Spanish Data Protection Authority
AEPD, Agencia Española de Protección de Datos
Calle Jorge Juan, 6. 28001 Madrid, Spain
https://www.aepd.es/
División de Innovación Tecnológica
dit@aepd.es

Response to ARF Discussion topics:

Topic O "Catalogues for Attestations"

Drawing on the rationale consistently presented in our previous responses to different discussion topics, the focus on this one, at least concerning data protection, should be on ensuring that these catalogues actively support and enforce data protection principles throughout the EUDI Wallet ecosystem.

- The catalogues can be a crucial tool for complying with the transparency principle. Users must be fully informed about what data is requested when using their wallet, how it will be disclosed, and for what purpose, thereby enabling them to exercise granular control over their personal data. Information about attributes, their disclosure rules, or associated trust models, for example, could be stored in catalogues and translated into clear, concise, and user-friendly language within the EUDI Wallet interface.
- The AEPD would like to emphasize the need for clear delineation of roles, responsibilities, and liabilities for all parties involved in the lifecycle of attestations defined in the catalogues, particularly regarding personal data protection obligations and the exercise of users' rights. How exactly is the *"description of the trust model and the governance mechanisms applied under the scheme, including the revocation mechanisms"* going to be made available in both human and machine-readable formats? Schemes could be registered with opaque trust models and governance mechanisms that obscure how data is processed (and potentially linked), thereby hindering transparency and preventing users from exercising granular control over their data. Additionally, schemes might be registered with ambiguous trust models and governance mechanisms or *"requirements in relation to the providers of the electronic attestations of attributes"* that make it difficult to assign controller/processor roles or hold parties accountable for potential GDPR infringements.
- Without a common standard and technical specification for request fields and catalogue content, including descriptions, requirements, statements, etc., we could suffer a proliferation of incompatible or poorly specified attestation schemes. This would create interoperability issues, increasing complexity for wallet implementations and Relying Parties, and potentially introducing increased security risks.

- We have concerns about CAT_07 *"The Commission SHALL enable a self-registration process of Attestation Rulebooks, without pre-approval by the registry, for both public and private entities"*. A lack of pre-approval means that inherently problematic schemes could be registered in the first place. This would shift the burden from proactive prevention to reactive enforcement, which may be too late to mitigate harm effectively. If catalogues end up storing "misleading entries", it could undermine trust in the entire EUDI Wallet ecosystem. Users' confidence and the adoption of the Wallet would suffer, as they would struggle to distinguish legitimate from fraudulent schemes.

  Significant risks, particularly from malicious schemes and "namesquatting", can be identified:

  - The most critical risk is the registration of attestation schemes designed to facilitate tracking, linking, or correlating user behavior. Without rigorous pre-approval, malicious parties could register schemes that structurally embed identifiers, enabling different kinds of linkability and observability. Furthermore, a malicious scheme could be designed in a way that, through its attribute definitions or underlying mechanisms, inadvertently or intentionally enables the linking of a user's pseudonyms to their real identity or allows tracking across different pseudonyms.
  - Maliciously designed schemes could define an excessive number of attributes for common use cases or encourage the disclosure of more personal data than is strictly necessary for a given purpose. Without pre-approval, schemes that promote oversharing could gain legitimacy directly through registry inclusion.
  - A malicious entity could register an attestation scheme with a name, semantic description, or identifier that closely resembles a legitimate, widely trusted one. This "namesquatting" could deceive users and Relying Parties into using an untrustworthy or harmful scheme.