NGI TRUST CHAIN

NGI FORUM 2023

WORKSHOP 5

DIGITAL IDENTITY AND DIGITAL WALLETS

- COMMON GROUND TO ENHANCE SCALABILITY AND ADOPTION -

WHY DO WE NEED DIGITAL ID WALLETS?

- Both people and organisations need better tools to allow **consent-driven** sharing of identity and entitlement information.
- The claims we make using these tools must be **verifiable**, and the whole system should be designed to support **data minimisation, privacy, confidence, and interoperability**.
- European Commission's eIDAS expert group has introduced its own set of preliminary specifications to support its vision for a key piece of any digital trust infrastructure: **digital wallets**.
- European Union Digital Identity Framework (EUDI) and EU Digital Identity Wallet Consortium (EWC).
- In terms of tooling, EU is setting stage for parties to develop ‘wallets’. This is the **Electronic Identification and Trust Services for electronic transactions** (eIDAS)

ADVANTAGES OF DIGITAL ID WALLETS OVER CONVENTIONAL ID DOCUMENTS

1. **Convenience**: Users can access all their digital IDs and credentials from a single app on their mobile device, eliminating the need to carry multiple physical documents.
2. **Enhanced Security**: Digital ID wallets offer enhanced security features such as encryption to protect personal information from theft or fraud.
3. **Instant Verification**: Replace manual, outdated, and time-consuming verification processes such as phoning the issuing organizations to verify someone's credentials, which can take weeks or months.
4. **Privacy:** People can control what information to share and with whom, which can help prevent unnecessary sharing of personal information and reduce the risk of identity theft or fraud.
5. **Accessibility:** Easily accessed and verifiable anywhere at any time, which makes it easier for users to get their personal identification documents whenever they need them.
6. **Cost Savings:** Digital ID wallets can help reduce the costs associated with traditional methods of identity verification including the high costs of organizations verifying the documents.

DIGITAL ID/WALLET STANDARDIZATION EFFORTS

1. The OpenWallet Foundation (OWF): develops and maintains open source code for wallets to enable and ensure wallet interoperability
2. Decentralization Identity Foundation: DIDComm 2.0, Well Known DID Configuration, Universal Resolver & Registrar, Identity Hubs, Sidetree Protocol, DID SIOP (Self-Issued OpenID)
3. World Wide Web(W3C) Consortium: DIDs, VCs, JSON-LD, ZCAP-LD, Linked Data Proofs, WebAuthn, CHAPI
4. Internet Engineering Task Force: URL, URI, URN, OAuth, JOSE (JWS/JWE/JWT)
5. Open ID Foundation: OIDC4VC, OIDC4VP
6. Hyperledger Foundation: Anoncreds, DIDComm 1.0, DID Exchange, DKMS, Interop Test Suite, Chained Credentials, Rich Schemas, Data Overlays, Biometric Service Providers, ToIP-Stack
7. Trust over IP Foundation: The ToIP Foundation aims to create the infrastructure necessary to support overlapping global ecosystems of verifiable digital trust on the web.
8. Oasis: SAML, XDI, KMIP, DKMS

EUROPEAN DIGITAL IDENTITY FRAMEWORK (EUDI) ARF

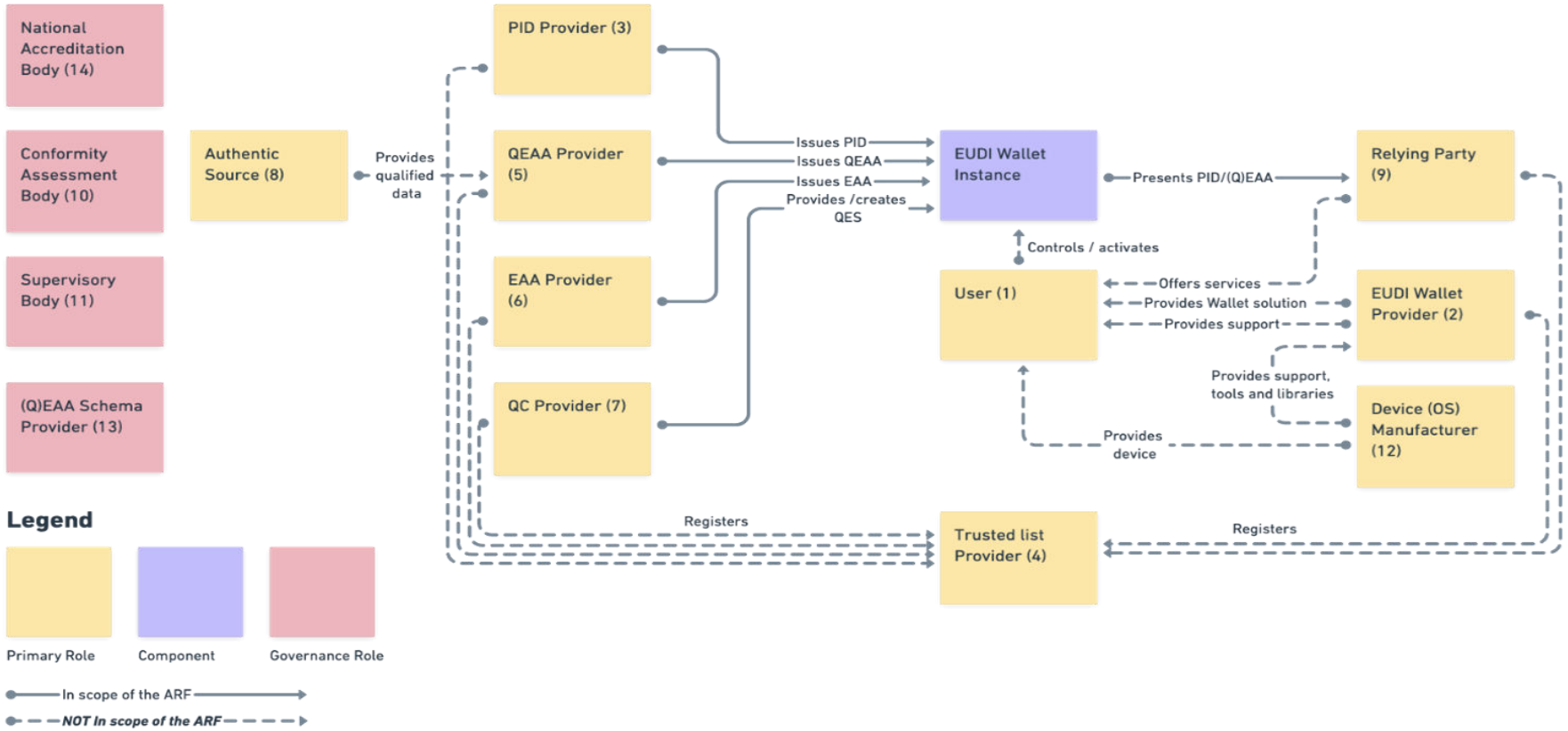
- The first published reference document titled the "**Architecture Reference Framework** (ARF)" that focuses on defining the key aspects of the digital wallet ecosystem needed to enable wallets to work together, or be interoperable, on a broad level across different regions and countries.

- EU ARF states that: An EUDI Wallet Solution is the entire product and service owned by an EUDI Wallet Provider, offered to all Users of that solution. The objective of the EUDI-wallet is "**to guarantee access to trusted digital identities for all Europeans allowing Users to be in control of their own online interactions and presence**."

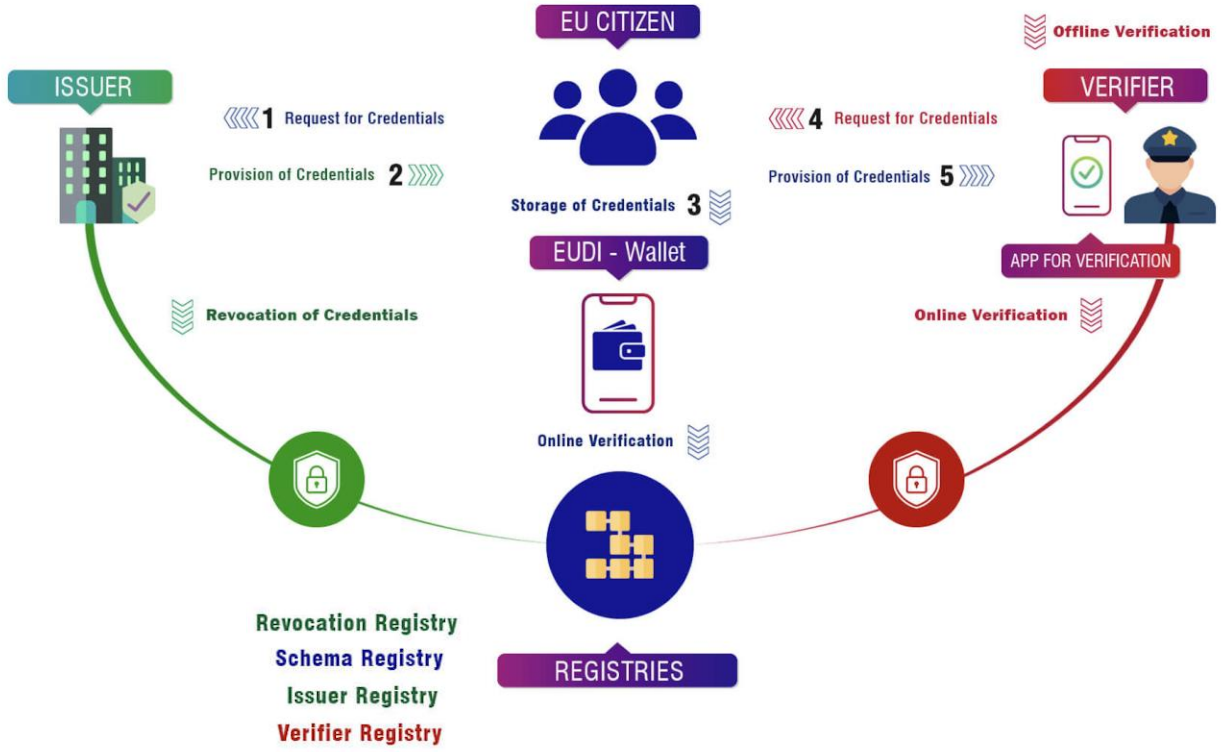
- Based on this definition it can be concluded that there are many functionalities to be developed and launched within a EUDI-wallet to provide a solution to responsible handling of personal data.

- The framework covers topics such as:
    1. The different roles in the ecosystem
    2. The types of data exchanged
    3. How the data is secured
    4. What standards and formats the data adheres to
    5. The protocols used to exchange that data

ARCHITECTURE REFERENCE FRAMEWORK (ARF)



DIGITAL ID/WALLET LIFE CYCLE / SERVICES



- Onboarding of a user
- Issuance of the EUDI Wallet
- Authentication of the user
- Display of the “EU Digital Identity Wallet Trust Mark”
- Request of person identification data (PID)
- Issuance of a PID
- Request for a (qualified) electronic attestation of attribute
- Request for a (qualified) electronic certificate
- Storage/Deletion of PID and/or (Q)EAAs
- Validation of a request from a relying party
- Presentation of PID or (Q)EAAs to a relying party
- Electronic identification (authentication) of an EUDI Wallet user
- Enabling the user to sign, seal

DIGITAL ID/WALLET FEATURES AND TECHNOLOGIES

Features

- User-centric (self-custody digital wallet)
- Device-agnostic digital wallet
- Interoperability (across different services and systems)
- Privacy-preserving
- Tamper-proof (system to store data)
- Confidentiality, Integrity, and Availability (CIA)
- Transparent, trustworthy, and secure record keeping
- Fraud prevention
- Decentralization (to reduce dependency on centralized authorities)
- Incentive mechanisms (to ensure fairness)
- Cross-border digital transactions
- Scalability
- Legal and regulatory-compliant infrastructure

Technologies

- Blockchain
- Verifiable Credentials (VC)
- Self-Sovereign Identity (SSI)
- Key-recovery mechanisms
- Multi-Party Computation
- Biometrics (User-Device Authentication)
- Decentralized reputation systems – a mechanism for assessing the reliability and behavior of entities over time, often through consensus algorithms or community feedback.
- Oracles - are intermediaries or bridges that enable communication between the blockchain and external (off-chain) sources
- Zero Knowledge Proofs (ZKP)
- Radio Frequency Identification (RFID), QR codes, Bluetooth
- Social Recovery mechanisms

BARRIERS TO DIGITAL ID WALLET ADOPTION

Technical

- Underpinning technologies remain relatively immature.
- Developers are still experimenting with ZKPs to make features such as revocation, recovery, and backups practicable.
- Switching to a decentralized model can require high upfront development costs.
- Challenges of standardization can create obstacles to achieving interoperability or the capacity of systems to exchange information.
- Many decentralized approaches also lack effective user interface and user-experience design.

Policy

- Policy objectives vary by jurisdiction; when presenting a policy challenge limited to a specific jurisdiction.
- Certain jurisdictions may not be committed to providing high-assurance official ID.
- Lack of political support can also be an obstacle to achieving decentralized ID.
- Without a mandate to foster innovation, stakeholders may not be sufficiently incentivized to take the steps necessary to achieve enhanced user privacy and security.

Governance & Implementation

- Decentralized ID systems face a communications challenge. Explaining the benefits of any novel technology can be difficult.
- Lack of recognition of the importance of digital ID can create a lack of user demand.
- Decentralized ID stakeholders also face the challenge of developing effective business models.
- Absence of effective mitigation strategies for the challenge of exclusion.

NGI TRUST CHAIN

WALLET FEATURES THAT DIFFERENTIATES AND CAN FORM KPIs

- Keys Management (multi-device support, delegation, recovery, rotation, custodial/non-custodial)
- Ledger (EVM/Non-EVM)/Non-Ledger based
- Data Storage/Presentation/Exchange Standards
- On-device/ Cloud Storage of credentials
- Hot/Cold Wallets
- Types of Claims supported : ERC 20 tokens, types of tokens, soulbound tokens
- Portability/Interoperability
- Usability /user experience
- Data minimisation strategy (ZKPs)
- Trusted issuers/verifiers
- Scalability

DIGITAL ID/WALLET CHALLENGES – LOOKING AHEAD!

- Even with a data wallet, it is not always clear to citizens which data is shared for what and with whom.
- All personal data in one data wallet creates a security risk for the citizen.
- A strong growth in different (i.e., sectoral) data wallets causes confusion among end users.
- Lack of business models to monetize from wallets
- Little functionality (e.g., only storage of personal data) in the data wallet stands in the way of broad adoption.
- Difficult to start because a stable basis (i.e., rules, standardization) is lacking.
- Legislative alignment takes far too long, causing the development and adoption of data wallets to stagnate.
- There is a lack of standardization for exchanging data between data wallets.
- Now regulating data wallets leads to stagnation of development.

NGI TRUST CHAIN

Thank you for your attention!

Questions?

Muttukrishnan Rajarajan

Professor of Security Engineering

Institute for Cyber Security,
City University of London, UK