AAI-enabling Apache

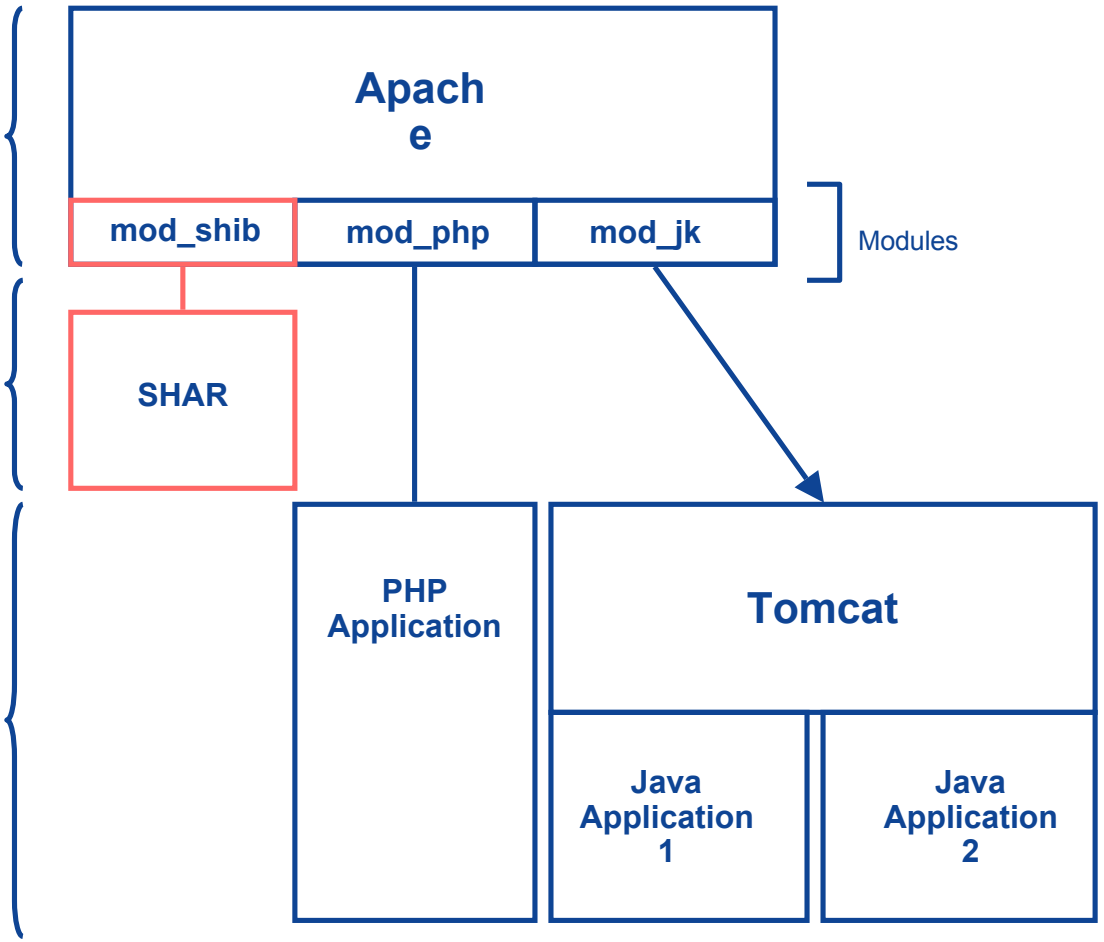
Valéry Tschopp, <tschopp@switch.ch>

Apache Software Components

- Apache Webserver
- Shibboleth Target (mod_shib)
- Tomcat Connector (mod_jk)
- PHP (mod_php)

- Shibboleth Target (SHAR)

- PHP Applications
- Java Applications (Tomcat, …)



Static Authorization in Apache

SWITCH
The Swiss Education & Research Network

Rules in **httpd.conf** or **.htaccess** for Shibboleth Target 1.2

Any AAI user

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

One user

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

All users except from VHO

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

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

SWITCH

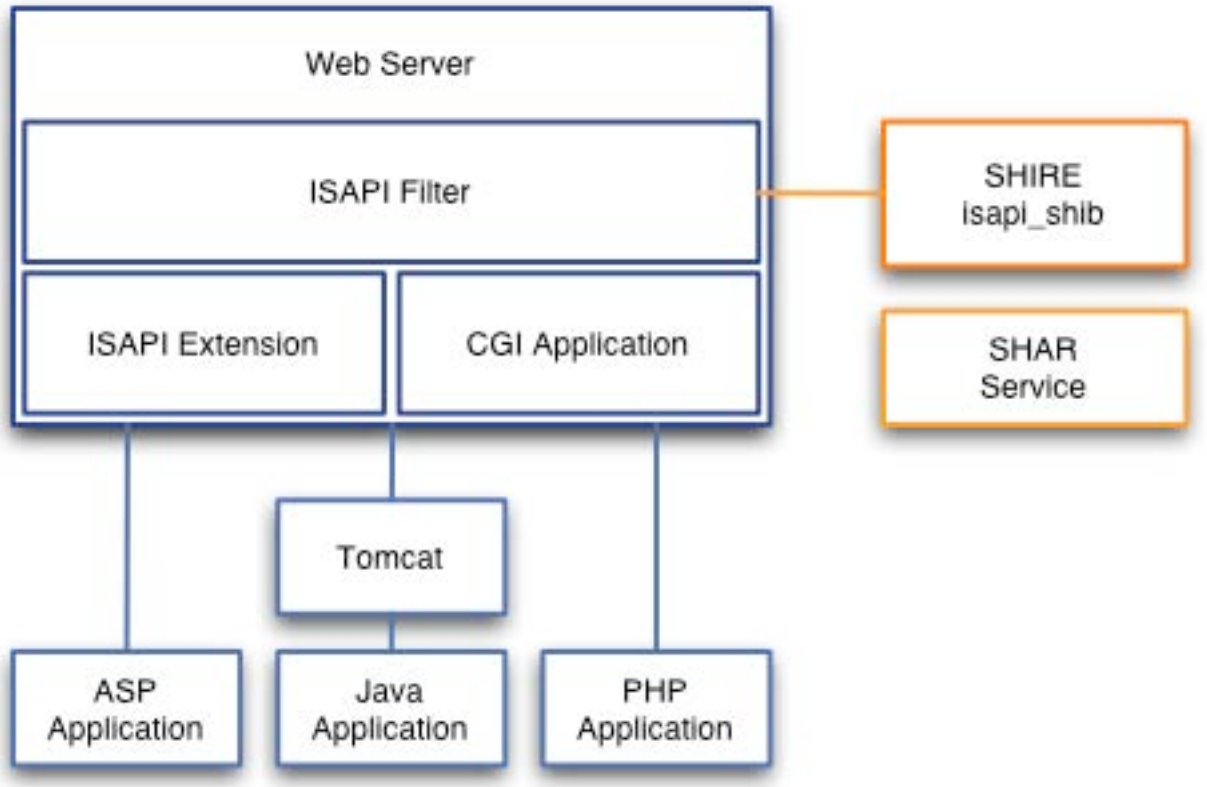
The Swiss Education & Research Network

AAI-enabling IIS

Patrik Schnellmann, <schnellmann@switch.ch>

Software Components

- IIS Web Server
- Shibboleth Target (isapi_shib)
- Shibboleth Target (SHAR)
- Tomcat via JK/JK2
- Dynamic Web Pages (ASP, Java, PHP, …)



Configuring Access Rules in IIS

SWITCH
The Swiss Education & Research Network

Rules in **shibboleth.xml** for Shibboleth Target 1.2

```
...
 <RequestMap applicationId="default">
   <Host name=”some.host.ch"
         scheme="http">
     <Path name="secure"
           requireSession="true"
           exportAssertion="false">
     </Path>
   </Host>
 </RequestMap>
...
```

⇨ isapi_shib forces authentication on requests for files in http://some.host.ch/secure/

isapi_shib, Future Features for IIS

SWITCH
The Swiss Education & Research Network

- In the current 1.2 version, access configuration is rather limited if we compare with the Apache counterpart
  - Fine grained access control has to be handled by the application
- The future version (1.3)
  - will include a plugin for access control rules
  - is expected to be released in early 2005

AAI-enabling Web Applications (personalized, dynamic content in PHP, ASP, Perl, Java, ...)

Ueli Kienholz, <kienholz@switch.ch>

Exporting AAI-Attributes to Applications with Apache

SWITCH
The Swiss Education & Research Network

httpd.conf

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

→ HTTP Headers
(e.g. HTTP_SHIB_SWISSEP_UNIQUEID)

Use attribute in PHP:

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

Exporting AAI-Attributes to Applications with IIS

SWITCH
The Swiss Education & Research Network

shibboleth.xml

```
<RequestMap ...>
 <Host ...>
  <Path name="secure"
        requireSession="true"
        ...>
```

HTTP Headers
(e.g. HTTP_SHIB_SWISSEP_UNIQUEID)

Use attribute in PHP:

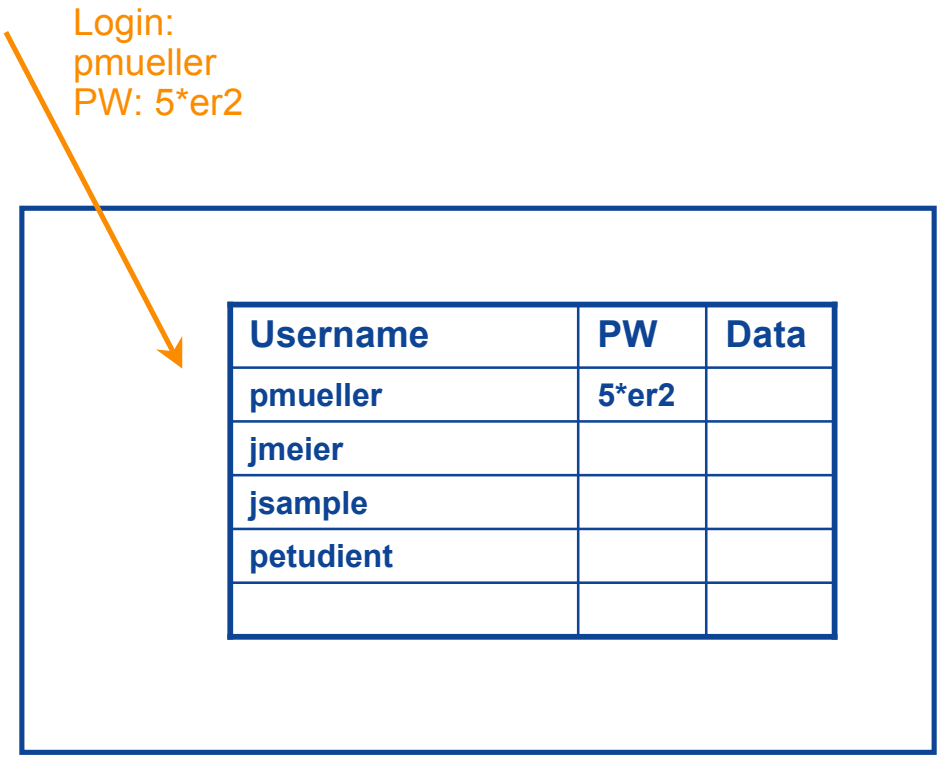
```
<?php
   $uniqueID = $_SERVER['HTTP_SHIB_SWISSEP_UNIQUEID'];
... ?>
```

Use attribute in ASP:

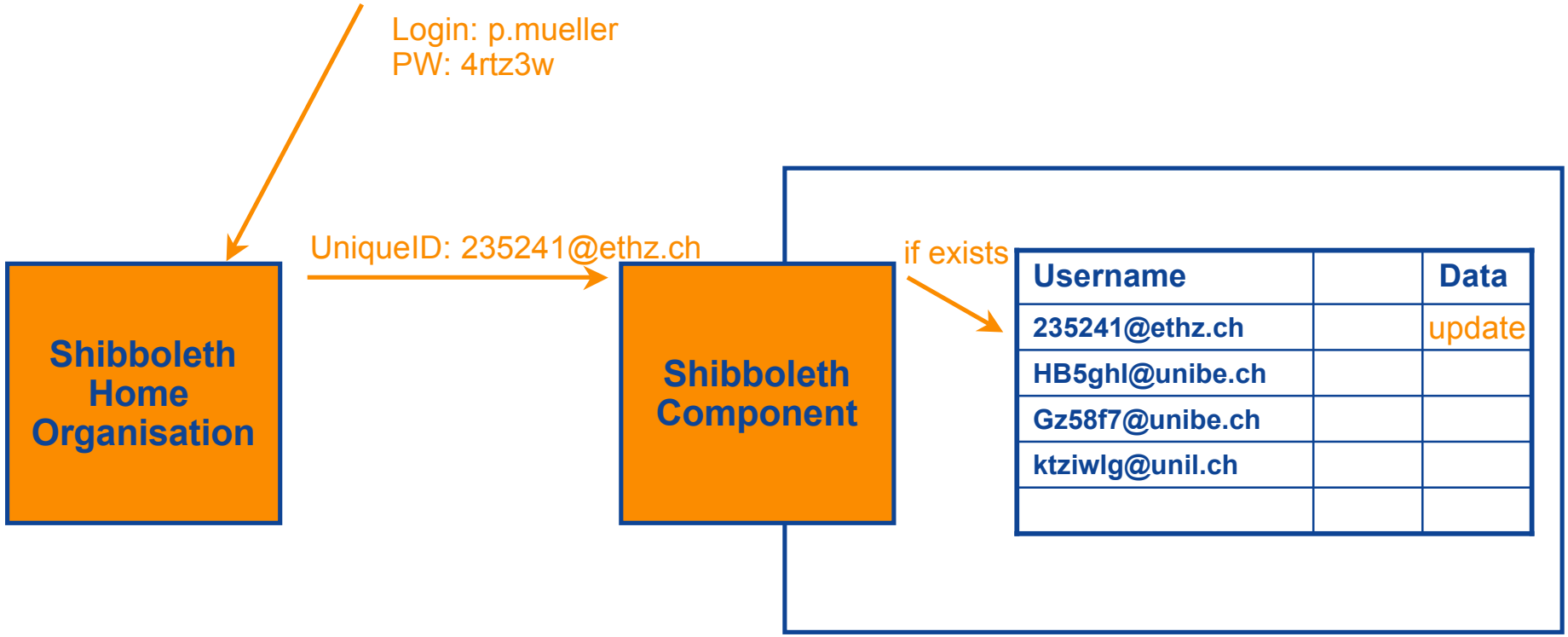
```
<%
  Set uniqueID = Request.ServerVariables("HTTP_SHIB_SWISSEP_UNIQUEID")
... %>
```

Personalized System, Non-Shibbolized

SWITCH
The Swiss Education & Research Network

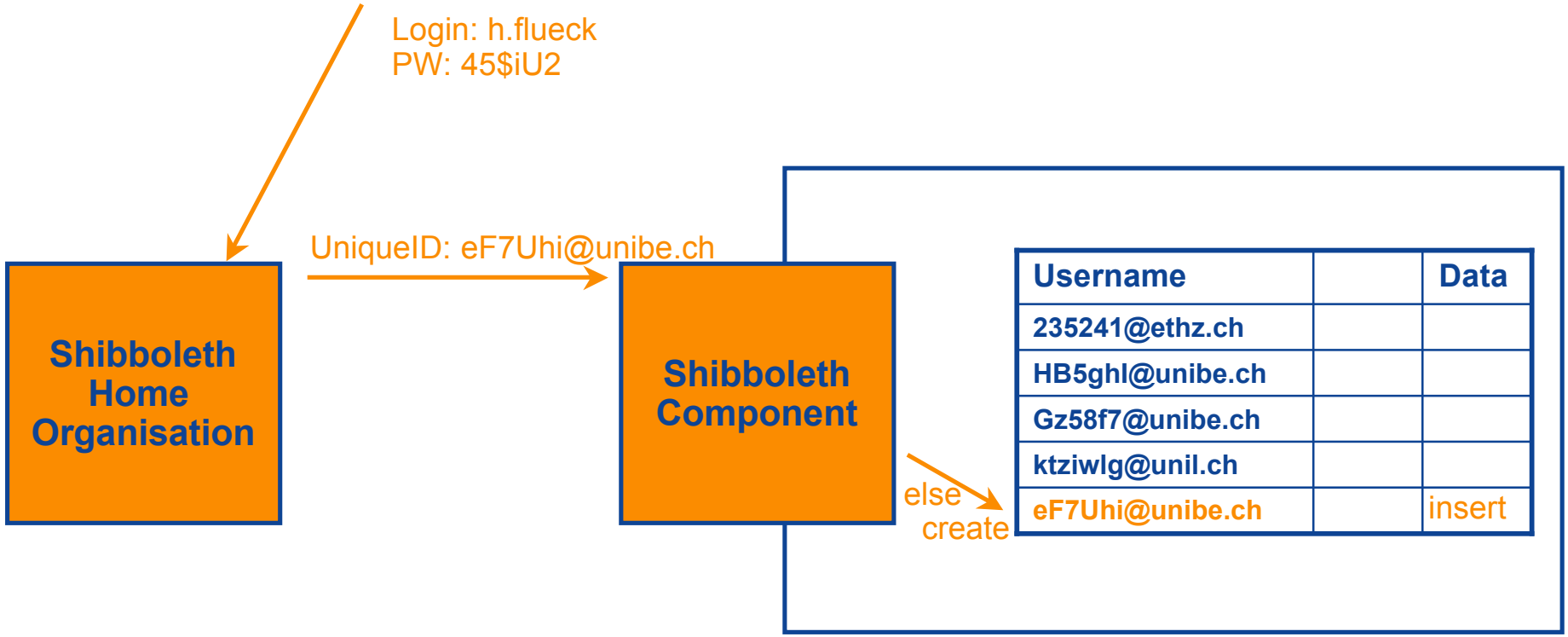


Personalized System, Shibbolized



Personalized System, Shibbolized, Creating New Users

SWITCH
The Swiss Education & Research Network



Sample personalized PHP-Application (without AAI)

SWITCH
The Swiss Education & Research Network

```
<?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 PHP-Application (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

Sample personalized ASP-Application (without AAI)

SWITCH
The Swiss Education & Research Network

```
<%
If Not(Session("counter") > 0) Then
  Session("counter") = 0
End If
Response.Charset="UTF-8"
Response.Write ("<?xml version=""1.0"" encoding=""UTF-8""?>" & _
  "<!DOCTYPE html PUBLIC ""-//W3C//DTD XHTML 1.1//EN""" & _
  """http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd"">" & _
  "<html xmlns=""http://www.w3.org/1999/xhtml"" xml:lang=""en"">")


If (isEmpty(Session("username"))) Then
    If (isEmpty(Request.Form("username"))) Then
%><pre><form method="POST" action="<% Response.Write(Request.ServerVariables("SCRIPT_NAME")) %>">
Username: <input type="text" name="username">
Password: <input type="text" name="password">
          <input type="submit" value="login">
</pre></form><%
    Else
            If (Request.Form("password") = "pass") Then
                    Session("username") = Request.Form("username")
            Else
                    Response.Write("Wrong password. Go back and try again!")
            End If
    End If
End If
If Not (IsEmpty(Session("username"))) Then
    Response.Write("<h3>Hello " + Session("username") + "!</h3>")
  If (Session("counter") > 0) Then
    Response.Write("<p>You were already here " & Session("counter") & " times!</p>" )
  End If
    Session("counter") = Session("counter") + 1

  If Not(isEmpty(Session("date"))) Then
    Response.Write("<p>Last visit: " & Session("date") & "</p>")
  End If
    Session("date") = MonthName(month(Now)) & " " & day(Now) & ", " & year(Now) & " " & Time
    Response.Write("<hr/>")
    Response.Write("Here comes whatever personalized application (WebMail, Calendar, Forum, Chat, Portal, E-Learning Platform, DB)")
End If
Response.Write("</html></body>")
%>
```

Login Form

Check password

Sample personalized ASP-Application (with AAI)

SWITCH
The Swiss Education & Research Network

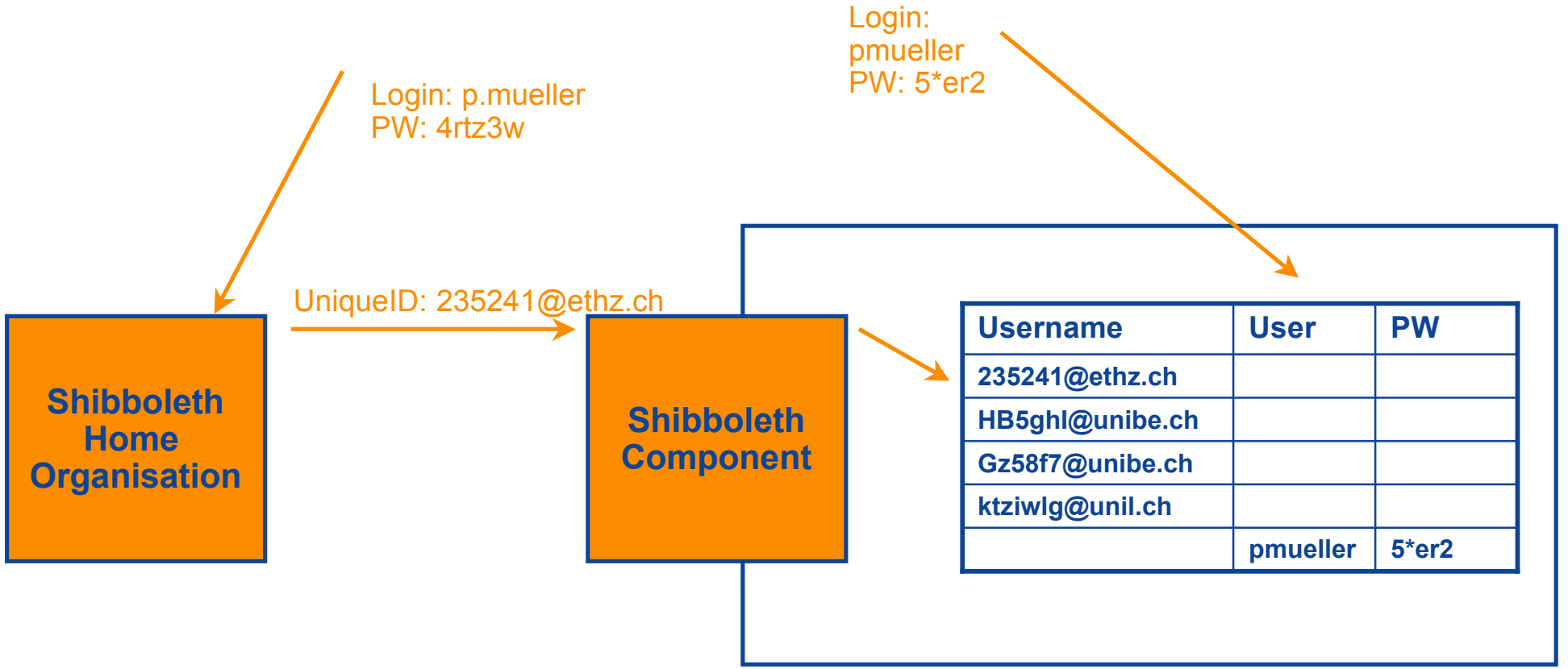
```
<%
Dim uniqueID, surname, givenname

If Not(Session("counter") > 0) Then
  Session("counter") = 0
End If
Response.Charset="UTF-8"
Response.Write ("<?xml version=""1.0"" encoding=""UTF-8""?>" & _
  "<!DOCTYPE html PUBLIC ""-//W3C//DTD XHTML 1.1//EN""" & _
  """http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd"">" & _
  "<html xmlns=""http://www.w3.org/1999/xhtml"" xml:lang=""en"">")

Set uniqueID = Request.ServerVariables("HTTP_SHIB_SWISSEP_UNIQUEID")
If (isEmpty(uniqueID)) Then
  Response.Write("Attribute (SwissEduPerson-) 'UniqueID' is missing.")
  Response.Write("<br/>Please contact the administrator of your AAI Home Organisation.")
Else
' Read Shibboleth attributes from HTTP server
  Set surname = Request.ServerVariables("HTTP_SHIB_PERSON_SURNAME")
  Set givenname = Request.ServerVariables("HTTP_SHIB_INETORGPERSON_GIVENNAME")

  If (isEmpty(surname) OR isEmpty(givenname)) Then
    Response.Write("<h3>Hello " & uniqueID & "!</h3>")
  Else
    Response.Write("<h3>Hello ")
    Response.Write((givenname) & " " & surname)
    Response.Write("!</h3>")
  End If

  If (Session("counter") > 0) Then
    Response.Write("<p>You were already here " & Session("counter") & " times!</p>" )
  End If
    Session("counter") = Session("counter") + 1

  If Not(isEmpty(Session("date"))) Then
    Response.Write("<p>Last visit: " & Session("date") & "</p>")
  End If
    Session("date") = MonthName(month(Now)) & " " & day(Now) & ", " & year(Now) & " " & Time
    Response.Write("<hr/>")
    Response.Write("Here comes whatever personalized application (WebMail, Calendar, Forum, Chat, Portal, E-Learning Platform, DB)")
End If
Response.Write("</html></body>")
%>
```

Check attributes

Use attributes

Personalized System, For Shib & non-Shib Users

SWITCH
The Swiss Education & Research Network



Summary

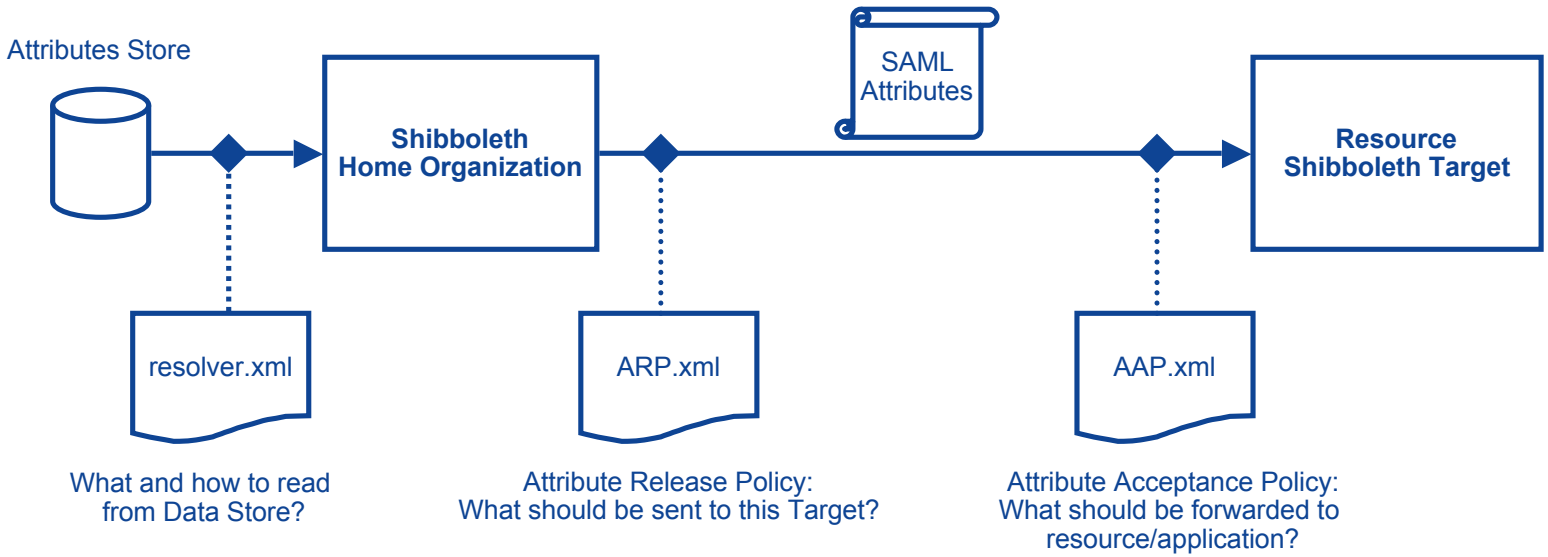
SWITCH
The Swiss Education & Research Network

	Apache	IIS
Static Content	Fine grained AuthZ Shibbolization straighforward	Only “valid_user” AuthZ for static content Shibbolization straighforward
Dynamic Content (Web Applications written in PHP, ASP, Perl, Java [running on Tomcat or other App-Servers], …)	AuthZ by Web Server (see above) and/or by Application Shibbolization by Adaptation of Code	

Attribute Transmission

Valéry Tschopp, <tschopp@switch.ch>

AAI Attribute Transmission



List of AAI Attributes and HTTP Headers

SWITCH
The Swiss Education & Research Network

AAI Attributes	HTTP Headers
swissEduPersonUniqueID	HTTP_SHIB_SWISSEP_UNIQUEID
surname	HTTP_SHIB_PERSON_SURNAME
givenName	HTTP_SHIB_INETORGPERSON_GIVENNAME
swissEduPersonHomeOrganization	HTTP_SHIB_SWISSEP_HOMEORGANIZATION
swissEduPersonHomeOrganizationType	HTTP_SHIB_SWISSEP_HOMEORGANIZATIONTYPE
eduPersonAffiliation	HTTP_SHIB_EP_AFFILIATION
mail	HTTP_SHIB_INETORGPERSON_MAIL
postalAddress	HTTP_SHIB_ORGPERSON_POSTALADDRESS
telephoneNumber	HTTP_SHIB_PERSON_TELEPHONENUMBER
swissEduPersonStudyBranch3	HTTP_SHIB_SWISSEP_SWISSEDUPERSONSTUDYBRANCH3
swissEduPersonStudyLevel	HTTP_SHIB_SWISSEP_SWISSEDUPERSONSTUDYLEVEL
swissEduPersonStaffCategory	HTTP_SHIB_SWISSEP_SWISSEDUPERSONSTAFFCATEGORY
swissEduPersonBirthdate	HTTP_SHIB_SWISSEP_DATEOFBIRTH
swissEduPersonGender	HTTP_SHIB_SWISSEP_GENDER
preferredLanguage	HTTP_SHIB_INETORGPERSON_PREFERREDLANGUAGE
homePostalAddress	HTTP_SHIB_INETORGPERSON_HOMEPOSTALADDRESS
homePhone	HTTP_SHIB_INETORGPERSON_HOMEPHONE
mobileTelephoneNumber	HTTP_SHIB_INETORGPERSON_MOBILE
swissEduPersonStudyBranch1	HTTP_SHIB_SWISSEP_SWISSEDUPERSONSTUDYBRANCH1
swissEduPersonStudyBranch2	HTTP_SHIB_SWISSEP_SWISSEDUPERSONSTUDYBRANCH2
swissEduPersonOrgDN	HTTP_SHIB_EP_ORGDN
swissEduPersonOrgUnitDN	HTTP_SHIB_EP_ORGUNITDN
swissEduPersonEntitlement	HTTP_SHIB_EP_ENTITLEMENT

SWITCH

The Swiss Education & Research Network

Deployment

Valéry Tschopp, <tschopp@switch.ch>

Deployment Guides

SWITCH
The Swiss Education & Research Network

- **Shibbolized Apache:**
  AAI Resource: Apache + Shibboleth Target 1.2
  http://www.switch.ch/aai/deployment.html
  http://shibboleth.internet2.edu

- **SWITCHaai Federation Configuration Files (Shibboleth Target 1.2)**
  - shibboleth.switchaai.xml
  - trust.switchaai.xml
  - sites.switchaai.xml
  - AAP.switchaai.xml

- **Samples Files (Apache 1.3)**
  - ca-bundle.switchaai.crt
  - apache.switchaai
  - httpd.switchaai.conf

SWITCHaai Settings

- shibboleth.switchaai.xml
  - Identifier in <Applications>
    providerId=urn:mace:switch.ch:SWITCHaai:pilot:<HOSTNAME>
  - SWITCHpki Server Certificate Location in <Credentials>
    /etc/apache/ssl.key/<HOSTNAME>.key
    /etc/apache/ssl.crt/<HOSTNAME>.crt
  - Error Pages Customization in <Errors>
    supportContact=<CONTACT_EMAIL>
    HTML pages, logo and stylesheet
  - SWITCHaai Federation Metadata
    <FederationProvider> for sites.switchaai.xml
    <TrustProvider> for trust.switchaai.xml
    <AAPProvider> for AAP.switchaai.xml

What you need to get...

SWITCH
The Swiss Education & Research Network

- **Shibboleth Install Package:**

  <http://www.switch.ch/aai/docs/shibboleth/internet2/1.2/>

- **Sample configuration files for SWITCHaai**

  <http://www.switch.ch/aai/docs/shibboleth/SWITCH/1.2/>

- **SWITCHpki certificate for your Web Server**

  <http://www.switch.ch/aai/certificates.html>

Deployment Guides

SWITCH
The Swiss Education & Research Network

- **Shibbolized IIS Web Server**

  AAI Resource: IIS Web Server + Shibboleth Target 1.2

  <http://shibboleth.internet2.edu>

  <http://www.switch.ch/aai/deployment.html>

- **SWITCHaai Federation Configuration Files (Shibboleth Target 1.2)**
  - shibboleth.switchaai.xml
  - trust.switchaai.xml
  - sites.switchaai.xml
  - AAP.switchaai.xml

- **Samples Files (IIS)**
  - ca-bundle.switchaai.crt

SWITCHaai Settings, I

- shibboleth.xml
  - Identifier in /Applications
    providerId=urn:mace:switch.ch:SWITCHaai:pilot:{HOSTNAME}
  - SWITCHaai Federation Metadata in /Applications/..
    AAPProvider C:/opt/shibboleth/etc/shibboleth/AAP.switchaai.xml
    FederationProvider C:/opt/shibboleth/etc/shibboleth/sites.switchaai.xml
    TrustProvider C:/opt/shibboleth/etc/shibboleth/trust.switchaai.xml
  - SWITCHpki Server Certificate Location in /CredentialsProvider/Credentials
    C:/opt/shibboleth/etc/shibboleth/{HOSTNAME}.key
    C:/opt/shibboleth/etc/shibboleth/{HOSTNAME}.crt

SWITCHaai Settings, II

- **shibboleth.xml** (… continued)
  - SHIRE-URL in /Applications/Sessions
  - Error Pages Customization in /Applications/Errors
    supportContact={CONTACT_EMAIL}
    HTML pages, logo and stylesheet
  - Protected Web Locations /SHIRE/RequestMapProvider/RequestMap
  - IIS Site ID Mapping /SHIRE/Implementation/ISAPI

Questions ?

SWITCH
The Swiss Education & Research Network

Q & A

http://www.switch.ch/aai

aai@switch.ch