Why?

- Europe is working towards a wallet-based identity ecosystem.
- Two protocols are in the core of the specification: ISO 18013-5:2021 (mDL) and OpenID4VC + Verifiable Credentials.
- The current version of the ARF has not yet decided on the trust fabric. However, for a real world ecosystem, it is clear an interoperable trust fabric will be needed.
- The OpenID Federation specification seems to have many characteristics that would allow such a wallet ecosystem to be defined.

This activity will investigate and test the use of the OpenID Federation protocol as a trust fabric for a wallet ecosystem.
Wallet instance attestation

-> How to know the Wallet asking for credentials is fit for purpose?
  • The wallet provider validates the wallet (software) and possibly OS is correct
  • But we do not want to depend on big tech to do it for us each and every time
  • We may have additional rules, depending on Wallet capabilities
  • We do not want to create wallet ‘islands’

Which components of OpenID Federation are used to express what?
Wallet Attestation Scenario - EUDI only
Wallet Attestation Scenario - EUDI only

1. **Attestation Credentials (JWT)**
   - Issuer issues credentials.
   - Wallet solution has OS hardware signature from vendor & OS provider.
   - Wallet provider builds trust chain to verify wallet provider issuer.
   - Issuer is a trusted issuer in the federation.

2. **Request credentials from issuer and presents attestation Credential JWT in attestation parameter**
   - Wallet solution presents credential JWT in the attestation parameter.
   - Hardware vendor and OS vendor issue device integrity statement (PKI).

3. **Builds Trust Chain to verify Wallet provider issuer**
   - Device Integrity Service is a trusted service for the provider.

4. **Is a trusted issuer in the federation**
   - EUDI TA Certification programme.
   - EU metadata rules.
Wallet Attestation Scenario - EUDI and other wallets

- **ISSUER**
  - Issues Credentials
  - (2) Request credentials from issuer and presents Attestation Credential JWT in attestation parameter

- **Wallet Solution**
  - Has OSI Hardware signature from vendor & OS provider
  - Hardware vendor and OS vendor issue device integrity statement (PKI)

- **Device Integrity Service**
  - Validates signature
  - Is a trusted service for the provider

- **wwWallet Solution**
  - (1) Attestation Credentials (JWT)
  - (2) Request credentials from issuer and presents Attestation Credential JWT in attestation parameter

- **wwWallet Provider**
  - (1) Attestation Credentials (JWT)
  - (3) Local metadata rules
    - “We do not need EIDAS High”
  - T
    - This wallet supports “Personalized”

- **National Intermediate**
  - Can build trust Chain
  - (3) Local metadata rules
  - e.g. eduGAIN
  - Sectoral Intermediate

- **edugain Trustmark Issuer**
  - Is a trusted issuer in the federation
  - edugain Trustmark
  - Sectoral metadata rules

- **EUDI TA Certification programme**
  - EU metadata rules
  - Is a trusted Issuer in the federation
Existing trust framework

- eduGAIN policy
- REFEDs specifications evaluation: https://edu.nl/wye4g

REFEDs specification

The information from the specifications is distributed in two ways:

- Entity metadata 😞
- As part of the transaction 😊
Personalized Access v.2

( And "Research and Scholarship", "Anonymous Access" & "Pseudonymous Access" )

The following was noted:

- The layout needs significant changes
- Use of SAML specific jargon, including “Entity Category”
- Contact details in OIDC specification only allow for a simple multivalued list of strings.
  -> proposal in github suggests a new claim, "contacts_detailed", supporting the same granularity as is used in the SAML implementation of the specification.
- It is not possible to have the same Trustmark exist both as a self-issued and at the same time as issued by a trustmark issuer
- Well developed mechanism to delegate the issuance and ownership of Trustmarks.
- Introduce a personalized scope to streamline the exchange of personal data

An example of what an adopted version of the specification might look like:
(Please note: the above is NOT a proposal to actually change the specification!)
RAF, MFA, SFA and SIRTFI

Assurance Framework

- The assurance profile already has a provision (section 7) on how to use the specification with OIDC.
- All statements which are part of this specification are expressed as claim values.

MFA and SFA framework

- The Multi- and Single Factor Authentication profile express all statements at transaction time.
- Both specifications already describe how to use these both in the SAML and in OIDC.
- In a wallet ecosystem, it might be relevant to transport this MFA or SFA information as part of a verifiable credentials statement, perhaps by extending RAF

SIRTFI

- The SIRTFI specification leverages metadata to signal compliance for both SPs/RP as well as IdP/OP.
- All of the challenges identified with ‘Personalized Access’ apply
- The OIDC specification supports the concept of contact details, but only as a simple multivalued list of strings. The SIRTFI specification mandates the presence of a security contact, as described in the Security Contact specification. To resolve this issue, a new claim, "contacts_detailed", could support the required granularity that is needed.