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 E "Pseudonyms, including User authentication mechanism"

We want to make the following observations concerning the discussion paper's global approach:

- Pseudonymisation is defined in the GDPR as *"means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"*. As with other discussion topics in the past, we suggest using the terms defined in the GDPR in the ARF if their meaning is precisely the same. If not, it is better to use another term or at least provide all the necessary clarifications and qualifications to avoid confusion. For this discussion topic this applies to pseudonym/ pseudonymization.
- An approach respecting data minimisation and data protection by design and by default principles could be to consider the use of pseudonyms a default for transactions, revealing identity data only as needed by a specific use case. As we have suggested before in this process, the registration of RPs is essential to distinguish use cases that require Know-Your-Customer (KYC) functionality (user identification). The use of pseudonyms should not be limited to specific services, RPs or use cases, it should be the default to prevent over-identification.
- A significant concern is the potential for linking pseudonyms to a user's real identity (identification). The ARF should ensure that pseudonyms are unlinkable to identities for the different Relying Parties and other parties participating in the ecosystem. Attestations in the WebAuthn specification could introduce identification issues if not handled carefully. Before making any decision, an in-depth analysis of all the different use cases is necessary.
- To avoid RP linkability, a single user should be able to use multiple pseudonyms with a single Relying Party.
- We welcome the proposal to ensure that pseudonyms are local to each Relying Party to avoid linkability across different RPs.
- Users should have complete control over their pseudonyms and the data they share when using them. The ARF should require a user-friendly, transparent interface for managing pseudonyms within the EUDI wallet. Users must be informed about when and why their pseudonyms are used and be able to view a complete transaction log

(including cancelled or unsuccessful transactions). The ARF should provide mechanisms for users to verify the registration data of RPs and thus easily distinguish when it is necessary to identify themself and when they can operate under a pseudonym.

- The ARF should consider how the pseudonym functionality interacts with other topics already discussed such as privacy risks (Topic A), re-issuance and batch issuance (Topic B) and the digital credentials API (Topic F). It is not easy to decide how to implement pseudonyms when the decisions taken in the previous topics are not known since there is a great interdependence between the topics in the aspects that refer to data protection. For example, the ARF should include mechanisms for secure key management related to pseudonyms. How would the implementation of HDK discussed in previous topics relate to that of the pseudonyms based on WebAuthn? Or, how would the Digital Credentials API support the use of pseudonyms?
- The choice of WebAuthn as the specification supporting the use of pseudonyms in the EUDI wallet reintroduces the problem we already discussed in topic F, the "webification" of the approach and the risks associated with the more or less mandatory introduction of an intermediary between the wallet and the RP. In this case, the WebAuthn Client should not prevent the wallet from carrying out all the checks set out in the regulation and the Implementing Acts, nor should the user receive from the wallet itself all the information necessary to comply with the transparency obligations.

In addition, we would like to comment on some specific points discussed in the paper and to answer some of your open questions:

- **Question 1: Should any other use cases be supported?**

In our comments on Topic A, we suggested that it would be beneficial to properly manage the risk from a data protection perspective to separate two types of wallet use cases clearly: 1) use cases in which the user must identify themself to the Relying Party and 2) use cases in which the user must not identify themself to the Relying Party.

This would help with the registration of RPs and the prioritization of data minimization and data protection by design and by default principles, making pseudonyms the default for use cases within Category 2. Identity data would be processed only when strictly necessary (use cases within Category 1). This is still the proper approach. Once this distinction has been made, each of these two main categories could be divided into new categories, such as those proposed in this new topic: authentication and presentation of attributes.

Relying Parties with use cases within Category 2 should not distinguish/discriminate/segregate users relying on pseudonyms and personal identification data (shared or processed for whatever other necessary reason).

- **Question 2: For both use cases: Should both cross-device and same-device flows be supported? I.e., should registration and authentication with pseudonyms be possible both when a user initiates the interactions with the Relying Party from the same device and with a device different from the one hosting the Wallet Unit? The answer to this question will impose requirements on the interfaces between the Wallet Unit and the client a user initiates the interaction with.**

  To ensure flexibility and user convenience, pseudonym registration and authentication should be supported using both cross-device and same-device flows. However, as the question establishes, the interfaces between the Wallet Unit and the client used to initiate the interaction must be carefully designed with data protection in mind.

  We would like to emphasize that it is essential that the user always controls pseudonyms, is aware of what data is being presented, and has clear explanations about the purpose of each data request, the relying party's identity, etc.

- **Question 3: For Use Case A: Should a single user be able to use their Wallet Unit to present several different pseudonyms to a single Relying Party? High-Level Requirements must be defined that enforces the answer to this question.**

  A single user should be able to use multiple pseudonyms with a single Relying Party. This is crucial for protecting the user's privacy and preventing the Relying Party from tracking their activities across different interactions (RP linkability threats). Each pseudonym should be treated as a separate and independent “alter ego”, without any link to the user's real identity or the other pseudonyms.

- **Question 4: For both use cases: What assurances must be given to the Relying Party? Such possible assurance exists on at least three levels:**

  1. No assurances are given to the Relying Party. I.e., the Relying Party is not even guaranteed that it is interacting with the Wallet Unit.
  2. The Relying Party is assured that the private key corresponding to the pseudonym being stored/authenticated *was* originally stored in a Wallet Unit.
  3. The Relying Party is assured that the private key corresponding to the pseudonym being stored/authenticated *is* stored in a non-revoked Wallet Unit.
  4. For use case B: The Relying Party is assured that the private key corresponding to the pseudonym used to authenticate is stored on the same Wallet Unit as originally presented PID/(Q)EA.

  As the discussion paper is written, it seems that an impossible choice must be made between security and privacy, and no solution is proposed or suggested to enable a RP to rely on an authentication performed with a pseudonym while guaranteeing the

unlikability property: *“higher assurances comes with a trade-off in terms of surveillance risks”.*

Again, it makes little sense to identify the threats and risks in the catalogue but not introduce an evidence-based discussion about how to avoid or mitigate them. Can both security and privacy be guaranteed with WebAuthn, and how? Or would the specification need to be modified, or a new "flavour" produced with certain specificities for the ARF? What would be the proposal that we can work on?