ITU workshop on "DLT security, identity management and privacy"

Decentralized Identity Management

Abbie Barbir , PhD, CISSP

Co-Rapporteur , Q10/17
Co-Founder - ADI Association
https://adiassociation.org/

Accountable Digital Identity | ADI Association

Geneva, Switzerland, 20 February 2023

Overview

- Introduction to Decentralized Identity management at SG 17
- Overview of Identity Evolution
- Decentralized Identity overview
- Digital Identity and Trust
- Accountable Digital Identity
- How can we increase Adoption
- Conclusions

ITU-T SG 17 Identity Management

SG17 is “Parent” for Joint Coordination Activities (JCAs) on Identity management

- **Q10/17 manages JCA IDM**
- Q10/17 recently merged with Q9/17 to have **a combined questions on IdM amd Telebioetric**

Q10/17 Identity management, telebiometrics architecture and mechanisms

Motivation and Focus Biometric

- Biometrics is gaining acceptance in identity verification/authentication in applications such as e-commerce, tele-medicine, and e-health.

Identity Management

- Identity management (IdM) is essential for securing enterprises and consumer facing applications.
- Identity vetting, authentication are essential for on-line security
- Developing requirements, capabilities, and strategies for achieving interoperability between different IdM systems is essential.
- Impact of decentralization (Distributed Ledgers) on identity systems including wallet, W3C decentralized identifiers and W3C verifiable credentials.
- Develop mechanisms for IdM interoperability to include identifying and defining applicable profiles to minimize interoperability issues?
- What are the requirements to protect IdM systems from cyber-attacks?

Joint Coordination Activity on Identity Management (JCA-IdM)

- Coordinates ITU-T identity management (IdM) work among
  - ITU-T Study groups and
  - External bodies
- Ensures ITU-T IdM work is well-coordinated between study groups, in particular with
  - SG2, SG13, SG15, SG16, and SG20.
- Analyzes IdM standardization items and publishes an roadmap with Q10/17
  - Maintains IdM roadmap and landscape document/WIKI.
- Acts as a point of contact within ITU-T and with other SDOs/Fora on IdM in order to avoid duplication of work
- In carrying out the JCA-IdM’s external collaboration role, representatives from other relevant recognized SDOs/Fora and regional/national organizations may be invited to join the JCA-IdM.

IdM Coordination with other bodies

Activities(2017-2021)

Recommendations:

1. X.1080.0 (03/2017) Access control for telebiometrics data protection
2. X.1080.1 (05/2018) e-Health and world-wide telemedicines - Generic telecommunication protocol
3. X.1093 (11/2018) Telebiometric access control with smart ID cards
4. X.1094 (03/2019) Telebiometric authentication using biosignals
5. X.1252 (04/2021) Baseline identity management terms and definitions [Revised X.1252(04/2010)]
6. X.1254 (09/2020) Entity authentication assurance framework – ITU [Revised X.1254(09/2012)]
7. X.1276 (05/2018) Authentication step-up protocol and metadata Version 1.0
8. X.1277 (11/2018) Universal authentication framework
9. X.1278 (11/2018) Client to authenticator protocol/Universal 2-factor framework
10. X.1279 (09/2020) Framework of enhanced authentication using telebiometrics with anti-spoofing detection mechanisms

Keeping up with Identity Management Trends

Draft Recommendations:

- X.1250rev and X.1251rev: These Recommendations will be updated to cover current market trends
- X.gpwd: Threat Analysis and guidelines for securing password and password-less authentication solutions
- X.oob-sa: Framework for out-of-band server authentication using mobile devices
- X.pet_auth: Entity authentication service for pet animals using telebiometrics
- X.srdidm : Security requirements for decentralized identity management systems using distributed ledger technology
- X.tas: Telebiometric authentication using speaker recognition
- Joint work:
  Q14/17 to develop X.1403 “Security guidelines for using distributed ledger technology for decentralized identity management”

Collaboration with FIDO Alliance, two new specifications were adopted

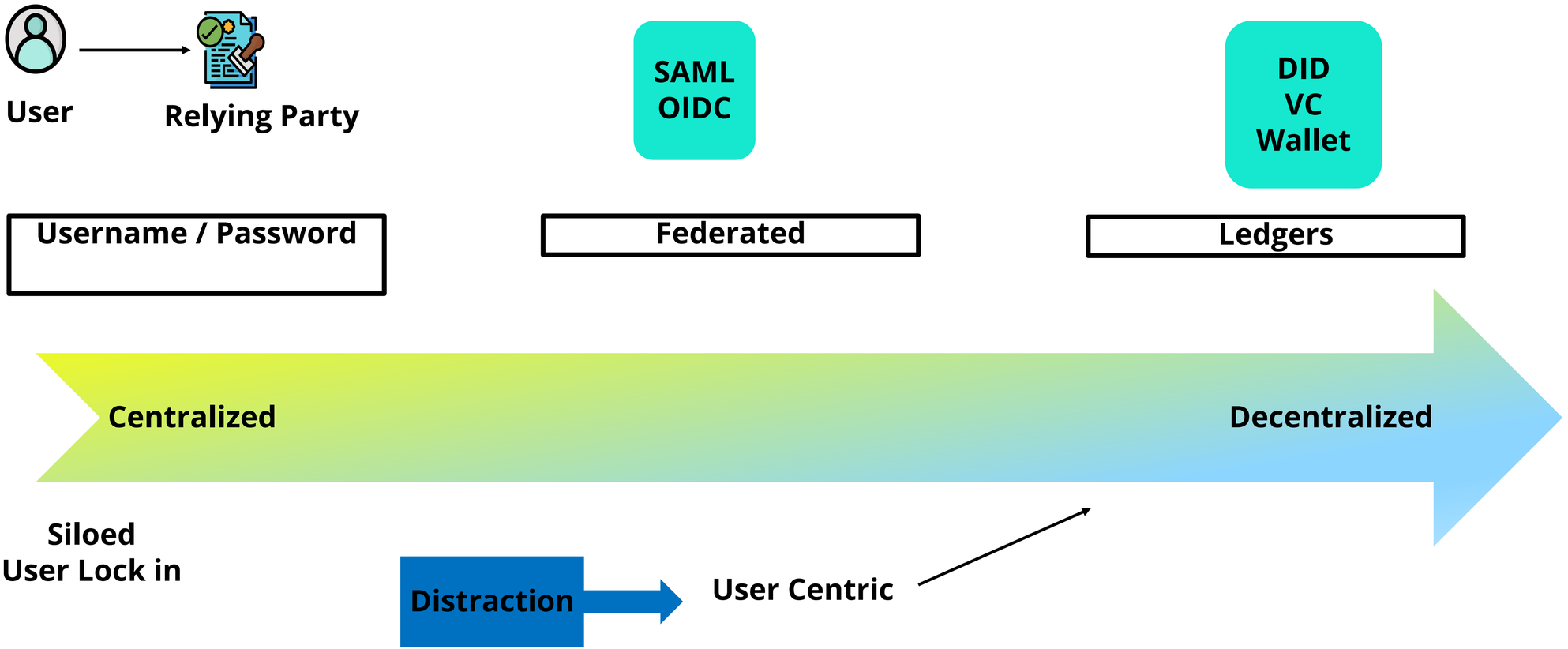
- X.1277: Universal authentication framework and
- X.1278: Client to authenticator protocol/Universal 2-factor framework

Collaboration with OASIS Electronic Secure Authentication (ESAT) TC to help secure QR code-based authentication systems because many password-less authentication systems rely on the use of QR codes to eliminate the password.

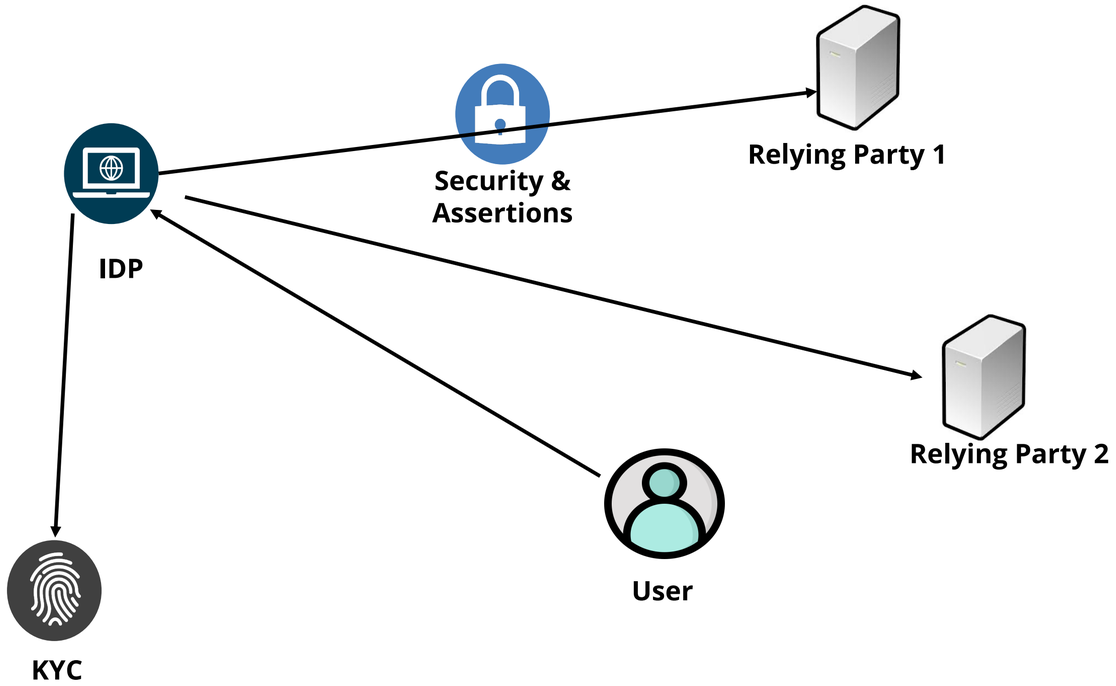
- OASIS ESAT TC published **"Secure QR Code Authentication Version 1.0 (SQRP)"** as OASIS Standard.

- Accountable Digital Identity Association, ADIA (https://adiassociation.org/)
- Global Assured Identity Network (GAIN https://nat.sakimura.org/2021/09/14/announcing-gain/)
- Trust Over IP (TOIP https://trustoverip.org/)
- Focus on Decentralized IdM systems
- Study Zero Knowledge solutions

Overview of Identity Evolution



Federated Identity



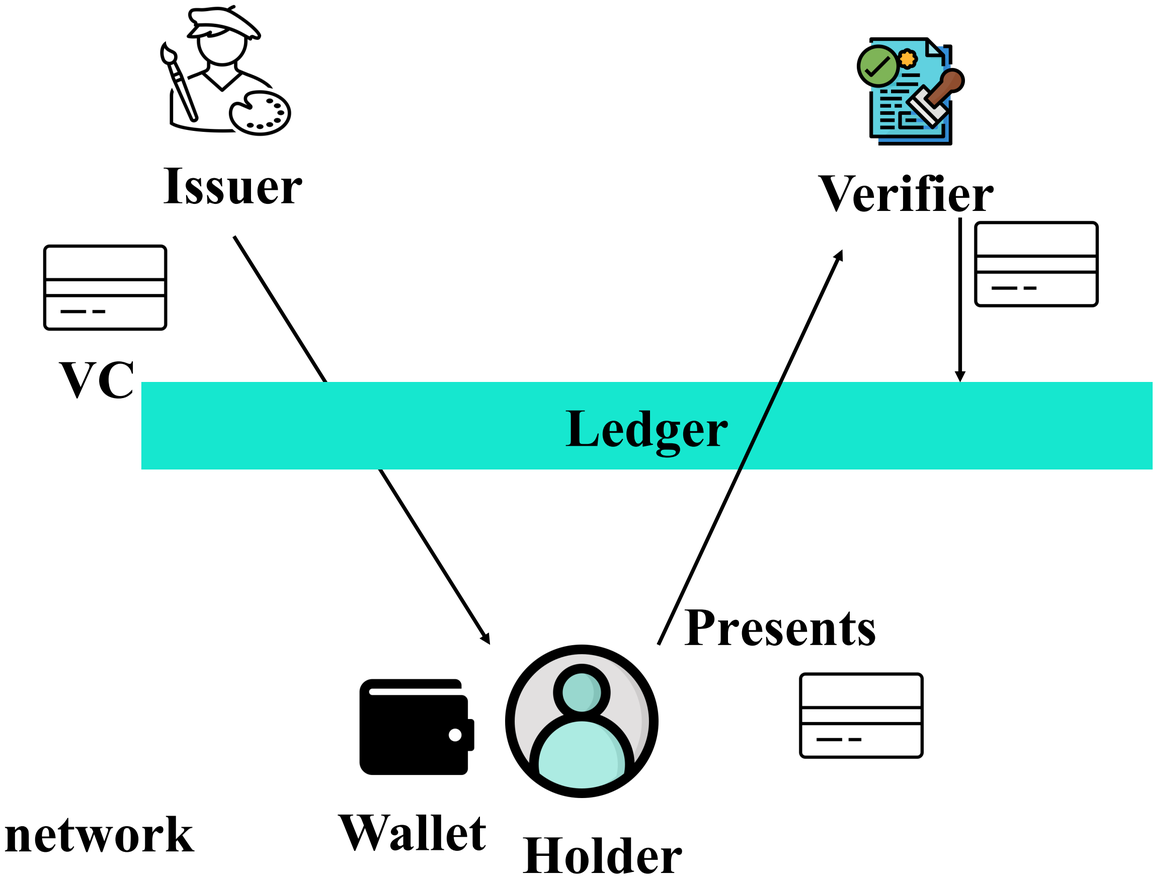
- Identity Data is control by multiple cooperating authorities with at least one IDsP
- SSO is enabled among participating entities
- Reduce reliance on multiple passwords
- KYC us Shared

- User benefits from reduced logon accounts
- Stronger authentication can be deployed since the effort is re-used
- Scalability is an issue
- User has limited input or control on how the trust relationships are formed
- User does not own their identity or their own data

Decentralized Identity

Core Features

- PKI is the foundation of trust
- Network effect through the use of Ledgers
- Peer to peer model
- User present VC to Verifier
- Changes Trust relationships with user in focus



Key Points

- PKI is central to decentralized identity
- Peer model shift focus from provider centric to network centric
- Peer model enables equal rights to all participants

Bootstrapping Identity

Identity Creation

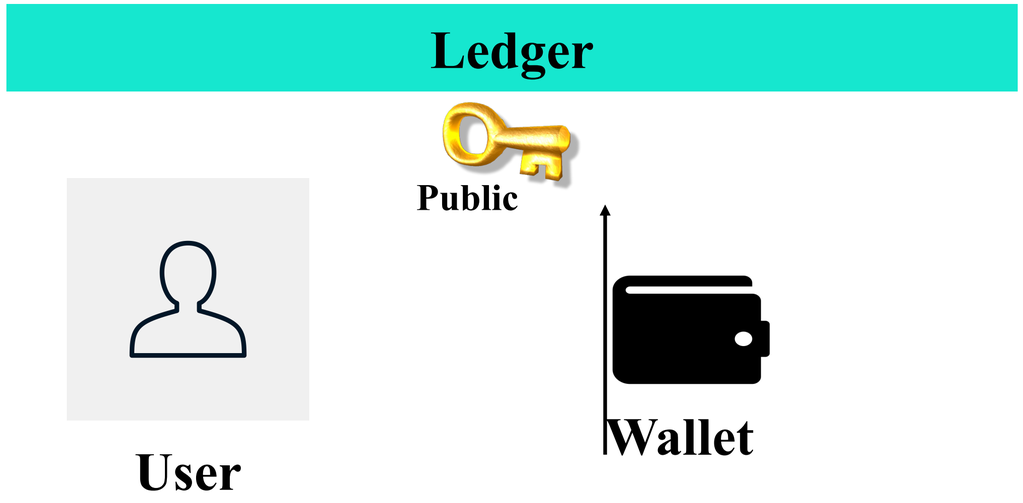
- Self Asserted Identity
- Issuer
- Wallet claim a location on the ledger by generating an Identifier
- Generates Key Pair (Public/Private)

Wallets

- Stores Verified Credentials
- Manage Identifiers and related keys
- Information published on ledge
- Credential exchange
  - No common standard yet
- Proof of possession at the presentation layer

Credential Verification

- Requires a public key

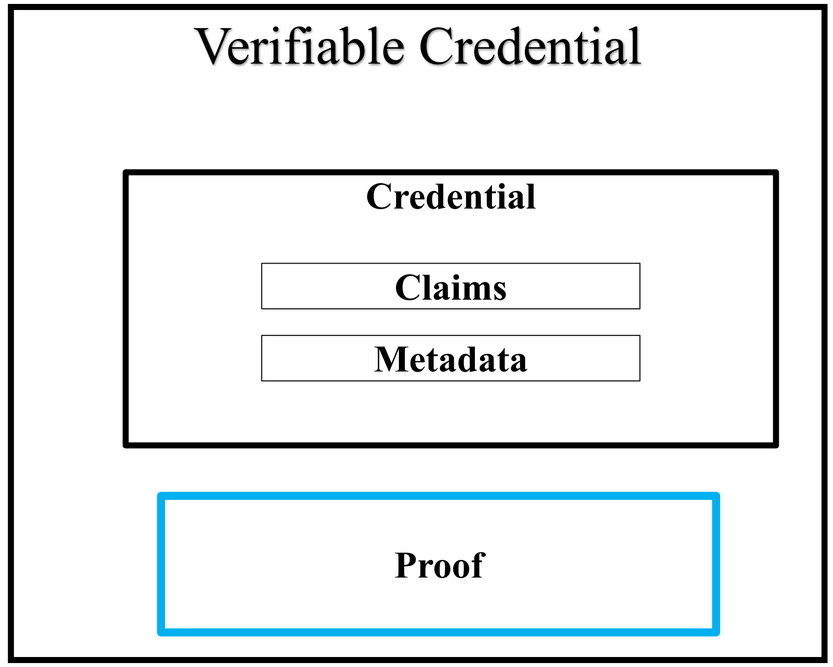


Verifiable Credentials

- **Verifiable Credentials Data Model v1.1**
  - **W3C Recommendation 03 March 2022 ;https://www.w3.org/TR/vc-data-model/**
  - **Defines a “Credential” and a “Verifiable Credential”**

A Credential is a set of one of more Claims with associated Credential Metadata

- **Claim** is an assertion (or statement) made about a subject (a person)
  - claim: Abbie (subject) is authorized to operate a vehicle (assertion)
- **Credential Metadata** refers to metadata providing info about the credential itself
  - For example, who is the issuer, issuance and expiration dates
    - Credential metadata for Abbie’s driver’s license:
      - Issuer: Florida state DMV
      - Date of issuance: : May 21, 1921
      - Expiry: May 21 , 1999
- **Proof** : Crypto Signature



Need to exceed real word use cases

A verifiable presentation is an endorsement of a subject at the time a verifiable credential is passed to a verifier

Credential Verification is Challenging

1. Is the issuer valid
2. How can I trust that the credential is about the same individual
3. Do I know the connect of the claims, do they mean the same thing to me
4. Has the credential been revoked
5. Is the issuer reputable
6. Has the claim been tampered with?
7. How to compare the validity of a claim about an individual if multi claims are available from different issuers
8. Is the claim being presented by the rightful Owner?
9. How do I make sure that my info is kept private

Trust / Governance ?

It is all about Trust

Trust Differences Federation Vs Decentralized

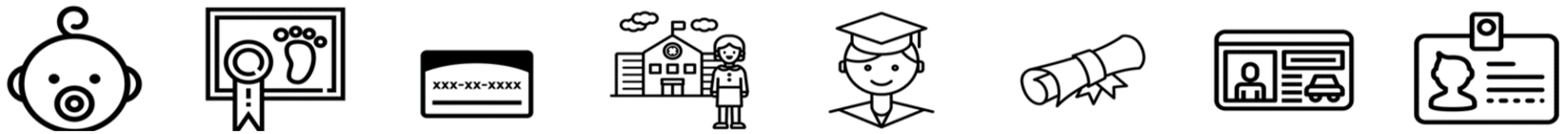
- **Federation** today based on SAML , Oauth (OIDC) are bi-directional trust
  - Parties do know and trust each other
  - Relationship is used to exchange user information

- **Decentralized Identity Trust Model**
- **Unidirectional by default**
  - Verifier can trust the issuer, but the issuer may not even know the verifier
  - Wallet play a large role to ensure privacy of user data
  - Wallet provider may have relationship with issuer and verifiers

Need to exceed real word use cases

Quick Refresh On ADI Interchange

Lifecycle of Identity In Real life



The march of time

John Smith

Identity Creation

Birth Record
Identity by - Parents
Certified by - Medical Facility
Issued by - Government

Issued:
Birth Certificate
SSN
Medical Records

Student Life

Based on Birth Cert
Enrollment in Elementary
Enrollment in School
Enrollment in University

Issued:
Student ID
Progress reports
Diploma

Adult Life

Based on Birth Cert, Diploma, SSN

Created / Issued:
Employee ID
Bank Account
Automobile Title
Real Estate Title
Medical Insurance
Health Records
....

Accountability

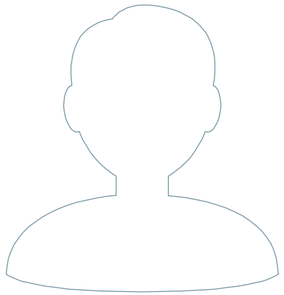
Identity Created by Trusted People & Given to John

Owned by John
Real person behind the Identity
John responsible for that Identity

Solution

Unique **Digital Address** for every user

- Given by a trusted Issuer
- Bound to human attributes (Name, DOB, Country ID)
- Unlocked by FIDO authentication
- control various Identity and Data Disclosures while interacting with Digital Services in real time directly from Issuing sources



Digital Address: **John.doe@DTX**

Fix the root cause, and stop treating the symptoms

Accountable Digital Identity | ADI Association

5 Core Principles of ADIA

We Do Not Own Personal Data

Personal ID Data Remains with Issuers Only

User's Consent for Data Disclosure

Issuers & Users Into the Value Chain

We Include All People in Digital Identity

ADI Interchange architecture

Issuers

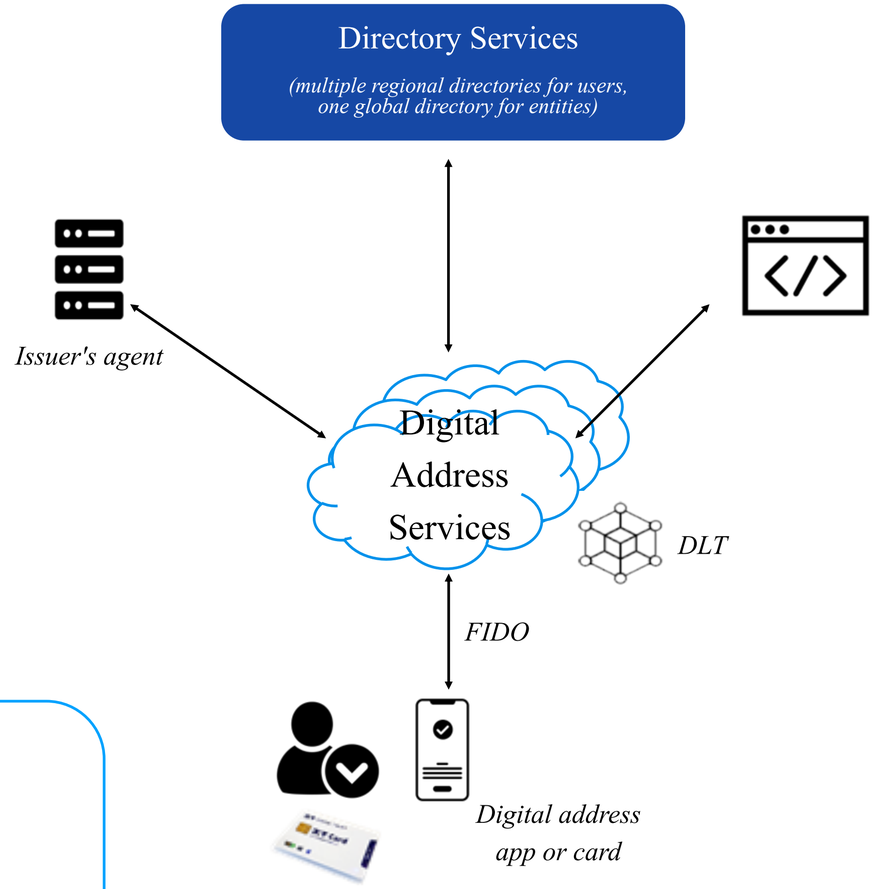
- Place of employment
- Educational institution
- Financial institution
- Driver's license issuing authority
- Passport issuing authority
- Medical facility

1 Create Digital Address

2 Issue Verifiable Credential

Easy integration for Issuer

API calls to create Verifiable Credential and publish to Digital Address



User

4 Prove identity biometrically using Digital Address

5 Provide consent to share Verifiable Credential*

Service Providers

- Digital retailer
- Healthcare provider
- Pharmacy
- Travel and transportation provider
- Prospective employer
- Insurer

3 Request Verifiable Credential*

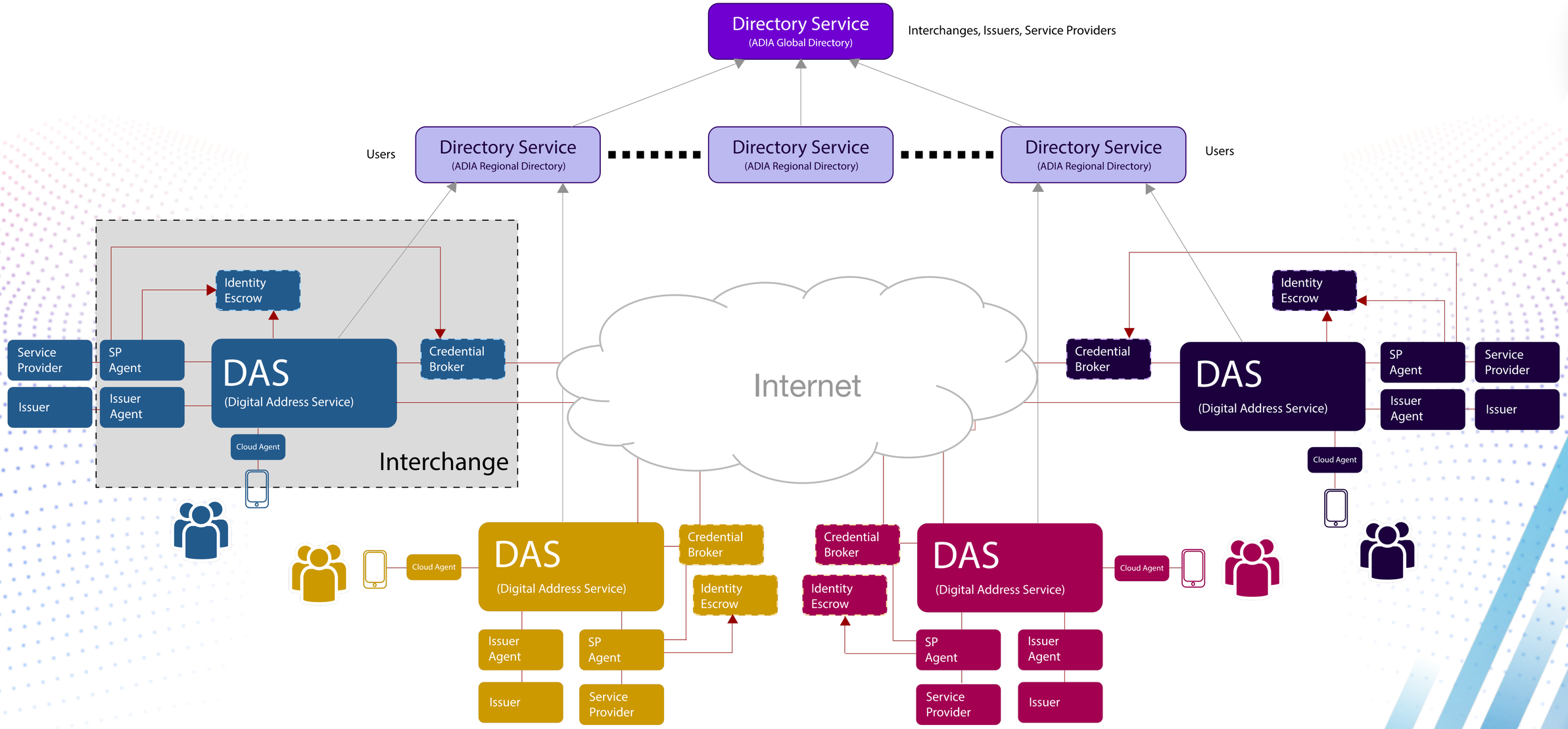
6 Validate before providing services

Easy integration for Service Provider

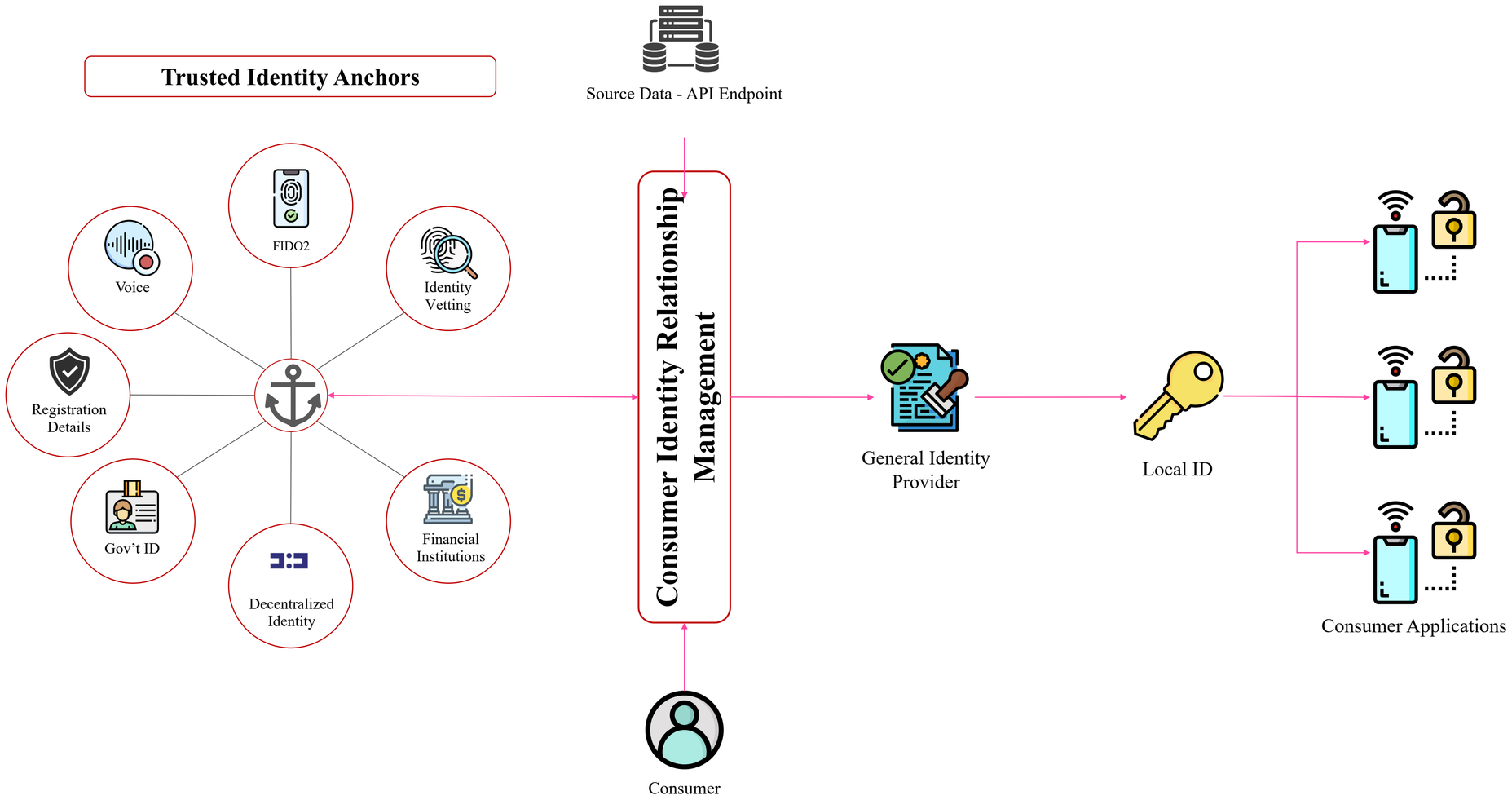
API calls to request and view Verifiable Credential

** Could be a particular claim instead of an entire credential*

ADIA Ecosystem



Adoption
Investigate Decentralization Options for Consumer Identity Relationship Management Portal



Q & A

It is all about Trust

Trust Differences Federation Vs Decentralized

- **Federation** today based on SAML , Oauth (OIDC) are bi-directional trust
  - Parties do know and trust each other
  - Relationship is used to exchange user information

- **Decentralized Identity Trust Model**
- **Unidirectional by default**
  - Verifier can trust the issuer, but the issuer may not even know the verifier
  - Wallet play a large role to ensure privacy of user data
  - Wallet provider may have relationship with issuer and verifiers

Need to exceed real word use cases