SWITCH

The Swiss Education & Research Network

Integration of Web-Applications in AAI

Patrik Schnellmann, <schnellmann@switch.ch>

Exporting AAI-Attributes to Applications

SWITCH
The Swiss Education & Research Network

shibboleth.xml

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

Environment-Variables
(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")
... %>
```

Snippet from AAP.xml

SWITCH
The Swiss Education & Research Network

Attributes in the Environment-Variables are controlled through AAP.xml

```
<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

AAI-based User-Management in personalized Web-Applications

Patrik Schnellmann <schnellmann@switch.ch>

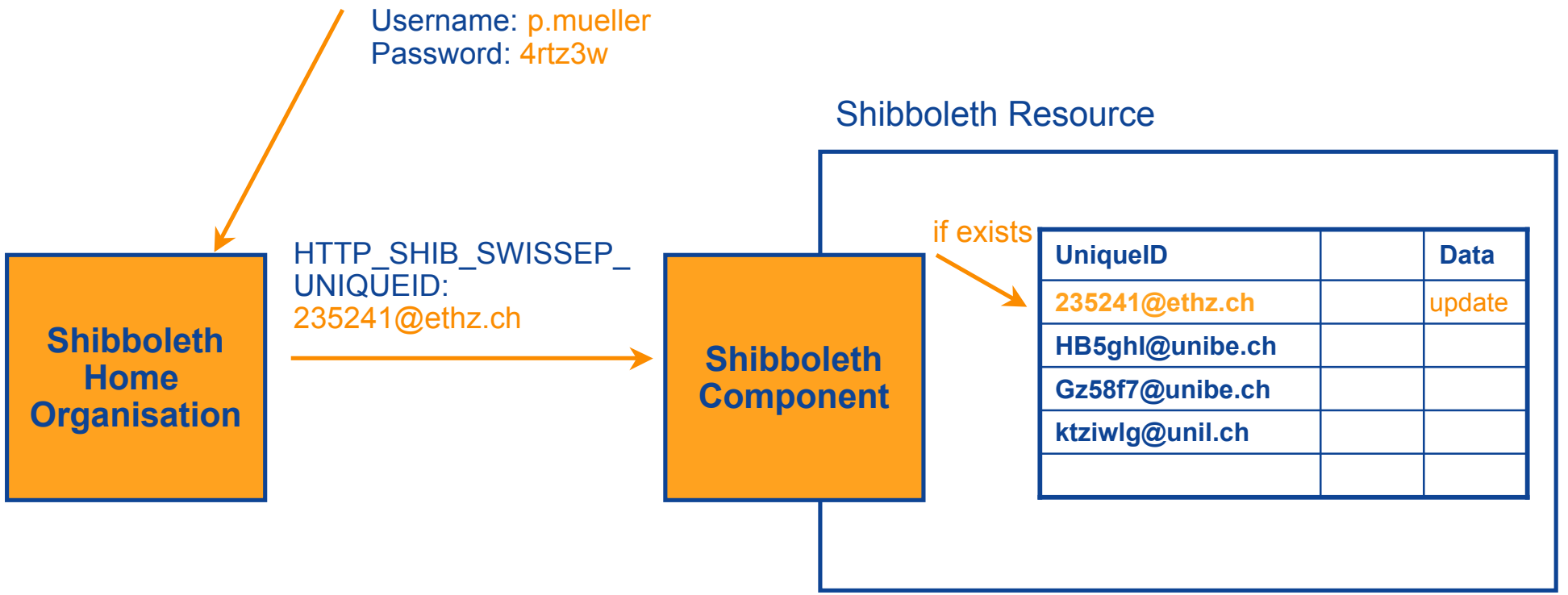
Personalized System, Non-Shibbolized

SWITCH
The Swiss Education & Research Network

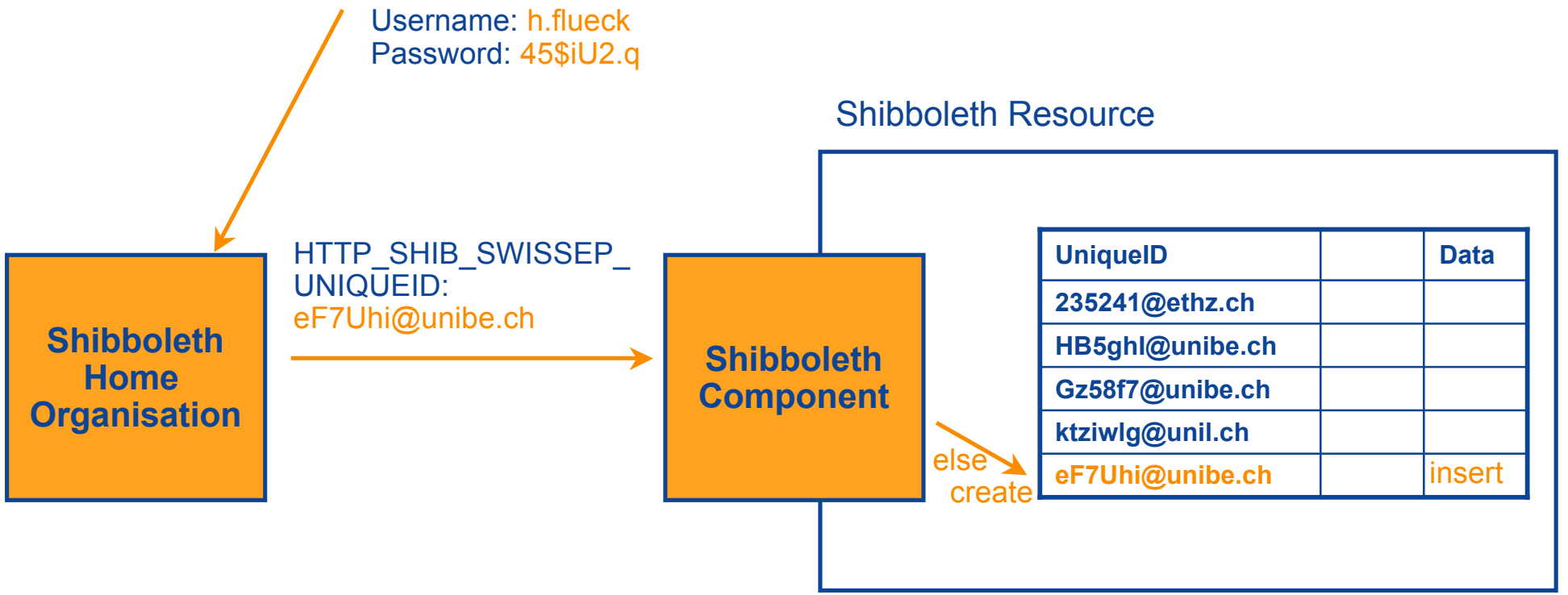
Username: pmueller
PW: 5*er2x+p

Username	Password	Data
pmueller	5*er2x+p	
jmeier		
jsample		
petudiant		

Personalized System, Shibbolized

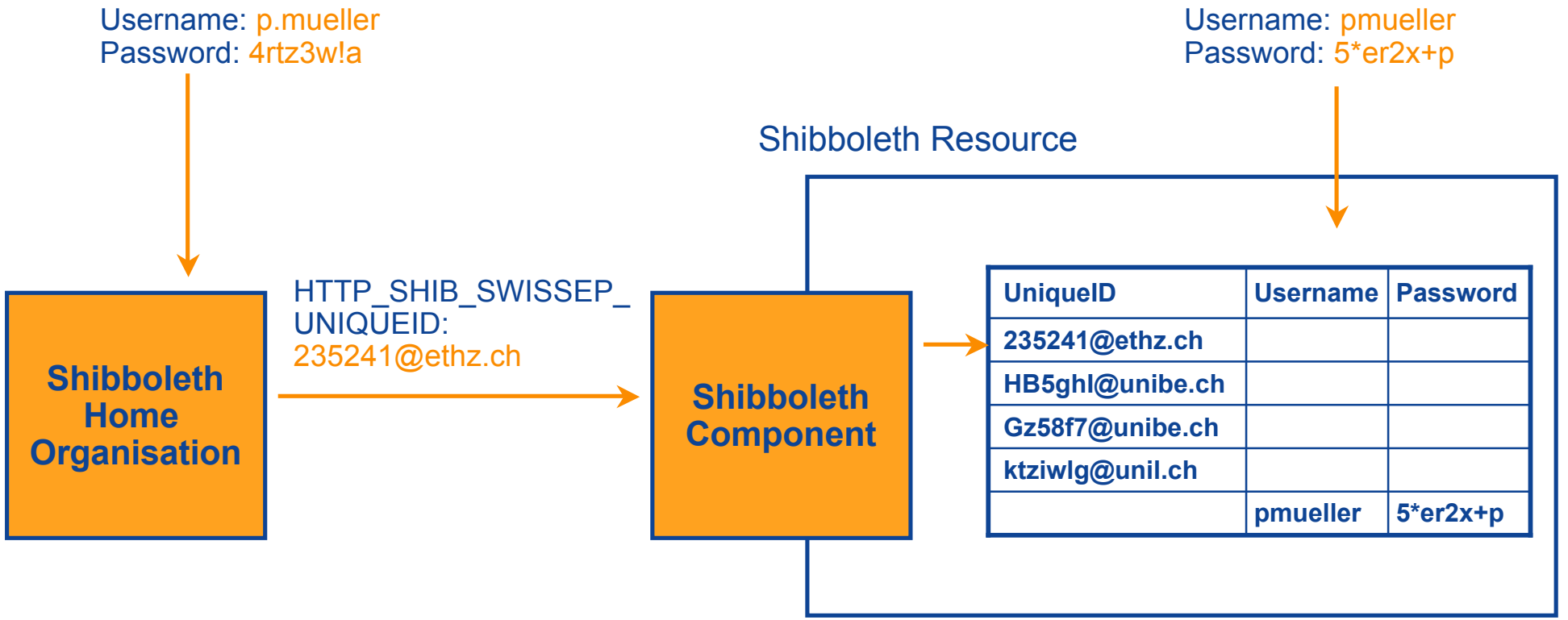


Personalized System, Shibbolized, Creating New Users



Personalized System, For Shib & non-Shib Users

SWITCH
The Swiss Education & Research Network



Sample personalized App (without AAI) in PHP

SWITCH
The Swiss Education & Research Network

```php
<?php
session_name('nonshib');                                    // Set session name
session_start();                                            // Use PHP session cookies
if (!isset($_SESSION['counter'])) {                         // Set session counter variable, if not set already
  $_SESSION['counter'] = 0;
}
print '<?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"><body>';

  if (empty($_SESSION['username'])) {                       // No user-session
    if (empty($_POST['username'])) {                        // No username submitted, show login form
?>
<pre><form method="POST" action="<?php
    print $_SERVER['SCRIPT_NAME'];
?>">Username: <input type="text" name="username">
Password: <input type="password" name="password">
          <input type='submit' value="login">
</pre></form><?php
    } else {                                                // Check password
      if ($_POST['password'] == "pass") {
        $_SESSION['username'] = $_POST['username'];         // Store username in session
      } else {
        print "Wrong password. Go back and try again!";
      }
    }
  }
  if (!empty($_SESSION['username'])) {                      // User is identified, show personalized page
    print "<h3>Hello " . $_SESSION['username']  . "!</h3>";
    if (!empty($_SESSION['counter'])) {
        print "<p>You were already here " . $_SESSION['counter'] . " times!";
    }
    $_SESSION['counter']++;
    if (!empty($_SESSION['date'])) {
        print "<p>Last visit: ". $_SESSION['date'];         // Show date of last visit
    }
    $_SESSION['date']= date("F j, Y, g:i a");
    print "<hr/>";
    print "Here comes whatever personalized application (WebMail, Calendar, Forum, Chat, Portal, E-Learning Plattform, DB)";
  }
  print "</body></html>";
?>
```

Login Form

Check password

http://teon.switch.ch/public/sample.php

Sample personalized App (without AAI) in ASP

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

http://teon.switch.ch/public/sample.asp

Sample personalized App (with AAI) in PHP

SWITCH
The Swiss Education & Research Network

```
<?php
session_start();                                          // Use PHP session cookies

if (!isset($_SESSION['counter'])) {                       // Set session counter variable, if not set already
  $_SESSION['counter'] = 0;
}
print '<?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"><body>';

$uniqueID = $_SERVER['HTTP_SHIB_SWISSEP_UNIQUEID'];       // Read Shibboleth attribute for Unique ID
if (empty($uniqueID)) {                                   // Unique ID attribute is missing
  print "Attribute (SwissEduPerson-) 'UniqueID' is missing.";
  print "<br/>Please contact the administrator of your AAI Home Organisation.";
}
else {
  $surname = $_SERVER['HTTP_SHIB_PERSON_SURNAME'];        // Read Shibboleth attributes for surname/givenname
  $givenname = $_SERVER['HTTP_SHIB_INETORGPERSON_GIVENNAME'];

  if (empty($surname) or empty($givenname)) {
            print "<h3>Hello " . $uniqueID . "!</h3>";
  }
  else {
      print "<h3>Hello " . $givenname . " " . $surname;
      print " (" . $uniqueID . ")!</h3>";
  }

  if ($_SESSION['counter'] > 0) {
    print "<p>You were already here ";
    print $_SESSION['counter'] . " times!</p>";           // Show number of visits
  }
  $_SESSION['counter']++;                                 // Increment session variable for number of visits
  if (isset($_SESSION['date'])) {
    print "<p>Last visit: " . $_SESSION['date'];          // Show date of last visit
  }
  $_SESSION['date'] = date("F j, Y, g:i a");
  print "<hr/>";
  print "Here comes whatever personalized application (WebMail, Calendar, Forum, Chat, Portal, E-Learning Platform, DB)";
}
print "</html></body>";
?>
```

Check attributes

Use attributes

http://teon.switch.ch/secure/sample.php

Sample personalized App (with AAI) in ASP

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

http://teon.switch.ch/secure/sample.asp

Configuring Access Rules – How it could be done with Apache

Configuring Access Rules in Apache

SWITCH
The Swiss Education & Research Network

Access rules in httpd.conf or .htaccess

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

Any AAI user

```
<Location /restricted>
  AuthType shibboleth
  require uniqueID 235241@ethz.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.>