

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 G “Zero Knowledge Proof”

We would like to make the following observations:

- As we have introduced in the discussion of previous topics, we think that it would be beneficial, from a data protection perspective, to separate two types of wallet use cases clearly: 1) use cases in which the user must identify themselves to the Relying Party and 2) use cases in which the user must not identify themselves to the Relying Party. To comply with the data protection by default requirement, we recommend considering the use of ZKP as a default for all transactions (in both groups of use cases), revealing identity data or relaxing the unlinkability property, for example, only as needed by a specific use case (very likely, within the first group).
- We understand the mention of the required changes to support ZKP schemes (attestation format, issuance and presentation protocols) as a potential disadvantage of introducing these schemes in the ARF. However, if all actors in the EUDI wallet ecosystem comply with the data protection by design requirement, ZKP is going to be supported from the beginning in their products and services design. We can try to minimize the number of changes, or their scope, in relation to previous versions of the ARF so as not to incur an additional cost for those actors that have already advanced in designs, prototypes, pilots, etc. But they are necessary changes to respect the rights and freedoms of citizens.
 - We interpret that attestation formats are still mDL and SD-JWT and that the changes contemplated here are the addition of new metadata or fields to these formats if necessary to support ZKP. Is that correct?
- Section 2 mentions “Additional privacy properties” for ZKP schemes (in addition to Selective disclosure, Relying Party unlinkability and Full unlinkability). It is not clear if this list is setting expectations for the ARF. Should the used ZKP schemes support all these properties? Are these desirable properties but not required by regulation? The relationship between this list and section 4.1, “Expectations from ZKP systems” must be clarified.
- Furthermore, since the HLRs to be included in the ARF are based on this list of expectations, they must be carefully defined. We strongly recommend focusing this

first discussion on deciding which properties must be guaranteed by the specified ZKP scheme.

- At the moment, we are missing at least two essential properties mandated by the regulation in section 4.1 and the HLR:
 - Unconditional or everlasting privacy: The ZKP scheme should support this property (from eIDAS2 “(a) not allow providers of electronic attestations of attributes or any other party, after the issuance of the attestation of attributes, to obtain data that allows transactions or user behaviour to be tracked, linked or correlated, or knowledge of transactions or user behaviour to be otherwise obtained, unless explicitly authorised by the user”), ensuring data protection indefinitely, even if future advancements in computational power (quantum computing) or cryptographic techniques render current methods obsolete. Transaction logs shall not offer any opportunity to link the user or learn hidden attributes in any circumstance in the future. For example, this is particularly important in use cases concerning medical records or elections.
 - Composite proofs: The ZKP should support this kind of presentation (from eIDAS2 “It should be technically possible for the user to selectively disclose attributes, including from multiple, distinct electronic attestations, and to combine and present them seamlessly to relying parties”), which is highly versatile for different use cases where multiple conditions must be verified simultaneously. Composite proofs can be designed to optimize the trade-offs between proof size, computational cost and verification time.
- Additional desirable properties such as blind issuance of attestations or repudiation capability (plausible deniability for both, issuance and presentation of attestations) or those mentioned in section 2 should be discussed to decide whether they are expected and new HLR are required.
- Performance baselines should also be included as HLRs because, otherwise, a ZKP scheme could guarantee all the established privacy properties but at a computational cost, storage overhead, or response times that are unaffordable for all or some use cases or devices. This could imply usability issues or the exclusion of most users for not having the proper device. What is considered acceptable for this ARF regarding these fundamental performance parameters?
- Once the expected properties are established and defined, a coverage map can be generated that clearly indicates which ZKP schemes meet each of these properties (always based on evidence since a theoretical evaluation is almost impossible in some cases, for example, concerning performance).
- It seems that REQUIREMENT 8 “A Wallet Solution SHALL ensure that integrated ZKP schemes introduce minimal to the PID or attestation issuance process” needs to fix the wording. Introduce minimal changes, interference, overload? And, why only for the issuance process?

- Implementing ZKP schemes may require complex infrastructure at issuers and changes in the wallet units or some essential protocols. If not managed well, this additional complexity could introduce new privacy threats and risks that should be objectively assessed before adopting any solution. A good example is the new interactions that may be required between attestation issuers, wallet units, and RPs, a potential source of linkability.