



Hackhofergasse 5/16

A-1190 Vienna

phone: +43 676 9409309

office@european-signature-dialog.eu

Streamlining Digital Obligations and Compliance in the EU Digital Omnibus

1. GENERAL REMARKS

Europe's digital regulatory framework has reached a critical point.

The proliferation of horizontal and sectoral acts - including the NIS 2 Directive, Cyber Resilience Act (CRA), Artificial Intelligence Act (AI Act), revised eIDAS Regulation, Data Act, and GDPR - has created a complex ecosystem that absorbs resources, slows innovation, and limits the competitiveness of European service providers.

Qualified Trust Service Providers (QTSPs), as the cornerstone of digital trust, face particularly acute challenges. **Multiple compliance regimes** (NIS, GDPR, DORA, eIDAS) and **overlapping audit obligations** have become unsustainable.

Providers dedicate **disproportionate resources** to **compliance and reporting**, rather than **innovation and service delivery**.

Meanwhile, global Big Tech firms keep setting de facto standards through simple, user-friendly solutions quickly adopted by European citizens.

These solutions, once entrenched, such as web browsers, operating systems, and payment wallets, become nearly impossible to displace, further **weakening Europe's competitiveness**.

2. KEY CHALLENGES

2.1 Fragmentation and Excessive Audits

QTSPs are subject to recurring audits from supervisory bodies, conformity assessment bodies (CABs), cybersecurity authorities under NIS 2, and data protection authorities under GDPR.

This creates a fragmented compliance landscape with divergent requirements and duplicative inspections.

Furthermore, accredited sector-standard audits and certifications should be regarded as sufficient compliance evidence by authorities and commercial clients. Customers should not request further or duplicative checks once an accredited audit has been passed.

Proposed :

Introduce a **single-audit framework** for QTSPs and other critical digital providers, recognized by all competent authorities (supervisory, NIS 2, GDPR, DORA). Formalize a mutual recognition principle: **one comprehensive audit report** from an accredited body should satisfy all overlapping obligations.

2.2 Misaligned Timelines and Missing Standards

Regulatory implementation calendars across digital acts are inconsistent.

For instance, AI Act and CRA impose compliance dates before publication of harmonised standards, leaving industry without benchmarks. The EUDI Wallet depends on over 190 standards still in development and without common certification schemes, yet implementation is scheduled by end of 2026, with interoperability as the goal to avoid national silos. Such misalignment creates legal uncertainty and discourages investment.

Proposed modification:

Introduce a **“stop-the-clock” clause** across all digital regulations, ensuring obligations take effect only **36 months after** the relevant harmonised standards are published in the Official Journal of the European Union. Enshrine this as a horizontal simplification rule in the Digital Omnibus, encouraging innovation-driven regulatory design.

2.3 Overlapping and Contradictory Legal Provisions

Persistent **inconsistencies appear across key regulations:**

- eIDAS 2 promotes EUDI Wallet for strong customer authentication (SCA); PSD2-3/PSR lack clarity on interoperability and liability.
- AMLR Article 22 allows eIDs with a Level of Assurance (LoA) Substantial to be used for opening bank accounts, which fully aligns with anti-money laundering (AML) requirements and risk controls, even in scenarios where the potential for damage or misuse is greater than signing a contract.

In contrast, Article 24 of eIDAS 2 demands LoA High for qualified certificates. This disparity underscores the need to move away from an incoherent approach and instead favor solutions that support adoption and simplicity for both citizens and businesses.

- The Digital Product Passport (ESPR) omits reference to qualified trust services under eIDAS, despite these providing scalable trust features. This risks redundant infrastructure where trusted digital identities already exist.

Applying eIDAS services to DPP would ensure data integrity and legal value, creating synergies with environmental and industrial goals.

Proposed modification:

Establish a **Regulatory Consistency Board** under DG CONNECT to resolve cross-regulatory contradictions before delegated acts are adopted.

Each new act should undergo **interoperability impact assessment** for consistency **with existing EU rules** (AI Act, CRA, NIS 2, eIDAS, PSD3/PSR, AMLR, ESPR). Mandate a **reality check on Levels of Assurance** (LoA), factoring in costs and benefits. Extend “stop-the-clock” where proportionality and practical feasibility are required.

2.4 Complexity and Unsustainable Compliance Costs for QTSPs

Operating under the eIDAS framework **already entails substantial financial and operational commitments**, including continuous investment in compliance, security certification, and infrastructure: each service (QES, QeRDS, QEAA, eArchiving) requires distinct conformity assessments, incident reports, and continuous supervision. When combined with the additional obligations introduced by the **NIS 2 Directive**, these requirements **significantly and disproportionately multiply the administrative and financial burden** on QTSPs, creating overlapping compliance layers that may not proportionally enhance overall security.

Additionally, the extension of CRA’s horizontal cybersecurity requirements to QTSPs would overlap with eIDAS’ thorough security obligations and cause legal uncertainty about which regime prevails. CRA’s broad requirements are suited for general digital products, not for the already high-assurance providers governed by eIDAS. This double regulation hampers innovation and increases costs.

Proposed modification:

- Establish a **Trust Service Simplification Track**, exempting QTSPs from redundant conformity assessments if existing regimes (NIS 2 or CRA) already prove sufficient guarantees.
- **Exclude QTSPs from the CRA**, letting eIDAS remain their main legal instrument; confine CRA to general digital products.
- Define a **proportional documentation regime** for low-risk services, allowing micro and small QTSPs to use simplified templates and risk-based reporting.

2.5 The EUDI Wallet: Excessive Standardisation and Delayed Benefits

The European Digital Identity Wallet rollout faces major hurdles: nearly 190 technical standards and certifications, postponed country deployments, and no sustainable business model for Wallet providers while robust national schemes (SPID, itsme, BankID, Identité Numérique, Evrotrust) already exist.

The proposed draft FprCEN/TS 18098 standard which mandated a hybrid remote identity verification process, requiring both automated biometric and manual human checks, and prohibiting fully automated onboarding, even when automation meets the highest security and reliability levels, was rightfully rejected by CEN member-states' representatives on 10.10.2025. This rejection is a step in the right direction. For the onboarding of personal identification data within European Digital Identity Wallets using identity documents, no additional requirements should be introduced under CEN/TS 18098 beyond those already established for Extended LoIP in ETSI EN 119 461 v2.1.1. This standard comprehensively defines the applicable use cases and remains the authoritative reference for identity proofing. Fully automated identity verification and binding to the applicant should be permitted to foster adoption and scalability of Wallet solutions, while hybrid biometric or manual processes should be mandated only in cases of clearly demonstrated exceptional risk. Creating new or overlapping standards for equivalent purposes should be explicitly avoided, as it adds complexity without tangible security or compliance benefits.

Proposed modification:

- Apply a **modular compliance model** under eIDAS 2: Wallet Providers should demonstrate conformity via existing QTSP certifications, **without duplicative audits**.
- Introduce a **Sustainability Assessment** for public investment in Wallet frameworks, ensuring clear cost-benefit analysis and realistic adoption forecasts including opportunities for viable market operators to build new business models with added value and without defining state monopolists instead of competitive market operators. This framework should also provide wide margins for attribute monetization, particularly through relying-party payment models that maximize user adoption and benefits for relying parties, and without defining state monopolists instead of competitive market operators.
- Recognise **LoA Substantial** as sufficient for business and cross-border scenarios until at least 2028, specifically for the application of Articles 24 and 51 of eIDAS, to ensure the practical adoption of LoA High eIDs and Wallets for issuing signature certificates without undermining real-world usability or creating disproportionate burdens for negligible benefit.
- Revise FprCEN/TS 18098 to allow secure, fully automated identity verification for remote onboarding, and to **not impose additional requirements** beyond those already defined in **ETSI EN 119 461 v2.1.1** for Extended LoIP identity proofing; mandate hybrid biometric/manual processes only where exceptional risk clearly requires.

2.6 The Future Business Wallet (EUBW)

The forthcoming European Business Wallet must be conceived as a **market-driven initiative, not a public monopoly**. It should reflect the logic of legal representation and enable interoperability with existing trust services.

Proposed modification:

Mandate that EUBW solutions be operated or delegated to **private QTSPs**, ensuring competition, innovation, and sustainability.

- Anchor the EUBW on existing **qualified trust services** (QES, QeRDS, QEAA, eArchiving) to avoid duplication.
- Permit **fee-based issuance and maintenance** to guarantee viable economic models, as business identities serve commercial, not fundamental-rights, purposes.
- Standardize the use of **LoA Substantial** for business operations, aligning with AMLR and DPP requirements, while allowing optional LoA High only for high-risk scenarios.

2.7 Regulatory Alignment for Cybersecurity and Trust

The coexistence of CRA, NIS 2, and CSA certification schemes leads to overlapping cybersecurity obligations.

Proposed modification:

- Repeal obsolete certification provisions of the Cybersecurity Act (CSA) and consolidate cybersecurity compliance within CRA and NIS 2.
- Establish a **one-stop reporting mechanism** operated by ENISA, covering incident notifications under CRA, NIS 2, GDPR, and DORA, which should be fully digital and automatable to minimize manual reporting effort.

2.8 Recognition of Existing Industry Standards

Many industries already apply internationally recognized standards (ISO 27001, EMVCo, GSMA eSA). Forcing re-certification under EU-specific schemes creates duplication and delays.

Proposed modification:

- Grant automatic **CRA and NIS 2 compliance equivalence** to providers certified under established international standards.
- Allow a **transitional period of 36 months** after publication of new European standards before deprecating existing ones.

About ESD

The European Signature Dialog (ESD) brings together major companies from across Europe's trust services sector to foster secure and trustworthy digital interactions in line with the highest EU standards. ESD acts as the main interlocutor for European and national institutions, providing expert advice and support, particularly for the European Commission, Parliament, and Council. As the recognized voice for trust services across Europe, ESD members work together to develop common regulatory positions and shape the digital trust ecosystem. Beyond Europe, ESD and its members serve as ambassadors, promoting European excellence and standards in digital security around the world.

For further information, please feel free to contact us: office@european-signature-dialog.eu