

SAML 2 VO Platform



SWITCH

Serving Swiss Universities

Thomas Lenggenhager

Lukas Hämmerle

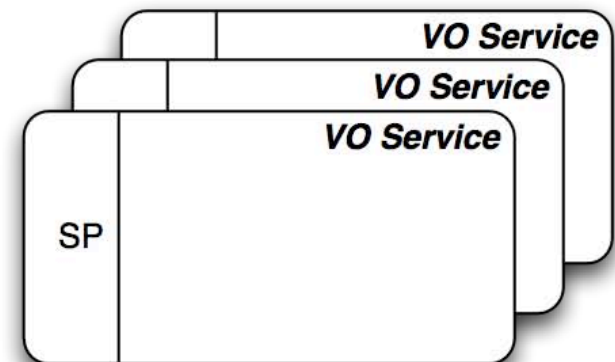
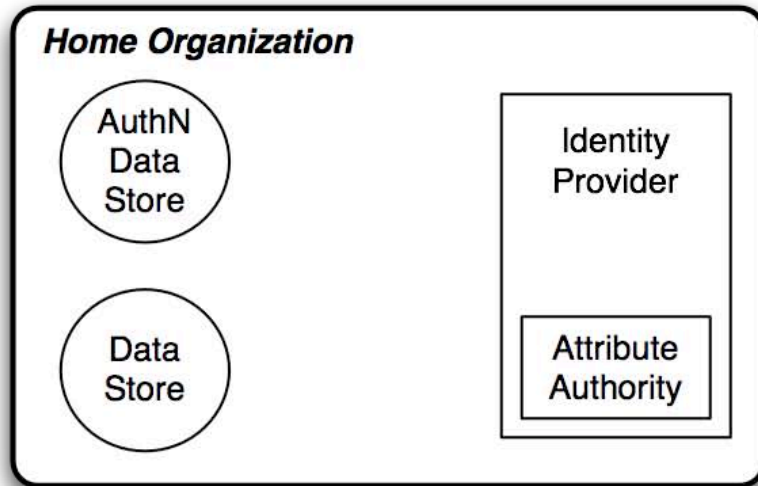
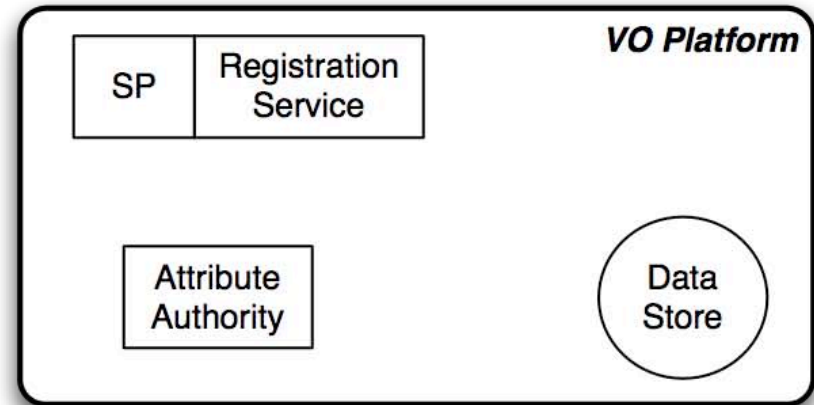
aai@switch.ch

Vienna, 8. September 2009

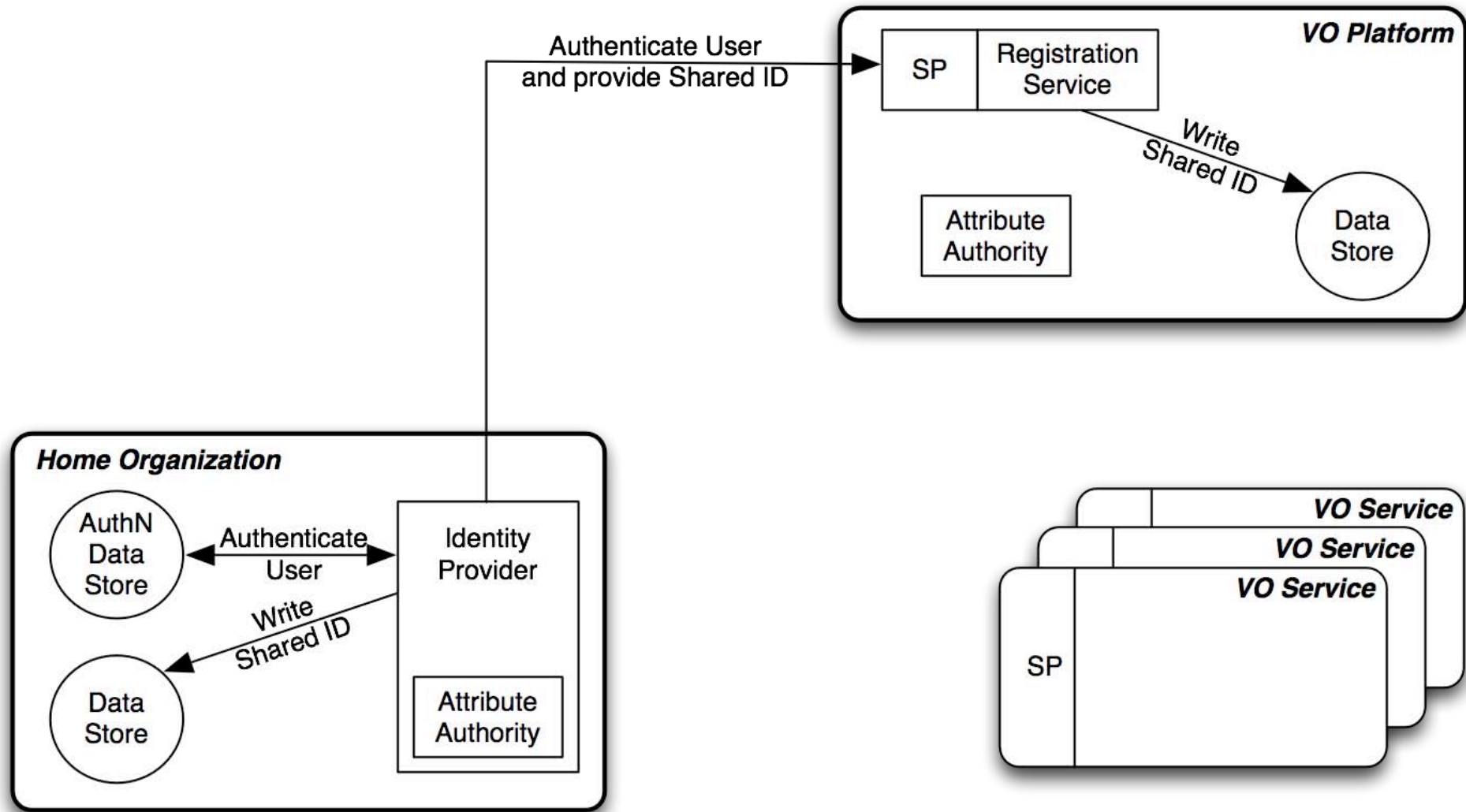
The Idea

- SP aggregates attributes
 - from users Home Institution, and
 - from VO Platform(s)
- Use standard SAML 2 back-channel attribute queries to SAML 2 Attribute Authorities

The Components



User registers on the VO Platform

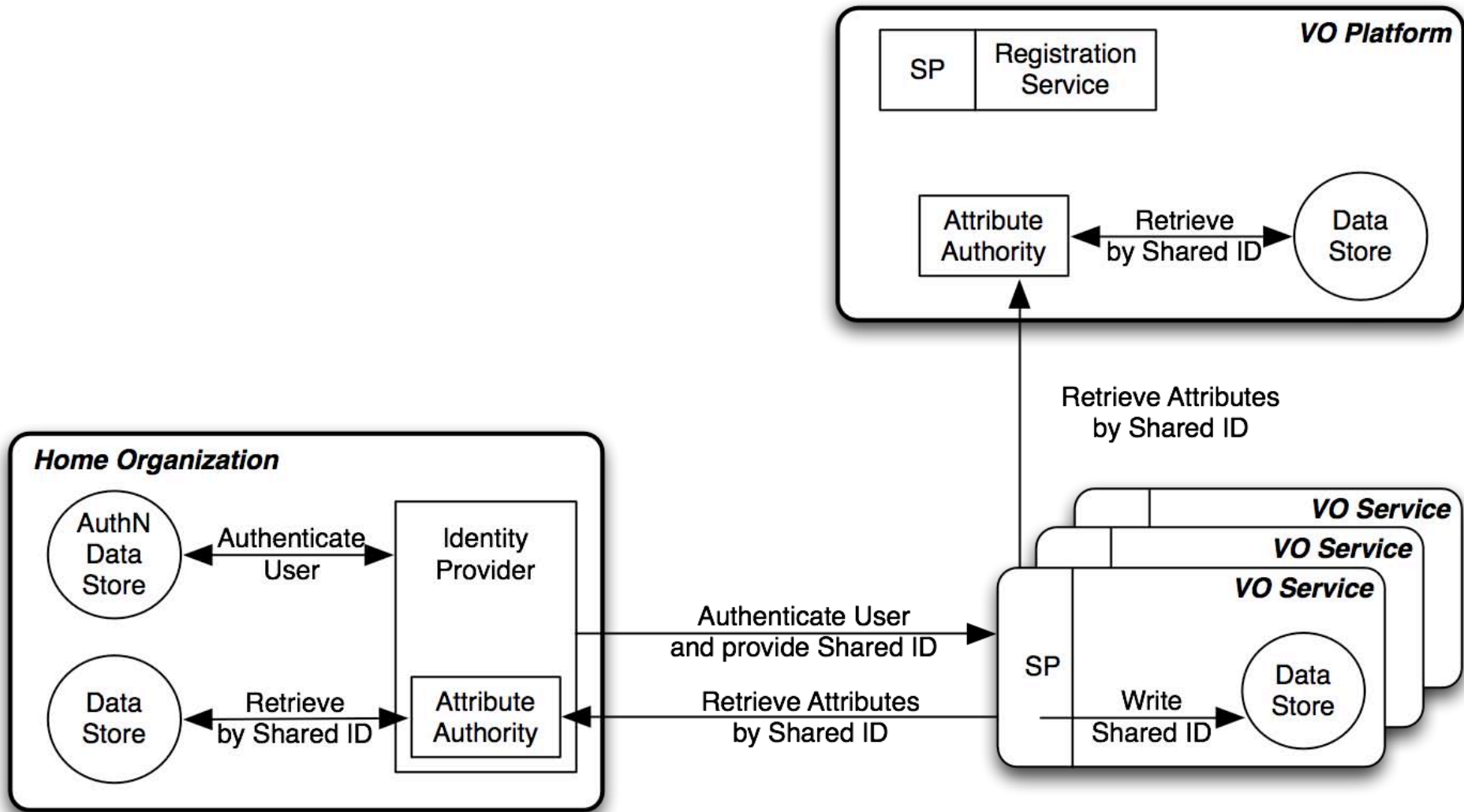


Shared ID

- Attribute known by Home IdP, VO Services SP and VO Platform
- Used as SAML 2 Persistent NameIdentifier for attribute request
- Could be a common identifier like eduPersonPrincipalName
 - Rather unlikely for generic VOs
 - Problematic if IDs are already widely known
- Could also be a value of the form eduPersonTargetedID that is generated by the IdP for an SP or group of VO SPs with:

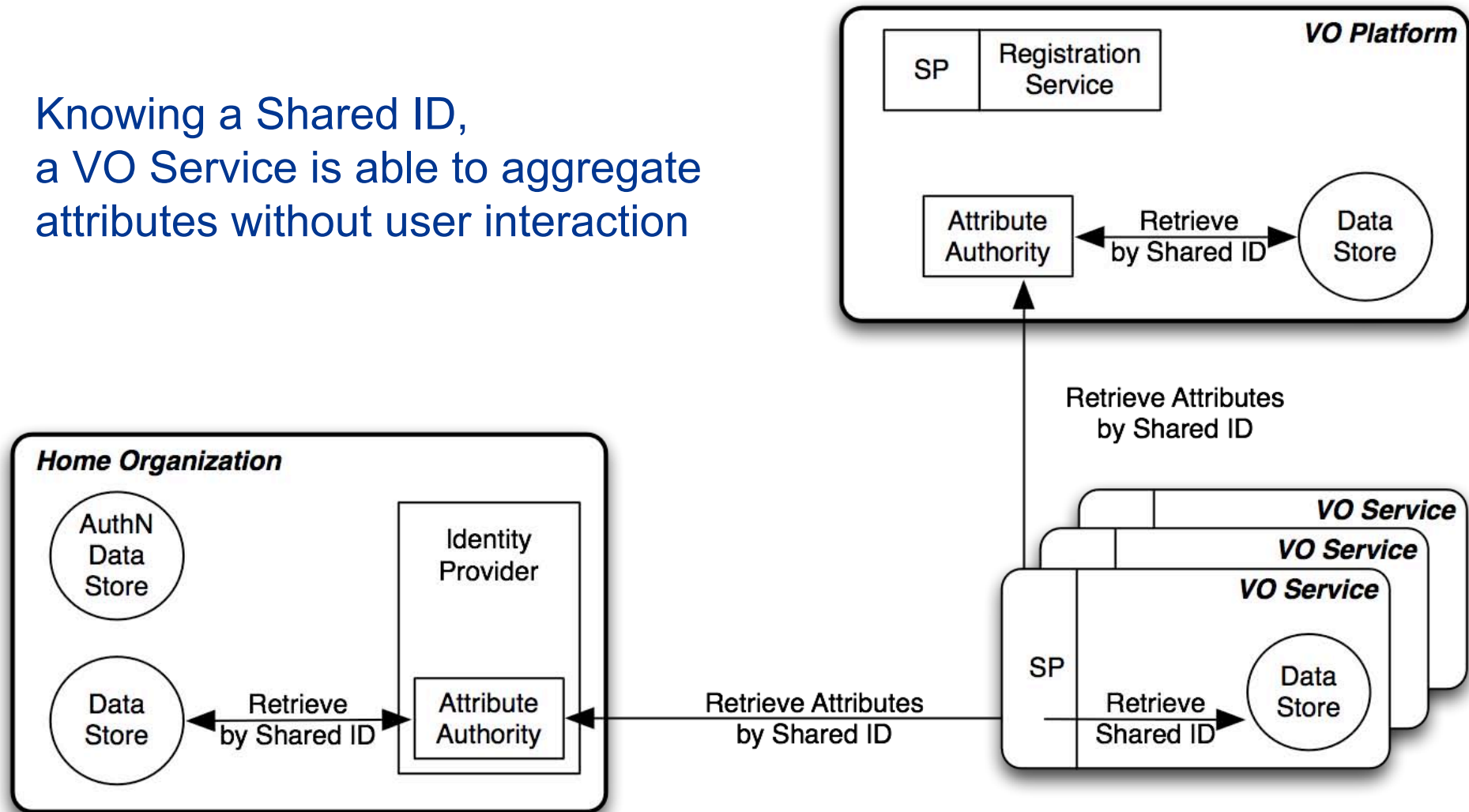
```
<EntityDescriptor entityID="http://vo.example.org/biomed">  
  <AffiliationDescriptor affiliationOwnerID="http://vo.example.org/vo">  
    <AffiliateMember>http://vo.example.org/vo</AffiliateMember>  
    <AffiliateMember>http://vo1.example1.org/sp1</AffiliateMember>  
    <AffiliateMember>http://vo1.example2.org/sp2</AffiliateMember>  
  </AffiliationDescriptor>  
</EntityDescriptor>
```

User connects to a VO Service



VO Service aggregates attributes

Knowing a Shared ID,
a VO Service is able to aggregate
attributes without user interaction



Authentication Request of an SP in a VO

If an SP acts as member of a group of VO Services,
it uses the common VO Services entityID
as SPNameQualifier in the authentication request

```
<AuthnRequest ID="12345" Version="2.0"  
  IssueInstant="2009-01-01T12:00:00Z">  
  <NameIDPolicy  
    SPNameQualifier="http://vo.example.org/biomed"/>  
</AuthnRequest>
```

Shibboleth SP with two static VO Platforms

- Two (VO) IdPs are queried in addition using eduPersonTargetedID as NameIdentifier

Shibboleth2.xml:

```
<AttributeResolver type="Chaining">
  <!-- Use a standard SAML query if no attributes
        are supplied during SSO. -->
  <AttributeResolver type="Query"/>

  <!-- Uses eduPersonTargetedID
        from IdP to query as NameID -->
  <AttributeResolver
    type="SimpleAggregation"
    attributeId="eduPersonTargetedID"
    format="urn:mace:dir:attribute-def:eduPersonTargetedID">
    <Entity>https://vo-idp.switch.ch/idp/shibboleth</Entity>
    <Entity>https://other-vo-idp.switch.ch/idp/shibboleth</Entity>
  </AttributeResolver>
</AttributeResolver>
```

<https://spaces.internet2.edu/display/SHIB2/NativeSPAttributeResolver>

Shibboleth SP with dynamic VO Platform(s)

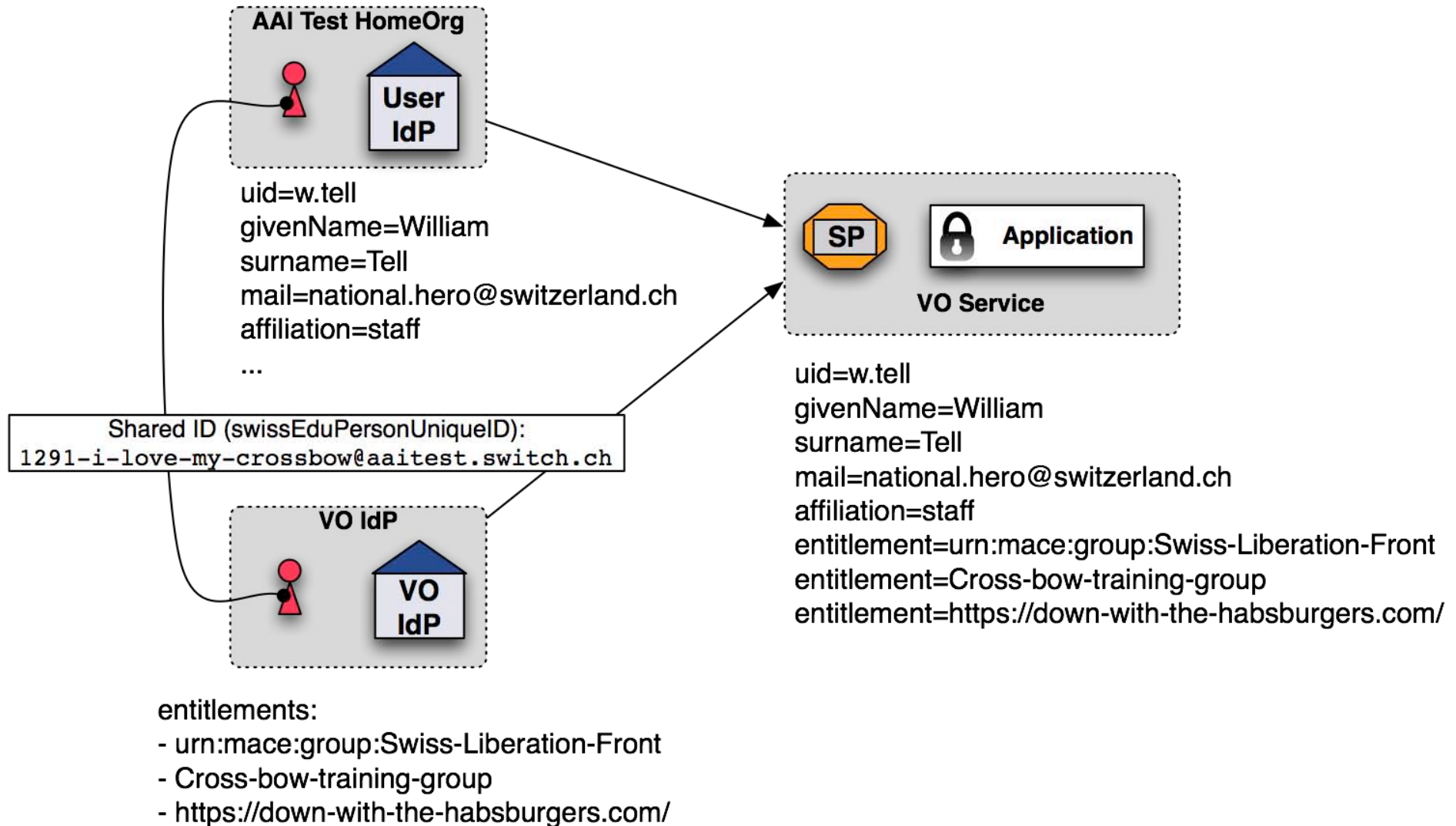
- Besides the static (VO) IdP the entitlement attribute is checked for entityIDs to query

Shibboleth2.xml:

```
<AttributeResolver type="Chaining">
  <!-- Use a standard SAML query if no attributes
        are supplied during SSO. -->
  <AttributeResolver type="Query"/>

  <!-- Uses eduPersonTargetedID
        from IdP to query as NameID -->
  <AttributeResolver
    type="SimpleAggregation"
    attributeId="eduPersonTargetedID"
    format="urn:mace:dir:attribute-def:eduPersonTargetedID">
    <EntityReference>Shib-EP-Entitlement</EntityReference>
    <Entity>https://vo-idp.switch.ch/idp/shibboleth</Entity>
  </AttributeResolver>
</AttributeResolver>
```

Demo Overview



Demo instructions

Demo uses the swissEduPersonUnique ID as shared ID:

- Access <https://dieng.switch.ch/vo-enabled/?simple>
- Use “AAI Test Home Organisation (Shibboleth 1.3)” as IdP
- Authenticate with “w.tell”/”demo” as username/password
- Entitlement attribute comes from VO IdP,
the other attributes from above selected user IdP
- Click on “Show Shibboleth assertions”

Advantages

- No additional protocols, pure SAML2
- VO Service application needs no modification
- Simple configuration on SP side (see previous slides)
- SP gets access to VO attributes the same way as any other IdP attribute
- Attribute requests to multiple VO platforms can be configured statically or dynamically

Disadvantages

- **SP in VO Services must know shared ID**
 - Is this a problem if the eduPersonTargetedID is the same for all SPs of the same group of VO Services?

Requirements for this approach

- **Shibboleth SP 2.2**
 - Already available, implements simple attribute aggregation
- **Shibboleth IdP 2.2 + AffiliationDescriptor extension**
 - Expected in early 2010
- **Registration Service on the VO Platform**
 - Needs to be implemented
 - Partly VO specific (e.g. processes)

<https://spaces.internet2.edu/display/~lajoie@idp.protectnetwork.org/VOPlatform>

<http://wiki.geant.net/bin/view/JRA3/VirtualOrganizations>

Simple Proof-of-Concept using GMT

- Soon finished...
- Idea is to use the Group Management Tool as VO Management interface
- GMT stores data in MySQL database so that group information can be read by Shibboleth IdP
- Names of groups a user is member of will be values for the entitlement attribute

