Trust Fabric
Sprint demo

Niels van Dijk
Diana Gudu
Gabriel Zachmann
Roland Hedberg
Mihály Héder

Sprint Demo, 23 January 2024

Public (PU)
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 declared the organizational trust out of scope. 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.
OIDFed Trust relationships to implement
Old4VP Flow with trust chains

Phase 1: wallet initiation
- Wallet Provider
- Verifier
- Credential Issuer
- Hintered IA (V)
- T. Anchor (V)
- Hintered IA (WP)
- T. Anchor (WP)
- Hintered IA (CI)
- T. Anchor (CI)

Establishes trust
- Wallet obtains Wallet Attestation (WTE)

Phase 2: user discovers verifier
- Interacts

Phase 3: wallet trusts verifier
- Obtains Verifier Metadata
- Looks up hinted authority
- Finds Trusted Anchor

Authorization Request (presentation definition)
- Wallet presents Wallet Attestation (WTE) including wallet provider URL
- Authorization Response (VP token with verifiable presentations)
- Looks up metadata
- Looks up hinted authority
- Finds trusted Anchor

Phase 4: verifier trusts wallet provider

Phase 5: verifier trusts credential issuer
- Looks up metadata
- Looks up hinted authority
- Finds trusted Anchor

Phase 6: Presented credential accepted
Challenges

• Wallet instance attestation
• Re-using existing trustframework
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?
Existing trust framework

- eduGAIN policy
- First attempt (WIP) to map and discuss REFEDs specifications: https://edu.nl/wye4g
Thank you! Questions?