



Hackhofergasse 5/16
A-1190 Vienna
phone: +43 676 940 9309
office@european-signature-dialog.eu
ZVR-nr: 579746942

ESD comments on the draft Implementing Regulation laying down the implementation arrangements for the Digital Product Passport registry

The European Signature Dialog (ESD) brings together leading companies providing qualified trust services to more than 250 million users across Europe in their everyday digital interactions. ESD promotes secure, trustworthy, and interoperable digital services in line with the highest European standards. As a recognised interlocutor for European and national institutions — including the European Commission, the European Parliament, and the Council — ESD actively contributes to shaping the European digital trust ecosystem.

Against this background, ESD welcomes the opportunity to provide comments on the draft Implementing Regulation laying down the implementation arrangements for the Digital Product Passport (DPP) registry.

ESD welcomes the proposed Implementing Act. Data authentication, integrity, and reliability are fundamental elements of the ESPR framework, and the proposed DPP registry infrastructure appropriately reflects these legal and operational requirements while also supporting the broader objectives of simplification and European data sovereignty.

In particular, the proposed reliance on qualified trust services under the eIDAS framework offers cost-effective, tested, scalable and highly secure solutions capable of protecting both the interests of economic operators and the overall trustworthiness of the system. At the same time, simplification is facilitated through the use of technologies already well known to citizens, businesses, software developers, and Member States.

The eIDAS framework represents a successful example of Europe's ability to establish interoperable and trusted digital infrastructures across borders. The proposed solution integrates naturally with existing European digital frameworks and complements broader strategic initiatives in the digital domain.

In this context, ESD would like to offer the following comments and suggestions, which could further optimise and strengthen the proposed Regulation:



(1) Dependency on the Cloud Sovereignty Framework: The draft states that the registry and relevant services (which could include the TSP-provided verification components) must comply with an "adequate level of sovereignty" based on the **Cloud Sovereignty Framework** once such services are available.

This adds an extra layer of technical and regulatory compliance for TSPs hosting their services including registering services for companies abroad in cloud environments. Some data governance regulations in foreign countries even require the data of persons of the respective country must be assessed on systems in this respective country first before it will be transferred to the EU. (e.g. data governance legislation in China).

DPP is based on global supply chains and not an intrinsic EU framework. Thus we need the support also from systems running abroad. (in special see Art. 5 (1) (b)).

Source:

Recital (26)

"In addition, the registry should comply, as soon as the relevant services become available on the Union market, with an adequate level of sovereignty, based on the Cloud Sovereignty Framework".

➡ We propose to add a point to recital 26 stating "Such provisions are applied only to the infrastructure directly providing the registry service."

(2) "Relevant Services" for Sovereignty: The requirement to comply with the Cloud Sovereignty Framework "as soon as the relevant services become available on the Union market" is highly ambiguous. It is unclear what specific services trigger this requirement or who determines their "availability."

Same source Recital 26 as under 1.

➡ This phrase should be deleted.

(3) Bracketed Text for Reporting: Recital 27 and Article 17 contain text in square brackets regarding the user's responsibility to notify the Commission of malicious behavior. This suggests that the legal obligation and scope of this responsibility are still being debated and are not yet finalized.



Source:

Recital (27)

"[Users have the responsibility to notify the Commission and, whether relevant, the affected national authorities immediately in case of suspected malicious behaviour.]"

➡ Clarification necessary.

(4) Interoperability of Identification Schemes: Article 3(i) mentions the creation of "identification and authorisation schemes for registry users". It is an open point whether these will be entirely new schemes or if they will fully leverage the existing **eIDAS interoperability framework** and the upcoming **European Digital Identity Wallets**.

Source:

Art. 3

"The registry shall consist of the following: (...) (i) identification and authorisation schemes for registry users"

➡ If possible, this topic should either be omitted or defined in a manner that avoids any interference with the existing eIDAS regulatory framework.

(5) Registry logs do not meet the requirements of an investigative instrument under ESPR

Art. 14(4) makes registry logs an investigative instrument. Market surveillance and customs authorities are granted access for investigations and audits. If logs cannot fulfill this function, Art. 14(4) is a toothless reference and the enforcement mechanism of ESPR itself is undermined. Two properties are missing:

- Art. 14(5): immutability required, no mechanism provided. Encryption and access controls (Recital 23) do not produce independent verifiability.
- Non-repudiation: log entries capture who acted, but do not bind this to the qualified identity from Arts. 4/5

Similar challenge (and solution) regarding long-term verification:

- A qualified seal remains verifiable over ten years, in our understanding, only if the certificate status and chain at the time of sealing are archived alongside it and secured by qualified timestamps — the same requirement as for log immutability.
- The draft does not address this requirement for DPP seals.

➡ A qualified timestamp (Art. 42 eIDAS) and identity binding would be the obvious mechanism. They cover both non-repudiation of log entries and long-term verification. Both



requirements are already codified in eIDAS as existing EU law; the draft should reference these instruments to ensure coherence with the existing legal framework.

(6) Conflation between the identity proofing level and the registration authorisation level

The definition of *identity verification process* in the implementing act establishing the DPP registry — "*the process by which a natural person or legal person provides the evidence of identity and of establishment that entitles such person to register a digital product passport in the registry*" — raises a logical concern.

The wording fails to distinguish between two layers that should remain distinct: *identity proofing* (verifying that a subject is who they claim to be) and *authorisation* (entitlement to perform a specific act within the registry, i.e. registering a DPP). These layers rest on different normative sources and belong to different procedural stages. Identity proofing is governed by established frameworks (ISO/IEC 29115, eIDAS 2.0 and Implementing Regulation (EU) 2015/1502, ETSI TS 119 461). Authorisation presupposes that the identity has already been ascertained and rests on attributes, roles or titles associated with the identified subject at a later stage (qualification as manufacturer, importer or authorised representative, existence of a mandate, and so on...).

The risk is twofold. The definition becomes tautological — identity proofing (verification, in the words of the implementing regulation) is qualified as valid because it produces the very legal effect (the entitlement) that should instead follow from an identity proofing already qualified on its own substantive requirements. More importantly, conflating the two layers may lead operators to assume that authorising attributes must be collected and verified *during* identity proofing. Such attributes are not identifying but authorising, and should be acquired in a distinct subsequent phase, based on their own authoritative sources and through mechanisms (e.g. verifiable attestations) consistent with the eIDAS 2.0 architecture.

A significant part of this ambiguity stems from the *grammatical construction* of the definition. The implementing act adopts an *active voice*, in which the natural or legal person is the subject and "provides the evidence of identity and of establishment". This places the economic operator — rather than the identity — at the centre of the definition, and frames identity proofing as an act of *production of evidence* by the applicant, implicitly suggesting that the applicant may be required to provide documents going beyond those attesting to identity. By contrast, ETSI TS 119 461 defines identity proofing as the "*process by which the identity, and possibly additional attributes, of an applicant is verified by the use of evidence attesting to the required identity attributes*". This *passive* formulation places identity — not the applicant — at the centre: the process is qualified by what is verified and against what evidence, without conflating it with authorisation.



➡ **Our proposal:** replace the definition of Art.2 (4) Identity verification process: *"the process by which a natural person or legal person provides the evidence of identity and of establishment that entitles such person to register a digital product passport in the registry"* with Identity proofing process: *"the process by which the identity, and possibly additional attributes, of an applicant is verified by the use of evidence attesting to the required identity attributes"*

For further information, please feel free to contact us:

office@european-signature-dialog.eu