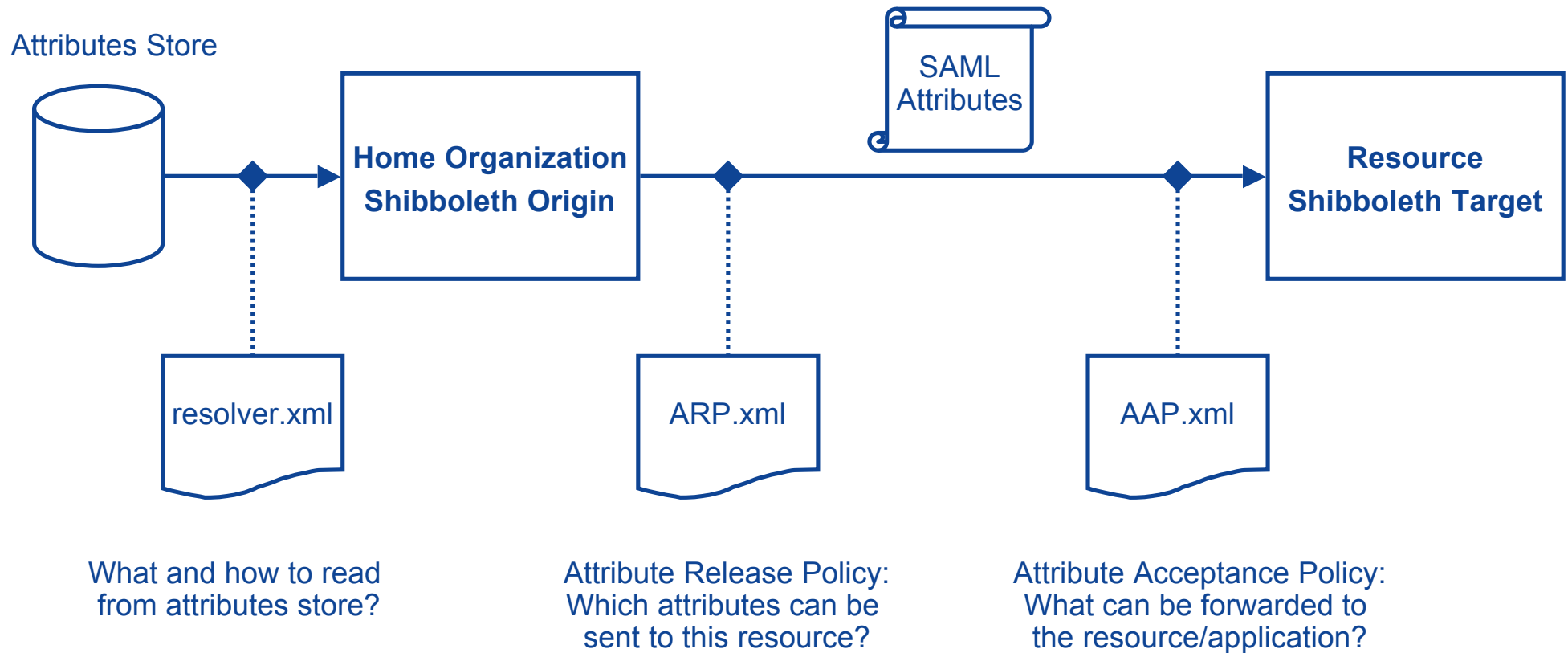

SWITCH

The Swiss Education & Research Network

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

Valéry Tschopp <tschopp@switch.ch>

AAI Attribute Transmission



AAI Attributes

HTTP Headers

swissEduPersonUniqueID	HTTP_SHIB_SWISSEP_UNIQUEID
surname	HTTP_SHIB_PERSON_SURNAME
givenName	HTTP_SHIB_INETORGPERSO_N_GIVENNAME
swissEduPersonHomeOrganization	HTTP_SHIB_SWISSEP_HOMEORGANIZATION
swissEduPersonHomeOrganizationType	HTTP_SHIB_SWISSEP_HOMEORGANIZATIONTYPE
eduPersonAffiliation	HTTP_SHIB_EP_AFFILIATION
mail	HTTP_SHIB_INETORGPERSO_N_MAIL
postalAddress	HTTP_SHIB_ORGPERSO_N_POSTALADDRESS
telephoneNumber	HTTP_SHIB_PERSON_TELEPHONENUMBER
swissEduPersonStudyBranch3	HTTP_SHIB_SWISSEP_SWISSE_DUPERSO_NSTUDYBRANCH3
swissEduPersonStudyLevel	HTTP_SHIB_SWISSEP_SWISSE_DUPERSO_NSTUDYLEVEL
swissEduPersonStaffCategory	HTTP_SHIB_SWISSEP_SWISSE_DUPERSO_NSTAFFCATEGORY
swissEduPersonBirthdate	HTTP_SHIB_SWISSEP_DATEOFBIRTH
swissEduPersonGender	HTTP_SHIB_SWISSEP_GENDER
preferredLanguage	HTTP_SHIB_INETORGPERSO_N_PREFERREDLANGUAGE
homePostalAddress	HTTP_SHIB_INETORGPERSO_N_HOMEPOSTALADDRESS
homePhone	HTTP_SHIB_INETORGPERSO_N_HOMEPHONE
mobileTelephoneNumber	HTTP_SHIB_INETORGPERSO_N_MOBILE
swissEduPersonStudyBranch1	HTTP_SHIB_SWISSEP_SWISSE_DUPERSO_NSTUDYBRANCH1
swissEduPersonStudyBranch2	HTTP_SHIB_SWISSEP_SWISSE_DUPERSO_NSTUDYBRANCH2
swissEduPersonOrgDN	HTTP_SHIB_EP_ORGDN
swissEduPersonOrgUnitDN	HTTP_SHIB_EP_ORGUNITDN
swissEduPersonEntitlement	HTTP_SHIB_EP_ENTITLEMENT

Exporting AAI-Attributes to Applications with Apache

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

shibboleth.xml

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

HTTP Headers
(e.g. HTTP_SHIB_SWISSEP_UNIQUEID)

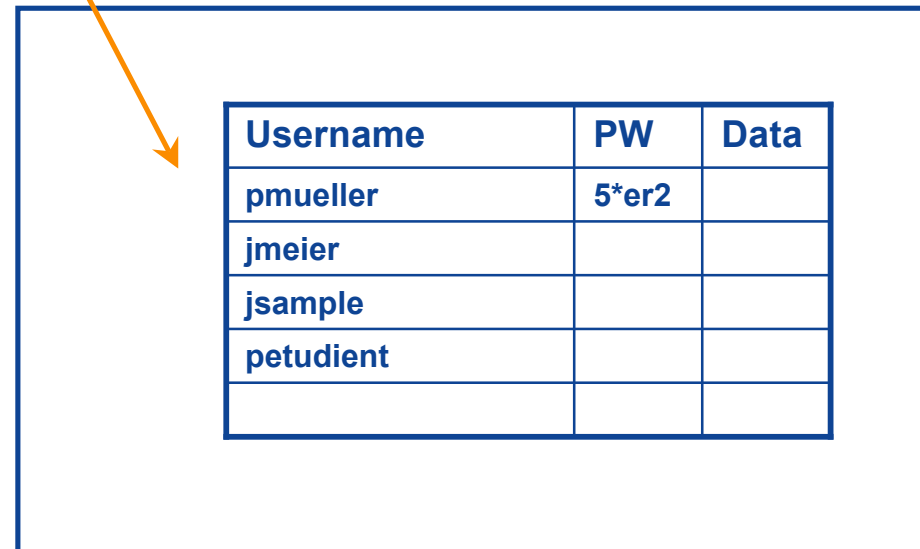
Use attribute in PHP:

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

Use attribute in ASP:

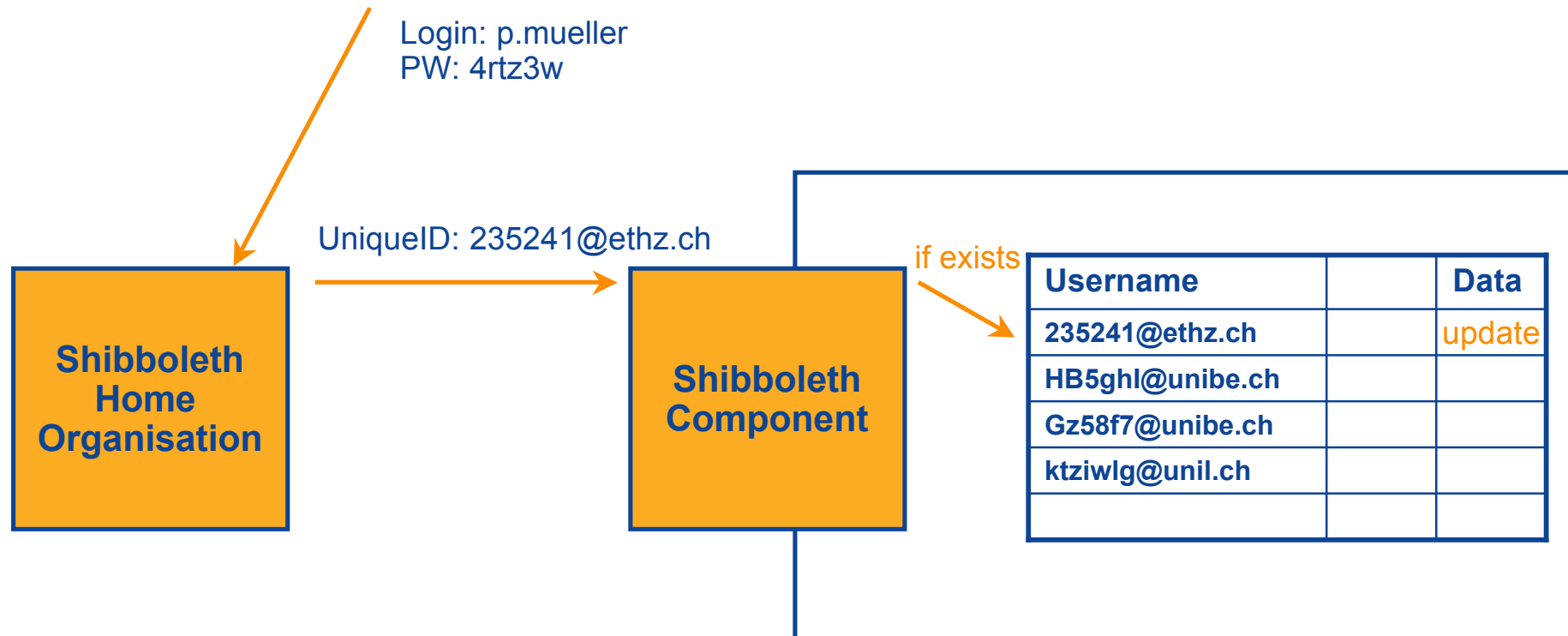
```
<%
  Set uniqueID = Request.ServerVariables("HTTP_SHIB_SWISSEP_UNIQUEID")
  ... %>
```

Login: pmueller
PW: 5*er2

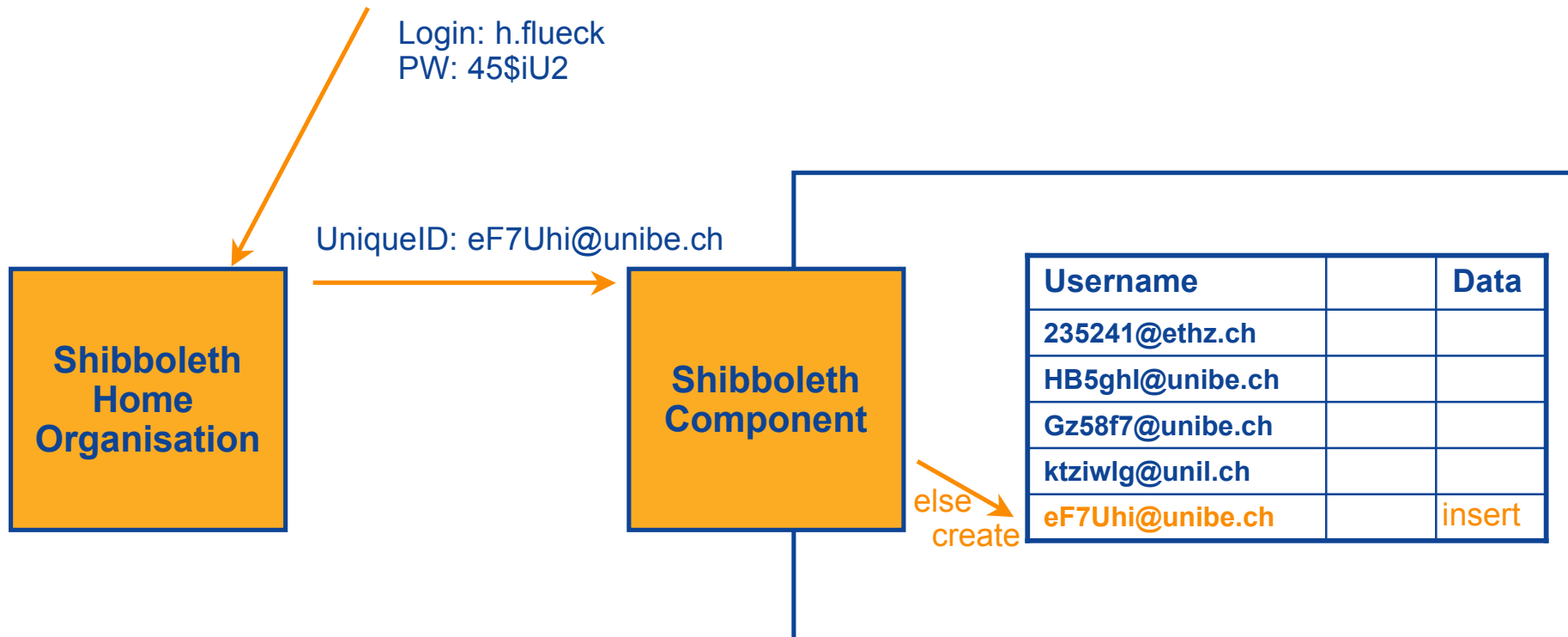


Username	PW	Data
pmueller	5*er2	
jmeier		
jsample		
petudiant		

Personalized System, Shibbolized



Personalized System, Shibbolized, Creating New Users



Sample personalized PHP-Application (without AAI)

```
<?php
  session_name('non-shibboleth');
  session_start();
  session_register('user');
  session_register('counter');
  session_register('date');

  echo "<html><body>";

  if (empty($user)) {
    if (empty($_GET['username'])) {
      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 {
      if ($_GET['password']=="pass") {
        $user = $_GET['username'];
      } else {
        echo "Wrong password. Go back and try again!";
      }
    }
  }

  if (!empty($user)) {
    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";
    $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>";
?>
```

```
// Use PHP session cookies
// Associate the variable $user with the session
// Associate the variable $counter with the session
// Associate the variable $date with the session
```

```
// No user-session
// No username submitted -> display login form
```

Login Form

```
// Check password
// Store username in session
```

Check password

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

Sample personalized PHP-Application (with AAI)

```
<?php
  session_name('shibboleth');
  session_start();
  session_register('counter');
  session_register('date');

  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_INETORGPPERSON_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)

```
<%
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.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)

```
<%
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_INETORGPERSOON_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

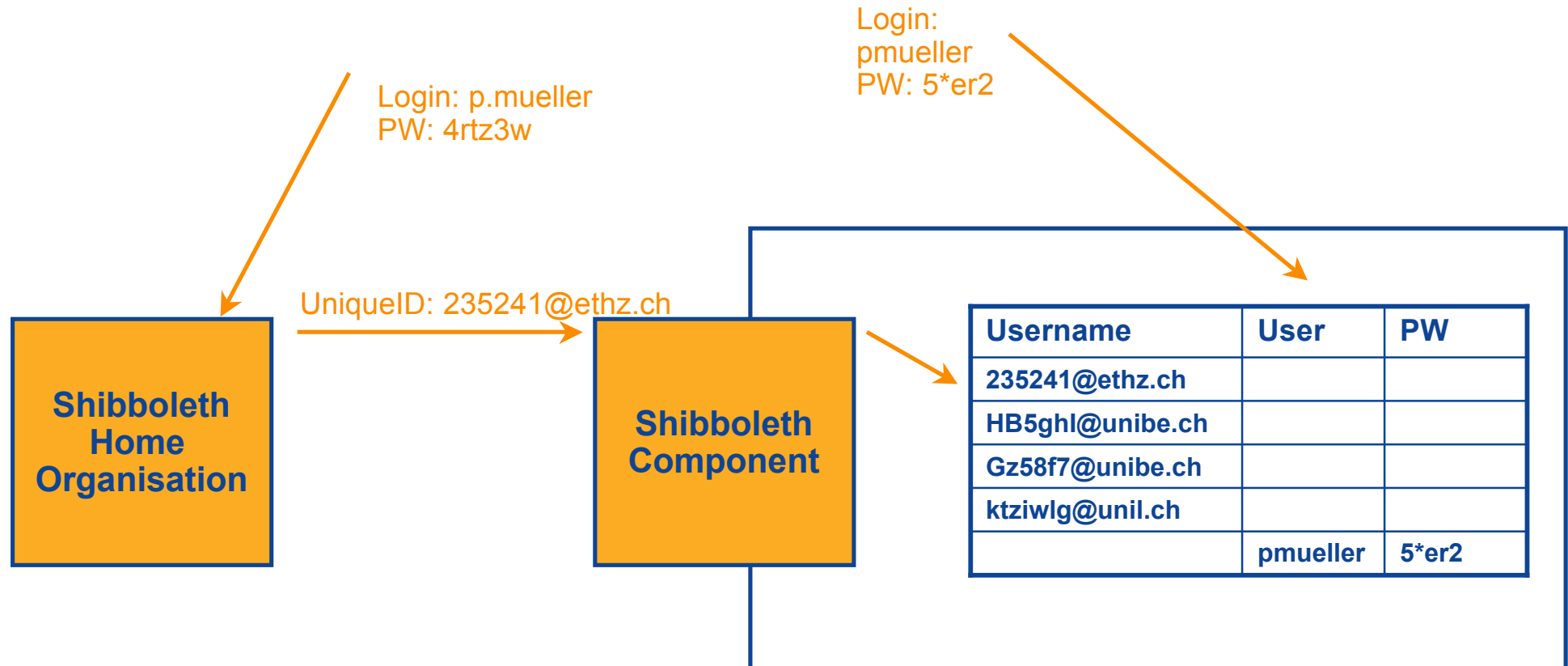
If (Session("counter") > 0) Then
    Response.Write("<p>You were already here " & Session("counter") & " times!</p>" )
End If
    Session("counter") = Session("counter") + 1

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



	Apache	IIS
Static Content	Fine grained AuthZ Shibbolization straightforward	Only “valid_user” AuthZ for static content Shibbolization straightforward
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	

Q & A

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

aai@switch.ch