Trust & Identity Incubator

Distributed Identity for Research - DI4R

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

Internet2 CAMP, Oct 5, 2021

Public

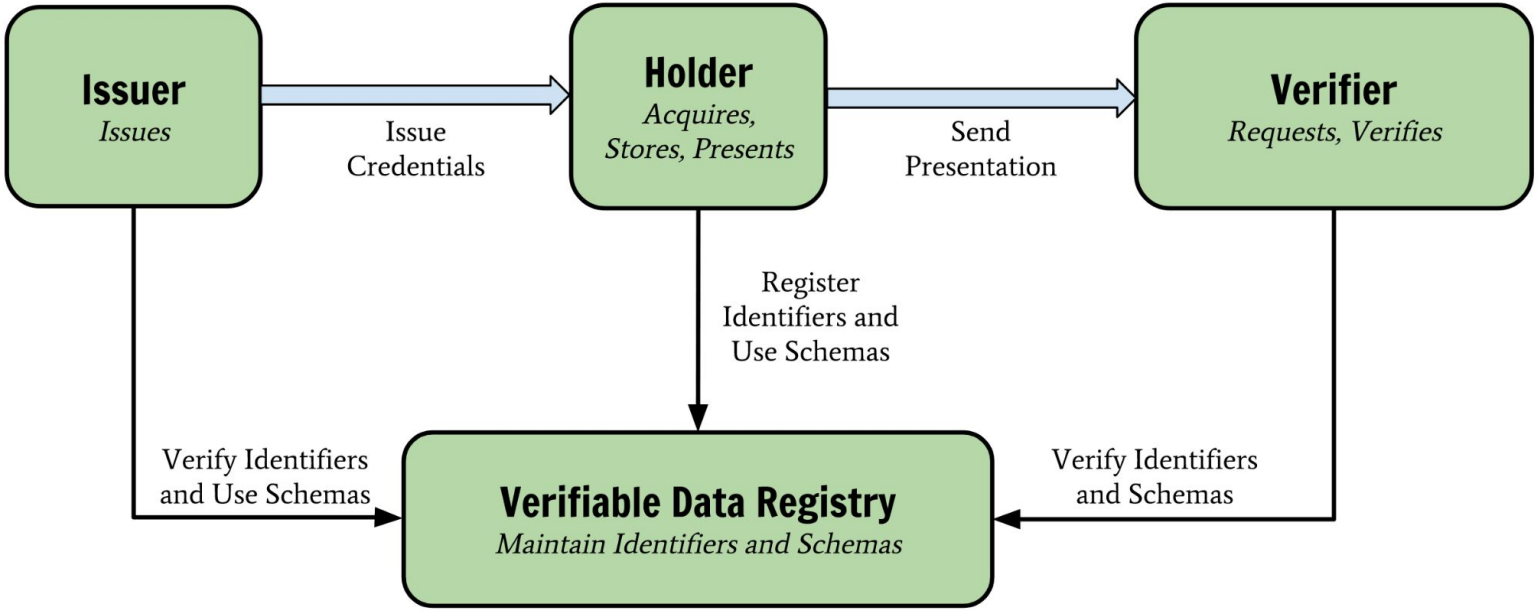
www.geant.org

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

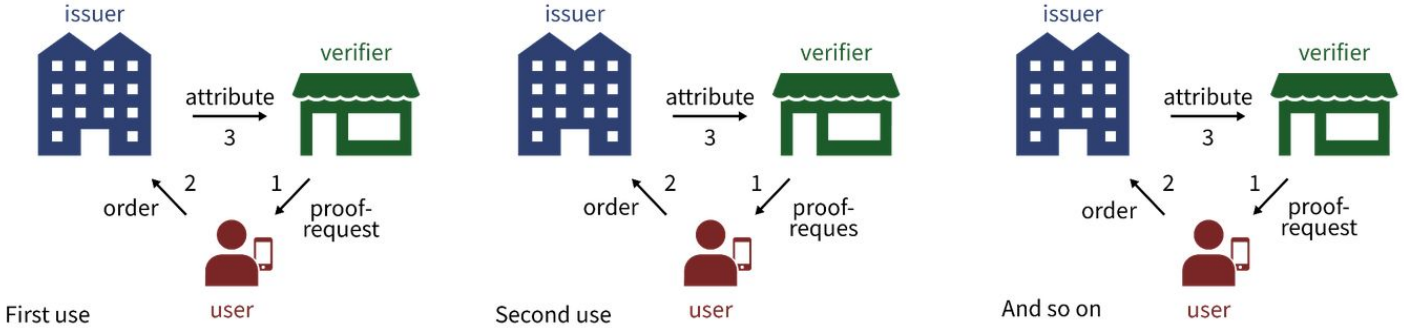
Distributed Identity



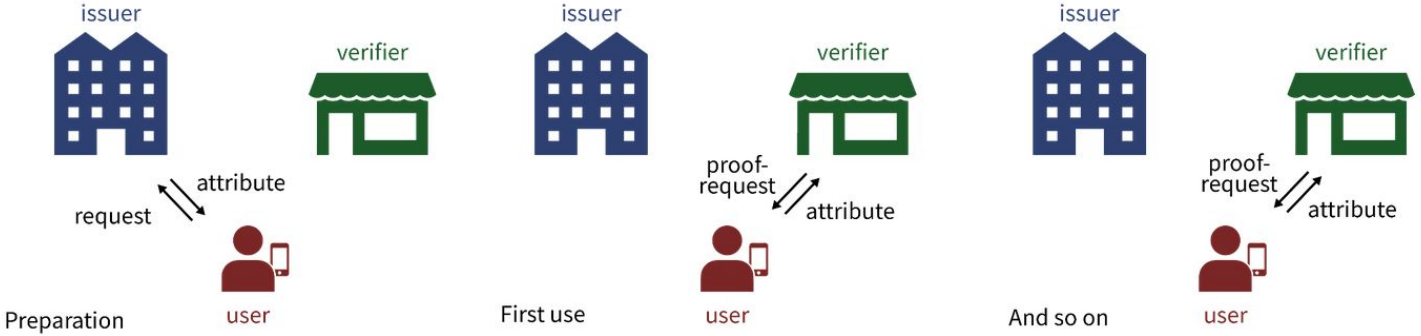
Source: W3C Verifiable Credentials Data Model, https://www.w3.org/TR/vc-data-model/

Attribute flow in Distributed Identity

Federation



Distributed Identity



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

Why investigate Distributed Identity?

User

- Direct control over personal data
- Issuers and Verifiers do not learn about users' behaviour
- No central infrastructure collects all user data
- Claims in wallet are atomic

Entities

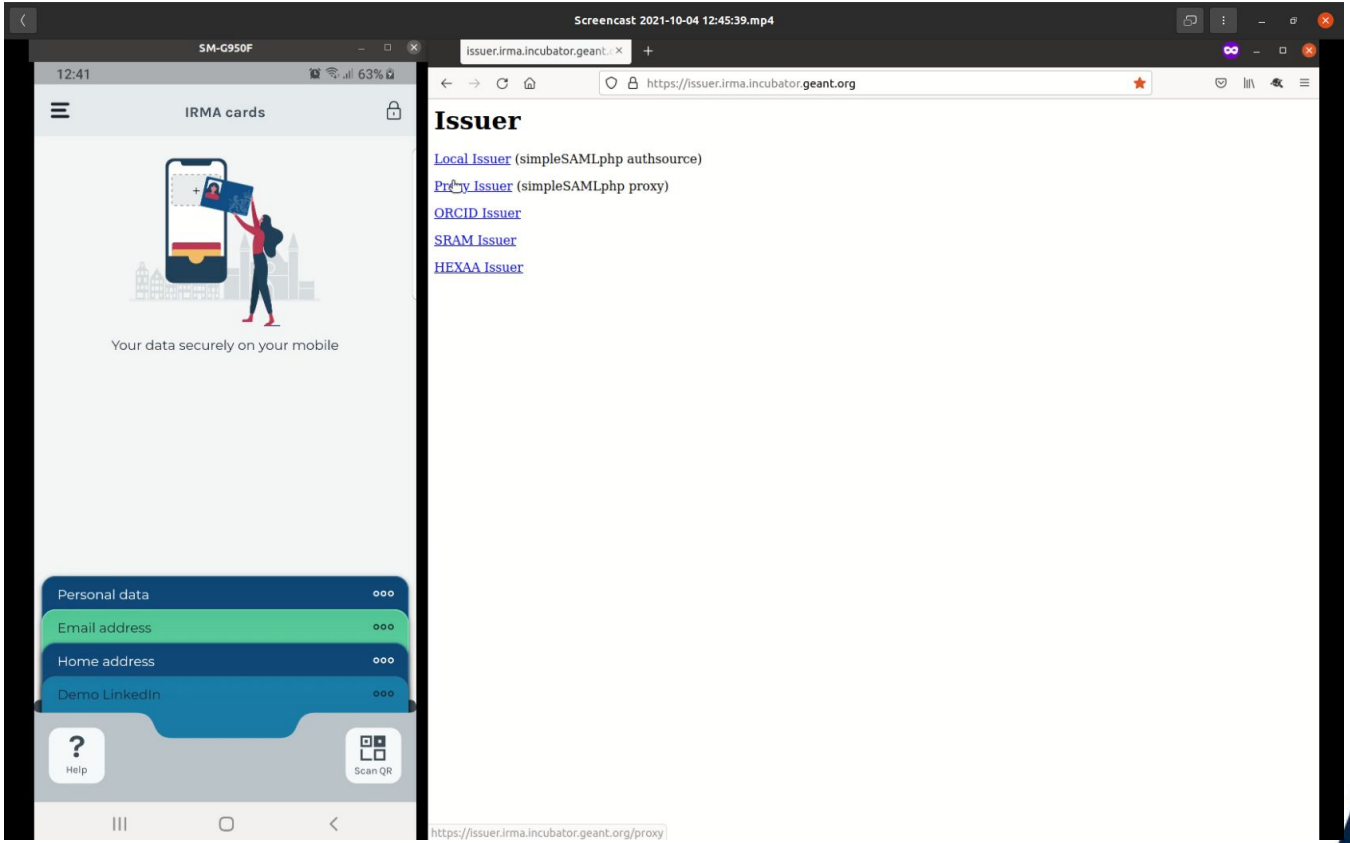
- Once claims are issued, the Issuer is no longer part of a transaction (unless a claim expires or is revoked).
- The service (Verifier) is responsible for handling claims w.r.t. verification, AuthZ and GDPR.

Why investigate Distributed Identity?

Ecosystem

- Collection and reuse of **claims** from multiple sources is easier as compared to existing protocols
- The service (**Verifier**) is primarily responsible for handling claims regarding verification, AuthZ and GDPR.

Use cases & Demo



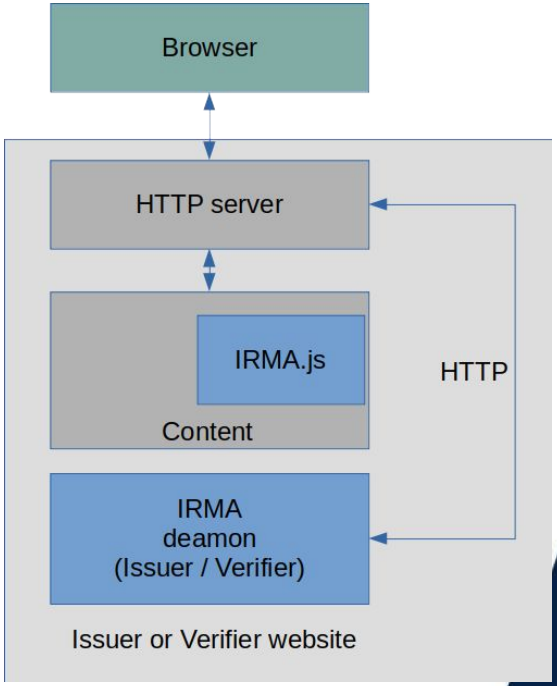
Proof of concept implementation: IRMA

- 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.
- Key material for production scheme baked into wallet app

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

IRMA Scheme - “Metadata”

master ▾ **irma-demo-schememanager** / geant-incubator / Issues / edugain-proxy / **description.xml** Go to file ···

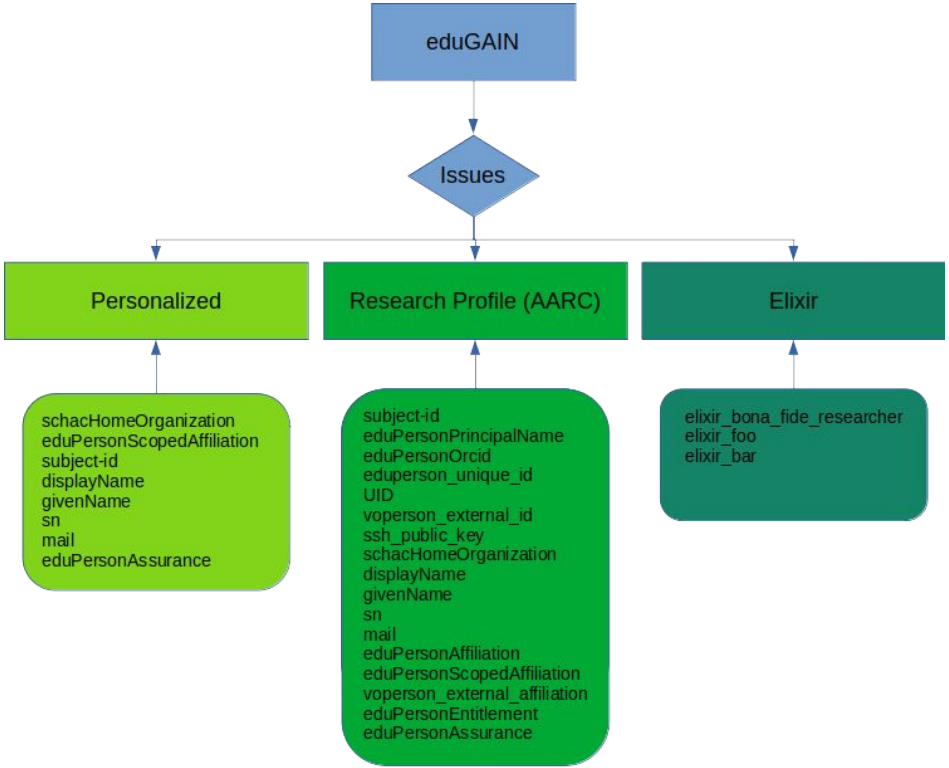
sietseringers Add empty NL translatios to new geant-incubator credential types — Latest commit 292e06b 26 days ago **History**

1 contributor

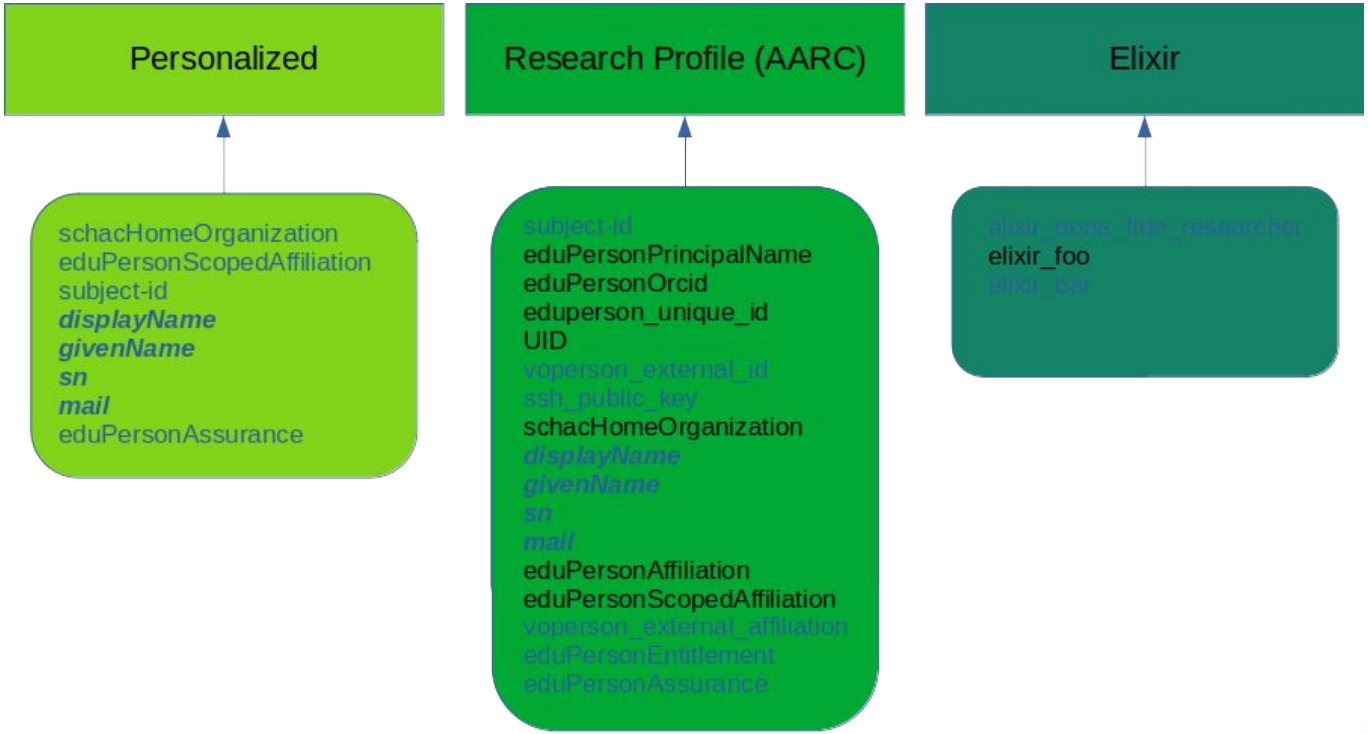
134 lines (134 sloc) | 5.51 KB — Raw | Blame

```
<IssueSpecification version="4">
    <Name>
        <en>Demo GÉANT Incubator eduGAIN proxy</en>
        <nl>Demo GÉANT Incubator eduGAIN proxy</nl>
    </Name>
    <ShortName>
        <en>edugain-proxy</en>
        <nl>edugain-proxy</nl>
    </ShortName>
    <SchemeManager>irma-demo</SchemeManager>
    <IssuerID>geant-incubator</IssuerID>
    <CredentialID>edugain-proxy</CredentialID>
    <Description>
        <en>This credential is used as part of the Distributed Identity for Research (DI4R) IRMA demo in the GÉANT Trust and Identity Incubator.\nThis credentia
        <nl>Deze credential wordt gebruikt als onderdeel van de Distributed Identity for Research (DI4R) IRMA demo, wat onderdeel is van de GÉANT Trust and Ident
    </Description>
    <ShouldBeSingleton>false</ShouldBeSingleton>
    <IssueURL>
        <en>https://privacybydesign.foundation/attribute-index/en/irma-demo.incubator.geant-incubator.edugain-proxy.html</en>
        <nl>https://privacybydesign.foundation/attribute-index/nl/irma-demo.incubator.geant-incubator.edugain-proxy.html</nl>
    </IssueURL>
    <ForegroundColor>#15222E</ForegroundColor>
    <BackgroundGradientStart>#EBEBEB</BackgroundGradientStart>
    <BackgroundGradientEnd>#FFFFFF</BackgroundGradientEnd>
    <IsInCredentialStore>false</IsInCredentialStore>
    <Category>
```

IRMA Scheme: Flexible trust root and Credential sets



Claim cherry picking



IRMA and assurance

IRMA app

- Claim TTL has to be set; cards will expire
- IRMA app protected by pin and JIT pin before release
- IRMA evaluated to be sufficient for eIDAS Substantial
- Issuers release towards user wallet on specific device
- No 2FA as there is no independence

Issuer assurance

- It is really easy to capture assurance if this is expressed in attributes (like RAF)
- We have no real way of expressing MFA (Authentication Context Class Reference)
- Cannot issue higher LOA beyond IRMA app capabilities

IRMA revocation

- Claim TTL has to be set: cards will expire
- Issuer can signal revocable claims on a per claim basis
- Issuer may revoke claim without breaking linkability
- If so indicated in scheme, verifier should check for non revocation proof

In conclusion

- IRMA does improve end user control over attributes
- Tracking behaviour is indeed impossible
- Is the app helpful or do we need to simplify GUI?
- Issuer chaining still untested
- Per claim revocability (untested)
- No fallback for mobile app at this time

- No central infrastructure collects all user data
- Not having a proxy reduces ops and legal burden
- Once claims are issued, the Issuer is no longer involved, this improves scalability
- What is the legal/GDPR model, as ‘consent’ is not applicable

In conclusion -2

- Use of app adds to improved LoA
- LoA enhancing is much easier because of the mobile platform

- Service can cherry pick claims from multiple issuers
- Non-requested data is not send

- A Distributed Identity model may provide a more flexible trust ecosystem, while it can still have similar trust properties as we have with eduGAIN

- Does an app provide us with better control over our ecosystem?

GÉANT
Networks • Services • People

Thank you

Any questions?

www.geant.org

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).