

MEMORANDUM

FROM: European Signature Dialog (ESD)

DATE: 5 February 2026

SUBJECT: Trust Services as an Enabling Layer for the Digital Product Passport – Contributions to Legal Certainty, Data Integrity and Interoperability under the ESPR

Executive Summary

The Ecodesign for Sustainable Products Regulation (ESPR) establishes the Digital Product Passport (DPP) as a key instrument to improve the environmental sustainability of products, ensure free movement within the internal market, and support responsible economic operators in meeting regulatory requirements.

To fulfil these objectives, the DPP system must be **reliable, secure, interoperable and economically proportionate**. In particular, ESPR explicitly requires **data integrity**, traceability and long-term accessibility of product information. These requirements apply across the entire DPP lifecycle and to all actors involved, including responsible economic operators and DPP service providers.

This memorandum outlines how **trust services as regulated under Regulation (EU) No 910/2014 (eIDAS)** can serve as a **horizontal governance and assurance layer** for the DPP framework.

When used as a mechanism of **presumed compliance**, trust services by default and by the law provide:

- ✓ integrity and authenticity of DPP data,
- ✓ non-repudiation and legal enforceability across Member States,
- ✓ interoperability between DPP systems,
- ✓ long-term availability and evidentiary value of product information.

Importantly, trust services offer these assurances **at marginal per-unit cost**, including for high-volume deployments, making them compatible with the Commission's objective to reduce compliance burdens, particularly for SMEs, through harmonisation and clarification of overlapping digital regimes. Their use allows the DPP framework to rely on **existing, supervised and auditable service models**, instead of creating parallel trust or certification schemes for DPP-specific purposes. Across the Union, millions of SMEs already use trust services on a daily basis, and therefore, adoption of these services in the DPP ecosystem would be very cost effective and fast.

1. Trust Services as a Foundation for Legal Certainty and Data Integrity

The DPP is intended to electronically register, process and share product information among economic operators, authorities and consumers. For this system to function effectively, DPP data must be:

- authentic and attributable to a responsible entity,
- protected against unauthorised modification,
- legally reliable across borders,
- available and verifiable over time.

Regulation (EU) No 910/2014 provides a **uniform EU-wide legal framework** for electronic signatures, seals, timestamps, authentication and electronic archiving. These instruments are specifically designed to ensure **data integrity, non-repudiation and cross-border legal recognition**, which are core functional requirements of the DPP system.

Rather than introducing new sector-specific trust regimes, trust services can act as a **horizontal enabler** across policy areas, supporting the ESPR while leaving technical implementation choices and business models to market actors.

1.1 Supporting a Level Playing Field and Regulatory Coherence

Applying trust services to DPP processes contributes to:

- **equal treatment** of responsible economic operators across Member States,
- **consistent verification** of DPP data regardless of where products are placed on the market,
- **prevention of unfair competition** through falsified or manipulated sustainability claims.

By relying on a single EU legal framework for trust, the DPP system avoids fragmentation and ensures coherence with other EU digital legislation.

1.2 Proportionality, Cost Efficiency and SME Compatibility

A recurring concern in DPP discussions is the **cost and complexity** of compliance, especially for SMEs and for new market entrants. Trust services address this concern in several ways:

- they are already **available** on the market **at very low marginal cost**, including fractions of a cent per transaction in large-scale use;
- millions of SMEs already use trust services on the daily basis;
- they **scale efficiently** from small operators to large industrial deployments;

- they allow SMEs to rely on external, **supervised service providers** rather than developing in-house compliance infrastructures.

This directly supports the Commission's objective that DPP-related requirements should not impose a disproportionate burden on companies, particularly small and medium-sized economic operators and service providers.

2. Contribution to the Strategic Objectives of the Digital Product Passport

2.1 Simplification and Support for Responsible Economic Operators

The Commission has highlighted that DPP service providers will support responsible economic operators in creating, registering and maintaining DPPs. Trust services facilitate this role by:

- providing **standardised methods** for authenticating DPP data,
- **clarifying responsibilities** between operators and service providers,
- **reducing the need** for multiple, overlapping control mechanisms.

This simplifies compliance and accelerates DPP rollout across product groups.

2.2 Legal Certainty for Market Actors and Authorities

Trust services under EU law provide:

- **legal presumption of authenticity and integrity**,
- **non-repudiation** of issued or updated information,
- **admissibility of digital evidence** in administrative and judicial proceedings.

When applied to DPP data, these effects ensure that sustainability and compliance claims can be **relied upon** by market surveillance authorities, business partners and consumers.

2.3 Interoperability and Alignment with International Standards

The Commission's standardisation request aims to facilitate interoperability between DPPs, covering data formats, APIs, storage and authentication. Trust services complement this work by:

- aligning with ISO standards for digital signatures and seals,
- fulfilling ESPR requirements on data integrity,

- remaining compatible with international instruments such as the **UNCITRAL (UNO) Model Law on Trust Services**, which provides recognised principles for digital trust beyond the EU.

This combination preserves EU legal certainty while allowing flexibility for global supply chains.

3. Trust Services Across the DPP Lifecycle

Trust services can support all core activities of DPP service providers identified by the Commission, including:

- creation of the DPP,
- creation of the data carrier,
- registration of the DPP,
- hosting and storage of DPP data,
- enabling updates,
- reporting,
- backup and recovery services.

3.1 Data Integrity and Authenticity

Electronic signatures and seals ensure that **DPP data**:

- is **protected against alteration**,
- can be **attributed to a specific legal entity**,
- remains **verifiable over time**.

This directly implements ESPR requirements on data integrity.

3.2 Secure Access and Update Control

Authentication mechanisms ensure that **only authorised persons** can:

- **access DPP information**,
- **modify lifecycle data**,
- **issue compliance or sustainability statements**.

This protects against fraud, data manipulation and unauthorized access, including industrial espionage, counterfeiting networks, and the issuance of false or misleading claims regarding regulatory compliance or sustainability performance.

3.3 Long-Term Preservation and Evidentiary Value

Electronic archiving and time-stamping services provide:

- **secure long-term storage** of DPP records,
- **verifiable timelines** for data creation and updates,
- **resilience against provider exit** or data loss.

These features directly support the Commission's focus on **long-term access to DPP information**.

4. Why CEN / ISO Standards Alone Are NOT Sufficient for DPP Trust and Governance

CEN and ISO standards, including prEN 18246, play a vital role in defining **technical specifications** for DPP data structures, interfaces and exchange mechanisms. However, technical standards alone do not address:

- who is authorised to issue or validate DPP-related attestations,
- how service providers are accredited and supervised,
- what legal liability applies in case of failure or misuse,
- how cross-border legal recognition is ensured.

Conclusion: prEN 18246 defines how DPP data may be structured and technically signed.

Trust services regulated under EU law determine who is **authorised to issue such signatures, under enforceable supervision and liability regimes**, and ensure that they have **legally binding effect** across the internal market, thereby providing the **indispensable governance layer** for the DPP.

5. International Dimension and Market Access

As DPP requirements apply to products placed on the EU market irrespective of origin, the DPP framework must accommodate global supply chains while preserving legal certainty, data integrity and a level playing field within the internal market.

Trust services regulated under EU law **enable international participation** in the DPP system through three complementary mechanisms:

5.1 Mutual Recognition with Third Countries

Where appropriate, the EU may pursue mutual recognition arrangements with third countries operating comparable trust frameworks, ensuring that:

- EU-issued electronic signatures and seals are **accepted for trade and regulatory purposes** abroad;
- equivalent third-country trust services are **recognised for use in the EU**, subject to reciprocity;
- cross-border supply chains benefit from **interoperable and legally reliable digital attestations**.

5.2 EU-Based Legal Representatives under the ESPR

Non-EU manufacturers and suppliers may participate in the DPP system by:

- appointing **EU-based legal representatives** in accordance with ESPR Article 28;
- **relying on trust services** regulated under EU law through those representatives;
- ensuring **accountability, regulatory visibility and enforceability within the Union**.

5.3 Tiered Trust Solutions Where Mutual Recognition Is Not Available

Where mutual recognition is not immediately feasible, the DPP framework should allow for **tiered trust solutions**, including:

- trust services regulated under EU law as the presumed-compliant mechanism;
- acceptance of advanced electronic signatures and seals, subject to proportionate risk assessment and audit requirements;
- future integration of electronic attribute attestations as they mature under EU law.

Together, these mechanisms allow the DPP system to remain open to international trade while safeguarding legal certainty, enforceability and trust for products placed on the EU market.

6. Avoiding Duplication and Reducing Compliance Burden

The Commission has emphasised the **need to streamline digital regulation and avoid overlapping frameworks**. Using trust services as a presumed-compliance mechanism:

- **avoids the creation of DPP-specific trust regimes,**
- **allows reuse of existing supervisory and audit structures,**
- **reduces compliance costs** for operators and service providers.

This supports better regulation principles and the objectives of the ongoing impact assessment.

7. Recommendations

ESD invites the Commission and relevant bodies to:

1. Recognise trust services as an **enabling layer for meeting DPP requirements** on integrity, authenticity and legal certainty.
2. Ensure **coherence between ESPR delegated acts and existing EU trust frameworks**.
3. Guide standardisation work to **ensure compatibility with legally recognised trust mechanisms**.
4. **Maintain proportionality**, especially for SMEs and emerging DPP service providers.

8. Conclusion

A reliable Digital Product Passport system requires **technical interoperability, legal certainty and economic proportionality**. Trust services provide these elements as a horizontal framework supporting the ESPR's environmental and internal-market objectives.

By building on existing EU instruments, the DPP framework can achieve its goals without fragmentation or unnecessary cost, while ensuring trust, accountability and long-term access to product information. ESD remains available to contribute to this process.

For further information, please feel free to contact us:

office@european-signature-dialog.eu