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 C "Wallet Unit Attestation (WUA) and Key Attestation"

We want to make the following observations:

- The discussion paper establishes this concept of *"the WUA to be treated as "any other attestation".* Although we understand the benefits of this approach, it must be noted that this is not the case as it has important specificities that must be considered:
  - It is an attestation issued by the Wallet Provider instead of by an attestation provider.
  - It is an attestation consumed by different ecosystem actors (attestation provider and Relying Parties) with different roles, requirements and needs.
  - It is an attestation playing a crucial role in the Wallet Unit revocation.
- We welcome the acknowledgement of this fact: *"As Relying Parties, PID Providers, and Attestation Providers have different needs from the WUA, the Wallet Unit must be able to differentiate what information is presented in different use cases"* and the establishment of the following requirement: *"The WUA needs to support selective disclosure."* We will need more information about the concrete implementation of this type of selective disclosure to better understand how it mitigates the privacy threats that the use of the same WUA for attestation providers and Relying parties implies.
- The discussion paper establishes that *"The WUA must support both long and short validity terms"*. Why is this requirement mentioned? Is it because the needs of attestation providers and RPS are different? Is the possibility of generating different WUAs (different validity terms or content) for one type of party and another considered? Because in this case, selective disclosure could be unnecessary.
  - We observe some inconsistency throughout the document regarding the validity period of the WUA: *"The WUA must support both long and short validity terms"* but, at the same time, *"The validity period of the WUA should be long, preferably as long as the expected lifetime of the Wallet Unit"*.
- The discussion paper states, "*The WUA should have the same format as other attestations. Note: pending discussion in Topic V, according to ARF 1.5.0 this implies either ISO/IEC 18013-5 or SD-JWT VC".* If this is the case, our advice concerning the unlinkability property is the same as provided for Topic A: parties receiving the WUA should not be able to use this attestation to track users across different

interactions, presenting the same public key multiple times at the same or different parties allows the materialization of linkability threats.
    - We need to clearly separate two types of WUA use cases: 1) use cases in which the user must identify themself to the party receiving it (attestation provider or Relying Party) and 2) use cases in which the user must not identify themself to the party receiving it (attestation provider or, more likely, Relying Party).
- The only solution to avoid linkability within the discussion paper framework is single-use WUAs. Each presentation is essentially isolated, and different presentations are inherently unlinkable (unlikability by design -> data protection by design).
- To prevent the Wallet Provider from learning how often the user uses WUAs or how such usage is spaced in time, Wallet Providers may periodically and asynchronously issue batches of single-use WUAs (pre-fetching a fixed number of attestations with an extended validity period once a month, for example) that can be stored in the wallet to be used/discarded when required (storage requirements may need to be adapted). This prevents this learning on user behaviour from being carried out and helps the provider to predict their attestations. Only in frequent-use situations would specific users need to request a new batch of attestations (for example, when only X WUAs are left from the last monthly batch) since they would have used up all the available ones.
- A different alternative could be deriving single-use WUAs from the "original" WUA created during wallet activation.
    - In this case, different WUAs could be derived for attestation issuers and for Relying Parties (different validity terms, content, etc.).
- The discussion paper states that *"The WUA must provide PID Providers and Attestation Providers assurance that the private PID or attestation key is bound to the same WSCD as the WUA private key."* We will need more information about the concrete implementation of cryptographic binding to better understand the privacy threats involved.
- While the capability to revoke Wallet Units is necessary, the method for doing so should not create new avenues for profiling or tracking users. Revocation mechanisms must employ privacy-preserving techniques.
- The same applies to the capability to revoke PID attestations, the proposed approach *"the PID providers must keep track of all Wallet Units (i.e. the WUAs) to which PID has been issued and periodically (e.g. daily) monitor this list to check if a WUA has been revoked*" should be carefully assessed from a data protection point of view once more details are available.
- The paper mentions that *"The Wallet Unit must handle the presentation of the WUA automatically, without the involvement of the User".* However, compliance with the transparency principle and the exercise of data protection rights must be ensured. The data subject must be informed about the personal data processing performed in a concise, transparent, intelligible, and easily accessible form, and they must be allowed to exercise all their data protection rights.

- This is essential concerning potential automated individual decision-making involving the WUA (mainly, the Wallet Unit revocation and the rest of the decisions that may come next). The data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express their point of view and to contest the decision.

Given the depth of this particular discussion, we cannot go into much more detail at this point. However, we will be happy to discuss in the future the threats and risks to privacy posed by the technical solutions that are ultimately assessed/selected in relation to the aspects discussed in this topic.