Next-Generation Identity Federations

Andreas Åkre Solberg

GÉANT
Identity Federations
GÉANT3 JRA3 Task 2

Solving current challenges,
and exploring next generation
Identity Management Systems.
# Identity Federations

## Participants

<table>
<thead>
<tr>
<th>Norway</th>
<th>Sweden</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denmark</td>
<td>Finland</td>
</tr>
<tr>
<td>Croatia</td>
<td>Netherlands</td>
</tr>
<tr>
<td>France</td>
<td>Czech Republic</td>
</tr>
<tr>
<td>Hungary</td>
<td>Poland</td>
</tr>
<tr>
<td>Switzerland</td>
<td>Spain</td>
</tr>
</tbody>
</table>

**Total effort:**

16MY in 4 years
Today's Identity Federations

Identity Provider

Authentication and user attributes

Service Provider

Authorative user data

Access control / authorization

Web-based
**User-Centric Identity**
Next generation Identity Systems puts the end user in control. How can educational Identity Federations meet this new Identity paradigm.

**Federation Harmonization**
Best-practices within several topics in Identity Federations. Increase interoperability.

**Beyond web-authentication**
Extending WebSSO to non-web clients and 'Service to Service' communication.

**Federation Lab**
Provide a common facility for service providers and identity providers to test interoperability and conformance, and test new ideas.

**Metadata distribution**
More distributed and independent architecture for Identity Federations Metadata.

**Virtual Org**
Collaborate across services, federations and countries.
Beyond web-authentication
Extending WebSSO to non-web clients and 'Service to Service' communication.

• Moonshot
  re-using roaming access for Web

• OAuth
  re-using webSSO for non-web use-cases.
Federation Lab
Provide a common facility for service providers and identity providers to test interoperability and conformance, and test new ideas.

Automated **saml2int** Conformance test suite

- ✔ Checking structure of AuthNRequest
- ✔ Checking metadata content
- ✔ Checking Response
- ✔ Checking attribute contents
- ✔ Checking signature

No problems found
Today's Identity Federations perfectly supports authentication, but does not properly support the need for authorization and additional user data for Virtual Organizations.
Virtual Organizations

Identity Provider

Authorative user data

Authentication and user attributes

Service Provider

Additional user data

Access control / authorization

VO Platform

additional user attributes, VO information
V

irtual

Organizations

Architecture

Virtual Organizations

WebUI Management

SP-Centric Attribute Aggregation (server)

VO Storage

Information model

SAML 2.0 AttributeQ + Affiliations

SAML 2.0 AttributeQ front-channel

OAuth + AttributeQ

LDAP

Data Access API

VO Service (client)
Virtual Organizations

Two proof of concept front-ends used within year 1

- SWITCH GMT
- SimpleSAMLphp VO
Virtual Organization Platform

This VO proof of concept (PoC) platform uses the SWITCH Group Management Tool (read GMT documentation) as VO administration interface to change the group membership of users like the test user "William Tell". The membership is then reflected in the VO attribute, which in this case is namePDP.PersonEntitlement. This attribute is available if the user accesses a VO service like VO Service Example choosing the "AAI Test Service" as his Home Organisation on the WAYF and authenticates with "w.tell" and "demo" as login name and password.

List of usernames and passwords you could use:

- vadmin/demo (AAI Test Home Organisation), "Hugo Boss"
- w.tell/demo (AAI Test Home Organisation), "William Tell"
- demouser/demo (AAI Demo Organisation), "Demouser SWITCHai"
- demouser2/demo (AAI Demo Home Organisation), "Demouser2 SWITCHai"

Members of Group: SwissResistance

<table>
<thead>
<tr>
<th>Name</th>
<th>Surname</th>
<th>Role</th>
<th>Action</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tester</td>
<td>Kersting</td>
<td>Group Administrator</td>
<td>Change</td>
<td>Remove</td>
</tr>
<tr>
<td>Demouser</td>
<td>SWITCHai</td>
<td>Group Administrator</td>
<td>Change</td>
<td>Remove</td>
</tr>
<tr>
<td>Hugo</td>
<td>Boss</td>
<td>Group Administrator</td>
<td>Change</td>
<td>Remove</td>
</tr>
<tr>
<td>Lukas</td>
<td>Hämmerle</td>
<td>Group Administrator</td>
<td>Change</td>
<td>Remove</td>
</tr>
<tr>
<td>William</td>
<td>Tell</td>
<td>Group Administrator</td>
<td>Change</td>
<td>Remove</td>
</tr>
<tr>
<td>Demouser2</td>
<td>SWITCHai</td>
<td>Member</td>
<td>Change</td>
<td>Remove</td>
</tr>
</tbody>
</table>

© 2010 SWITCH GMT V1.3

Logged in as: Hugo Boss (Global Administrator role class)
Virtual Organization Platform

This VO proof of concept (PoC) platform uses the SWITCH Group Management Tool (read GMT documentation) as VO administration interface can change the group membership of users like the test user "William Tell". The membership is then reflected in the VO attribute, which in the eduPersonEntitlement attribute. This attribute is available if the user accesses a VO service like VO Service Example choosing the "AAI Test § 1.3)" as his Home Organisation on the WAYF and authenticates with "w.tell" and "demo" as login name and password.

List of usernames and passwords you could use:

- voadmin/demo (AAI Test Home Organisation), "Hugo Boss"
- w.tell/demo (AAI Test Home Organisation), "William Tell"
- demouser/demo (AAI Demo Organisation), "Demouser SWITCHaii"
- demouser2/demo (AAI Demo Home Organisation), "Demouser2 SWITCHaii"

### Administration Interface

<table>
<thead>
<tr>
<th>Group</th>
<th>Members</th>
<th>Authorization Files</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BaselRapperswil</td>
<td>0</td>
<td>Add</td>
<td>Manage</td>
</tr>
<tr>
<td>DieEidgenossen</td>
<td>2</td>
<td>Add</td>
<td>Manage</td>
</tr>
<tr>
<td>FreeSwitzerland</td>
<td>4</td>
<td>Add</td>
<td>Manage</td>
</tr>
<tr>
<td>SwedishSwissAlliance</td>
<td>3</td>
<td>Add</td>
<td>Manage</td>
</tr>
<tr>
<td>SwissResistance</td>
<td>6</td>
<td>Add</td>
<td>Manage</td>
</tr>
<tr>
<td>Registered Users</td>
<td>8</td>
<td>Add</td>
<td>Manage</td>
</tr>
<tr>
<td>Pending User Requests</td>
<td>1</td>
<td>-</td>
<td>Manage</td>
</tr>
<tr>
<td>Pending Invitation Tokens</td>
<td>3</td>
<td>-</td>
<td>Manage</td>
</tr>
</tbody>
</table>

© 2010 SWITCH GMT V1.3

Logged in as: Hugo Boss (Global Administrator role class)
Virtual Organizations
Proof of concept
User Interface

Anyone can create a new Virtual Organization. Login and fill out the form above.
Registering new members of a Virtual Organization

Virtual Organization: European Research Project

Identifier: geant
Name: European Research Project
Description: Participants from 16 different countries accessing multiple web services. This Virtual Organization simplifies access control.

Registering new members
Give the following secret URL to potential members of this organization, and they will be automatically signed up. Later you can edit their attributes.

https://vo rnd feide no simplesaml /module.php/virtualorg/register.php?id=geant&token=482a0381c83f97822f9b9b7249;

Members

<table>
<thead>
<tr>
<th>User ID</th>
<th>Name</th>
<th>E-mail</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No organisations registered
Managing attributes for a user.
By a VO manager.
Combination of managed and pre-populated attributes.
Use-cases to be solved in 2010

- CLARIN
- TERENA Wiki-s (REFEDS)
- ...

GÉANT
Virtual Organizations

SP-Centric Attribute Aggregation (server)

Alternative data access APIs
- SAML 2.0 AttributeQ + Affiliations
- SAML 2.0 AttributeQ front-channel
- OAuth + AttributeQ
- LDAP

Data Access API

VO Service (client)

SP-Centric Attribute Aggregation
Solution to a generic problem. Re-use in multiple use-cases.
How can multiple Service Providers exchange information about a user in a privacy enhancing way?
Identity Federations
GÉANT3 JRA3 Task 2

Solving current challenges, and exploring next generation Identity Management Systems.

Andreas Åkre Solberg
http://rnd.feide.no