measures. They should regularly test, review, and update their crisis management plans.

NIS2 directive 2022/2555:

(102) Where essential or important entities become aware of a significant incident, they should be required to submit an early warning without undue delay and in any event within 24 hours. That early warning should be followed by an incident notification. The entities concerned should submit an incident notification without undue delay and in any event within 72 hours of becoming aware of the significant incident, with the aim, in particular, of updating information submitted through the early warning and indicating an initial assessment of the significant incident, including its severity and impact, as well as indicators of compromise, where available. A final report should be submitted not later than one month after the incident notification. The early warning should only include the information necessary to make the CSIRT, or where applicable the competent authority, aware of the significant incident and allow the entity concerned to seek assistance, if required. Such early warning, where applicable, should indicate whether the significant incident is suspected of being caused by unlawful or malicious acts, and whether it is likely to have a cross-border impact. Member States should ensure that the obligation to submit that early warning, or the subsequent incident notification, does not divert the notifying entity's resources from activities related to incident handling that should be prioritised, in order to prevent incident reporting obligations from either diverting resources from significant incident response handling or otherwise compromising the entity's efforts in that respect.

Article 23:

4. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority:



- (a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;
- (b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;
- (c) upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates;
- (d) a final report not later than one month after the submission of the incident notification under point (b), including the following:
 - (i) a detailed description of the incident, including its severity and impact;
 - (ii) the type of threat or root cause that is likely to have triggered the incident;
 - (iii) applied and ongoing mitigation measures;
 - (iv) where applicable, the cross-border impact of the incident;

These measures ensure that financial entities are promptly informed of any developments that could affect the quality and reliability of the trust services they receive, enabling them to take timely corrective actions.

*DORA Article 30
requirements*

Art. 30 (3)

(c) requirements for the ICT third-party service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies that provide an appropriate level of security for the provision of services by the financial entity in line with its regulatory framework;

*Corresponding requirements in regulations and laws for
Trust Services*

Trust Service Provider implement and test business continuity plans and have ICT security measures, tools, and policies that ensure an appropriate level of security for service delivery.

Here's a breakdown of what the sources say about these requirements:

Business Continuity and Disaster Recovery:

Trust service providers (TSPs) need a business continuity plan or a disaster recovery plan that addresses potential compromises, losses, or suspected compromises of a CA's private key.

TSPs' systems data required to resume CA operations should be backed up and stored in safe locations to allow for timely restoration of operations after incidents or disasters.

Backup arrangements should be tested regularly to ensure they meet the requirements of business continuity plans.

Incident reporting and responses must be timely and coordinated to quickly respond to incidents and limit the impact of security breaches, which should be reported as soon as possible after the incident.

ETSI EN 319 401:

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.

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-7.11.2-04X: The TSP shall test at planned 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.

ETSI EN 319 411-1:

6.4.8 Compromise and disaster recovery

OVR-6.4.8-01: The requirements identified in ETSI EN 319 401 [9], clauses 7.9 and 7.11, shall apply.

In addition the following particular requirements apply:

TSP systems data backup and recovery:

OVR-6.4.8-02: TSP's systems data necessary to resume CA operations shall be backed up and stored in safe places, preferably also remote, suitable to allow the TSP to timely go back to operations in case of incident/disasters.

OVR-6.4.8-03: In line with ISO/IEC 27002 [i.7], clause 12.3: Back-up copies of essential information and software should be taken regularly.

OVR-6.4.8-04: Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

OVR-6.4.8-05: Back-up arrangements should be regularly tested to ensure that they meet the requirements of business continuity plans.

OVR-6.4.8-06: Backup and restore functions shall be performed by the relevant trusted roles specified in clause 6.4.4.

OVR-6.4.8-07 [CONDITIONAL]: If risk analysis identifies information requiring dual control for management, for example keys, then dual control should be applied to recovery.

CA key compromise:

OVR-6.4.8-08: The TSP's business continuity plan (or disaster recovery plan) shall address the compromise, loss or suspected compromise of a CA's private key as a disaster.

OVR-6.4.8-09: The processes planned as per requirement

OVR-6.4.8-08 shall be in place.

NOTE: It is suggested that the plan includes a requirement that all subject certificates are revoked. This is not necessarily applicable to short-term certificates.

OVR-6.4.8-10: Following a disaster, the TSP shall, where practical, take steps to avoid repetition of a disaster.

ETSI EN 319 411-3:

7.44 Incident reporting and response

b) The CA shall act in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. All incidents shall be reported as soon as possible after the incident.

c) Audit processes, meeting requirements specified in clause 7.4.11, shall be invoked at system startup, and cease only at system shutdown.

7.4.5 Incident reporting and response

b) The CA shall act in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. All incidents shall be reported as soon as possible after the incident.

c) Audit processes, meeting requirements specified in clause 7.4.11, shall be invoked at system startup, and cease only at system shutdown.

(...)

7.4.8 Business continuity management and incident handling

The requirements identified in EN 319 401 [10], clause 6.4.8 shall apply. In addition the following particular requirements apply:

CA systems data backup and recovery

a) CA systems data necessary to resume CA operations shall be backed up and stored in safe places suitable to allow the CA to timely go back to operations in case of incident/disasters.

NOTE 1: In line with ISO/IEC 27002 [i.7], clause 10.5.1: Back-up copies of essential information and software should be taken regularly. Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure. Back-up arrangements should be regularly tested to ensure that they meet the requirements of business continuity plans.

ICT Security Measures, Tools, and Policies:

Both qualified and non-qualified TSPs are obligated to implement suitable technical and organizational measures to handle security risks to their trust services. These measures should align with the degree of risk, considering the latest technological advancements.

TSPs need to take measures to prevent and minimize the impact of security incidents and inform stakeholders of any adverse effects.

TSPs are expected to use cryptographic methods reflecting current best practices to ensure the security and reliability of their trust services.

Physical and environmental security controls are to be in place to protect facilities housing system resources, including measures for physical access control, protection against natural disasters and theft, and ensuring fire safety.

TSPs should have security procedures protecting systems and communications between systems within secure zones. They should configure CA systems by removing or disabling unused accounts, applications, services, protocols, and ports.

Article 19 eIDAS regulation, 910/2014:

"Security requirements applicable to trust service providers

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. 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."

ETSI EN 319 411-2 Clause 6.4

ETSI EN 319 411-1, clause 6.4

ETSI EN 319 401, clauses 5, 6.3 and 7.3

ETSI EN 319 401, clause 7.6

ETSI EN 319 401, REQ-7.4-04A to REQ-7.4-09

ETSI EN 319 401, clause 7.2

ETSI EN 319 401, clause 7.10

ETSI EN 319 401, clauses 7.9 and 7.11

ETSI EN 319 401, clause 7.12 (termination)

ETSI EN 319 411-2 Clause 6.5

ETSI EN 319 411-1, clause 6.5

ETSI EN 319 401, clause 7.5

ETSI EN 319 401, REQ-7.4-10, REQ-7.8-16 and REQ-7.8-17

ETSI EN 319 401, clause 7.7

ETSI EN 319 401, clause 7.8

ETSI EN 319 411-1, clause 6.4.8

ETSI EN 319 411-1, clause 6.4.8

ETSI EN 319 401, clauses 7.9 and 7.11

"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."

ETSI EN 319 411-1, clause 6.4.8

ETSI EN 319 411-1, clause 6.4.8

ETSI EN 319 401, clauses 7.9 and 7.11

eIDAS regulation 2024/1183, recital 73:

Trust service providers should use cryptographic methods reflecting current best practices and trustworthy implementations of those algorithms in order to ensure security and reliability of their trust services.

ETSI EN 319 411-1 V1.4.1:

OVR-6.4.2-07: Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation.

OVR-6.4.2-08: The TSP's physical and environmental security policy for systems concerned with certificate generation and revocation management services shall address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.

OVR-6.4.2-09: Controls shall be implemented to protect against equipment, information, media and software relating to the TSP's services being taken off-site without authorization.

OVR-6.4.2-10: Other functions relating to TSP's operations may be supported within the same secured area provided that the access is limited to authorized personnel.

OVR-6.4.2-11: Root CA private keys shall be held and used physically isolated from normal operations such that only designated trusted personnel have access to the keys for use in signing subordinate CA certificates

6.5.7 Network security controls

OVR-6.5.7-01: The requirements identified in ETSI EN 319 401 [9], clause 7.8 shall apply.

In addition the following particular requirements apply:

OVR-6.5.7-02: The TSP shall maintain and protect all CA systems in at least a secure zone and shall implement and configure a security procedure that protects systems and communications between systems inside secure zones and high security zones.

OVR-6.5.7-03: The TSP shall configure all CA systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations.

Specific Security Controls:

Physical Security: Implement physical and environmental security controls to protect the facility housing system resources.

Network Security: Maintain and protect all CA systems in a secure zone and implement security procedures for systems and communications between zones.

Access Control: Implement access control monitoring and alarm facilities. Access to secure zones and high-security zones should be granted only to trusted roles.

Compromise and Disaster Recovery: The TSP's business continuity plan shall address the compromise, loss, or suspected compromise of a CA's private key as a disaster.

ETSI EN 319411-3:

7.4.5 Dissemination

c) Dissemination application shall enforce access control on attempts to add or delete certificates and modify other associated information.

Revocation management

d) Continuous monitoring and alarm facilities shall be provided to enable the CA to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

NOTE 4: This may use, for example, an intrusion detection system, access control monitoring and alarm facilities.

ETSI EN 319 411-1:

OVR-6.5.7-04: The TSP shall grant access to secure zones and high security zones to only trusted roles.

OVR-6.5.7-05: The Root CA system shall be in a high security zone.

6.5.8 Timestamping

NOTE: Not in the scope of the present document. See ETSI EN 319 421 [i.15] for policy requirements for TSPs issuing time-stamps.

6.6 Certificate, CRL and OCSP profiles

6.6.1 Certificate profile

GEN-6.6.1-01: The certificates shall meet the requirements specified in ISO/IEC 9594-8/Recommendation ITU-T X.509 [7] or IETF RFC 5280 [8].

Broader Policy and Management:

TSPs are responsible for conforming with prescribed procedures, even when outsourcing functionality.

Senior staff and executives involved in certificate generation and revocation management should be free from commercial, financial, or other pressures that might negatively influence trust in their services.

TSPs shall provide the capability to allow third parties to check and test all the certificate types that the TSP issues.

ETSI EN 319 411-1

6.8.6 Representations and warranties

OVR-6.8.6-01: Void.

NOTE 1: TSP has the responsibility for conformance with the procedures prescribed in this policy, even when the TSP's functionality is undertaken by outsourcers.

OVR-6.9.1-03: The senior executive, senior staff and staff in trusted roles, of the TSP concerned with certificate generation and revocation management shall be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.

NOTE: The TSP may need to take into account privacy requirements.

6.9.2 Additional testing

OVR-6.9.2-01: The TSP shall provide the capability to allow third parties to check and test all the certificate types that the TSP issues.

OVR-6.9.2-01A: In the context of OVR-6.9.2-01, the TSP may use certificates issued on the production environment.

OVR-6.9.2-01B [CONDITIONAL]: When certificates issued on the production environment are used for testing purpose in the context of OVR-6.9.2-01A, such production certificates shall conform to the applicable certificate policy requirements.

Requirements for qualified trust service providers

take appropriate measures against forgery and theft of data

have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body

ensure lawful processing of personal data in accordance with Directive 95/46/EC

establish and keep updated a certificate database

eIDAS Regulation 910/2014, article 24.2:

24.2 (g) take appropriate measures against forgery and theft of data;

ETSI EN 319 411-2, clause 6.4

ETSI EN 319 411-1, clause 6.4

ETSI EN 319 401, clauses 5, 6.3 and 7.3

ETSI EN 319 401, clause 7.6

ETSI EN 319 401, REQ-7.4-04A to REQ-7.4-09

ETSI EN 319 401, clause 7.2

ETSI EN 319 401, clause 7.10

ETSI EN 319 401, clauses 7.9 and 7.11

ETSI EN 319 401, clause 7.12 (termination) Clause 6.5

ETSI EN 319 411-1, clause 6.5

ETSI EN 319 401, clause 7.5
ETSI EN 319 401, REQ-7.4-10, REQ-7.8-16 and REQ-7.8-17
ETSI EN 319 401, clause 7.7
ETSI EN 319 401, clause 7.8

(i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article 17(4);

ETSI EN 319 411-2, clause 6.4.9
ETSI EN 319 411-1, clause 6.4.9
ETSI EN 319 401, clause 7.12

24.2 (j) ensure lawful processing of personal data in accordance with Directive 95/46/EC.

ETSI EN 319 411-2, clause 6.8.4
ETSI EN 319 411-1, clause 6.8.4
ETSI EN 319 401, REQ-7.13-05

24.2 (k) in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database.

ETSI EN 319 411-2, clause 6.1
ETSI EN 319 411-1, clause 6.1

*DORA Article 30
requirements*

Art. 30 (3)

(d) the obligation of the ICT third-party service provider to participate and fully cooperate in the financial entity's TLPT as referred to in Articles 26 and 27;

*Corresponding requirements in regulations and laws for
Trust Services*

Trust Service Providers (TSPs) are obliged to perform penetration testing:

Penetration Testing Requirement: 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. The penetration test should be performed at least once per year. 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.

ETSI EN 319 401:

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.

Vulnerability Scanning: The TSP should 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. The vulnerability scan should be performed once per quarter.

ETSI EN 319 401:

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.

The sources don't explicitly use the term "threat-led penetration testing," but the risk assessment and vulnerability scanning requirements imply that penetration testing should be informed by potential threats relevant to the TSP's operations.

*DORA Article 30
requirements*

Art. 30 (3) (e) the right to monitor, on an ongoing basis, the ICT third-party service provider's performance, which entails the following:

EN Official Journal of the European Union L 333/52 27.12.2022

(i) unrestricted rights of access, inspection and audit by the financial entity, or an appointed third party, and by the competent authority, and the right to take copies of relevant documentation on-site if they are critical to the operations of the ICT third-party service provider, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies;

(ii) the right to agree on alternative assurance levels if other clients' rights are affected;

*Corresponding requirements in regulations and laws for
Trust Services*

The ability for financial entities and competent authorities to monitor a Trust Service Provider's (TSP) performance on an ongoing basis, including rights of access, inspection, audit, and cooperation, - eventually by third party auditors - is facilitated by several regulations such as NIS2 directive. It entails several key aspects:

Rights of Access, Inspection, and Audit:

Competent authorities in the scope of NIS2 have **unrestricted rights** to access, inspect, and audit the TSP. This includes the right to take copies of relevant documentation on-site if they are critical to the TSP's operations. In case of a severe incident financial entities could trigger such an inspection or audit if necessary:

NIS2 directive 2012/2555, article 32/33:

2. Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to:

- (a) on-site inspections and off-site supervision, including random checks conducted by trained professionals;
- (b) regular and targeted security audits carried out by an independent body or a competent authority;
- (c) ad hoc audits, including where justified on the ground of a significant incident or an infringement of this Directive by the essential entity;
- (d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned;
- (e) requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;
- (f) requests to access data, documents and information necessary to carry out their supervisory tasks;
- (g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

*DORA Article 30
requirements*

(iii) the obligation of the ICT third-party service provider to fully cooperate during the onsite inspections and audits performed by the competent authorities, the Lead Overseer, financial entity or an appointed third party; and

(iv) the obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits;

*Corresponding requirements in regulations and laws for
Trust Services*

Supervisory Powers and Measures:

Competent authorities must have a **minimum list of supervisory measures** and means to supervise essential and important entities. This includes on-site inspections and off-site supervision conducted by trained professionals.

These authorities can request information necessary to assess cybersecurity risk-management measures and compliance.

Article 58:

1. Each supervisory authority shall have all of the following investigative powers:

- (a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;
- (b) to carry out investigations in the form of data protection audits;
- (c) to carry out a review on certifications issued pursuant to Article 42(7);
- (d) to notify the controller or the processor of an alleged infringement of this Regulation;
- (e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
- (f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

These rights are designed to **ensure compliance** with regulations and to verify the TSP's operational effectiveness.

(122) In order to strengthen the supervisory powers and measures that help ensure effective compliance, this Directive should provide for a minimum list of supervisory measures and means through which the competent authorities can supervise essential and important entities. In addition, this Directive should establish a differentiation of supervisory regime between essential and important entities with a view to ensuring a fair balance of obligations on those entities and on the competent authorities.

Therefore, essential entities should be subject to a comprehensive ex ante and ex post supervisory regime, while important entities should be subject to a light, ex post only, supervisory regime. Important entities should therefore not be required to systematically document compliance with cybersecurity risk-management measures, while the competent authorities should implement a reactive ex post approach to supervision and, hence, not have a general obligation to supervise those entities. The ex post supervision of important entities may be triggered by evidence, indication or information brought to the attention of the competent authorities considered by those authorities to suggest potential infringements of this Directive. For example, such evidence, indication or information could be of the type provided to the competent authorities by other authorities, entities, citizens, media or other sources or publicly available information, or could emerge from other activities conducted by the competent authorities in the fulfilment of their tasks.

(125) The competent authorities should ensure that their supervisory tasks in relation to essential and important entities are carried out by trained professionals, who should have the necessary skills to carry out those tasks, in particular with regard to conducting on-site inspections and off-site supervision, including the identification of weaknesses in databases, hardware, firewalls, encryption and networks. Those inspections and that supervision should be conducted in an objective manner.

The effective exercise of these rights **cannot be impeded or limited** by other contractual arrangements or implementation policies.

Audits and Security Scans:

Regular and targeted security audits can be carried out by an **independent body or a competent authority**. Ad hoc audits may also occur if there's a significant incident or an infringement of the relevant directive.

See sources above.

Security scans based on **objective, non-discriminatory, fair, and transparent risk assessment criteria** are also part of the monitoring process.

See sources above.

Cooperation with Relevant Authorities:

Competent authorities should cooperate with relevant authorities of the Member State concerned under Regulation (EU) 2022/2554.

NIS2 directive 2022/2555:

4. In order to ensure that the tasks and obligations of the competent authorities, the single points of contact and the CSIRTs are carried out effectively, Member States shall, to the extent possible, ensure appropriate cooperation between those bodies and law enforcement authorities, data protection authorities, the national authorities under Regulations (EC) No 300/2008 and (EU) 2018/1139, the supervisory bodies under Regulation (EU) No 910/2014, the competent authorities under Regulation (EU) 2022/2554, the national regulatory authorities under Directive (EU) 2018/1972, the competent authorities under Directive (EU) 2022/2557, as well as the competent authorities under other sector-specific Union legal acts, within that Member State.

5. Member States shall ensure that their competent authorities under this Directive and their competent authorities under Directive (EU) 2022/2557 cooperate and exchange information on a regular basis with regard to the identification of critical entities, on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents affecting entities identified as critical entities under Directive (EU) 2022/2557, and the measures taken in response to such risks, threats and incidents. Member States shall also ensure that their competent authorities under this Directive and their competent authorities under Regulation (EU) No 910/2014, Regulation (EU) 2022/2554 and Directive (EU) 2018/1972 exchange relevant information on a regular basis, including with regard to relevant incidents and cyber threats.

Article 32:

10. Member States shall ensure that their competent authorities under this Directive cooperate with the relevant competent authorities of the Member State concerned under Regulation (EU) 2022/2554. In particular, Member States shall ensure that their competent authorities under this Directive inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity that is designated as a critical ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554. with this Directive.

Role of Supervisory Authorities:

Member States must designate supervisory bodies to carry out supervisory activities. These bodies ensure that qualified TSPs meet regulatory requirements through ex-ante and ex-post supervisory activities.

eIDAS regulation 910/2014:

(30) Member States should designate a supervisory body or supervisory bodies to carry out the supervisory activities under this Regulation. Member States should also be able to decide, upon a mutual agreement with another Member State, to designate a supervisory body in the territory of that other Member State.

(31) Supervisory bodies should cooperate with data protection authorities, for example, by informing them about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached. The provision of information should in particular cover security incidents and personal data breaches.

Article 17:

3. The role of the supervisory body shall be the following:

(a) to supervise qualified trust service providers established in the territory of the designating Member State to ensure, through ex ante and ex post supervisory activities, that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in this Regulation;

Reporting and Transparency:

Supervisory bodies must report to the Commission about their main activities. Breaches of security or loss of integrity must be communicated to supervisory bodies and, where applicable, to other relevant bodies.

eIDAS regulation 910/2014:

4. For the purposes of paragraph 3 and subject to the limitations provided therein, the tasks of the supervisory body shall include in particular:

(a) to cooperate with other supervisory bodies and provide them with assistance in accordance with Article 18;

(b) to analyse the conformity assessment reports referred to in Articles 20(1) and 21(1);

(c) to inform other supervisory bodies and the public about breaches of security or loss of integrity in accordance with Article 19(2);

(d) to report to the Commission about its main activities in accordance with paragraph 6 of this Article;

(e) to carry out audits or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers in accordance with Article 20(2);

These regulations and measures collectively ensure that the monitoring of a TSP's performance is not only possible but also a required and ongoing process, promoting accountability, security, and compliance via competent authorities and their corresponding conformity assessment bodies.

*DORA Article 30
requirements*

- (f) exit strategies, in particular the establishment of a mandatory adequate transition period:
- (i) during which the ICT third-party service provider will continue providing the respective functions, or ICT services, with a view to reducing the risk of disruption at the financial entity or to ensure its effective resolution and restructuring;
- (ii) allowing the financial entity to migrate to another ICT third-party service provider or change to in-house solutions consistent with the complexity of the service provided.

*Corresponding requirements in regulations and laws for
Trust Services*

When a Trust Service Provider (TSP) exits or terminates its services, several measures must be taken to ensure continuity and minimize disruption for customers relying on qualified signatures. These measures include having **termination plans, transferring obligations, and maintaining accessible information**.

The following regulatory requirements show how a TSP can continue providing the respective functions for qualified signatures during exit:

Termination Plans: Qualified TSPs must have up-to-date termination plans to ensure service continuity, as verified by a supervisory body. These plans should address how the TSP will handle ongoing services and data after cessation.

eIDAS regulation 910/2014, recital 41

(41) To ensure sustainability and durability of qualified trust services and to boost users' confidence in the continuity of qualified trust services, supervisory bodies should verify the existence and the correct application of provisions on termination plans in cases where qualified trust service providers cease their activities.

eIDAS regulation 910/2014, Article 24(2):

(i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article 17(4);

ETSI EN 319 411-2, clause 6.4.9

ETSI EN 319 411-1, clause 6.4.9

ETSI EN 319 401, clause 7.12

Transfer of Obligations: The TSP should transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period. This includes registration information, revocation status information, and event log archives.

ETSI 319 411-3:

7.4.9 CA termination

The requirements identified in EN 319 401 [10], clause 6.4.9 shall apply. In addition the following particular requirements apply:

a) Regarding the requirement "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" this shall apply to registration information (see clause 7.3.1), revocation status information (see clause 7.3.6) and event log archives (see clause 7.4.11) for their respective period of time as indicated to the subscriber and relying party (see clause 7.3.4).

Data Accessibility: TSPs must record and keep accessible all relevant information concerning data issued and received, even after the TSP's activities have ceased. This is crucial for providing evidence in legal proceedings and ensuring service continuity.

eIDAS regulation 910/2014, Article 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;

ETSI EN 319 411-1, REG-6.2.2-18

ETSI EN 319 411-1, REG-6.3.4-07, REG-6.3.4-08, and REG-6.3.4-17

ETSI EN 319 411-1, REG-6.3.8-02

ETSI EN 319 411-1, REG-6.4.5-04

ETSI EN 319 411-2, clause 6.4.6

ETSI EN 319 411-1, clause 6.4.6

ETSI EN 319 411-2, clause 6.4.9

ETSI EN 319 411-1, clause 6.4.9

ETSI EN 319 401, clause 7.12

ETSI EN 319 401, REQ-7.3.2-02

Certificate Database Management: Qualified TSPs issuing qualified certificates need to establish and maintain an updated certificate database. In the event of ceasing operations, the TSP must either revoke the qualified certificates valid at the time or ensure that its certificate database can be taken over by another qualified TSP. The TSP should also ensure the database is maintained, and if they cannot, the supervisory body will ensure its continuation at the TSP's expense.

**Detailed regulations in each national signature act,
for example: Austrian Signature Act:**

Beendigungsplan und Vertrauensinfrastruktur

§ 9. (1) Ein qualifizierter VDA hat der Aufsichtsstelle zumindest drei Wochen im Vorhinein die geplante Einstellung seiner Tätigkeit anzuzeigen.

(2) Sofern der qualifizierte VDA qualifizierte Zertifikate ausstellt, hat er die im Zeitpunkt der Einstellung seiner Tätigkeit gültigen qualifizierten Zertifikate zu widerrufen oder dafür Sorge zu tragen, dass zumindest seine Zertifikatsdatenbank von einem anderen qualifizierten VDA übernommen werden kann und wird. Auch im Fall des Widerrufs der qualifizierten Zertifikate hat der qualifizierte VDA sicherzustellen, dass die Zertifikatsdatenbank weitergeführt wird; kommt er dieser Verpflichtung nicht nach, so hat die Aufsichtsstelle als Teil ihrer Vertrauensinfrastruktur (§ 14 Abs. 3) für die Weiterführung der Zertifikatsdatenbank auf Kosten des qualifizierten VDA Sorge zu tragen.

Informing Relevant Parties: The TSP must inform affected entities of the termination, including cross-certified TSPs. This communication ensures that all parties are aware of the changes and can take necessary actions.

ETSI 319 411-1:

6.4.9 Certification Authority or Registration Authority termination (...)

NOTE: Affected entities to be informed of termination under ETSI EN 319 401 [9], REQ-7.12-10 include cross certified TSP.

Revocation Status: The TSP needs to handle the revocation status for unexpired certificates that have been issued.

These measures ensure that during the exit of a TSP, the functions necessary for qualified signatures continue to be provided, minimizing disruption for customers and ensuring effective resolution and restructuring.

ETSI EN 319 411-3, 7.4.9:

b) Regarding the requirement "The TSP shall state in its practices the provisions made for termination of service" this shall also include the handling of the revocation status for unexpired certificates that have been issued.

*DORA Article 30
requirements*

By way of derogation from point (e), the ICT third-party service provider and the financial entity that is a microenterprise may agree that the financial entity's rights of access, inspection and audit can be delegated to an independent third party, appointed by the ICT third-party service provider, and that the financial entity is able to request information and assurance on the ICT third-party service provider's performance from the third party at any time.

*Corresponding requirements in regulations and laws for
Trust Services*

The Conformity Assessment Body shall ensure that the TSP's information security risk assessment and risk treatment properly reflect its activities and extend to the boundaries of activities concerning trust services. The financial entity could verify by the published audit or existence on the EU trust list that the TSP fulfills all its obligations.

ETSI EN 319 411-3:

7.4.1 Audit Scope

7.4.1.0 Audit Scope General

The documentation of the Conformity Assessment Body shall include the policies and procedures for implementing the audit process, including check lists used in the audit and the procedures for assessing the conformity of the TSP, the trust services it provides or the component service or collection of components being assessed with the criteria against which the audit is carried out. The audit team shall audit the TSP and the trust service(s) it provides, covered by the defined scope, against all applicable audit requirements. When the scope of the assessment is a component service or a collection of components services, the audit team shall evaluate them only against the requirements identified as applicable to the specific component service or collection.

NOTE: The following requirements are considered particularly relevant to separately assessed providers of component services: obligations of external organizations; subcontracting, outsourcing or other third party arrangements and termination.

The Conformity Assessment Body shall ensure that the scope and boundaries of the trust services of the TSP are clearly defined in terms of the characteristics of the business, the organization, facilities, assets and technology.

The Conformity Assessment Body shall ensure that the TSP's information security risk assessment and risk treatment properly reflect its activities and extend to the boundaries of activities concerning trust services.

The Conformity Assessment Body shall ensure that interfaces with services or activities that are not completely within the scope of the trust services are included in the TSP's information security risk assessment.