

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



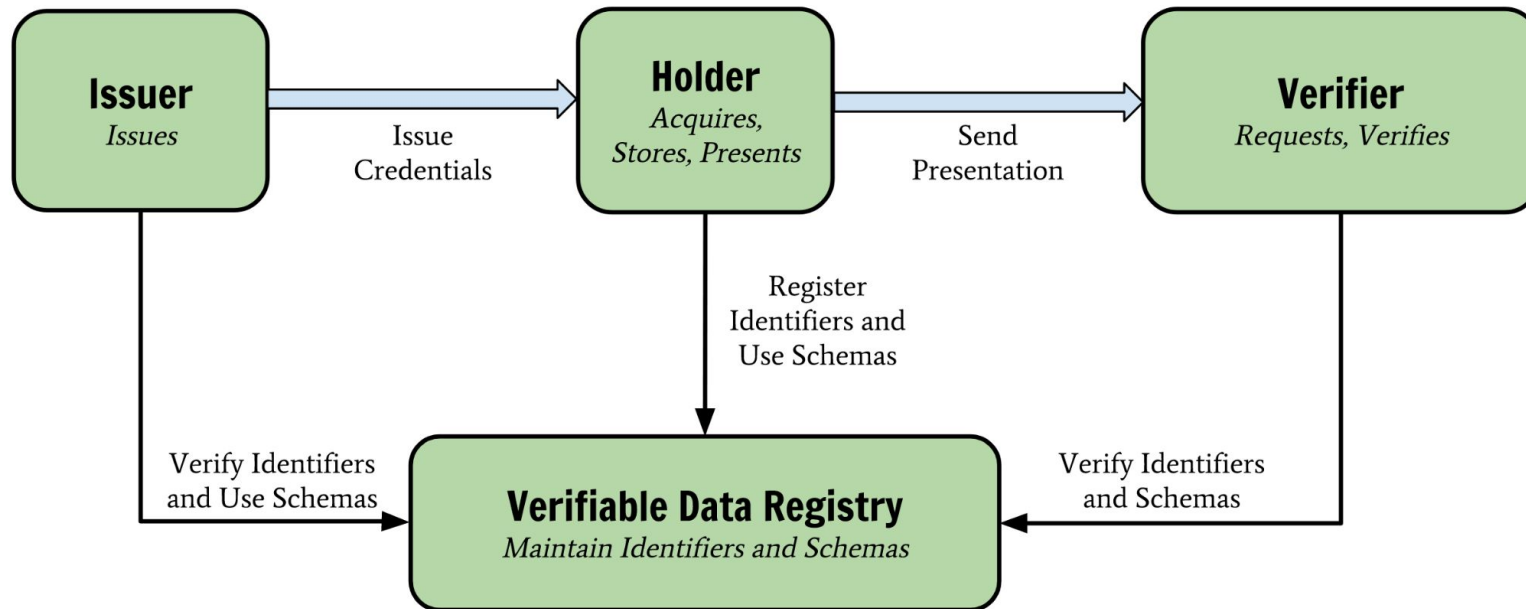


Introduction

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

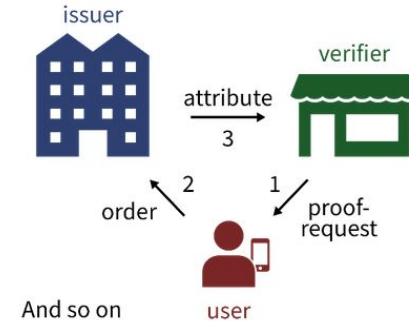
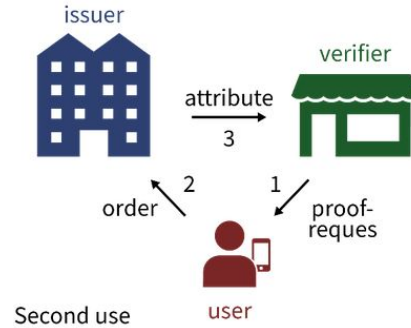
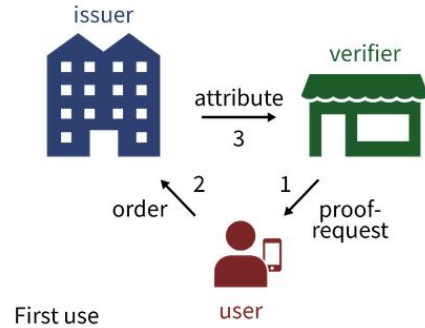


Source: W3C Verifiable Credentials Data Model, <https://www.w3.org/TR/vc-data-model/>

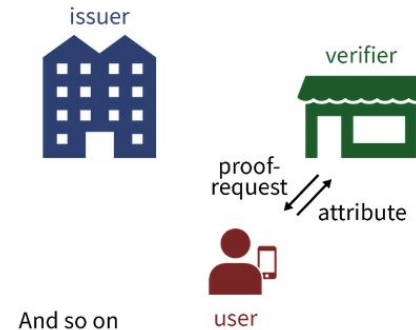
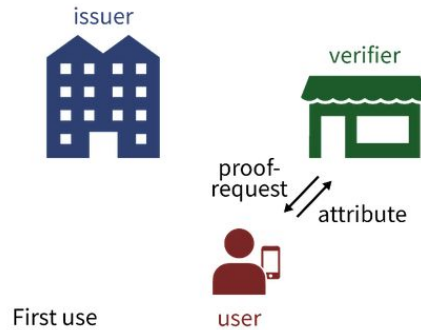
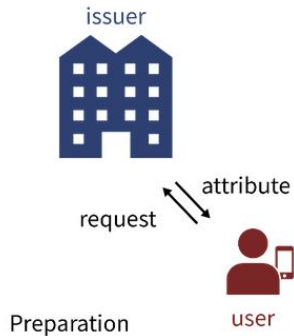


Attribute flow in Distributed Identity

Federation



Distributed Identity

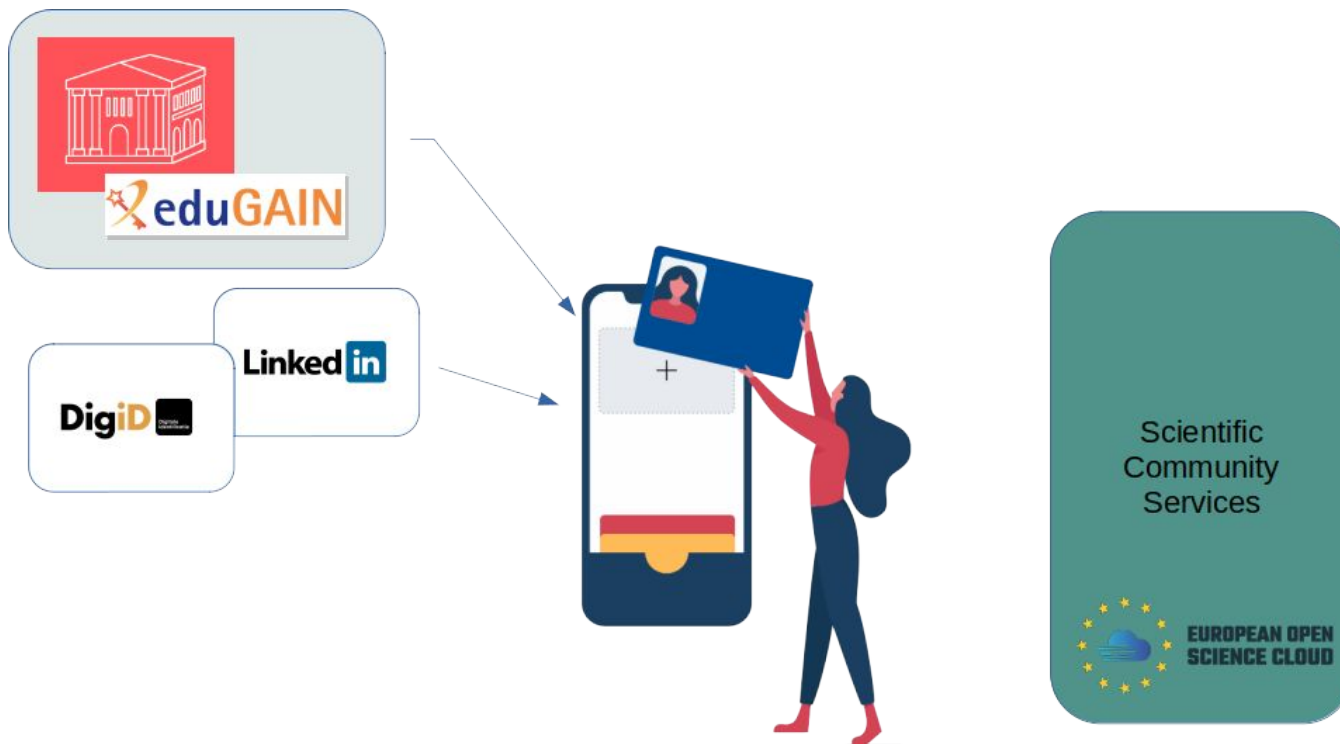




Why investigate Distributed Identity?

- 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

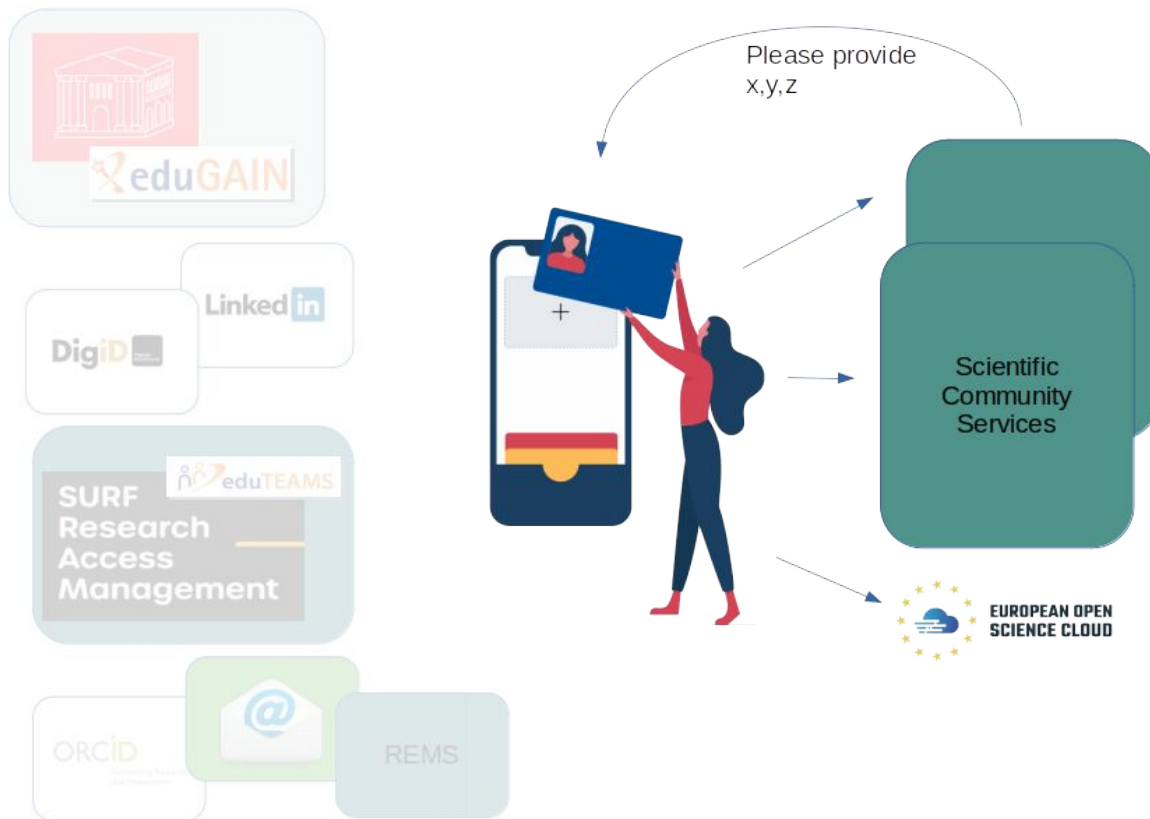


Step 3: Enhance profile





Step 4: Provide profile information





Proof of concept implementation: IRMA

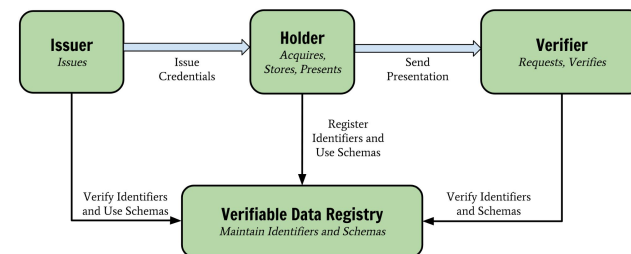
- IRMA, “I Reveal My Attributes” is a system for attribute-based authentication: it is not about who you are, but what you are.
- Developed by the Privacy by Design Foundation (PBDF), being actively tested by many organisations, including SURF, commercial entities and various branches of the Dutch government.

IRMA implementation



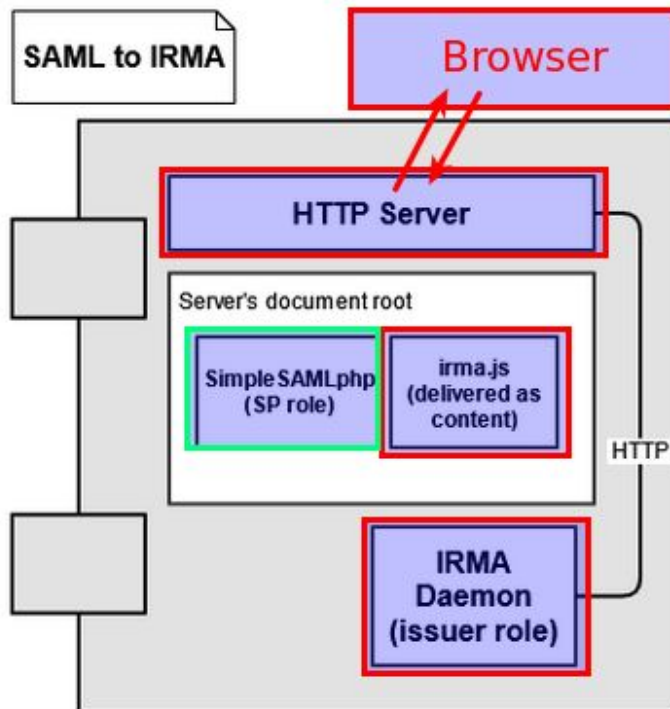
Implements all elements Verifiable Credentials model:

- **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.
- **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.



Demo

The image shows a split-screen demonstration of the IRMA system. On the left is a mobile app interface titled "IRMA cards" with the slogan "Your data securely on your mobile". It features a list of demo services: SURF Research Access Management, Personal data, Email address (highlighted in green), Home address, GÉANT Incubator eduGAIN proxy, and LinkedIn. On the right is a web browser interface for "Login with IRMA". It displays a message: "Some service requested authentication. To authenticate, follow the instructions on your IRMA app." Below this is a "SHOWING ATTRIBUTE(S)" dialog box with the IRMA logo and a QR code. The dialog text reads: "A website requests that you disclose some IRMA attributes. Please scan the QR code with your IRMA app." A "CANCEL" button is visible at the bottom right of the dialog.




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"

master | [irma-demo-schememanager](#) / [geant-incubator](#) / [Issues](#) / [edugain-proxy](#) / [description.xml](#) Go to file ...

 **sietseringers** Add empty NL translation to new geant-incubator credential types Latest commit 292e96b 26 days ago [History](#)

1 contributor

134 lines (134 sloc) | 5.51 KB Raw Blame ✎ 🗑️

```

1 <IssueSpecification version="4">
2   <Name>
3     <en>Demo GÉANT Incubator eduGAIN proxy</en>
4     <n1>Demo GÉANT Incubator eduGAIN proxy</n1>
5   </Name>
6   <ShortName>
7     <en>edugain-proxy</en>
8     <n1>edugain-proxy</n1>
9   </ShortName>
10  <SchemeManager>irma-demo</SchemeManager>
11  <IssuerID>geant-incubator</IssuerID>
12  <CredentialID>edugain-proxy</CredentialID>
13  <Description>
14    <en>This credential is used as part of the Distributed Identity for Research (DI4R) IRMA demo in the GÉANT Trust and Identity Incubator.\nThis credential
15    <n1>Deze credential wordt gebruikt als onderdeel van de Distributed Identity for Research (DI4R) IRMA demo, wat onderdeel is van de GÉANT Trust and Ident
16  </Description>
17  <ShouldBeSingleton>false</ShouldBeSingleton>
18  <IssueURL>
19    <en>https://privacybydesign.foundation/attribute-index/en/irma-demo.incubator.geant-incubator.edugain-proxy.html</en>
20    <n1>https://privacybydesign.foundation/attribute-index/nl/irma-demo.incubator.geant-incubator.edugain-proxy.html</n1>
21  </IssueURL>
22  <ForegroundColor>#15222E</ForegroundColor>
23  <BackgroundGradientStart>#EBEBEB</BackgroundGradientStart>
24  <BackgroundGradientEnd>#FFFFFF</BackgroundGradientEnd>
25  <IsInCredentialStore>false</IsInCredentialStore>
26  <Category>

```



IRMA Scheme: eduGAIN Proxy

Personalised EC

```
<Attribute id="schacHomeOrganization" optional="true">  
<Attribute id="eduPersonScopedAffiliation" optional="true">  
<Attribute id="subject-id" optional="true">  
<Attribute id="displayName" optional="true">  
<Attribute id="givenName" optional="true">  
<Attribute id="sn" optional="true">  
<Attribute id="mail" optional="true">  
<Attribute id="eduPersonAssurance" optional="true">
```

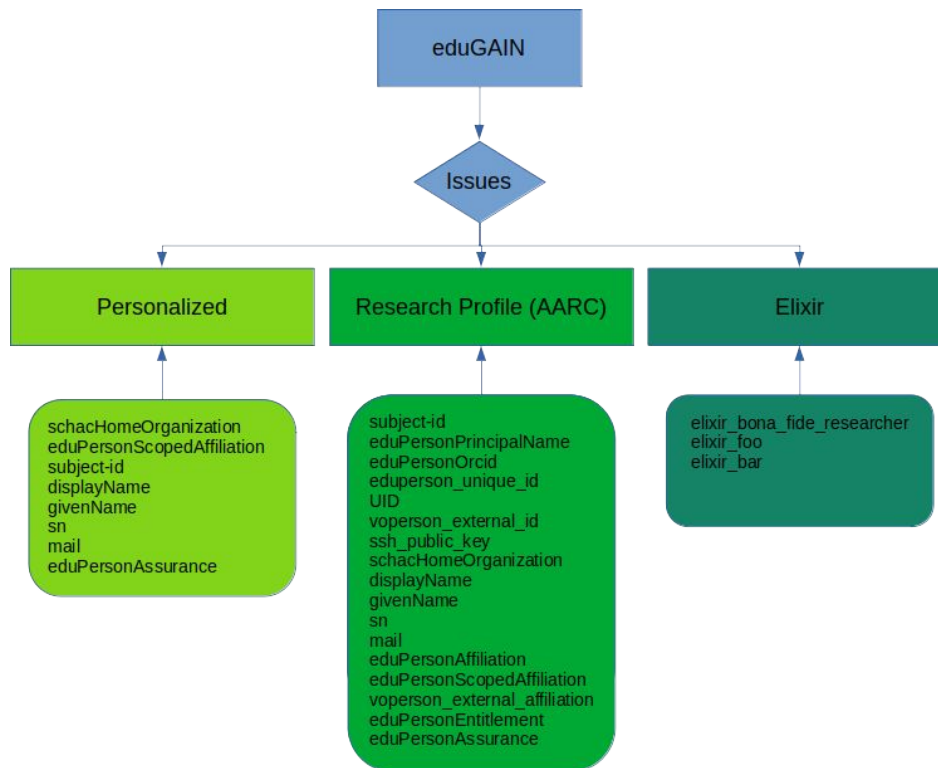


IRMA Scheme: Research AAI

```
<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">
```

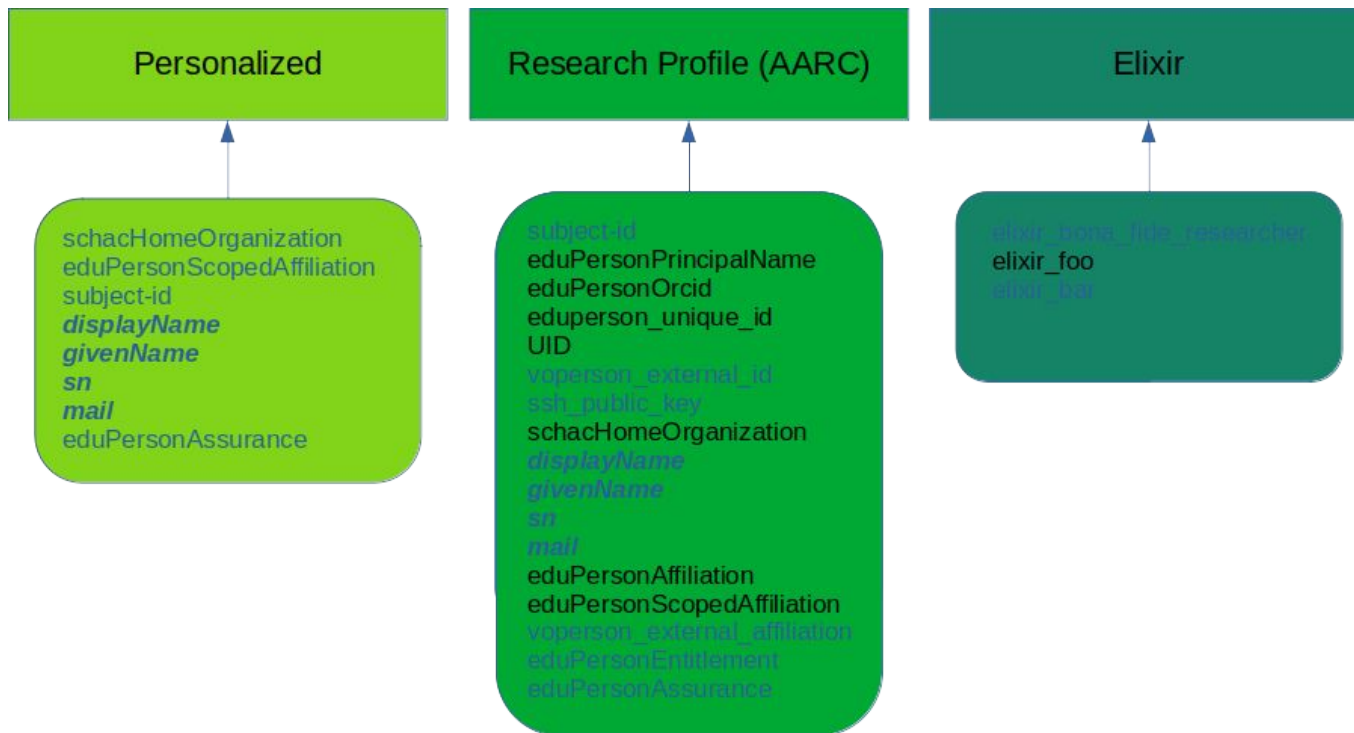


IRMA Scheme: Flexible trust root





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
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
- Offline usage
- 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

