

Paloma LLaneza

A Lawyer's Perspective: How to 'Qualify' Trust Services

CA Day

Heraklion - 26 September 2024



How does a lawyer's mind work?

- We are presented with a problem or asked for advice based on the interpretation of the law or contracts (binding between the parties who enter into them).
- Legal systems are based on published laws (European continental system) or precedent (Anglo-Saxon system).
- Our specialty is the law.



Soft law

- Increasingly, and derived from the Anglo-Saxon system, laws are complemented by norms, standards, technical documentation, public and/or private schemes that:
 - Are not mentioned in the text of acts, laws or regulations;
 - Are not published in any official journal;
 - Are not indexed in legal sources, judicial cases or precedent; and
 - Are not publicly or freely accessible, such as ISO standards or standards from national standardisation bodies.

By the way, ETSI standards ARE publicly and freely accessible

**When a lawyer is
tasked with
advising a client on
the qualification
process, they face a
treasure hunt**



certidas



Treasure hunt

- Under the scope of the eIDAS1 Regulation:
 - Not every trust service can be qualified. The list of qualifying services is published in a specific version of an ETSI-ESI Technical Specification;
 - The implementing act that was supposed to reference applicable standards never materialised;
 - The applicable ETSI-ESI technical standards of the eIDAS1 scheme come from decisions made by national supervisors who agreed on the conformity assessment scheme.

A lawyer navigates an unfamiliar environment and must acquire knowledge that is counterintuitive to their training and experience



certeidas

These new knowledge is ...

- Knowledge of third-party conformity assessment systems → There are no legal norms that regulate them.
- Knowledge of what an accredited scheme is → In the case of Spain, there is a mention in the Industry Law and a regulation governing the accreditation body ENAC.
- Knowledge of what standardisation is and how standards are developed → Private entities generate standards.
- Knowledge of how standards are created: private entities represented in technical working groups that reach consensus agreements.

A new perspective on regulation that includes regulatory instruments that do not appear in official bulletins and involves private entities reaching non-binding consensus agreements.

Conformity Assessment Scheme for Trust Service Providers (TSPs)

Based on Regulation eIDAS and EN 319 403

- ❖ Purpose: Ensure that Trust Service Providers (TSPs) meet legal requirements across the European Union.
- ❖ Process:
 - ✓ Audit and Certification: TSPs are audited by accredited bodies to verify their compliance with standards. ETSI EN 319 403
 - ✓ EU-Wide Scope: This scheme ensures that TSPs operate under a common trust framework across Europe.

Value of Conformity Assessments Across the EU

- ❖ Regulation (EU) 2019/515 of the European Parliament and of the Council of 19 March 2019 establishes the framework for the mutual recognition of certifications issued by nationally accredited conformity assessment bodies. This regulation aims to facilitate the application of the principle of mutual recognition and eliminate illegal obstacles to the free movement of goods and services in the European single market.
- ❖ It establishes procedures to minimise the possibility of creating illegal obstacles to the free movement of goods already legally marketed in another Member State.
- ❖ This regulation replaces the previous Regulation (EC) No 764/2008.

What is a Qualified Trust Service Provider (QTSP)?

- A Qualified Trust Service Provider (QTSP) is a Trust Service Provider (TSP) that meets specific requirements under the eIDAS Regulation and has undergone a formal qualification process.
- QTSPs provide trust services that meet the highest standards of security and reliability, ensuring that digital transactions are secure, legally binding, and interoperable across the European Union.

How is a Trust Service Provider Qualified under eIDAS?

- The qualification process under eIDAS requires a TSP to meet strict criteria set out in the regulation, which involves:
 - **Conformity Assessment:** A TSP must undergo a conformity assessment conducted by an accredited conformity assessment body. This process evaluates whether the TSP complies with the relevant eIDAS requirements, including security measures, procedures, and technical specifications.
 - **Supervisory Body Approval:** Once the conformity assessment is complete, the supervisory body of the respective Member State reviews the findings and determines whether the TSP should be granted qualified status.
 - **Continuous Monitoring:** After being granted qualified status, the QTSP is subject to ongoing supervision to ensure compliance with the eIDAS requirements over time.

Why is Qualification Important under eIDAS?

- **Legal Certainty:** Qualified status ensures that trust services are legally recognised across the EU, providing assurance to users that the services meet stringent security and technical standards.
- **Interoperability:** QTSPs can operate seamlessly across all EU Member States, supporting the free flow of digital services and cross-border transactions.
- **Market Advantage:** Being recognized as a QTSP can offer significant competitive advantages, as it signals trustworthiness and compliance with the highest legal and security standards.

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

This European Standard specifies general policy requirements for Trust Service Providers (TSPs), regardless of the specific trust services they offer.

Scope and Applicability

- ✓ Applies to all types of TSPs, providing a foundation for trust services in the European digital market.
- ✓ Aims to meet requirements of the eIDAS Regulation and the NIS2 Directive.
- ✓ Addresses general requirements for security management and cybersecurity of both qualified and non-qualified trust services.

Significance

ETSI EN 319 401 V3.1.1 plays a crucial role in:

- ✓ Establishing a harmonized framework for trust services across the EU
- ✓ Enhancing interoperability and trust in digital transactions
- ✓ Providing a foundation for specific trust service standards
- ✓ Addressing cybersecurity requirements in line with evolving EU regulations

Updates in Version 3.1.1

There are several key differences and updates from the previous version 2.3.1:

- **Alignment with NIS2 Directive:** The new version aims to meet the requirements of the NIS2 Directive (EU) 2022/2555, which identifies qualified trust service providers as essential entities subject to cybersecurity risk management measures.
- **Enhanced cybersecurity focus:** There's a stronger emphasis on cybersecurity requirements to align with the evolving EU regulatory landscape.
- **Supply chain management:** A new section (7.14) has been added, covering supply chain policy, procedures, processes, and third-party agreements.
- **Vulnerabilities and Incident management:** Section 7.9 has been expanded to include more detailed requirements on monitoring, logging, incident response, reporting, event assessment, and post-incident reviews.
- **Updated references:** The document includes references to newer EU regulations and standards, such as the Digital Services Act, Data Governance Act, and the proposed European Digital Identity Framework.
- **Restructuring:** Some sections have been reorganized or expanded to provide more comprehensive guidance.
- **Annex updates:** Annex A provides a mapping between requirement numbers in version 2.3.1 and the new version, indicating significant changes in structure and content.
- **Broader regulatory alignment:** The standard now aims to support compliance with a wider range of EU regulations related to digital services, data governance, and cybersecurity.

Paloma Llaneza
pllaneza@certicar.es



Thanks!

certeidas