SWITCH

The Swiss Education & Research Network

Configuring Access Rules in Apache

Ueli Kienholz, <kienholz@switch.ch>
Valéry Tschopp, <tschopp@switch.ch>

Configuring Access Rules in Apache

SWITCH
The Swiss Education & Research Network

Rules in httpd.conf or .htaccess

```
<Location /secure>
  AuthType shibboleth
  require valid-user
</Location>
```

Any AAI user

```
<Location /restricted>
  AuthType shibboleth
  require uniqueID 314592@aaitest.switch.ch
</Location>
```

One user

```
<Location /secure>
  AuthType shibboleth
  require homeOrganizationType ~ ^[^vV][^hH][^oO]
</Location>
```

All users except from VHO

Reference: http://www.switch.ch/aai/docs/shibboleth/internet2/1.2/deploy-guide-target1.2.html#4.d.

Combining multiple Attributes

SWITCH
The Swiss Education & Research Network

- **Default behaviour: OR**
- **Behaviour with ShibRequireAll (Shibboleth 1.2): AND**

```
<Location /secure>
  AuthType shibboleth
  ShibRequireAll on
  require affiliation student
  require homeOrganization aaitest.switch.ch
</Location>
```

- **In future: API and XACML**

Snippet from AAP.xml

SWITCH
The Swiss Education & Research Network

```
<AttributeRule Name="urn:mace:switch.ch:attribute-def:swissEduPersonUniqueID"
               Header="Shib-SwissEP-UniqueID" Alias="uniqueID">
  <AnySite>
     <AnyValue/>
  </AnySite>
</AttributeRule>

<AttributeRule Name="urn:mace:dir:attribute-def:sn"
               Header="Shib-Person-surname" Alias="surname">
  <AnySite>
     <Value Type="regexp">^.+$</Value>
  </AnySite>
</AttributeRule>
```

SWITCH

The Swiss Education & Research Network

Linking Web-Applications with AAI

Ueli Kienholz, <kienholz@switch.ch>
Valéry Tschopp, <tschopp@switch.ch>

Exporting AAI-Attributes to Applications

SWITCH
The Swiss Education & Research Network

```
<Location /secure>
  AuthType shibboleth
  ShibExportAssertion on
  require valid-user
</Location>
```

httpd.conf

→ Environment-Variables
(e.g. HTTP_SHIB_SWISSEP_UNIQUEID)

```
<?php
$uniqueID = $_SERVER['HTTP_SHIB_SWISSEP_UNIQUEID'];
…
?>
```

sample.php

SWITCH

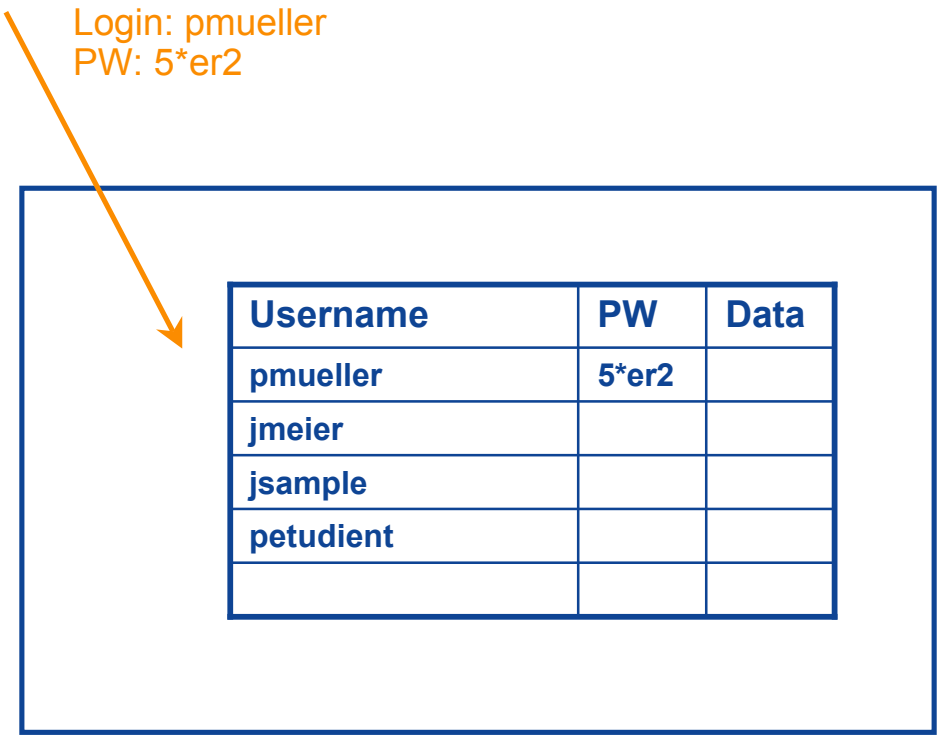
The Swiss Education & Research Network

AAI-based User-Management in personalized Web-Applications

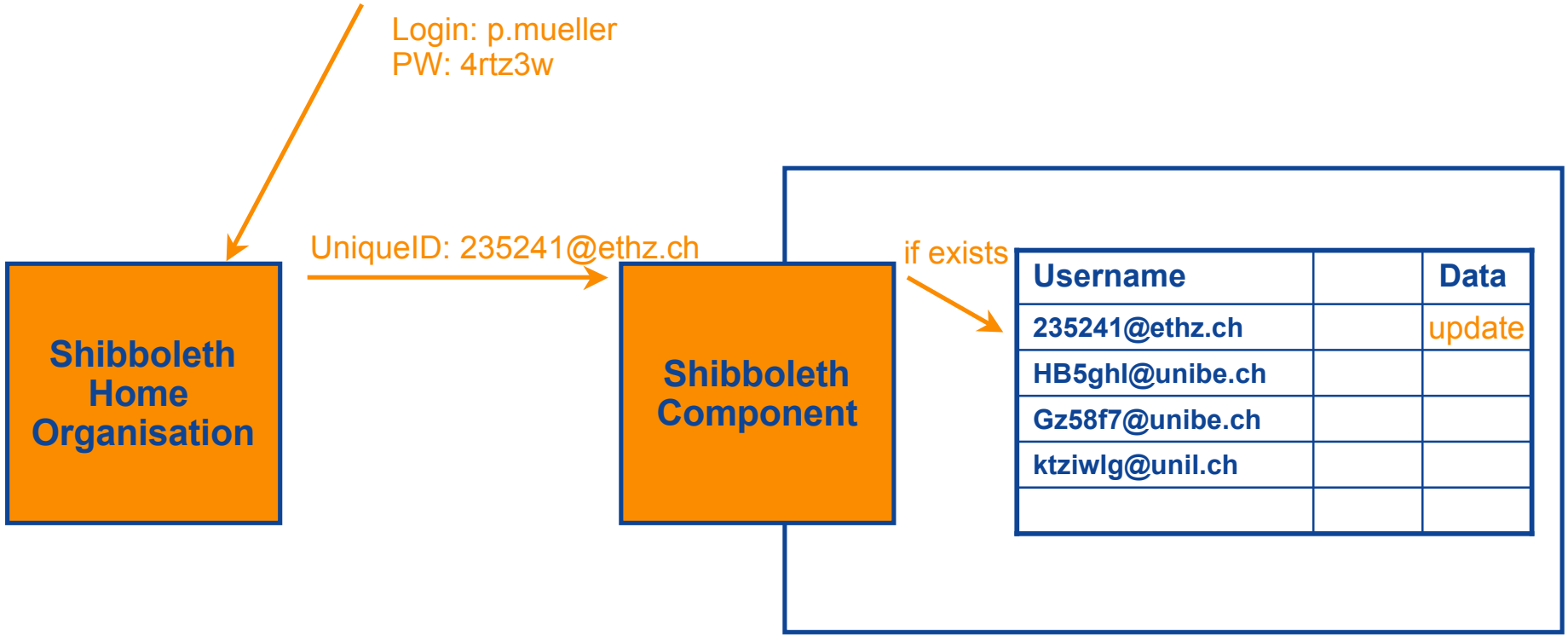
Ueli Kienholz, <kienholz@switch.ch>
Valéry Tschopp, <tschopp@switch.ch>

Personalized System, Non-Shibbolized

SWITCH
The Swiss Education & Research Network

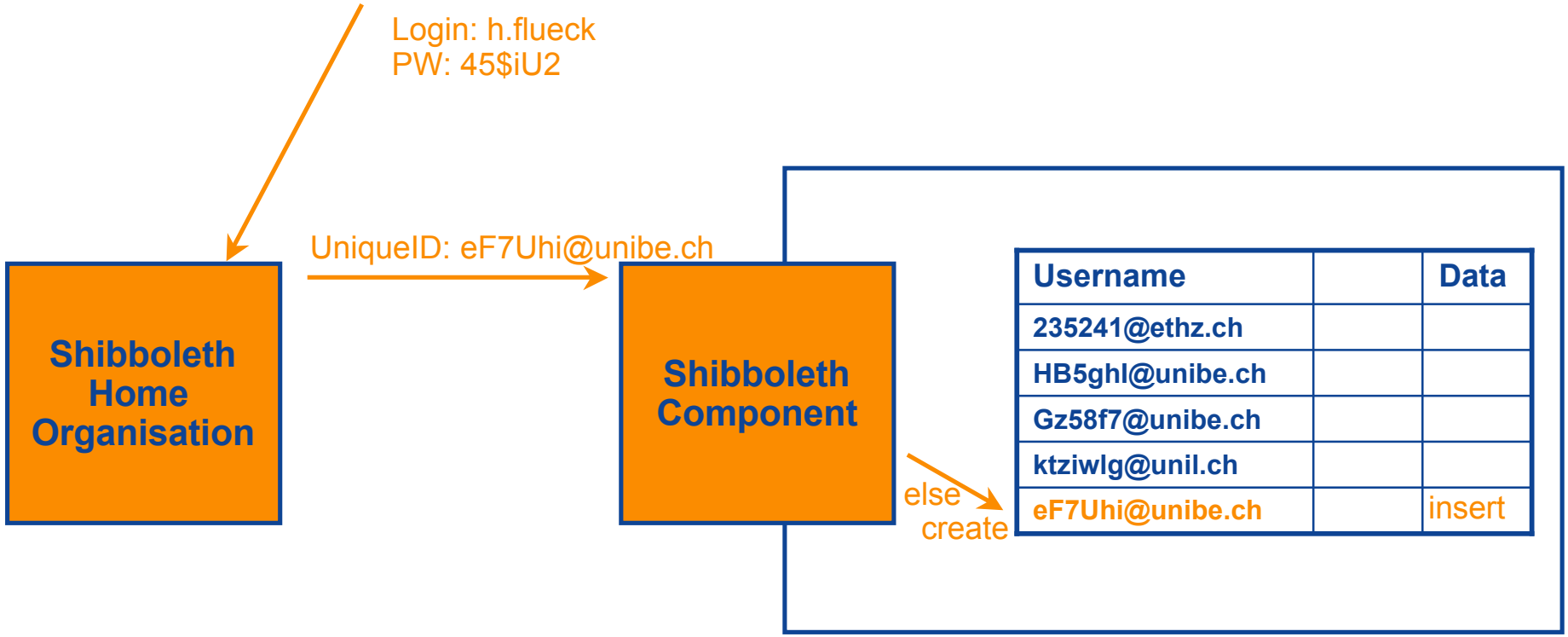


Personalized System, Shibbolized



Personalized System, Shibbolized, Creating New Users

SWITCH
The Swiss Education & Research Network



Sample personalized App (without AAI)

SWITCH
The Swiss Education & Research Network

```php
<?php
  session_name('non-shibboleth');
  session_start();                                  // Use PHP session cookies
  session_register('user');                         // Associate the variable $user with the session
  session_register('counter');                      // Associate the variable $counter with the session
  session_register('date');                         // Associate the variable $date with the session

  echo "<html><body>";

  if (empty($user)) {                               // No user-session
    if (empty($_GET['username'])) {                 // No username submitted -> display login form
      echo "<form method='GET'>";
      echo "Username:<input type='text' name='username'><br>";
      echo "Password:<input type='password' name='password'>";
      echo "<input type='submit' value='login'>";
      echo "</form>";
    }
    else {                                          // Check password
      if ($_GET['password']=="pass") {
        $user = $_GET['username'];                  // Store username in session
      } else {
        echo "Wrong password. Go back and try again!";
      }
    }
  }

  if (!empty($user)) {                              // User is identified -> display personalized page
    echo "<h3>Hello $user !</h3>";

    if (!empty($counter)) echo "<p>You were already here $counter times!";
    $counter++;

    if (!empty($date)) echo "<p>Last visit: $date";     // Display date of last visit
    $date= date("F j, Y, g:i a");

    echo "<hr>";
    echo "Here comes whatever personalized application (WebMail, Calendar, Forum, Chat, Portal, E-Learning Plattform, DB)";
  }

  echo "</body></html>";
?>
```

Login Form

Check password

https://koolau.switch.ch/nonshib/sample.php

Sample personalized App (with AAI)

SWITCH
The Swiss Education & Research Network

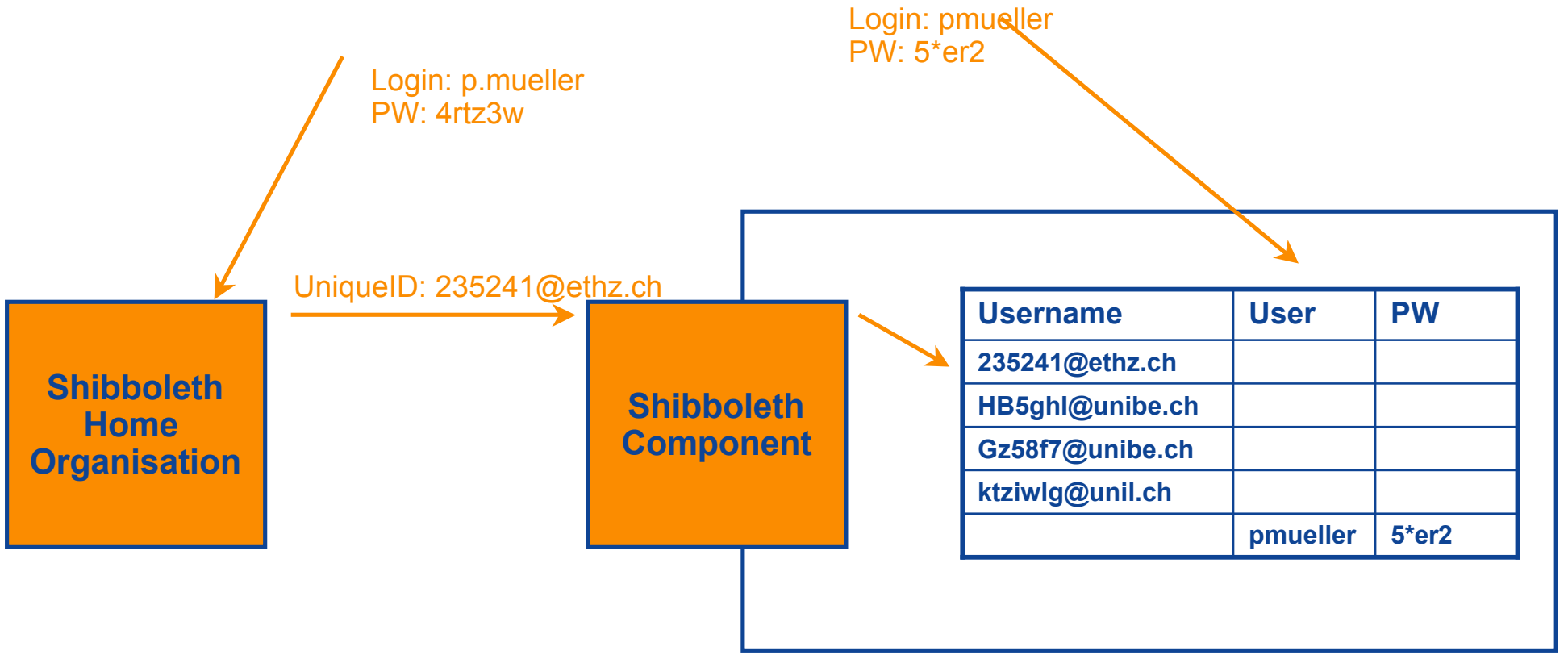
```php
<?php
  session_name('shibboleth');
  session_start();                                  // Use PHP session cookies
  session_register('counter');                      // Associate the variable $counter with the session
  session_register('date');                         // Associate the variable $date with the session

  echo "<html><body>";

  $uniqueID = $_SERVER['HTTP_SHIB_SWISSEP_UNIQUEID'];   // Read Shibboleth attribute
  if (empty($uniqueID)) {                           // UniqueID attribute is missing
    echo "Attribute (SwissEduPerson-) 'UniqueID' is missing.";
    echo "<br>Please contact the administrator of your AAI Home Organisation.";
  }
  else {
    // Read Shibboleth attributes from HTTP server
    $name = $_SERVER['HTTP_SHIB_PERSON_SURNAME'];
    $name= utf8_decode($name);
    $firstname= $_SERVER['HTTP_SHIB_INETORGPERSON_GIVENNAME'];
    $firstname= utf8_decode($firstname);

    if (empty($name) or empty($firstname)) {
      $username= $uniqueID;
    }
    else {
      $username= "$firstname $name ($uniqueID)";
    }

    echo "<h3>Hello $username !</h3>";

    if (!empty($counter)) echo "<p>You were already here $counter times!";
    $counter++;

    if (!empty($date)) echo "<p>Last visit: $date";     // Display date of last visit
    $date= date("F j, Y, g:i a");

    echo "<hr>";
    echo "Here comes whatever personalized application (WebMail, Calendar, Forum, Chat, Portal, E-Learning Plattform, DB)";
  }

  echo "</body></html>";
?>
```

Check for required attributes

Preprocess attributes

https://koolau.switch.ch/shib/sample.php

Personalized System, For Shib & non-Shib Users



SWITCH

The Swiss Education & Research Network

The AAIportal as a Tool for User-Mangement

Ueli Kienholz, <kienholz@switch.ch>
Valéry Tschopp, <tschopp@switch.ch>

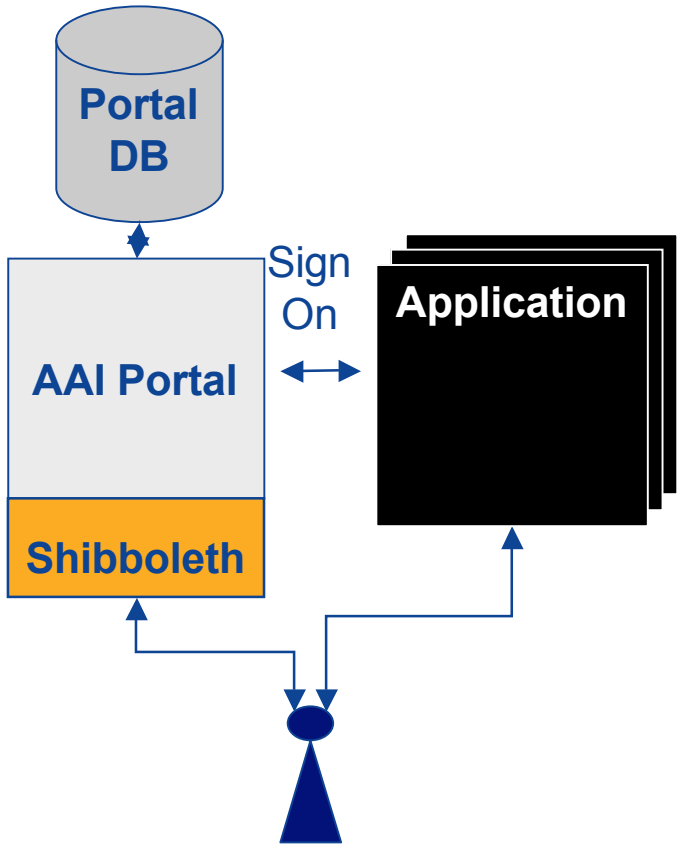
The AAIportal

SWITCH
The Swiss Education & Research Network

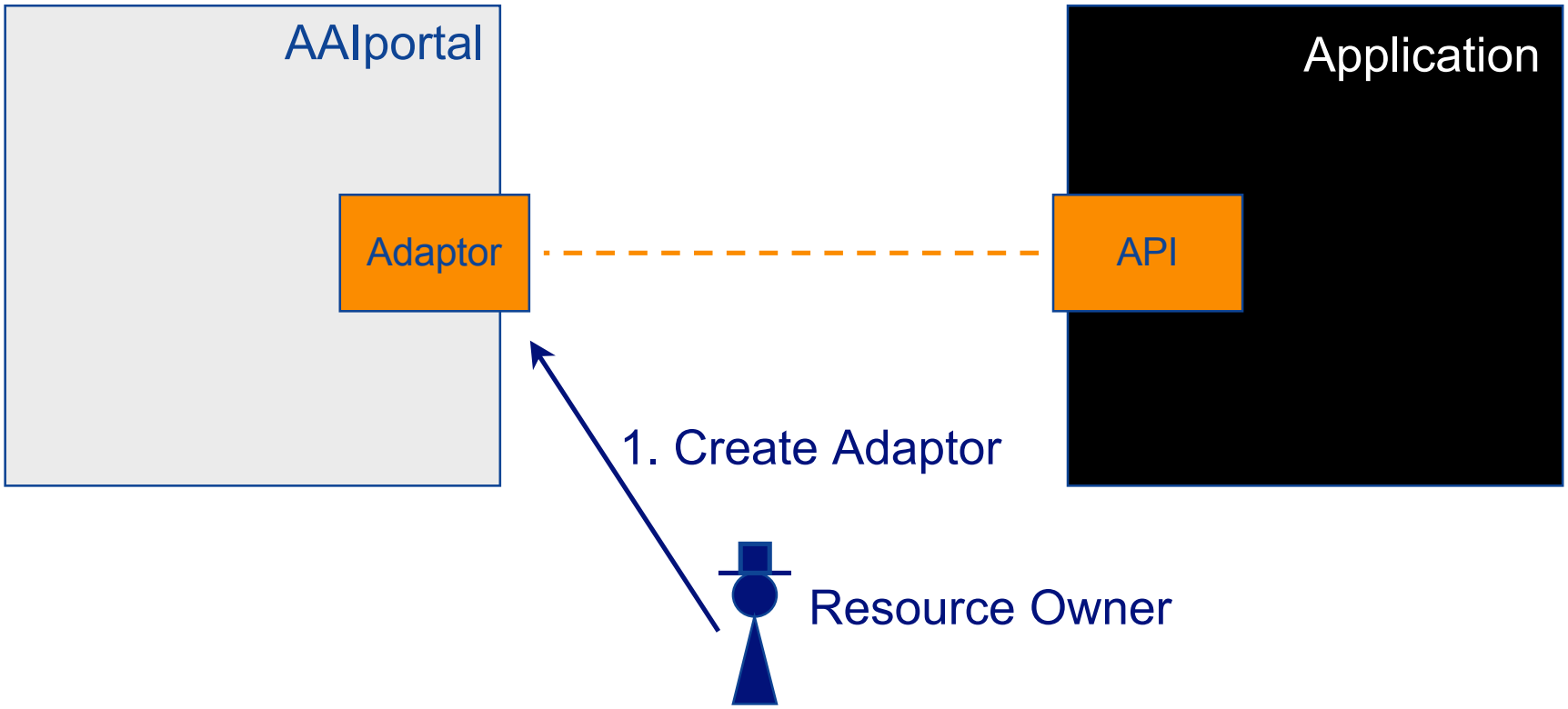
- Originally developed by IAM at Uni Bern
- Since 2004 maintained by SWITCH
- Further developed by IAM & SWITCH
- Open-Source project
  http://aai-portal.sourceforge.net/

AAIportal Overview

- Portal Functionality
- Authentication Gateway
- User Management
- Adaptors to "Black boxes"



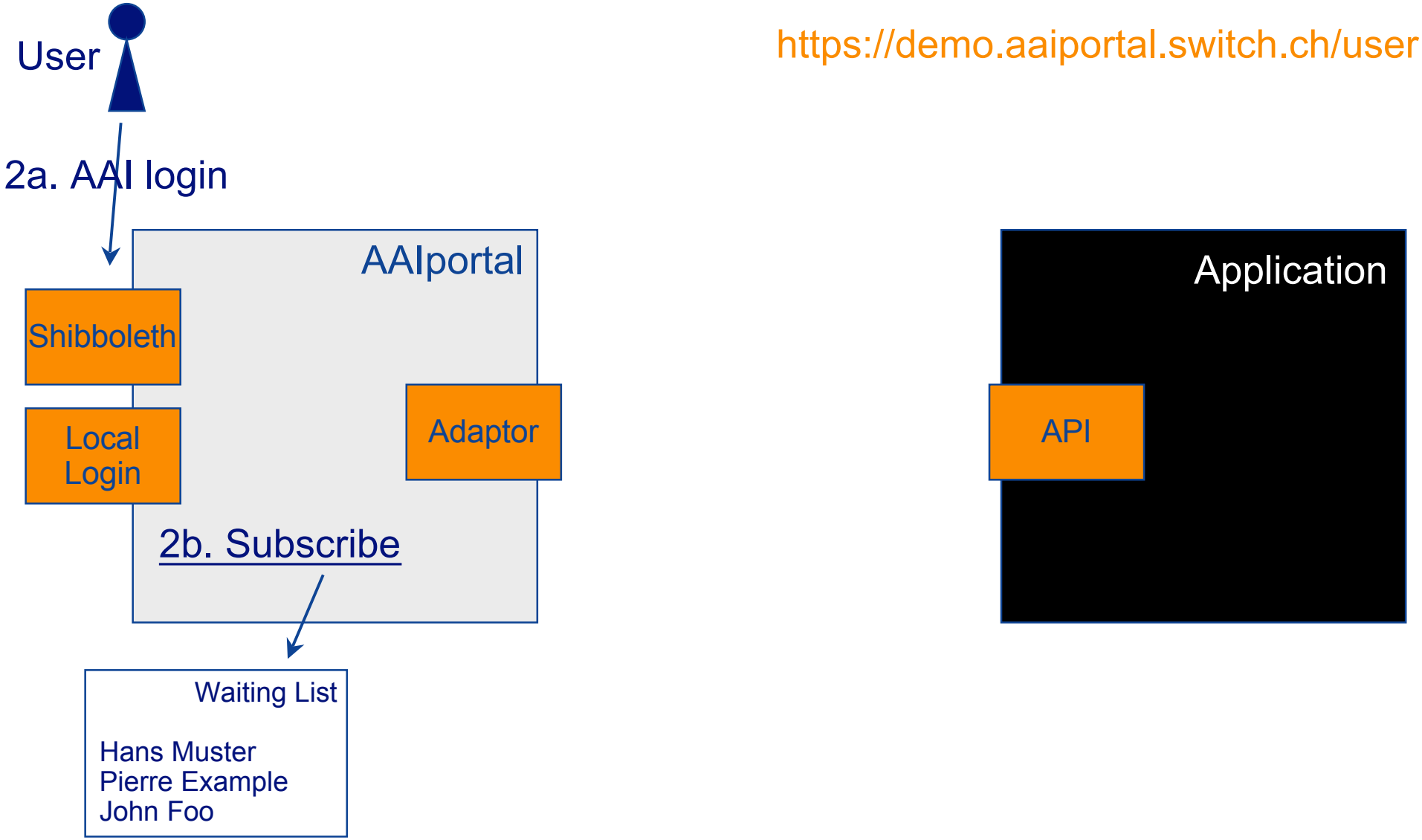
AAIportal Step 1) Resource Owner creates new Adaptor



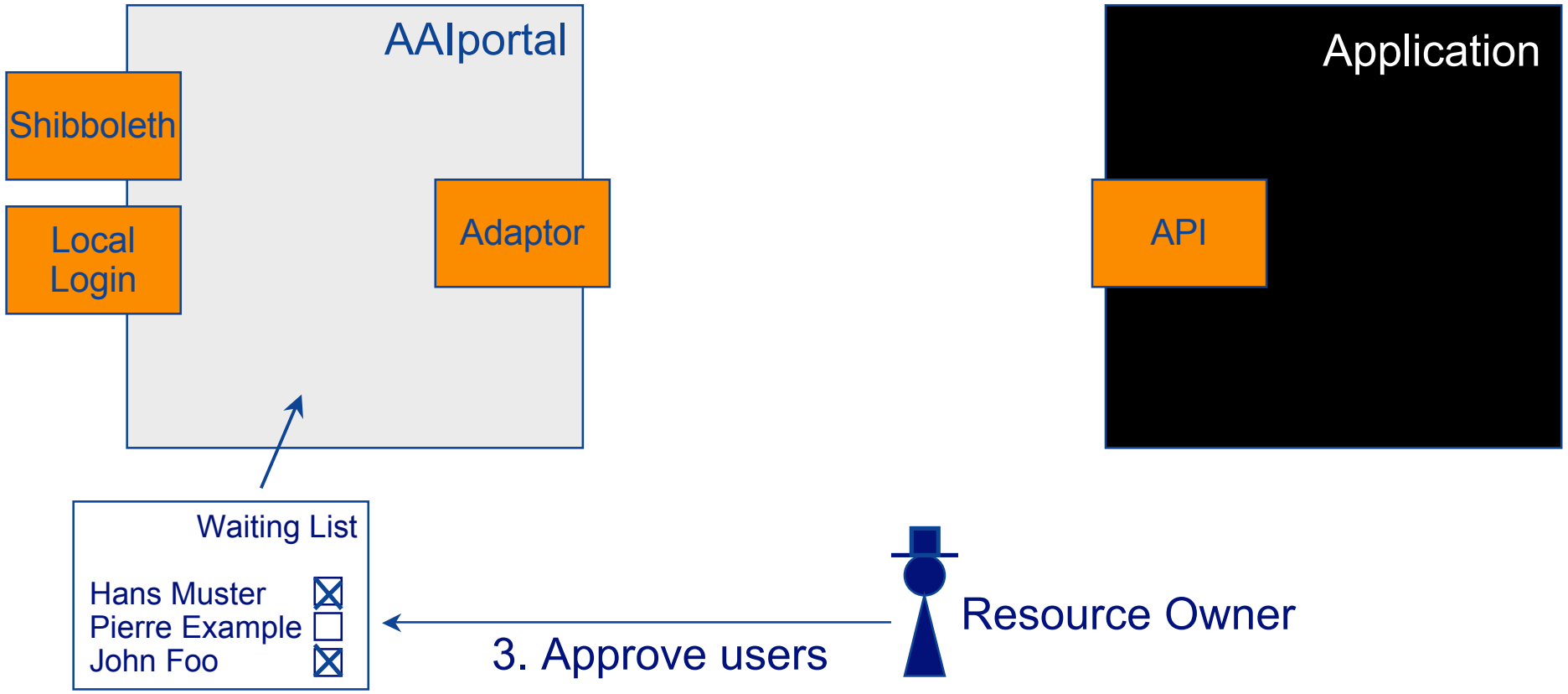
AAIportal Step 2) Users Subscribe to Resource

SWITCH
The Swiss Education & Research Network

https://demo.aaiportal.switch.ch/user



AAIportal Step 3) Resource Owner grants access



AAIportal Step 4) User accesses Resource

https://demo.aaiportal.switch.ch/user