

Hackhofergasse 5/16

A-1190 Vienna

phone: +43 676 9409309

office@european-signature-dialog.eu

Embedding Trust Services Across EU Digital Regulation

From Omnibus to Future Legislative Initiatives

Executive Summary

Europe's digital future depends on trust. As the European Union advances its ambitious simplification agenda through the Digital Omnibus, a unique opportunity arises to reduce complexity, lower compliance costs, and strengthen Europe's digital and data sovereignty. To succeed, **trust must be embedded at the foundation of this effort.**

Qualified Trust Services (QTS), as defined under the eIDAS Regulation, are already legally recognised, interoperable across all Member States, and supervised under EU law. They provide not only simplification and interoperability, but also a set of essential guarantees: **integrity, authenticity, legal validity, confidentiality, and resilience**. These principles are indispensable for a digital ecosystem that is both simplified and sovereign.

Embedding QTS by default into the Digital Omnibus ensures that simplification is not achieved at the expense of citizens' rights or Europe's strategic autonomy. It delivers:

- **Cost and complexity reduction** through harmonised, EU-wide trust frameworks.
- **Sovereignty and resilience** by relying on European-supervised providers.
- **Legal certainty and accountability** for digital interactions across borders.
- **Interoperability and recognition** across the Single Market.

Trust is not an optional add-on—it is the structural backbone of a secure, competitive, and sovereign digital Europe.

1. Context and Policy Alignment

The European digital acquis has grown increasingly complex, with multiple sectoral and horizontal rules that are difficult to implement consistently across Member States. Businesses—particularly

SMEs and mid-cap companies—face high compliance costs due to fragmented frameworks, overlapping reporting obligations, and lack of legal clarity.

The European Commission’s *Digital Omnibus* aims to address these challenges by streamlining digital regulation, cutting administrative costs, and ensuring legal predictability. At the same time, the Union has set clear priorities for sovereignty, cybersecurity, and global competitiveness.

Qualified Trust Services provide a ready-made foundation for these goals.

Already harmonised through eIDAS and legally binding across the EU, they bring legal certainty, interoperability, and security — while reducing complexity and cost.

2. Trust Services as Default Enablers

2.1 Reducing Complexity and Compliance Costs

Trust services deliver **data integrity, authenticity, and legal validity** out of the box. By embedding them across legislation, regulators avoid duplicating verification mechanisms in multiple sectors. This enables “compliance by design” and lowers administrative burdens, particularly for SMEs.

2.2 Ensuring Sovereignty and Security

Qualified providers operate exclusively under EU jurisdiction. Their services guarantee **encryption, confidentiality, and access management**, ensuring sensitive data is protected from non-EU dependencies while enabling strong authentication and zero-trust architectures.

2.3 Enabling Legal Accountability and Auditability

QTS ensure **non-repudiation, auditability, and traceability**, providing legally binding evidence that holds in court. These capabilities are directly relevant to compliance with the AI Act, GDPR, the Cyber Resilience Act, Data Act and other digital legislation, where verifiable logs and proof of actions are critical.

2.4 Supporting Interoperability and Business Continuity

Standardisation under eIDAS ensures **cross-border interoperability and mutual recognition**, reducing friction in public procurement, compliance, and business operations. Trust services also strengthen **business continuity and resilience**, providing legal and technical certainty during disputes, outages, or incidents. Cross-border interoperability is key to European businesses’ competitiveness. A healthy European digital ecosystem boosts productivity and strengthens European businesses in the digital race.

3. Policy Recommendations

To ensure that the Digital Omnibus delivers on its objectives of simplification, cost reduction, and competitiveness while safeguarding Europe’s sovereignty, the European Signature Dialog (ESD) recommends the following:

1. Default Inclusion of Qualified Trust Services

- Mandate the use of QTS across all new and revised EU digital legislation.
- Mandate the access of QTSPs to public registries cross-border.
- Ensure the integration of QTS “by default” in the Digital Product Passport framework, where trust services can safeguard data integrity, authenticity, and provenance throughout supply chains, guaranteeing verifiable product information and cross-border recognition of certifications.

2. Harmonisation of Frameworks

- Use QTS as the anchor for aligning the digital acquis and reducing compliance burdens.
- Encourage Member States to standardize access to public registries.

3. Safeguarding European Sovereignty

- Ensure EU-supervised trust services remain the preferred standard in regulation and procurement.
- Only European QTSPs should be able to access public registries by default to be able to provide services such as attribute attestation to private and business wallets.

4. Reducing Compliance Costs

- Build on interoperable trust frameworks to streamline reporting and verification requirements.
- Disallow national regulations that curb the operation of QTSPs cross-border.
- Using QTSP services should provide “by default” compliance of identification, authentication, messaging, attribute attestation, archiving, confidentiality, encryption, authenticity and integrity of data.

5. Future-Proofing Through Integration

- Embed QTS not only in the Digital Omnibus, but also in the forthcoming Digital Fitness Check and beyond, ensuring resilience as technology evolves.

Conclusion

Qualified Trust Services already provide Europe with the guarantees needed for a simplified and sovereign digital society: **integrity, authenticity, non-repudiation, legal validity, authentication, confidentiality, access management, auditability, interoperability, and resilience.**

Embedding them by default into the Digital Omnibus will:

- Simplify regulation,
- Reduce compliance costs,
- Safeguard sovereignty, and
- Enhance competitiveness.

Trust must be structural, not optional.

By anchoring **“trust services by default”** as a guiding principle for all digital legislation—starting with the Omnibus and extending to future packages on simplification—the EU can achieve lasting simplification, cost reduction, accountability, security and sovereignty for citizens and businesses alike.

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