

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.

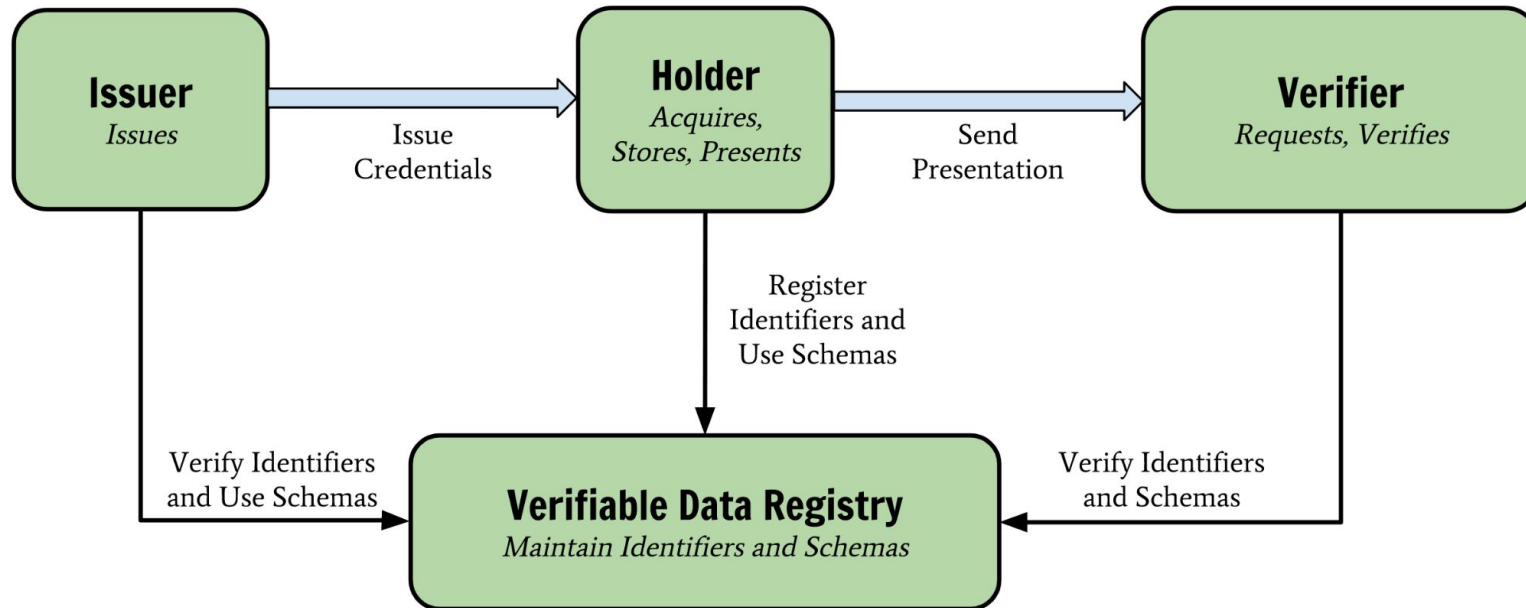
- Collect use cases
- Create a proof-of-concept platform to test and validate the requirements
- Use an existing platform



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 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

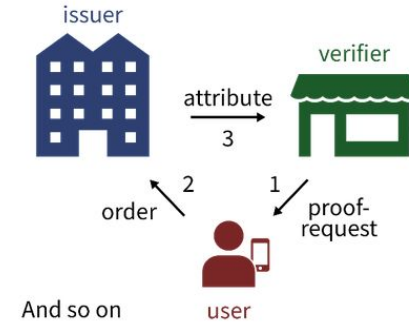
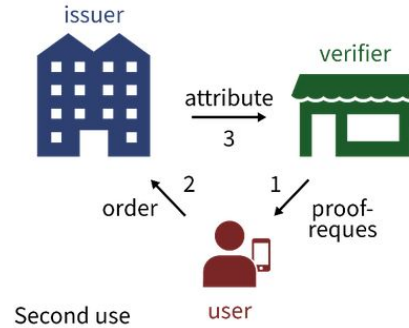
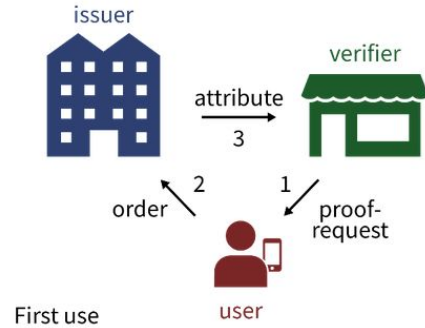


Source: W3C Verifiable Credentials Data Model, <https://www.w3.org/TR/vc-data-model/>

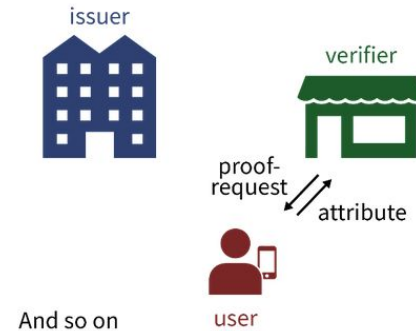
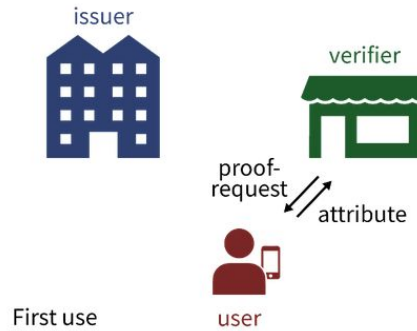
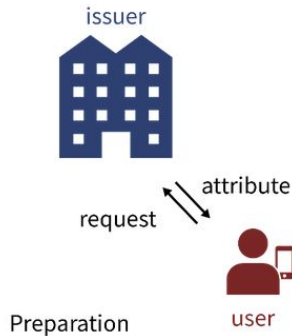


Attribute flow in Distributed Identity

Federation



Distributed Identity





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

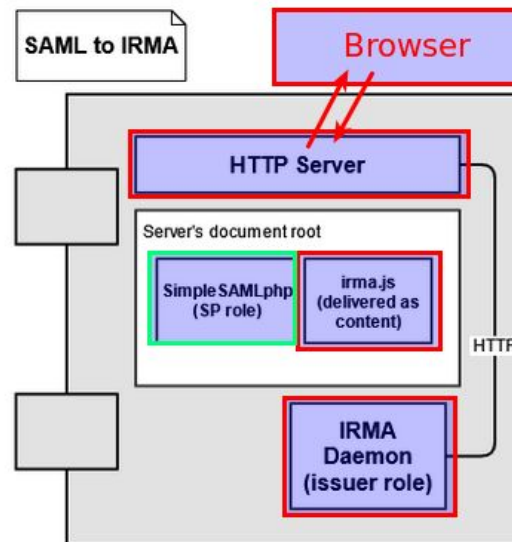
- IRMA, “I Reveal My Attributes” is a system for attribute-based authentication: it is not about who you are, but what you are.
- Developed by the Privacy by Design Foundation (PBDF), being actively tested by many organisations, including SURF, commercial entities and various branches of the Dutch government.

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





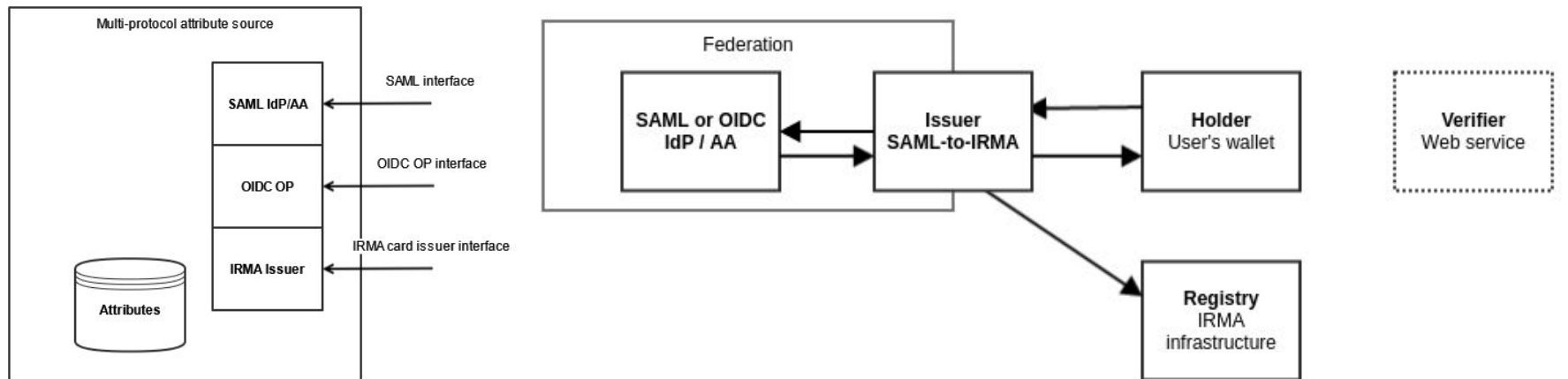
IRMA security and trust



- Implements *idemix*_[1] to provide 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 the **credentials** that may be used.
- Schemes are hosted by a **trusted third party**, currently PBDF.

Use cases and demo 1

- **IdP:** - SAML + OIDC + IRMA Issuer (SimpleSAMLphp)
- **SAML/OIDC ↔ IRMA:** IRMA token translation
- **Independent attribute registry:** ORCID



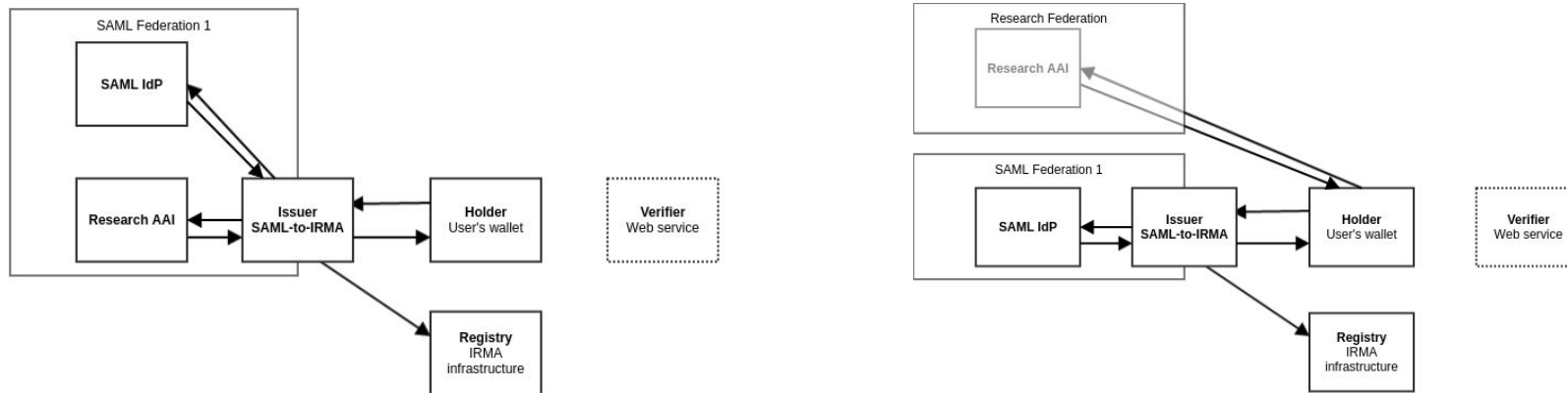


Use cases and demo 2

- Research AAI Issuer: SRAM/eduTEAMS & HEXAA**

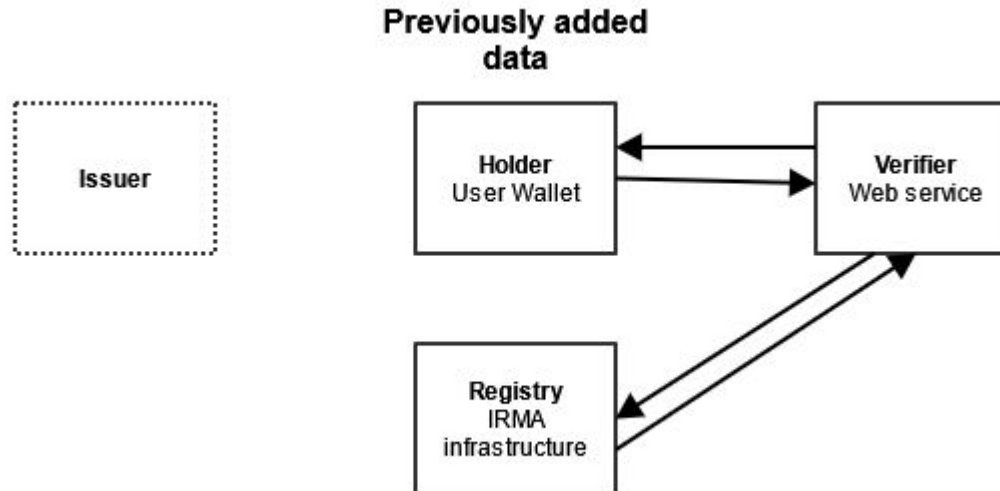
SRAM: SURF Research Access Management

HEXAA: roles-and-permissions Virtual Organization manager for SAML federations



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, REFEDS Assurance Framework
- Explore app improvements:
 - 2FA, large cards, multiple issuers flow

- Suggestions are welcome...

Thank you

Any questions?

www.geant.org

