Trust & Identity: What’s next ?!

GN4-2 Project - Next Generation Trust & Identity Technology Development

Maarten Kremers

Task Leader Trust & Identity Technology Development, GN4 Project
Technical Product Manager & Project manager T&I, SURFnet

Internet2 TechEx 2017, San Francisco, CA
16th October 2017
The GN4-2 Project and T&I

Trust & Identity Operations

- eduGAIN
- eduPKI
- eduroam

Trust & Identity Development

- eduGAIN Development – Federation and Campus
- eduGAIN Development – e-Research and Service Providers
- Trust & Identity Technology Development
- eduroam Service Development
GN4-2 - Trust & Identity Technology Development

- OpenID Connect Federations
- eduKEEP – Towards a User Driven Identity Federation
- REFEDS Authentication profiles & Step-Up Service
- eIDAS & eduGAIN
eduKEEP – The Challenge

Overcome the organisation-centric identity model shortcomings

- Identities are tightly coupled with role and affiliation
- Poor support for dynamic and loose relationships
- Identities bootstrapping
- Multiple concurrent affiliations
eduKEEP – The Approach

User-driven, persistent, privacy preserving, institutional backed identity (UPPII)

The user identity is created *outside* the organisation

The organisation *validates* the user identity

The organisation *link* the user identity to role and affiliation

and / or

The organisation *bootstrap* a local user account leveraging the external identity
eduKEEP – The Possibilities

Registration / Alumni / lifelong learners

One identity to rule them all
To register, join another university, become an alumni

Researchers

One identity in concurrent projects with multiple affiliations and for all publication work (with help of ORCID and friends)

Teachers

One identity for interacting with their learners across multiple universities

Third Parties Services

Supports longer-term client-relationship. Offerings and conditions can be based on roles available at given time
eduKEEP – Current eduID initiatives

- **SWITCH EduID (Switzerland)**
  - Central user-centric IdP, enriching identities with attributes from Home Organisations

- **SUNET EduID (Sweden)**
  - Central user-centric IdP to bootstrap identities at Home Organisations

- **GARR**
  - eGOV IDs, IdP/Proxy & Aas (Italy)
  - Considering to use an Idp/SP Proxy to link eGOV IDs to Home Organisations Attribute Authorities
## eduKEEP – Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>SWITCH edu-ID</th>
<th>SUNET eduid</th>
<th>GARR IdP/SP Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A - Target audience</strong></td>
<td>R&amp;E Community</td>
<td>R&amp;E Community</td>
<td>R&amp;E Community</td>
</tr>
<tr>
<td><strong>B - A new identifier is provided</strong></td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td><strong>B1 - Identity suitable for AuthN</strong></td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td><strong>B2 - Long-term identity</strong></td>
<td>YES</td>
<td>YES</td>
<td>YES *</td>
</tr>
<tr>
<td><strong>B3 - Persistent identifier</strong></td>
<td>YES</td>
<td>YES</td>
<td>YES *</td>
</tr>
<tr>
<td><strong>B4 - Globally Unique Identifier</strong></td>
<td>YES **</td>
<td>YES **</td>
<td>YES *</td>
</tr>
<tr>
<td><strong>C - IdP acting on behalf of Home Organisation IdPs</strong></td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
</tr>
</tbody>
</table>

* external dependency  
** confirmed identities
## eduKEEP – Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>SWITCH edu-ID</th>
<th>SUNET eduID</th>
<th>GARR IdP/SP Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>D- Account Linking</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>D1- Linked Account AuthN</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>E- Self asserted Identity</td>
<td>YES</td>
<td>YES</td>
<td>YES *</td>
</tr>
<tr>
<td>E1- Identity Assurance Elevation</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>E2- VO-based vetting</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>F- Attribute Aggregation at IdP</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>G- Attribute Release Policy - Delegate Management to Home Organisations</td>
<td>YES</td>
<td>NO</td>
<td>YES *</td>
</tr>
</tbody>
</table>

* external dependency
** confirmed identities
eduKEEP – Observations

Best Practices
- The incremental approach of SWITCH eduID
- The Assurance Level elevation model of SUNET eduID
- Solid policy and security

Long Lived Identities and edulDs are on the way forward
- BYOID
- 1st class citizenship
- The path to be further determined
EduKEEP – Towards a User Driven Identity Federation

October 2017: Best Current Practices Document

Architecture
Policy
Features

2018: Best Current Practices Pilot

eduID SWITCH
eduID SUNET
GARR
Develop profiles for Authentication support in REFEDS

Develop Step-up service
REFEDS Profiles for Authentication

 Authentication vector
- Base Level Authentication Profile
- Single Factor (Good Entropy) Profile
- MFA Profile

REFEDS Assurance Framework (RAF)
<table>
<thead>
<tr>
<th>Authentication Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base Level Authentication Profile</strong></td>
</tr>
<tr>
<td>• Base profile</td>
</tr>
<tr>
<td>• No explicit authentication requirements</td>
</tr>
<tr>
<td>• draft done, REFEDS consultation pending</td>
</tr>
<tr>
<td><strong>Single Factor (Good-Entropy) Profile</strong></td>
</tr>
<tr>
<td>• Requirements for single factors</td>
</tr>
<tr>
<td>• BCP for password scenarios</td>
</tr>
<tr>
<td>• In progress</td>
</tr>
<tr>
<td><strong>MFA Profile</strong></td>
</tr>
<tr>
<td>• Requirements for MFA</td>
</tr>
<tr>
<td>• Done</td>
</tr>
</tbody>
</table>
Primary audience: Research Collaborations

Collaboration with AARC
• Use cases
• User / community requirements
• Architecture

In progress:
• Analyzing different approaches

Both Identity and Authentication Step-UP

Potential pilots (Autumns 2018)

Next Steps
• Timeline
• Testing scalability

Deliver Step-Up Service
eIDAS

- electronic IDentification, Authentication and trust Services (Upcoming EU regulation)
- Leverage the use of eGOV IDs for higher LoA in the R&E federations
- Technical interoperability with build proxy, technical pilots done
- Interoperability comparison between the frameworks
eIDAS & eduGAIN SG adopted the ‘global’ approach. This approach will be taken as baseline in conversations with the eIDAS representatives.

National gateway per national R&E federation and the national node.

Service with a global scope that acts as a gateway the eduGAIN inter-federation and eduGAIN.
https://wiki.geant.org/display/gn42jra3/Task+3%3A+Next+Generation+Trust+and+Identity+Technology+Development+-+TrustTech
Thank you

maarten.kremers@surfnet.nl