Trust & Identity Incubator

Distributed Identity for Research - DI4R

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

Sept 22, 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

Attribute flow in Distributed Identity

Source: https://privacybydesign.foundati翁/irma-explanation/#architecture
Why investigate Distributed Identity?

- Buzzword compliance?
- 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.
Step 1: Establishing Identity
Step 2: Collect Research Community data
Step 3: Enhance profile
Step 4: Provide profile information
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 issuer and verifier
IRMA security and trust

- Implements *idemix*[^1] to provide anonymity and unlinkability.
- **Issuer**s 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 **Issuer**, their **key material** and the **credentials** that may be used.
- Schemes are hosted by a **trusted third party**, currently PBDF.

Demo

Your data securely on your mobile

IRMA cards

Login with IRMA

Some service requested authentication. To authenticate, follow the instructions on your IRMA app.

Get IRMA attributes

Copyright © 2007-2021 UNINETT AS

SHOWING ATTRIBUTE(S)

A website requests that you disclose some IRMA attributes. Please scan the QR code with your IRMA app.

CANCEL
Work done

- Implement and improve IRMA issuer in SimpleSAMLphp
- Test verification of claims from multiple schemes
- Explore the best way to describe the scheme
- Discuss IRMA ‘metadata’ distribution risks
- Investigate assurance
  - Device assurance
  - Expressing assurance form source
- Investigate revocation
- Multi valued attributes
IRMA Scheme - “Metadata”

```
<specification version="4">
  <name>
    <entity>GEANT Incubator edUGAIN proxy</entity>
    <input>GEANT Incubator edUGAIN proxy</input>
  </name>
  <shortname>
    <entity>edUGAIN-proxy</entity>
    <input>edUGAIN-proxy</input>
  </shortname>
  <schemeManager>irma-demo</schemeManager>
  <IssuerID>geant-incubator</IssuerID>
  <CredentialID>edUGAIN-proxy</CredentialID>
  <description>
    This credential is used as part of the Distributed Identity for Research (DIR) IRMA demo in the GEANT Trust and Identity Incubator. This credential is used in the EDGSIR demo, which is part of the GEANT Trust and Identity Incubator.
  </description>
</specification>
```
IRMA Scheme: eduGAIN Proxy

Personalised EC

```xml
<Application id="schacHomeOrganization" optional="true">
<Application id="eduPersonScopedAffiliation" optional="true">
<Application id="subject-id" optional="true">
<Application id="displayName" optional="true">
<Application id="givenName" optional="true">
<Application id="sn" optional="true">
<Application id="mail" optional="true">
<Application id="eduPersonAssurance" optional="true">
```
IRMA Scheme: Research AAI

ATTRIBUTE DEFINITIONS:

ATTRIBUTE ID: subject-id
Optional: true

ATTRIBUTE ID: eduPersonPrincipalName
Optional: true

ATTRIBUTE ID: eduPersonOrcid
Optional: true

ATTRIBUTE ID: eduperson_unique_id
Optional: true

ATTRIBUTE ID: UID
Optional: true

ATTRIBUTE ID: voperson_external_id
Optional: true

ATTRIBUTE ID: ssh_public_key
Optional: true

ATTRIBUTE ID: schacHomeOrganization
Optional: true

ATTRIBUTE ID: displayName
Optional: true

ATTRIBUTE ID: givenName
Optional: true

ATTRIBUTE ID: sn
Optional: true

ATTRIBUTE ID: mail
Optional: true

ATTRIBUTE ID: eduPersonAffiliation
Optional: true

ATTRIBUTE ID: eduPersonScopedAffiliation
Optional: true

ATTRIBUTE ID: voperson_external_affiliation
Optional: true

ATTRIBUTE ID: eduPersonEntitlement
Optional: true

ATTRIBUTE ID: eduPersonAssurance
Optional: true
IRMA Scheme: Flexible trust root

- **eduGAIN**
  - **Issues**
    - **Personalized**
      - `schaHomeOrganization`
      - `eduPersonScopedAffiliation`
      - `subjectId`
      - `displayName`
      - `givenName`
      - `sn`
      - `mail`
      - `eduPersonAssurance`
    - **Research Profile (AARC)**
      - `subjectId`
      - `eduPersonPrincipalName`
      - `eduPersonOid`
      - `eduPerson_unique_id`
      - `UID`
      - `vperson_external_id`
      - `ssh_public_key`
      - `schaHomeOrganization`
      - `displayName`
      - `givenName`
      - `sn`
      - `mail`
      - `eduPersonAffiliation`
      - `eduPersonScopedAffiliation`
      - `vperson_external_affiliation`
      - `eduPersonEntitlement`
      - `eduPersonAssurance`
    - **Elixir**
      - `elixir_bona_fide_researcher`
      - `elixir_too`
      - `elixir_bar`
Claim cherry picking

Personalized

- schacHomeOrganization
- eduPersonScopedAffiliation
- subject-id
- displayName
- givenName
- sn
- mail
- eduPersonAssurance

Research Profile (AARC)

- Subject-id
- eduPersonPrincipalName
- eduPersonOrcid
- eduperson_unique_id
- UID
- voperson_external_id
- ssh_public_key
- schacHomeOrganization
- displayName
- givenName
- sn
- mail
- eduPersonAffiliation
- eduPersonScopedAffiliation
- voperson_external_affiliation
- eduPersonEntitlement
- eduPersonAssurance

Elixir

- elixir_node_fido_researcher
- elixir_foo
- elixir_bar
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. Issue may revoke claim without breaking linkability
- If so indicated in scheme, verifier will check for revocation
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 administrative 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; unused data is not send

- A Distributed Identity model may provide a more flexible 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?
Thank you

Any questions?

www.geant.org