



Hackhofergasse 5/16

A-1190 Vienna

phone: +43 676 940 9309

office@european-signature-dialog.eu

ZVR-nr: 579746942

Business Cases of Qualified Trust Services for IT-Security Applications (NIS2)

Contents

- A. Introduction and Aim of this Document
- B. Specific Application Possibilities of Qualified Trust Services:
- C. About European Signature Dialog (ESD)
- D. Legal notice
- E. ANNEX – eIDAS trust services suitable for use in IT Security Applications

A. Introduction and Aim of this Document

Strengthening IT security is one of the key challenges of our time. Multiple international crises, persistent threat scenarios, and rising concerns over digital sovereignty are driving lawmakers to act. It is therefore logical that the European legislator adopted several important legal instruments in the past legislative period.

One of the most significant is undoubtedly Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union ("NIS2").

NIS2 obliges Member States to adopt a **national cybersecurity strategy**. It also requires the designation of **national Computer Security Incident Response Teams (CSIRTs)** tasked with addressing risks and incidents. A **Single Point of Contact** is intended to facilitate cross-border cooperation among authorities in different Member States.

NIS2 imposes stricter requirements than its predecessor on both national authorities and private-sector stakeholders across a wide range of industries, while also harmonising the sanctioning powers of Member States. To achieve these objectives, NIS2 provides for the possibility of mandating the use of specially certified products and components in sensitive areas for entities subject to its provisions.

In addition, the final sentence of Article 24(1) paragraph 2 of NIS2 states:

"Furthermore, Member States shall encourage essential and important entities to use qualified trust services."

NIS2 thus offers a legal entry point for establishing business models for **qualified trust services** in the field of network and information security. However, these business models rely on **Member States actively promoting and adopting such services**.

A review conducted by the European Signature Dialog (ESD) in January 2025 on the implementation status of NIS2 across ten EU Member States revealed that many had yet to implement the directive. Only two Member States (Italy and Romania) had even included the obligation to promote qualified trust services in their national implementation laws. In none of the Member States examined were concrete administrative recommendations or usage guidelines for qualified trust services provided.

As of May 2025, the European Commission found that 19 Member States had still not sufficiently transposed NIS2, prompting it to prepare infringement proceedings.

From ESD's perspective, Article 24(1) paragraph 2 has not been properly implemented in any of the Member States analysed.

This creates a clear need to **develop and promote concrete use cases for qualified trust services**, which can then be referenced at the national legislative or administrative level to fulfil NIS2 obligations.

Qualified trust services, as defined under Regulation (EU) No 910/2014 ("eIDAS"), last amended in 2024, are particularly well suited for use by NIS2-obligated entities. These services and their providers ("QTSPs") are subject to rigorous regulation, regular audits by independent conformity assessment bodies, and ongoing supervision by national authorities.

Their regulation is intended to foster trust in digital environments and replace analog equivalents such as stamps, signatures, official documents, and formal delivery mechanisms. With the eIDAS revision, QTSPs themselves have also become subject to NIS2, linking the trust service and the provider under a single security framework.

This document therefore pursues the following objectives:

1. To urge EU Member States to **implement NIS2 as swiftly and thoroughly as possible**, thereby strengthening IT security in Europe.
2. To draw attention to the fact that Article 24(1) paragraph 2 NIS2—the obligation to encourage the use of qualified trust services by entities subject to NIS2—has **not yet been implemented in most Member States**.
3. To **disseminate and compile viable use cases** for qualified trust services in the IT security domain, providing a foundation for both fulfilling Article 24(1) paragraph 2 and enhancing Europe's cybersecurity in a targeted and effective way.

B. Specific Application Possibilities of Qualified Trust Services:

- **Use of QWAC to Secure Websites Against Phishing Attacks**

Qualified Website Authentication Certificates (QWACs) contain the verified identity of the domain holder, including validation of their internet domain.

Under the 2024 eIDAS reform, browsers are required to display QWACs in a user-friendly manner. QWACs are therefore effective tools in preventing phishing and related attacks. Phishing is on the rise and poses an increasing threat to individuals, particularly in the context of critical infrastructure.

It is in the interest of both citizens and businesses that the websites of critical infrastructure providers and comparable institutions are clearly recognisable as genuine and authentic. When a QWAC is used, consumers can more easily and instantly recognise whether a website relies on a validated identity.

This not only enhances protection against phishing but also helps combat disinformation, as users can verify whether a website and its content are genuine and trustworthy. Furthermore, the entry of sensitive data on fake websites can be prevented, as the user is able to identify at a glance whether the site is based on a validated identity.

In contrast, conventional TLS certificates only validate the domain itself, allowing phishing attacks to remain a threat.

Examples of Attacks That Could Have Been Prevented:

- Phishing email requesting customers to update their account data:
https://www.t-online.de/digital/aktuelles/id_100415938/warnung-fuer-commerzbank-kunden-betrueger-verschicken-neue-phishing-mails.html
- Fake websites imitating media brands to promote harmful behaviour:
<https://www.welt.de/wirtschaft/article241159399/Anlagebetrug-Der-gefaelschte-Hoehle-der-Loewen-Artikel.html>

- **Securing QR Codes with QWACs Against Qlshing and QRIjacking Attacks**

The starting point for this topic is a similar IT security issue that has been a concern for supervisory authorities for some time. It stems from attack vectors associated with the use of unsecured QR codes.

The use of a QWAC to secure QR codes offers a potential countermeasure against Qlshing or QRIjacking attacks (i.e., phishing via QR codes, redirection to a phishing page, or the substitution of a QR code within an active application).

When a user scans a QR code, the validated identity of the domain holder—and not merely the domain name, which can be easily manipulated—is displayed before the link opens, in line with the eIDAS requirement for user-friendly display. This enables the user to instantly identify the true destination of the QR code.

Examples of Attacks That Could Have Been Prevented:

- A QR code placed over a vending machine redirects users to a phishing website:
<https://www.heise.de/news/Quishing-Zunahme-von-Phishing-Betrugsmasche-mit-QR-Codes-9852122.html>
- An analogue phishing letter with a fake QR code is delivered to a customer's mailbox:
<https://www.br.de/nachrichten/netzwelt/betrug-mit-qr-code-falsches-bankschreiben-geht-um,UMdn0ji>

- **QSeal and QEVS for Securing the Origin and Authenticity of Important Documents and Publications**

QSeal has long been used to ensure the authenticity and origin of documents. This traditional application is equally relevant for entities subject to NIS2 obligations.

In particular, QSeal is suitable for protecting critical internal documents (e.g., processes, work instructions) as well as external communications (e.g., digital business letters, consumer information, press releases) against social engineering, phishing, or disinformation attacks.

QSeal validation can be conducted securely and efficiently through QEVS—completely automatically and without the need for human interaction—directly within the application (e.g., CRM systems or electronic files) to verify the origin, validity, and authenticity of the sealed content.

Examples of Attacks That Could Have Been Prevented:

- A manipulated work instruction is inserted as part of a so-called CEO fraud to trick the finance department into transferring funds to the fraudster's account:
<https://polizei.nrw/en/article/ceo-fraud-high-risk-of-fraud-for-companies>
- A fake press release spreads false information—such as purported site closures—potentially impacting the company's stock value:
<https://www.waz-online.de/lokales/wolfsburg/vw-fake-internetseite-verbreitet-vermeintlichen-ig-metall-plan-BRWGPDV4HBCV5PZLICNZDGO3R4.html>

- **PSD2 Model with QWAC/QSeal for Interface Protection and Automated Data Exchange**

The so-called PSD2 model offers a secure method for accessing data through interfaces involving multiple access roles across different parties—without the need for complex and error-prone manual onboarding procedures.

The model is named after the European legal act that regulates and establishes this interface authentication system: the Payment Services Directive 2 (Directive EU 2015/2366). This directive enables payment service providers to access banking APIs for payment initiation and account information retrieval.

At first glance, the PSD2 model resembles the system of authorization certificates. Both approaches rely on PKI infrastructures and certificates with validated identities and attributes for access control. However, unlike authorization certificates, the PSD2 model utilizes the well-established eIDAS tools—QSeal and QWAC—offering a publicly validated PKI anchored in the EU Trusted List. This eliminates the need for developing separate standards, certification schemes, trust service providers, or infrastructures.

Moreover, the architecture is market-open, allowing QWAC and QSeal to be applied in other contexts. To regulate interface access, specific attributes must be embedded in the corresponding certificates to define the type and scope of access.

This mechanism is equally applicable to NIS2-obligated entities—for instance, in automated data exchanges between supervisory authorities and obligated entities (such as legal interception) or among various obligated entities themselves.

Examples of Attacks That Could Have Been Prevented:

- A data leak occurs via an unsecured API:
<https://www.derstandard.at/story/3000000227326/hacker-erbeuten-33-millionen-telefonnummern-bei-authy>
- Data shared with a recipient exceeds authorized limits:
<https://rsw.beck.de/aktuell/daily/meldung/detail/rechtswidrige-polizeiermittlungen-mit-daten-aus-der-luca-app>

- **Onboarding Processes Involving QSeal, QET, and QES to Mitigate Supplier and Product Compliance Risks**

In today's rapidly evolving digital landscape, businesses face increasing pressure to demonstrate compliance, ensure transparency, and maintain the integrity of their supply chains.

Qualified electronic seals (QSeal), qualified electronic timestamps (QET), and qualified electronic signatures (QES) have emerged as powerful tools to address these challenges. These digital solutions can enhance business processes in a variety of applications, from **supply chain management** to the upcoming **Digital Product Passport (DPP)**.

As supply chains become more complex, verifying compliance with regulations—such as cybersecurity protocols and environmental standards—becomes increasingly critical. Qualified electronic seals and timestamps offer a robust solution:

The upcoming Digital Product Passport initiative by the EU aims to enhance product transparency and sustainability. Qualified electronic tools play a vital role in its implementation:

- **Data Authenticity:** QSeal can certify the origin and integrity of information contained in the DPP, ensuring that product data is reliable and verified.
- **Chronological Tracking:** QET can document the lifecycle of a product—from raw material sourcing to end-of-life—providing a clear timeline for sustainability efforts.
- **Compliance Documentation:** QES and QSeal can be used to validate compliance documentation, user manuals, and safety information required in the DPP.

The application of these digital tools extends to various sectors:

- **Textiles and Fashion:** Brands can use QSeal to certify the ethical sourcing of materials and production processes.
- **Electronics:** Manufacturers can use QET at critical stages in the product lifecycle, aiding in recycling efforts and compliance with environmental standards.
- **Automotive:** QSeal can secure component traceability data, facilitating recalls and supporting circular economy practices.
- **Financial Industry:** QSeal can secure supply chain documentation in accordance with Article 30 of the DORA Regulation.

QSeal and QES are fundamental in ensuring the **authenticity** of digital documents:

Tamper-Evident: Any unauthorized alterations to sealed documents become immediately apparent, preserving the integrity of records.

Origin Verification: Electronic seals function as a digital corporate stamp, unequivocally identifying the source of the document or data.

Scalability: These tools can be applied to individual documents or deployed at scale for high-volume operations, making them suitable for organizations of all sizes.

By adopting these technologies, businesses can stay ahead of regulatory requirements, strengthen the credibility of their supply chains, and prepare for the implementation of the Digital Product Passport. In an era where data integrity and origin are paramount, these digital tools deliver the assurance and efficiency that modern enterprises and consumers demand.

- **Usage of QES, QSeal, and QEAA for Authorization, Authentication, and KYC Processes**

Qualified trust services are well-suited for identification and authentication processes involving both natural and legal persons (KYC) and are already widely used in this context—particularly in anti-money laundering, where they are recognized as suitable tools under current EBA guidelines and, in the future, under the EU AML Regulation.

KYC processes are not limited to anti-money laundering; they are also applicable for the remote onboarding of employees, freelancers, suppliers, and service providers to prevent impersonation attacks and identity fraud.

The relevant qualified trust services include QES for natural persons and QSeal for legal entities. Required credentials and attributes—such as diplomas, licenses, qualifications, and existing certifications—can be verified and validated using QEAA.

- **Secure Delivery of Emails Using QERDS**

The secure transmission of emails and attachments is essential for mitigating IT-related risks.

Communications from unverified actors can lead to impersonation attacks, phishing, and the distribution of malicious attachments.

These risks can be prevented by using QERDS, which ensures high-assurance identification of both sender and recipient, while also confirming successful message delivery.

QERDS thus provides the necessary foundation for the secure exchange of electronic invoices and contracts—whether between NIS2-obligated entities and their suppliers or service providers, or between such entities and supervisory authorities or certification bodies.

- **Electronic Archiving of Important Data Using QEAS**

NIS2-obligated entities are subject to a wide range of retention requirements.

Complete, secure, and auditable storage of evidence and data in various formats is essential—particularly in preparation for conformity assessments and audits by the relevant supervisory authorities.

By using a QEAS, the effort required for compliant archiving can be significantly reduced, while simultaneously ensuring the necessary security and safeguarding the completeness and integrity of the stored data.

- **Use of QEAA for Access Control, Particularly in Zero Trust Networks**

Zero Trust Security is an increasingly adopted concept aimed at enhancing IT security. It is based on the principle that no user, device, or network should be inherently trusted.

Unlike traditional security models—which assume that the internal network is trustworthy and focus on controlling access from the outside—Zero Trust approaches require continuous verification and authentication of all users and devices, regardless of their origin or location.

Authentication is often performed using credentials and attestations signed with certificates. Qualified trust services—particularly Qualified Electronic Attestation of Attributes (QEAA)—can be effectively used in this context.

QEAs enable the mapping of different rights and roles, as well as access to various applications and systems. They offer the distinct advantage that all data contained within the attestation is verified, originates from a verified issuer, and is interoperable across multiple applications.

- **Preservation with PQC Against Algorithm Compromise; QTSPs as Experts in Post-Quantum Cryptography**

Given the anticipated advancements in quantum computing over the coming years, it will become necessary to replace current encryption methods—such as RSA—with **post-quantum cryptography (PQC)**.

Qualified trust services are fundamentally based on cryptographic methods. The revised eIDAS Regulation has already established the regulatory framework to ensure that these services continually rely on up-to-date and secure cryptographic standards.

This means that companies subject to NIS2 requirements can benefit seamlessly from the transition to PQC-based solutions when relying on qualified trust services.

At the same time, Qualified Trust Service Providers (QTSPs) will gain substantial expertise in PQC during this transition—expertise that can also be leveraged in the company's non-trust-service applications, particularly within its own corporate PKI.

C. 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.

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.

D. Legal Notice

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

The European Signature Dialog presents the views and opinions of its experts in this document; however, no guarantees are made, and no liability is assumed.

All parties are encouraged to carefully assess their individual circumstances and reach their own informed conclusions.

Where appropriate, the European Signature Dialog strongly recommends consulting qualified professionals to address specific legal or regulatory matters, particularly in specialized areas of law.

In case you wish more information please write us:

European Signature Dialog

Mail to office@european-signature-dialog.eu

D. ANNEX

eIDAS Trust Services Suitable for Use in IT Security Applications

The following qualified trust services under eIDAS are generally suitable for application in IT security contexts and thus for entities subject to NIS2 obligations:

- **Qualified Electronic Signatures (QES)**

- **Integrity Assurance:** Electronic signatures confirm the authenticity and integrity of digital documents, ensuring that compliance records have not been altered since their creation.
- **Legal Validity:** These tools provide legal proof that documents remain unchanged, which is essential for demonstrating compliance with regulatory requirements.

- **Qualified Electronic Seals (QSeal)**

- **Integrity Assurance:** Electronic seals confirm the authenticity and integrity of digital documents, ensuring that compliance records have not been altered since their creation.
- **Legal Validity:** These tools provide legal proof that documents have remained unchanged, which is essential for demonstrating compliance with regulatory requirements.

- **Qualified Electronic Timestamps (QET)**

- **Time-Bound Proof:** Qualified timestamps bind data to a specific date and time, providing irrefutable evidence of when compliance measures were implemented or verified.

- **Qualified Electronic Preservation Services (QEPS)**

- **Preservation of Evidential Value:** These services preserve the evidential value of electronic signatures and seals, ensuring they can still be successfully validated years later using current cryptographic standards.

- **Qualified Electronic Validation Services (QEVs)**
 - **Proof of Validity:** QEVs provide sealed validation reports that serve as definitive proof of a signature's or seal's validity, eliminating the need for third-party verification.
- **Qualified Website Authentication Certificates (QWAC)**
 - **Verified Domain/URL and Ownership:** QWAC verifies both the domain/URL and the identity of the domain owner.
 - **User-Friendly Display:** Browsers must display the use of a QWAC in a user-friendly way, making it easy to verify if communication is taking place with a QWAC-secured site.
 - **Encryption of Data Traffic:** Like any TLS certificate, QWAC encrypts the data traffic between communicating parties.
- **Qualified Electronic Registered Delivery Services (QERDS)**
 - **Integrity of the Data:** QERDS establishes a presumption of integrity and authenticity for transmitted data.
 - **Identification of Sender and Recipient:** Both sender and recipient are identified at a high level of assurance, extending the legal presumption to their identities.
 - **Verified Receipt:** There is also a presumption of successful receipt and associated timestamp.
- **Qualified Electronic Attestation of Attributes (QEAA)**
 - **Original Documentary Evidence:** QEAA's carry the same evidential value as analogue documents issued by authentic sources, attesting to specific attributes or qualifications.
- **Qualified Electronic Archiving Services (QEAS)**
 - **Integrity and Accuracy of Archived Data:** These services provide a legal presumption of the integrity, authenticity, completeness, and accuracy of archived data.
 - **Proof of Data Origin:** The legal presumption also extends to the origin of data, as specified within the archive.
- **Qualified Electronic Ledgers (QEL)**
 - **Unambiguous and Accurate Chronological Order:** There is a legal presumption that entries are unambiguous, chronologically correct, and consecutive.

- ***Integrity of the Entries:*** A presumption also applies to the integrity and authenticity of all ledger entries.