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 P "Secure Cryptographic Interface between the Wallet Instance and WSCA"

The Secure Cryptographic Interface (SCI) is a critical element within the ARF and has significant implications for GDPR compliance. Its design directly determines if the strong security of the WSCD will translate into robust data protection and privacy for the EUDI Wallet user. It could become a vulnerable point that compromises the entire system's adherence to GDPR principles and requirements.

A major gap is the lack of European or international SCI standards. Section 3 of the discussion paper lists existing technologies and alternatives but does not show how they align with ARF High-Level Requirements in different scenarios, such as when the Wallet Secure Cryptographic Device is remote. Without harmonized standards, implementations could differ widely in data protection aspects. This variety will introduce privacy and data protection risks and will make assigning GDPR roles (controller or processor) and accountability for interface-level breaches difficult.

We recommend:

1) To rigorously test the different alternatives ensuring, with solid evidence, that all of them will allow the different SCI implementations to fully align with the HLRs. Such systematic evaluation provides a strong foundation to propose SCIs harmonized standards in the different possible scenarios. We have specific concerns about personal data flows when remote HSMs provide WSCD functionality.
2) Once these standards are defined, SCI certification and independent auditability by trusted third parties (for example, Data Protection Authorities) will be crucial to establish transparency and build confidence among stakeholders, ensuring the available solutions meet all the established requirements.

The interaction across the SCI between the Wallet Instance (controlled by the Wallet Provider) and the WSCA/WSCD (hardware-protected, possibly device manufacturer-dependent) must be clear in every scenario. This clarity ensures everyone knows who is responsible for specific data protection aspects, such as transparency mechanisms or user rights.

In addition:

- The most critical risk is that the SCI could enable tracking and correlation of user behaviour. Even with advanced cryptographic primitives in WSCD, exposing persistent identifiers or static cryptographic signatures during routine operations can allow parties such as Attestation providers or RPs to link users.
- Allowing Wallet providers to access information, through the SCI, about cryptographic operations or key usage unnecessary for Wallet services violates unobservability. As a result, providers could gain insight into users' transactions, enabling profiling and surveillance.
- A poorly specified SCI could expose raw cryptographic operations and primitives either implicitly or explicitly, and transfer unnecessary data, such as key metadata, device/attestations state, or verbose logs. These behaviours could infringe the data minimisation principle.
- The technical complexity of the SCI and the implementation of automated operations through this interface can make it difficult to provide users with clear, transparent, and user-friendly information about when and how their sensitive cryptographic operations are performed and what data flows are taking place across the interface. Explicit notifications and user's involvement are essential to comply with transparency and control requirements.