Trust Fabric

Sprint demo

Niels van Dijk
Diana Gudu
Gabriel Zachmann
Roland Hedberg
Mihály Héder

Sprint Demo, 23 january 2024
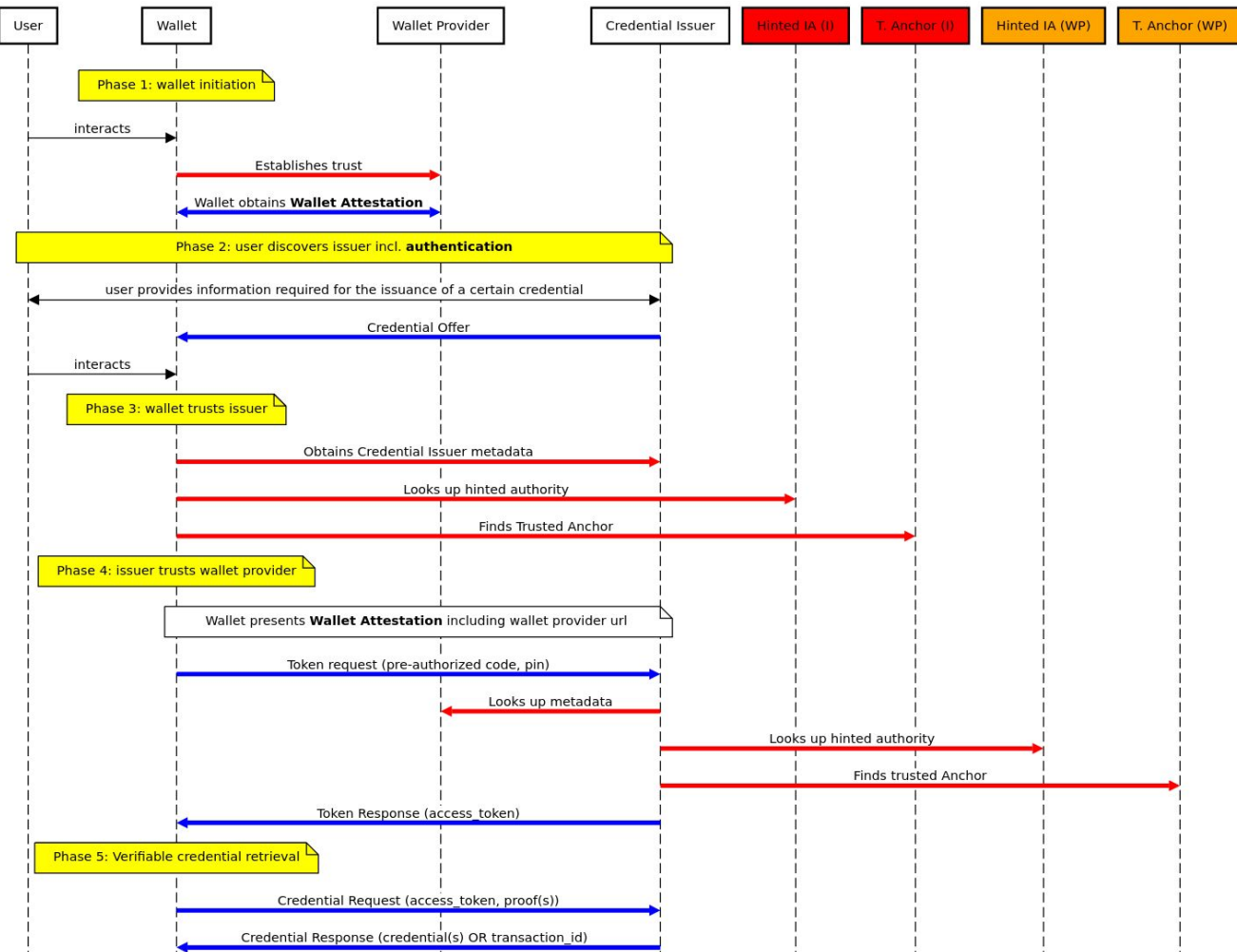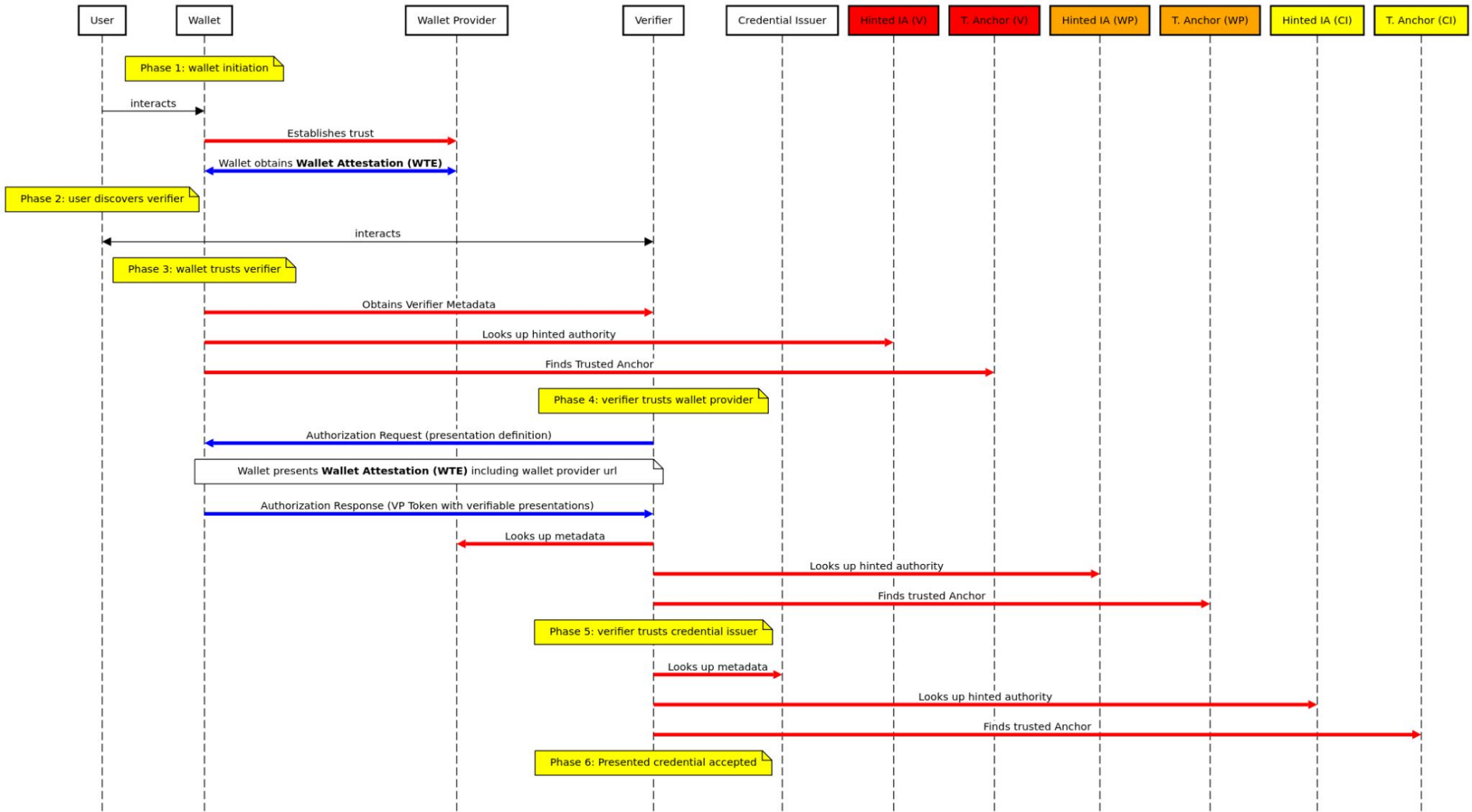
GN5-1

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

Dashed red line: OIDFed Trust chain

OID4VCI Code Flow with Trust chains

User | Wallet | Wallet Provider | Credential Issuer | Hinted IA (I) | T. Anchor (I) | Hinted IA (WP) | T. Anchor (WP)

Phase 1: wallet initiation

interacts

Establishes trust

Wallet obtains **Wallet Attestation**

Phase 2: user discovers issuer incl. **authentication**

user provides information required for the issuance of a certain credential

Credential Offer

interacts

Phase 3: wallet trusts issuer

Obtains Credential Issuer metadata

Looks up hinted authority

Finds Trusted Anchor

Phase 4: issuer trusts wallet provider

Wallet presents **Wallet Attestation** including wallet provider url

Token request (pre-authorized code, pin)

Looks up metadata

Looks up hinted authority

Finds trusted Anchor

Token Response (access_token)

Phase 5: Verifiable credential retrieval

Credential Request (access_token, proof(s))

Credential Response (credential(s) OR transaction_id)

OID4VP Flow with Trust chains

| User | Wallet | Wallet Provider | Verifier | Credential Issuer | Hinted IA (V) | T. Anchor (V) | Hinted IA (WP) | T. Anchor (WP) | Hinted IA (CI) | T. Anchor (CI) |

Phase 1: wallet initiation

User → Wallet: interacts

Wallet → Wallet Provider: Establishes trust

Wallet ↔ Wallet Provider: Wallet obtains **Wallet Attestation (WTE)**

Phase 2: user discovers verifier

User ↔ Verifier: interacts

Phase 3: wallet trusts verifier

Wallet → Verifier: Obtains Verifier Metadata

Wallet → Hinted IA (V): Looks up hinted authority

Wallet → T. Anchor (V): Finds Trusted Anchor

Phase 4: verifier trusts wallet provider

Verifier → Wallet: Authorization Request (presentation definition)

Wallet presents **Wallet Attestation (WTE)** including wallet provider url

Wallet → Verifier: Authorization Response (VP Token with verifiable presentations)

Verifier → Wallet Provider: Looks up metadata

Verifier → Hinted IA (WP): Looks up hinted authority

Verifier → T. Anchor (WP): Finds trusted Anchor

Phase 5: verifier trusts credential issuer

Verifier → Credential Issuer: Looks up metadata

Verifier → Hinted IA (CI): Looks up hinted authority

Verifier → T. Anchor (CI): 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

Demo

Thank you! Questions?