Trust & Identity Incubator

Distributed Identity for Research - DI4R

Niels van Dijk, Martin van Es, Mihály Héder, Branko Marović

June 2, 2021

Public

www.geant.org

Introduction

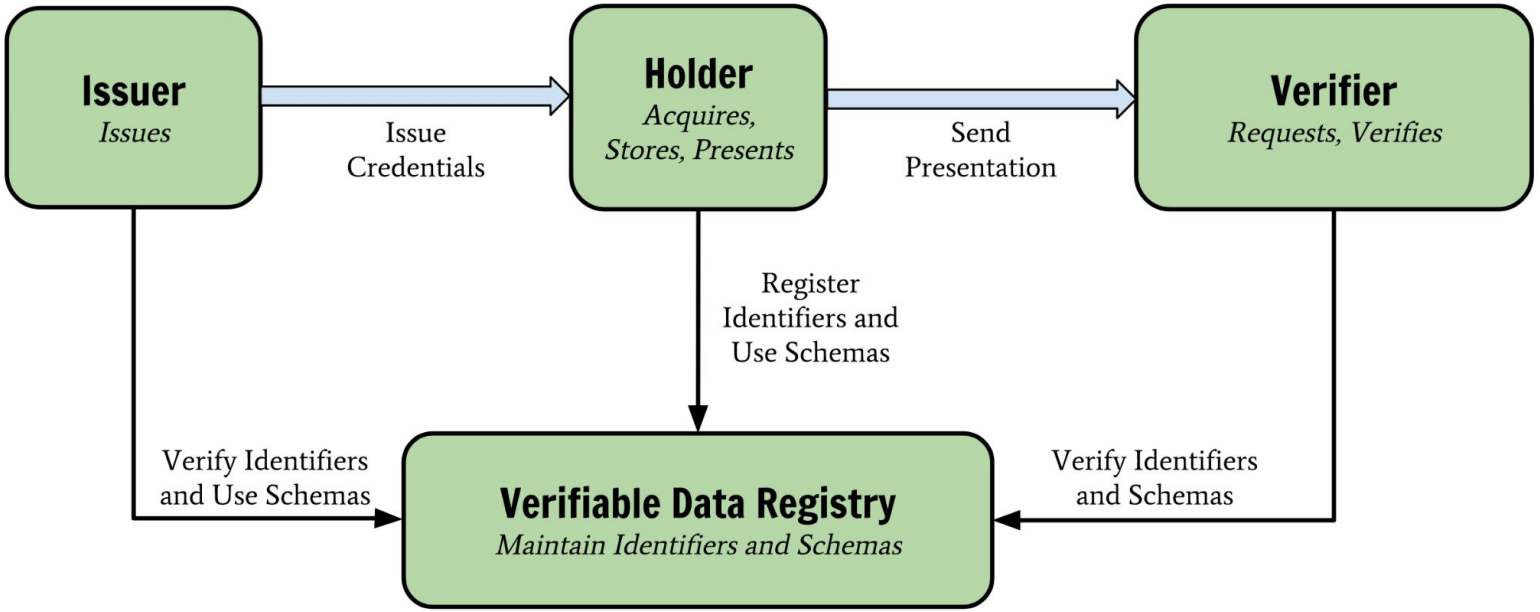
This activity explores the use of a distributed approach to provide digital identities in the context of managing research access.

- Collect use cases
- Create a proof of concept platform to test and validate the requirements
- use an existing platform

Distributed Identity

- The users (**Holder**) collect identity information (**claims**) themselves and directly control the release.
- Claims are collected into a **‘Wallet’**, e.g., on a mobile device
- Authoritative sources provide the claims to the user (**Issuers**), often after proof of ownership
- To get access to a service, the service requests a proof from the users that they possess certain claims and verifies the claims (**Verifier**)
- A **verifiable data registry** (registry) is used by all parties to ensure trust

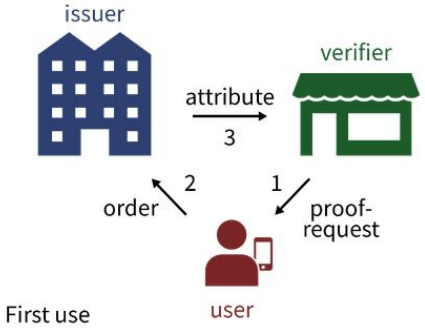
Distributed Identity



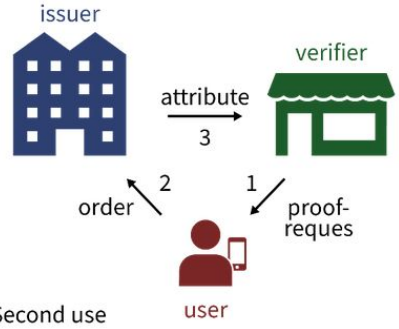
Source: W3C Verifiable Credentials Data Model, https://www.w3.org/TR/vc-data-model/

Attribute flow in Distributed Identity

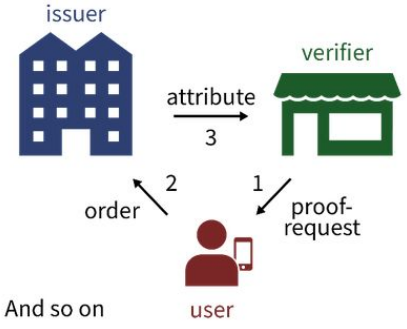
Federation



First use

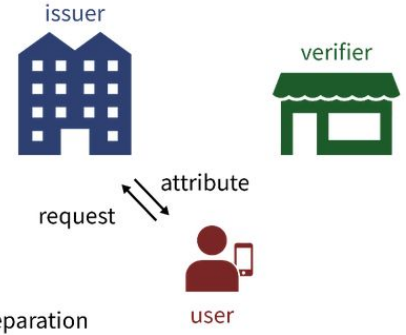


Second use

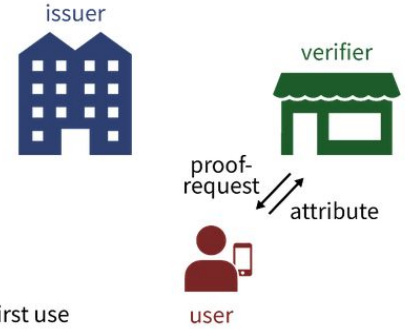


And so on

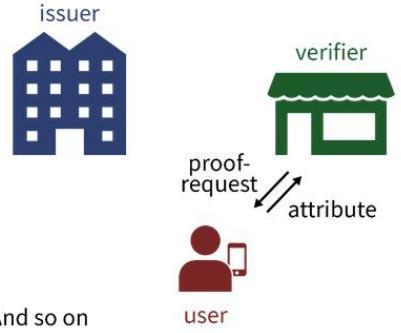
Distributed Identity



Preparation



First use



And so on

Source: https://privacybydesign.foundation/irma-explanation/#architecture

Why use Distributed Identity?

- Direct end-user control over attribute release improves privacy and data protection
- Issuers and Verifiers do not learn about users behaviour
- No central infrastructure collects all user data
- AuthN is decoupled from providing attributes
- Collection and reuse of claims from multiple sources is easier as compared to existing protocols
- Once claims are issued, the Issuer is no longer part of a transaction (Unless a claim expires or is revoked)
- The Service (Verifier) is primarily responsible for handling claims regarding verification, AuthZ and GDPR

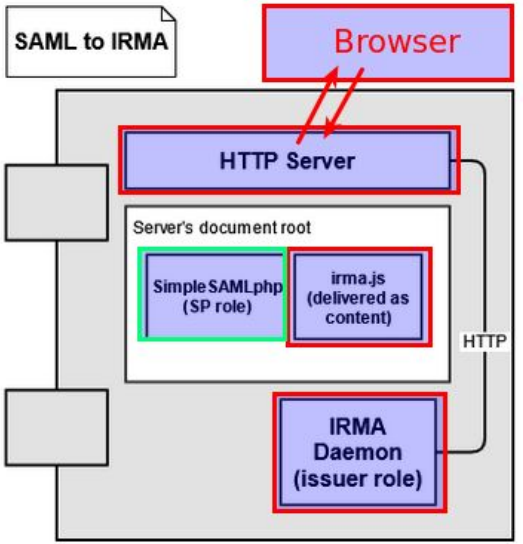
Proof of concept implementation: IRMA

- IRMA, “I Reveal My Attributes” is a system for attribute-based authentication: it is not about who you are, but what you are.
- Developed by the Privacy by Design Foundation (PBDF), being actively tested by many organisations, including SURF, commercial entities and various branches of the Dutch government.

IRMA implementation

Implements all elements Verifiable Credentials model:

- Issuer & Verifier: a frontend javascript + backend daemon
- Wallet as an iOS and Android app
- The registry is implemented as a centralized service,
  without the use of a blockchain
- All components are open source



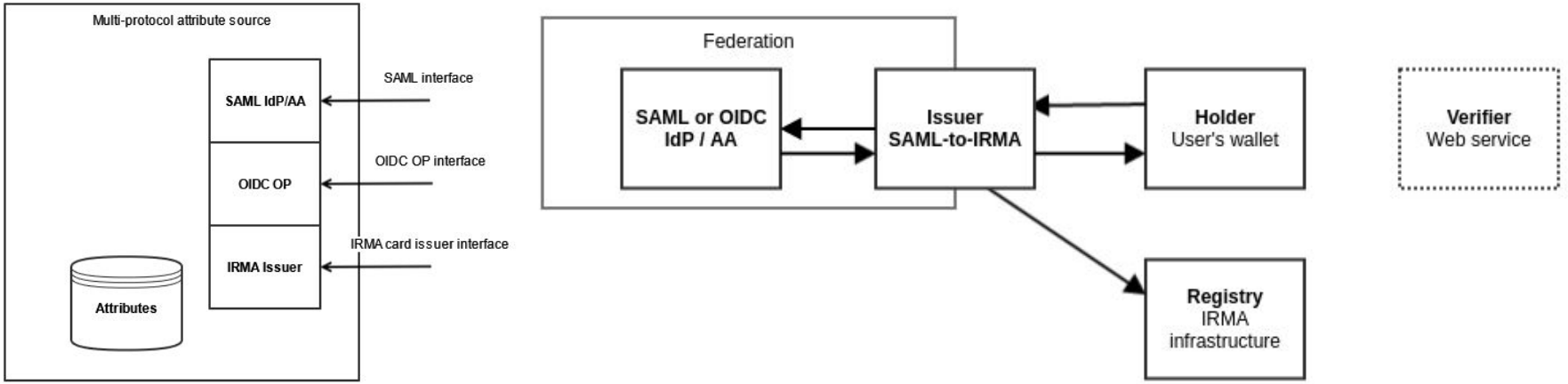
IRMA security and trust

- Implements idemix[1] providing anonymity and unlinkability.
- Issuers release signed credentials: groups of attributes .
- The user creates “zero-knowledge proof” of ownership of credentials and may selectively release attributes to the verifier.
- Verifier can test the validity of issuer as well as proof of knowledge from the users.
- A scheme lays out its Issuers, their key material and also the credentials that may be used.
- Schemes are hosted by a trusted third party (currently PBDF).

[1] https://hyperledger-fabric.readthedocs.io/en/release-1.3/idemix.html#what-is-idemix

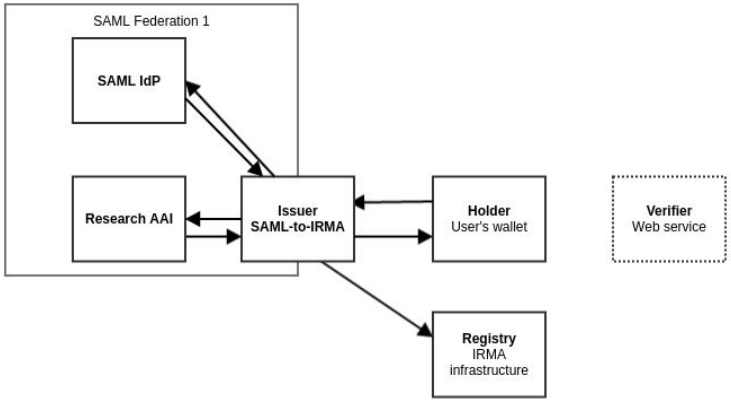
Use cases and demo -1

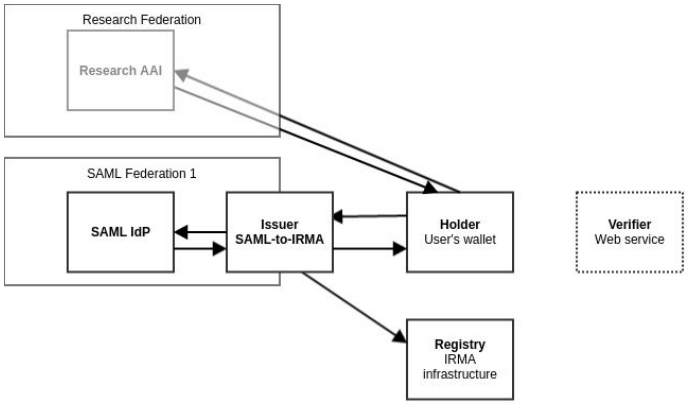
- “IdP”: - SAML + OIDC + IRMA Issuer (SimpleSAMLphp)
- “SAML/OIDC ⇔ IRMA”: IRMA token translation
- “Independent attribute registry”: ORCID



Use cases and demo -2

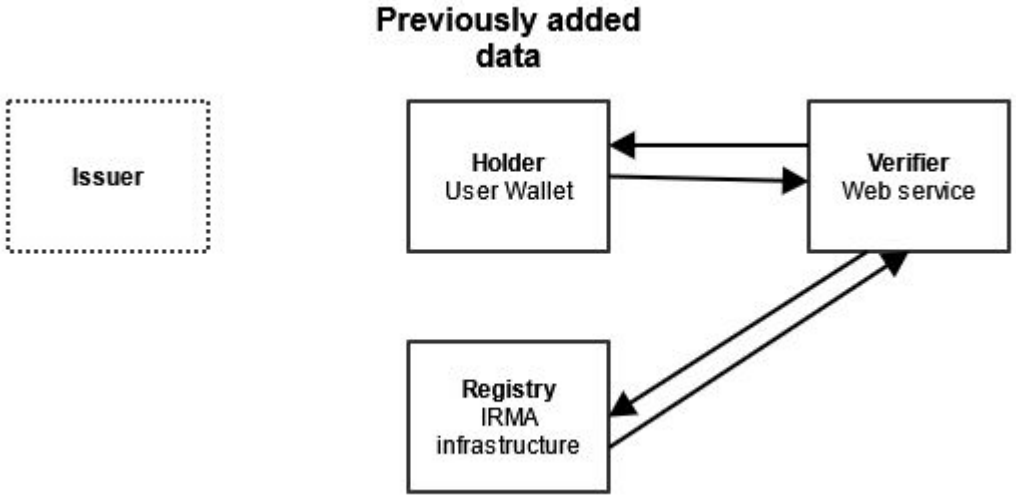
- “Research AAI Issuer”: SRAM/eduTEAMS & HEXAA





Use cases and demo -3

- Verifier: any service



TODOs:

- Discuss with Stakeholders
- Explore the best way to describe the scheme
- Test verification of claims from multiple schemes
- Discuss IRMA ‘metadata’ distribution risks
- Investigate assurance:
  - AuthN separation, revocation, lifetime, RAF
- Explore app improvements:
  - 2FA, large cards, multiple issuer flow

- Suggestions are welcome…

GÉANT
Networks • Services • People

Thank you

Any questions?

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 3 project (GN4-3).
The research leading to these results has received funding from
the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).