# CEN / ETSI Questions to EUDI Wallet Large Scale Pilots

# Introduction

CEN & ETSI is developing standards in support of the EU Digital Identity Wallet and would welcome response to the following questions. Where further information is available, elaborating on the answers and providing detailed descriptions, this would be appreciated.

## 1 General Questions

|  |  |
| --- | --- |
| **Question** | **Response** |
| 1.1 What use is made of trust services in support of the pilot applications including trust service (qualified and non-qualified) for EAA, issuance of (qualified and non-qualified) signing/seal certificates and remote signing services?  |  |
| 1.2 What are the main issues to be addressed for the use of trust services and supporting the use of e-signatures and e-seals?  |  |
| 1.3 What are the main issues to be addressed for interoperability of credentials?  |  |
| 1.4 Is revocation of PID / EAA attestations supported? If so using what protocol? |  |
| 1.5 Are there any issues that that you feel would benefit from wider discussion with ETSI and CEN?  |  |
| 1.6 Where technical gaps are identified between the eIDAS legal text and ARF which might be forwarded to the reference wallet developer? |  |

## 2 PID Onboarding Questions

|  |  |
| --- | --- |
| **Questions**  | **Response** |
|  |  |
|  |  |
| 2.1 Now that the final text recommends interoperability for PID on-boarding, do LSP consider the impact of this requirement in their PoC ? or do LSP only implement transaction phase (after on-boarding is achieved)? |  |
| 2.2 Have you identified specific formats for PID attestations? |  |
| 2.3 Have you identified scenarios/use case of PID on-boarding? |  |
| 2.4 Do you envision access control to PID during operational phase? |  |
| 2.5 Do you consider that a minimum access control over PID disclosure should be enforced by the wallet to meet the requirements of security and privacy as mandated by LoA ‘High”? |  |
| 2.6 Do you consider that PID presentation shall only be carried out within a transaction of LoA “High” or do you consider that PID could also be presented within a transaction of LoA “Substantial” (or even “Low”)? If so for which types of use cases PID should be presented within a transaction of LoA “High”, and for which use cases PID should be presented within a transaction of LoA “Substantial”? |  |
| 2.7 Have you considered the case/need of PID update/management? Do you see a need for interoperability for PID update, or do you consider that national solutions/approaches is sufficient? How do you envision to carry it out? Do you envision access control over this operation? Defined by whom? Do you consider to subject it – amongst other criteria – to the strength/quality of the authentication protocol carried out by the RP? Do you plan to implement this functionality within your LSP?  |  |
| 2.8 Regarding the disclosure of PID, do you envision to have it controlled by access rules enforced by the wallet itself? Defined by whom? Do you consider to subject it – amongst other criteria – to the strength/quality of the authentication protocol carried out by the RP? Do you plan to implement this functionality within your LSP? |  |

## 3 Use Case Questions

Please provide the following technical details for each use case supported:

|  |  |
| --- | --- |
| **Questions**  | **Response** |
| 3.1 Please briefly describe the use case  |  |
| 3.2 Are credentials presented using:1. ISO/IEC 18013-5, or
2. OpenID4VP or
3. Both
4. Other protocols
 |  |
| 3.3 Is the key used to authenticate the presentation to the relying party:1. A wallet specific key
2. A PID specific key
3. A TSP certified key
4. Other key specifically used to selectively disclose attributes
5. Self certified key
 |  |
| 3.4 Is the ownership key used in presentation certified as:1. In accordance with ISO/IEC 18013-5
2. Using DID document issued by the wallet issuers
3. Using DID Document issued by a EAA
4. Using OpenID Federation
5. Using SIOPv2
6. Other, please specify
 |  |
| 3.5 What mechanism is used to identify trusted sources of certification of keys, identification information and attributes other than TSPs?Is this similar to ETSI TS 119 612 trust list ? |  |
| 3.6 Can credential presented using selective disclosure? If yes is this 1. Using SD-JWT
2. Using ISO 18013-5 MSO
3. Using other protocols
4. Using Zero Knowledge Protocols
 |  |
| 3.7 How is the subject of an EAA represented in an EAA:1. A TSP-User represented by a PID of wallet holder
2. A TSP-User represented by a Pseudonym
3. Another legal / natural person, identified as a() or (b) above for which the TSP user has authorisation to represent for the purpose of requesting EAA.
4. An object, represented by an unambiguous identifier, for which the TSP-User has authorisation to represent using one or more EAA.
 |  |
| 3.8 Are EAA formatted in accordance with:1. W3C verifiable credentials data model?
2. ISO/IEC 18013-5
3. Other
 |  |
| 3.9 Are EAA issued in accordance with OpenID4VCI? |  |
| 3.10 How are Relying Party request authentication keys certified1. Using TSP signing / sealing certificate issued for natural or legal persons
2. Using QTSP signing / sealing certificate issued for natural or legal persons
3. Using certificate assigned through register of relying parties?
4. Other, please describe
 |  |
| 3.11 What Authentic sources are used as source of EAA attributes?Is this done through online access? If so how is access secured?  |  |
| 3.11 If there other specific technical features of the protocols used that should be taken into account in standardisation, please provide details. |  |

## 4. Secure Cryptographic Element / Device Questions

The Architecture and Reference Framework foresees three different wallet solutions to store and manage cryptographic keys:

1. Embedded secure element or trusted execution environment for mobile devices,
2. External device, e. g. secure element or smart card,
3. Backend device, i. e. hardware security module.
4. Combination of a-c

All four solutions would require different protection profiles for the certification of the wallet’s key management system. Combinations of a-c might require even more protection profiles. WG17 would like to prioritise on the more relevant ones.

|  |  |
| --- | --- |
| **Questions**  | **Response** |
| 4.1 Does the choice of the wallet’s key management system (a-d from above) have any influence on the considered use cases? |  |
| 4.2 If yes, please describe the influence of the key management systems. Especially, what functionality from the wallet’s secure element is required from the use cases. |  |
| 4.3 What type(s) of key management system will be part of the use cases? |  |
| 4.4 Will there be one preferred key management system for the wallet, e. g. embedded secure element for mobile devices? |  |
| 4.5 Do you think all types of key management systems will be used in future wallet implementations? |  |
| 4.6 In terms of certification readiness and availability, do you see one key management system that is more advanced than the other? If yes, please describe. |  |
| 4.7 Are there any requirements from the use cases that need to be considered in the certification of the wallet’s key management system? |  |