(Improved) UIs for Discovery Service

and Identity Providers using extended metadata

SWITCH
Serving Swiss Universities

Lukas Hämmerle
lukas.haemmerle@switch.ch

Vienna, 17. February 2010

Disclaimer

- All of the following slides describe work in progress!
- Details could and will change!
- Don’t rely on details (yet)!

Concepts, graphics and ideas by:

- Chad La Joie (ITUMI, Internet2)
- Rod Widdowson (Steading System Software, Internet2)
- Lukas Hämmerle (SWITCH)

The Problem

- User interfaces in federated applications have a great potential for improvements (see JISC Interface Study*)

- Especially IdP Discovery could benefit from improvements

- Users are not displayed enough information
  - before Identity Provider discovery choice
  - before authentication
  - before attribute consent decision

* http://sites.google.com/site/publisherinterfacestudy/

The Consequences

- Metadata should contain more information to facilitate discovery and allow users to make informed decisions

- New user interface concept for Discovery Service and on Identity Provider is required!

The Solution

- **IdP Discovery and Login UI Entity Attributes Profile**
  "Defines a set of entity attributes for use with IdP discovery and user authentication interfaces" (Draft version!)
  https://spaces.internet2.edu/display/~lajoie@idp.protectnetwork.org/Home (Discovery Attributes ODT)

- **New Interface Concepts for DS, IdP and uApprove**
  Concept created by Chad La Joie
  https://spaces.internet2.edu/display/~lajoie@idp.protectnetwork.org/DSUI

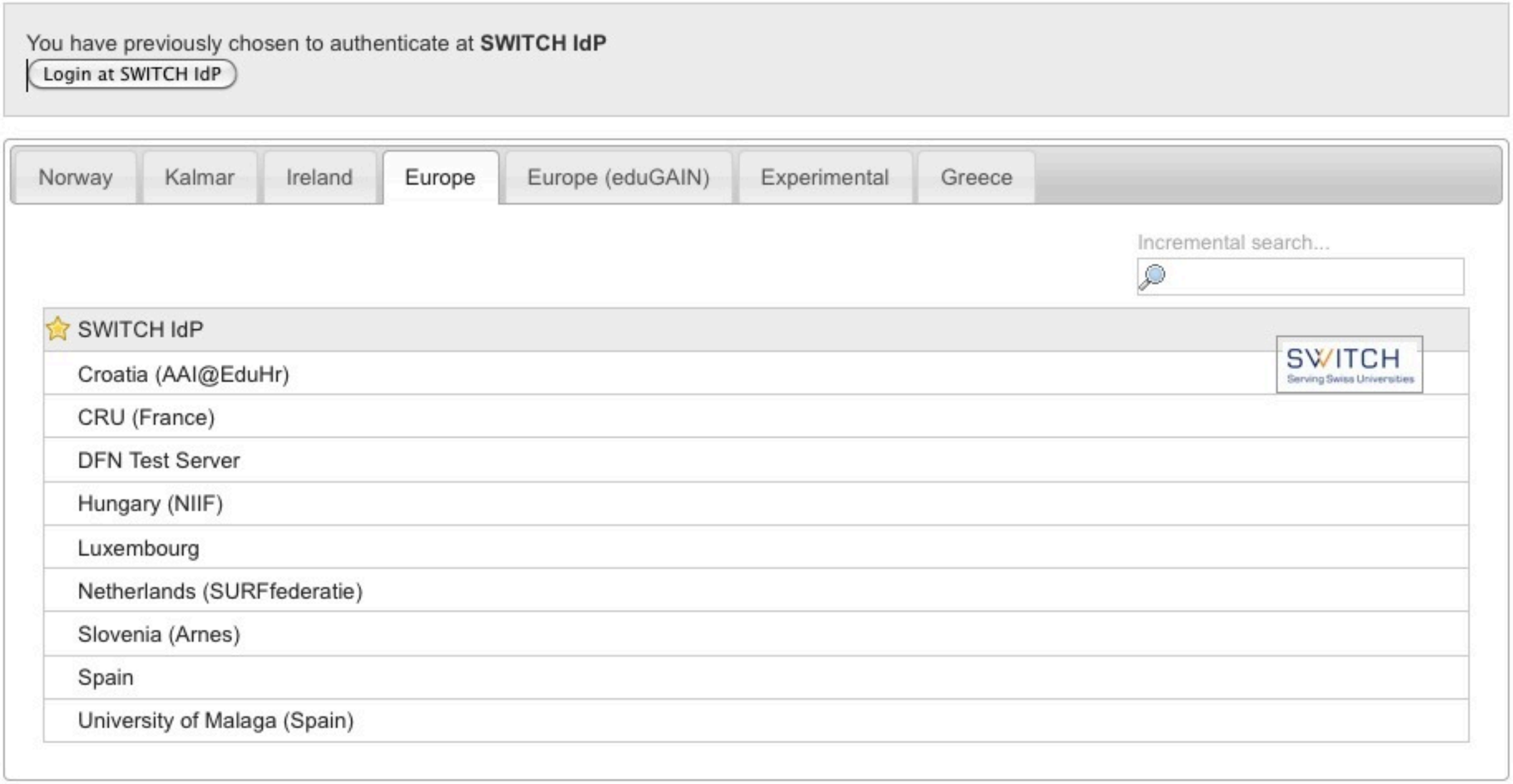
Current State of the DS Interfaces

- Classic central WAYF/Discovery Service is worst possible solution today
  - No integration into Service Provider
  - Different look&feel and different host name/domain
  - No customization possible
  - Has served its purpose in the beginning but hopefully will vanish soon

- Better and more advanced Discovery Service interfaces:
  - SimpleSAML PHP
  - Embedded WAYF

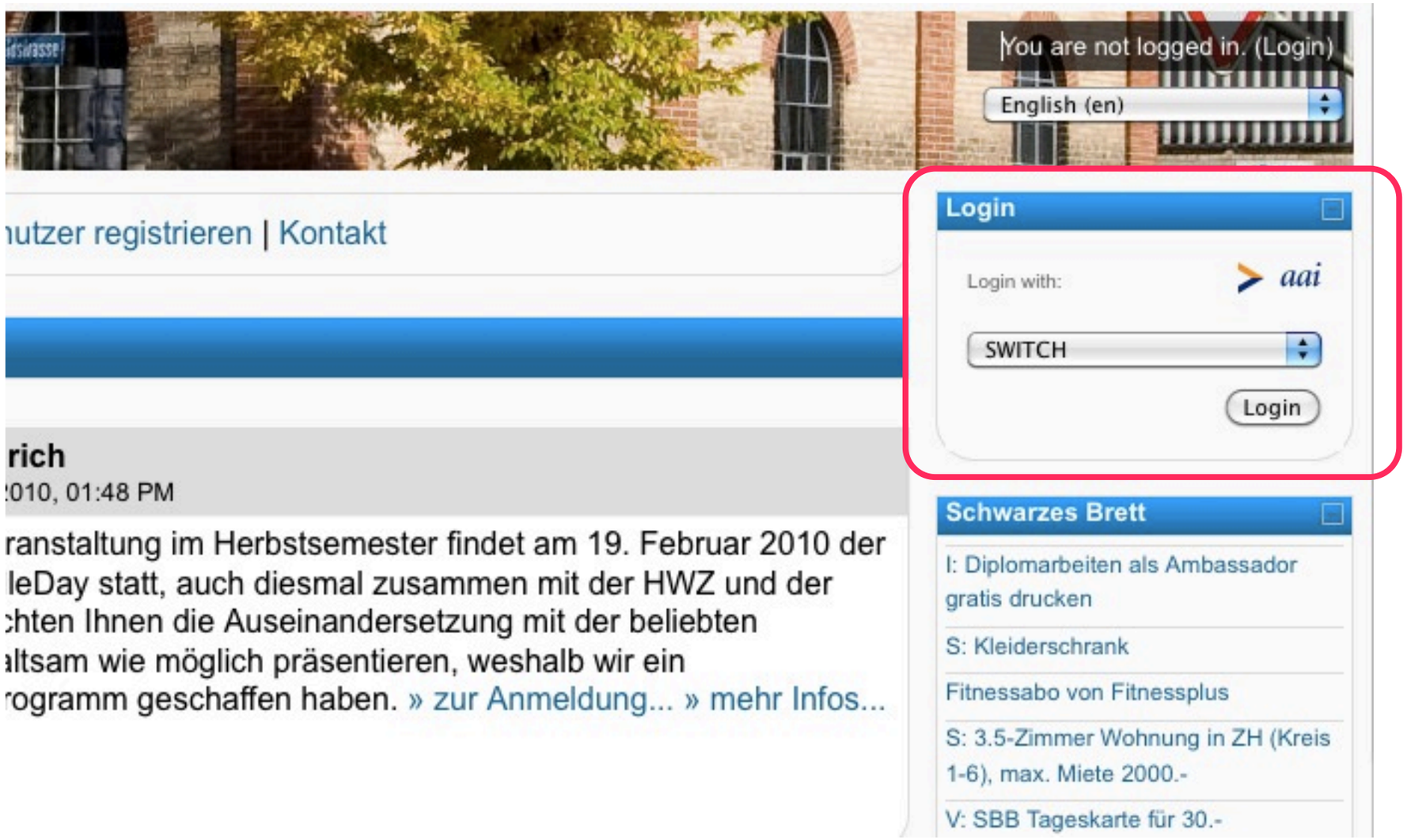
Discovery Service in SimpleSAML PHP

+ Good first approach that shows the direction to go
- But displayed information is not standardized/read from metadata
- DS not tightly integrated into actual service



(Embedded) Discovery Service

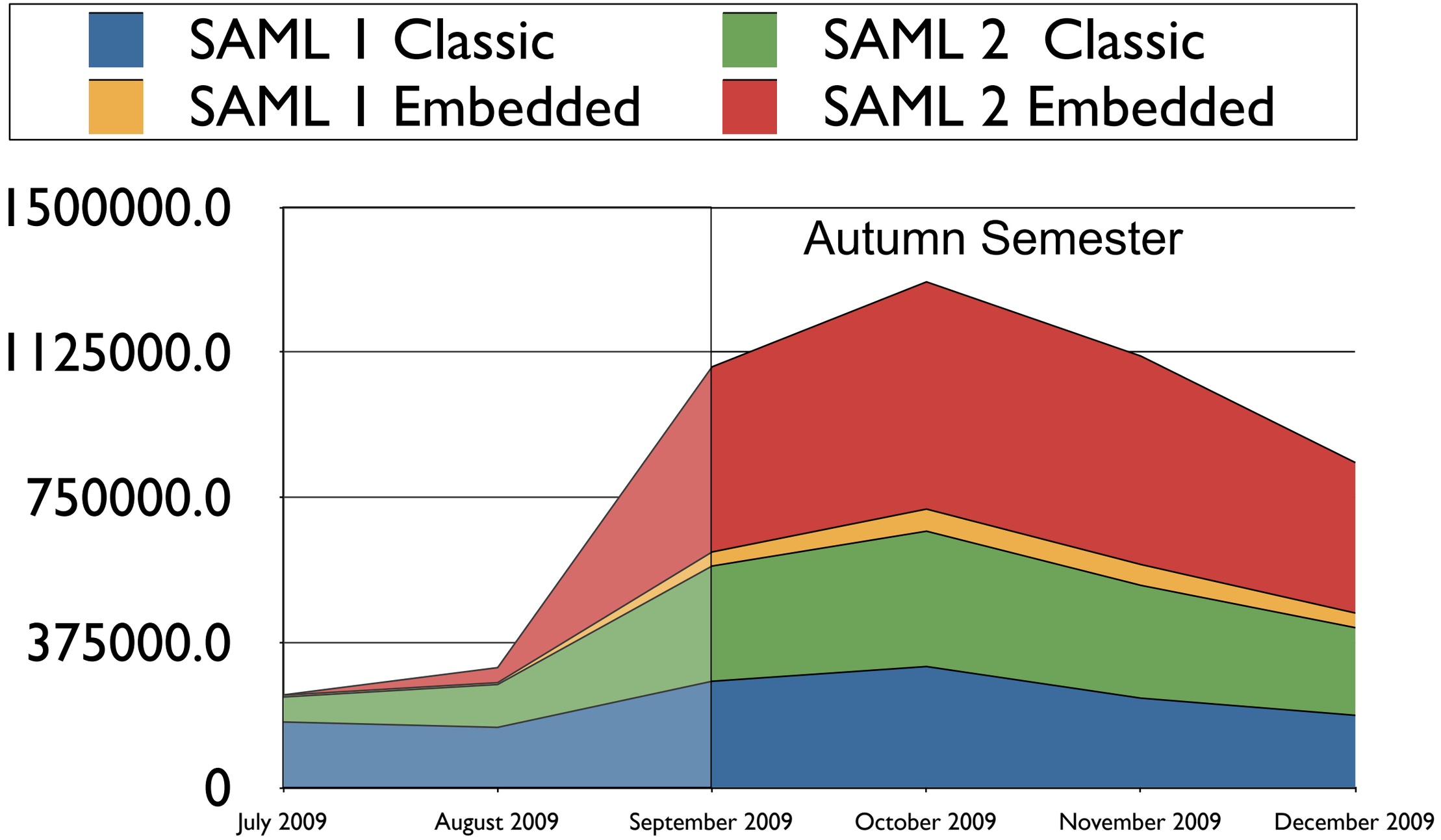
+ Good integration into service
- But not always scalable and only little information displayed



See http://elearning.zhaw.ch/

Operators of large SPs favour Embedded WAYF

More than 50% of requests now use Embedded WAYF



Number of Discovery Responses on central wayf.switch.ch per month

Todays Attribute Consent in uApprove

+ A good start (better than no consent at all)
- But is information sufficient to make a decision?

SWITCH aai

About AAI : FAQ : Help : Privacy

This is the Digital ID Card to be sent to '**eva.unibas.ch**':

Digital ID Card	
Surname	**Hämmerle**
Given name	**Lukas**
E-mail	**lukas.haemmerle@switch.ch**
Unique ID	**498752@switch.ch**

☐ Don't show me this page again. I agree that my Digital ID Card (possibly including more data than shown above) will be sent automatically in the future.

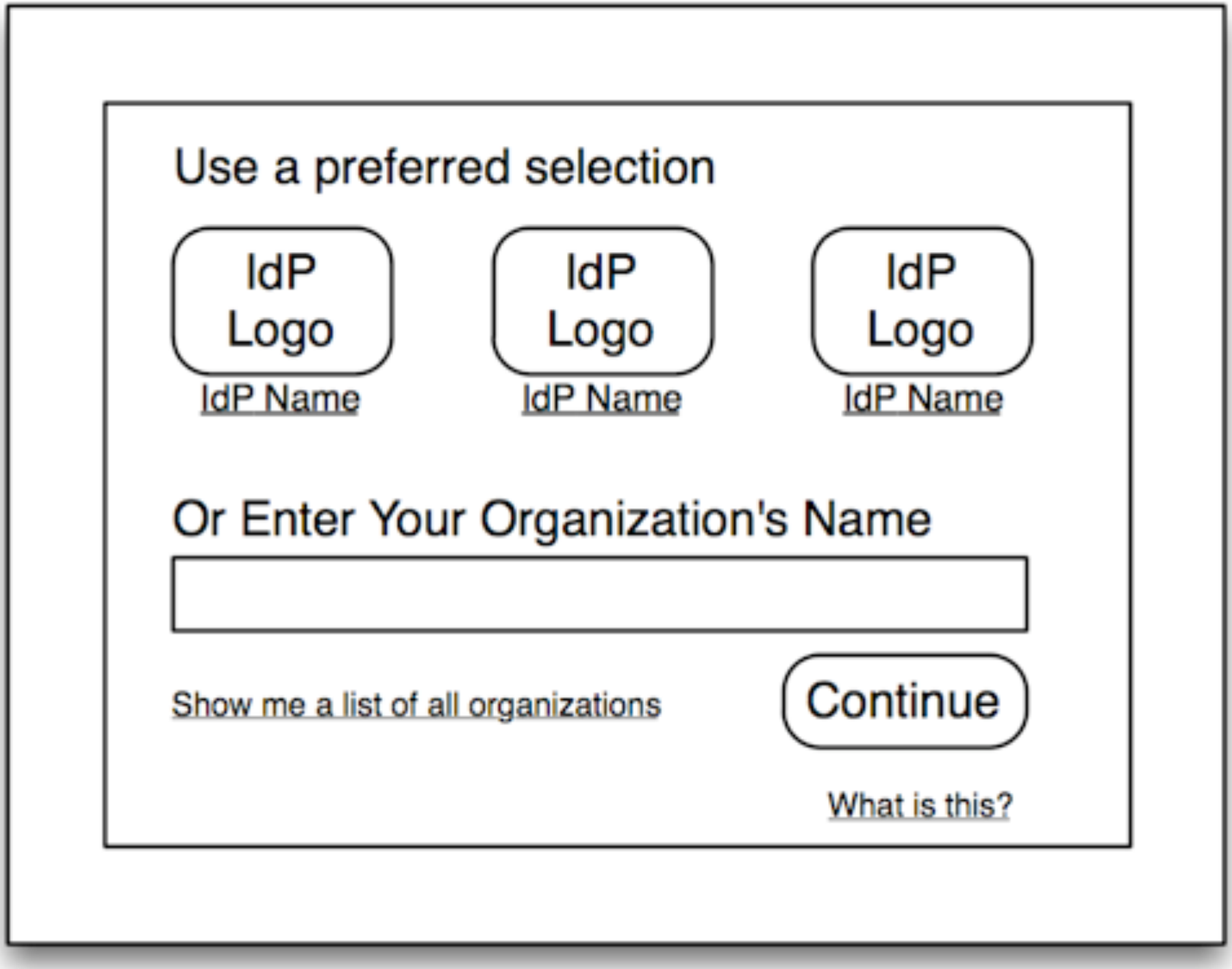
Cancel Confirm

The New Approach

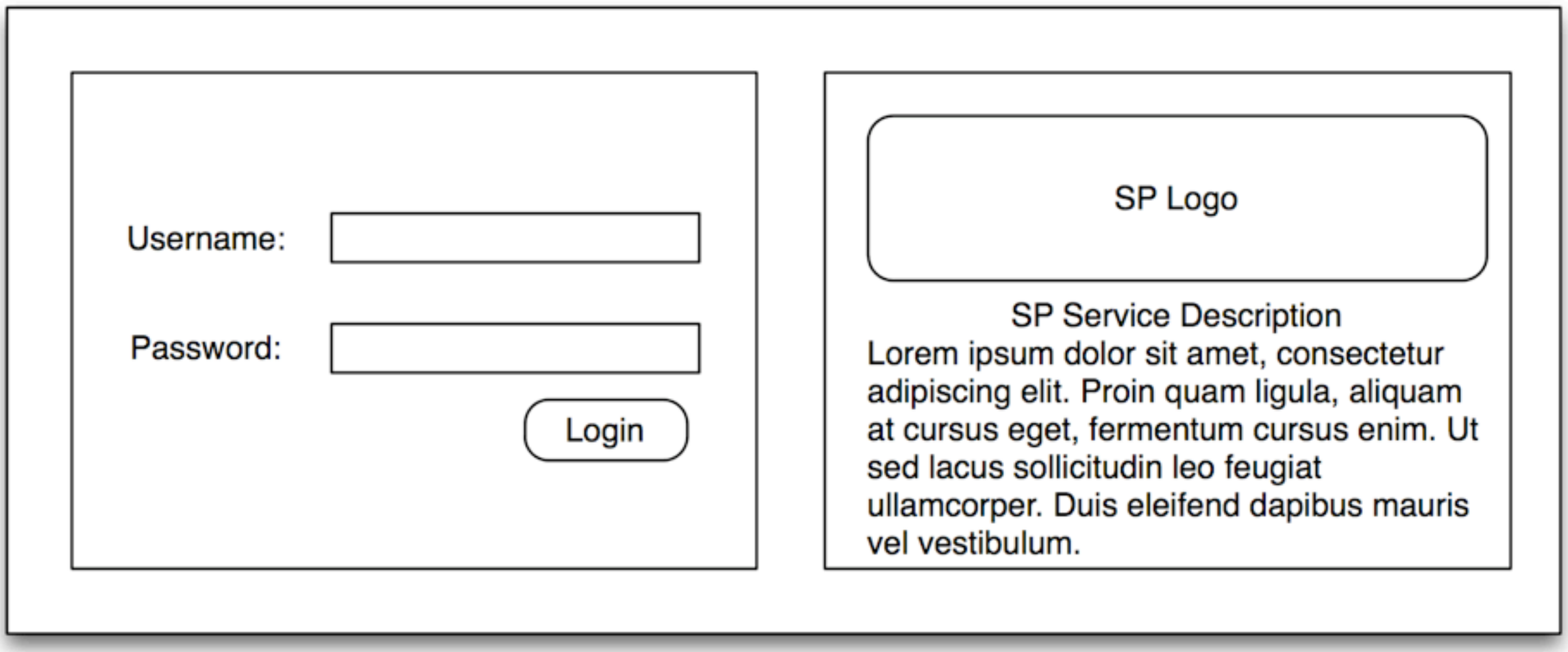
Use an embedded-like Discovery Service that integrates well into an application!

Use additional entity attributes contained in metadata (in form of standardized Entity Attributes) to display more information ...

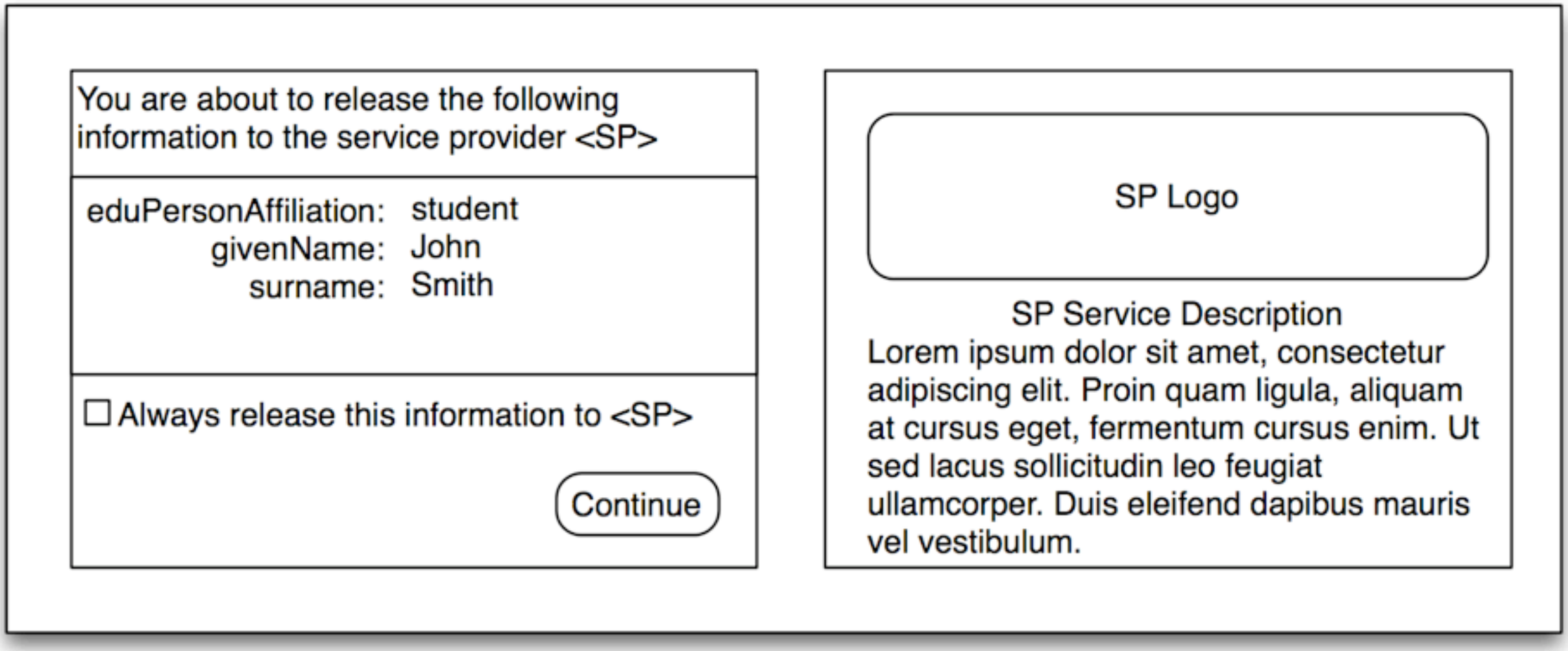
... during IdP discovery



... during authentication



... and before attribute consent



Proposed Metadata Attributes

Used as Entity Attribute in the Extension element of an entity

- Display Name
- Description
- Logo
- Information URL
- IP Hint
- Domain Hint
- Geolocation Hint

Where are MD attributes included?

In EntityAttributes extension element of an EntityDescriptor

```
<!-- SWITCH Identity Provider EntityDescriptor -->
<EntityDescriptor
 entityID="https://aai-logon.switch.ch/idp/shibboleth">
  <Extensions>
    <shibmd:Scope xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
     regexp="false">switch.ch</shibmd:Scope>
    <mdattr:EntityAttributes
      <saml:Attribute
        [...]
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </Extensions>
    <IDPSSODescriptor
     protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol
            urn:oasis:names:tc:SAML:1.1:protocol urn:mace:shibboleth:1.0">
[...]
```

Also see http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.pdf

Example of Display Name

- Multilingual
- Zero or more values

```
<saml:Attribute
      Name="urn:oasis:names:tc:SAML:metadata:attribute:ui:displayName"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
   <saml:AttributeValue xsi:type="md:localizedNameType" xml:lang="en">
      University of Zurich
   </saml:AttributeValue>

   <saml:AttributeValue xsi:type="md:localizedNameType" xml:lang="de">
      Universtität Zürich
   </saml:AttributeValue>
</saml:Attribute>
```

Example of Description

- Multilingual
- Zero or more values
- SP: Description of the service being offered
- IdP: Description of the community serviced

```
<saml:Attribute
 Name="urn:oasis:names:tc:SAML:metadata:attribute:ui:description"
 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
  <saml:AttributeValue xsi:type="md:localizedNameType" xml:lang="en">
    Swiss Education & Research Network
  </saml:AttributeValue>
  <saml:AttributeValue xsi:type="md:localizedNameType" xml:lang="de">
    Das Schweizerische Hochschul- und Forschungsnetzwerk
  </saml:AttributeValue>
</saml:Attribute>
```

Example of Logo Attribute

- Multilingual
- Should have transparent background (GIF or PNG)
- Should offer at least 16x16 or 16:9 format
- Should be served via https URL

```
<saml:Attribute
      Name="urn:oasis:names:tc:SAML:metadata:attribute:ui:logo"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
   <saml:AttributeValue xsi:type="UILogoType"
         xml:lang="en"
         href="http://www.switch.ch/logo.png"
         height="51"
         width="172">
      http://switch.ch/resources/images/logo.gif
   </saml:AttributeValue>
</saml:Attribute>
```

Example of Information URL

- Multilingual
- Should contain URL to more detailed localized information about the entity than in entity Description

```
<saml:Attribute
      Name="urn:oasis:names:tc:SAML:metadata:attribute:ui:infoURL"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
   <saml:AttributeValue xsi:type="md:localizedURIType" xml:lang="en">
      http://www.switch.ch
   </saml:AttributeValue>

   <saml:AttributeValue xsi:type="md:localizedNameType" xml:lang="de">
      http://www.switch.ch/de
   </saml:AttributeValue>

</saml:Attribute>
```

Example of IP Hint

- Must contain zero or more IPv4 or IPv6 CIDR blocks

```
<saml:Attribute
      Name="urn:oasis:names:tc:SAML:metadata:attribute:ui:hint:cidr"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue>130.59.0.0/16</saml:AttributeValue>
    <saml:AttributeValue>2001:620::0/96</saml:AttributeValue>
</saml:Attribute>
```

Example of Domain Hint

- Must contain zero or more domain names
- Could be used in combination with reverse DNS-lookup

```
<saml:Attribute
      Name="urn:oasis:names:tc:SAML:metadata:attribute:ui:hint:domain"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue>unizh.ch</saml:AttributeValue>
    <saml:AttributeValue>uzh.ch</saml:AttributeValue>
</saml:Attribute>
```

Example of Geolocation Hint

- Must contain one or more geographic coordinates
- Coordinates must be decimal and using World Geodetic System (2d) coordinate system

```
<saml:Attribute
      Name="urn:oasis:names:tc:SAML:metadata:attribute:ui:hint:geolocation"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
   <saml:AttributeValue>47.37328,8.531126</saml:AttributeValue>
</saml:Attribute>
```

Why Using MD Attributes at All?

The SAML MD specification already includes two elements that partially overlap these attributes.

- **<OrganizationDisplayName>** Element
  Only names the organization but not the entity. What if an organization operates multiple Identity Providers?

- **<ServiceDescription>** Element
  Only (optionally) appears for Service Providers but not for Identity Providers. No means of expressing description for an Identity Provider.

Proof-of-Concept for WAYF/Discovery Service

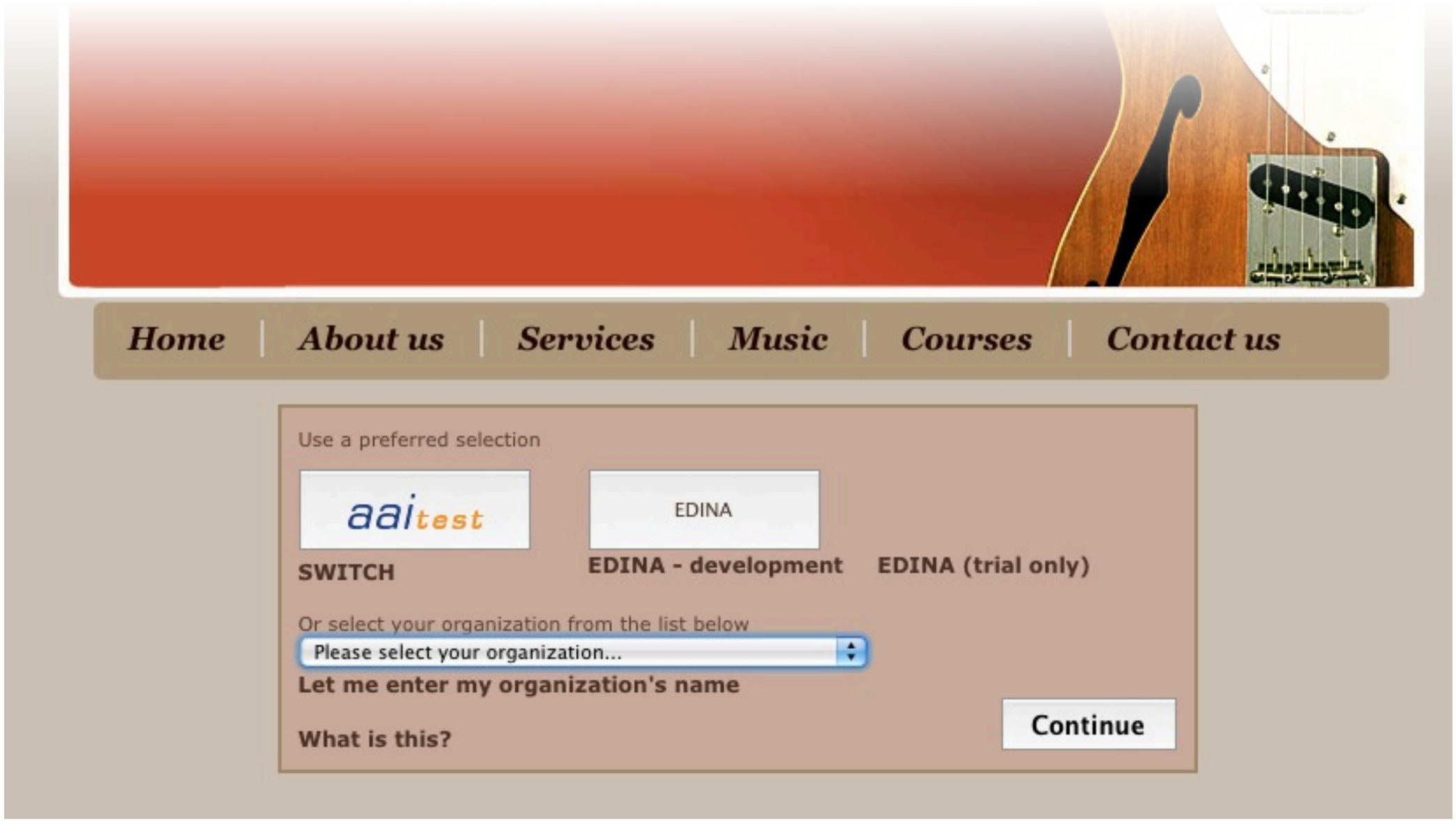
- Works similar to the SWITCH Embedded WAYF
- Will use JSON data structure that contains relevant information from metadata
- JSON will be generated by an SP handler
  - e.g. /Shiboleth.sso/IdPs.json
- SP really knows which IdPs it can communicate with

How to use this new Discovery Service

To embed the Discovery Service:

1. Add `<div id="dsoi"></div>` container DIV
2. Add configuration Javascript:
   - E.g. `<script src="ds-conf.js" [...]></script>`
   - Contains URL to JSON file, e.g. `/Shibboleth.sso/IdPs.json`
   - Allows appearance customization and localization
3. Add logic JavaScript from SP handler or local file
   - E.g. `<script src="/Shibboleth.sso/DS.js" [...]></script>`
   - Or from a local JavaScript file that fully can customized

Discovery Service Proof-Of-Concept



Try DS yourself: https://dieng.switch.ch/i2ds/musicschool/

Summary

- In order to improve the user interface, additional information must be displayed to the user

- Entity Attributes in the metadata can provide additional entity information

- Discovery Service should be embedded directly into a resource

- Proof-Of-Concept of Discovery Service and Identity Provider using presented concepts soon to be finished