AAI Login Demo

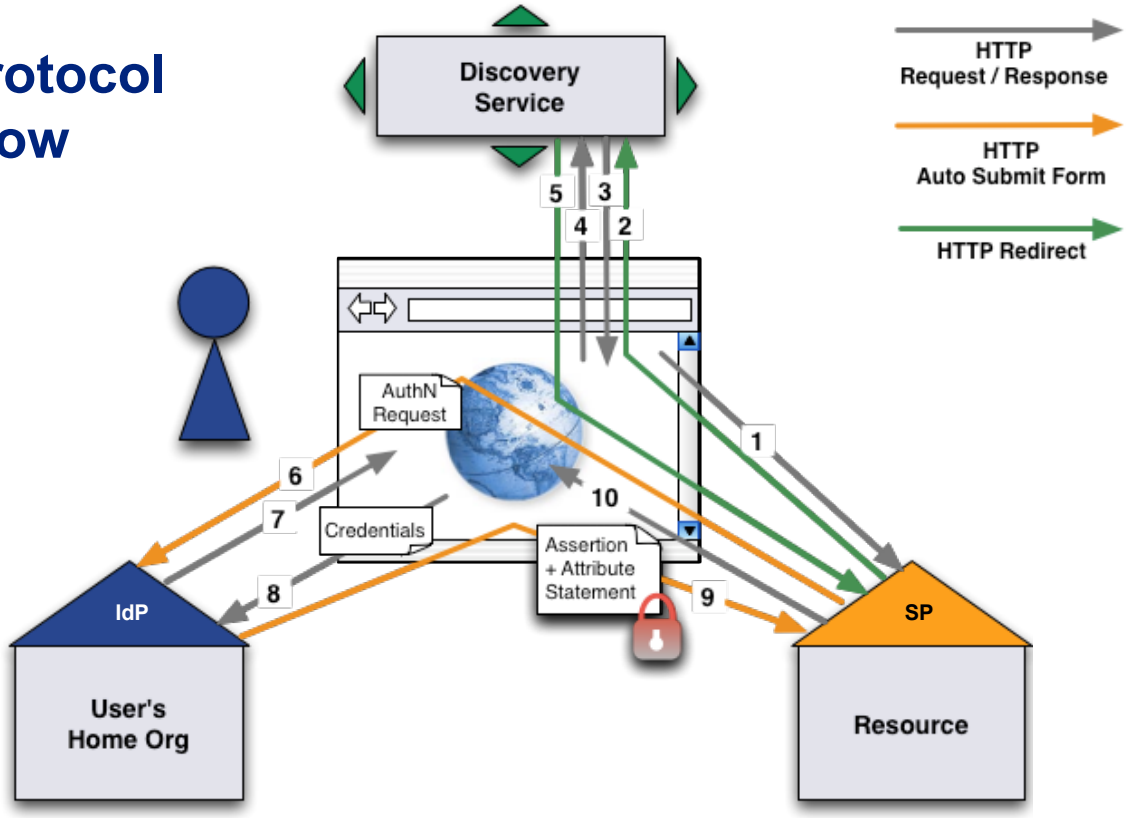
SWITCH

SWITCHaai Team
aai@switch.ch

Agenda

- Illustration of protocol flow
  SAML2, Web Browser SSO
- Live demonstration

Protocol Flow

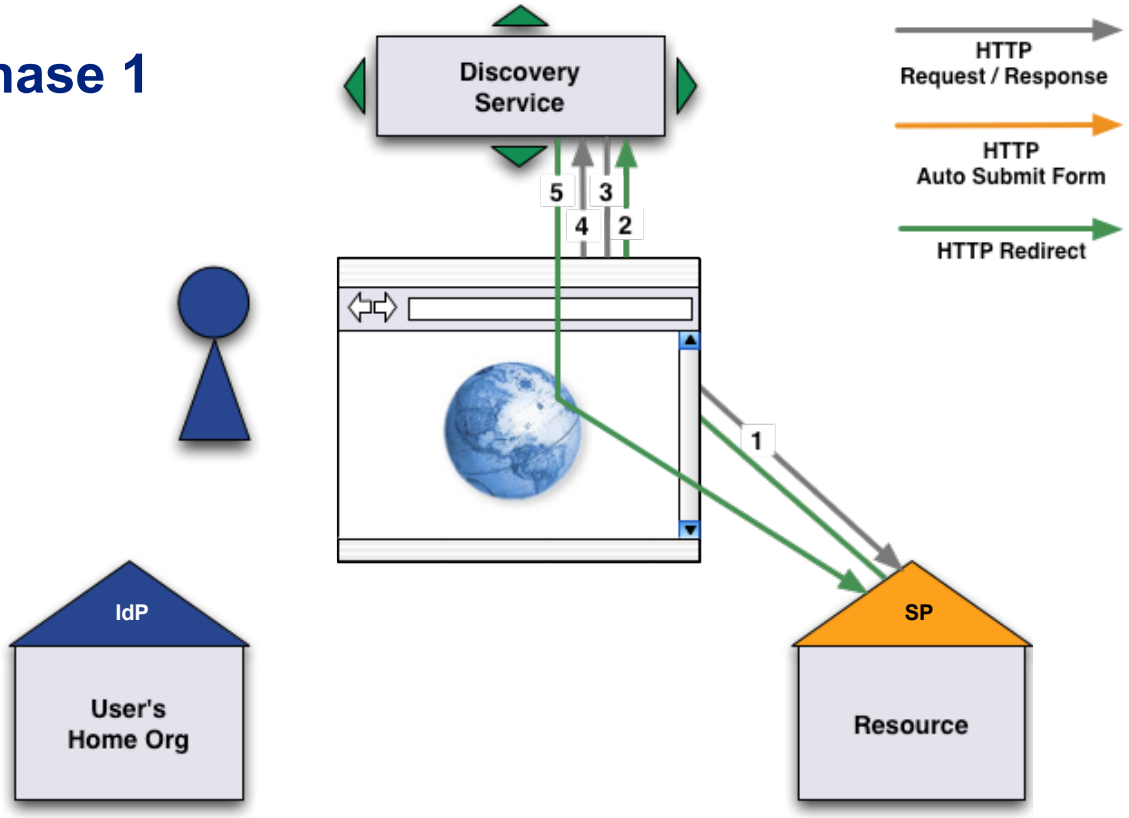


https://www.switch.ch/aai/demo/

Phase 1

First access to the Service Provider and Identity Provider discovery

Phase 1



First access to the Service Provider and Identity Provider discovery

① The user opens a web browser and accesses the Service Provider.

② The user is redirected to the Discovery Service by the Service Provider. Consequently, the web browser sends a new request to the Discovery Service.

③ The Discovery Service answers with the web page that allows the user to select an Identity Provider.

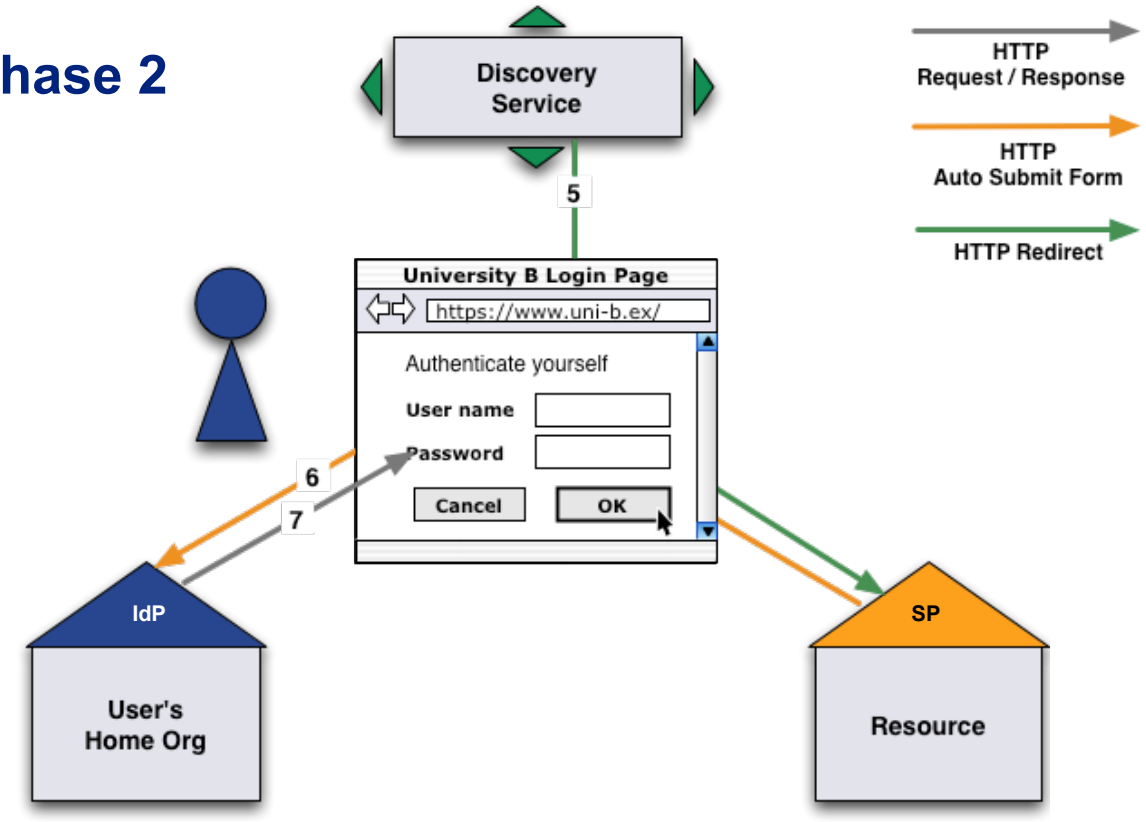
④ On the Discovery Service page, the user submits the Identity Provider selection.

⑤ The Discovery Service sends a redirect to the SP return destination, including the IdP selection.

Phase 2

Session initiation and authentication request

Phase 2



SAML AuthN Request

Plain HTML:

```
<html>
  <body onload="document.forms[0].submit()">
    <form method="POST" action="https://aai-demo-idp.switch.ch/idp/profile/SAML2/POST/SSO">
      <input type="hidden" name="RelayState" value="ss:mem:23e3a3b1268acd89dc226bb1ce0d0c6ba7ecf773"/>
      <input type="hidden" name="SAMLRequest"
          value="PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1scD0idXJuOm9hc2lzOm5h...
          ...YXRlPSIxIi8+PC9zYW1scDpBdXRoblJlcXVlc3Q+"/>
    </form>
  </body>
</html>
```

SAML AuthN Request (Base64 decoded)

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    AssertionConsumerServiceIndex="1"
    Destination="https://aai-demo-idp.switch.ch/idp/profile/SAML2/POST/SSO"
    ID="_f2f27516ec08af29501c749629b119d3"
    IssueInstant="2008-02-27T12:17:40Z"
    Version="2.0">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    https://aai-demo.switch.ch/shibboleth
  </saml:Issuer>
  <samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
      AllowCreate="1"/>
</samlp:AuthnRequest>
```


Session initiation and authentication request

⑤ The browser is redirected to the Service Provider by the Discovery Service.

⑥ The session initiator of the Service Provider creates an authentication request and returns it within an auto-submit-post-form to the browser.

The browser posts the SAML AuthN Request automatically to the Identity Provider using JavaScript.

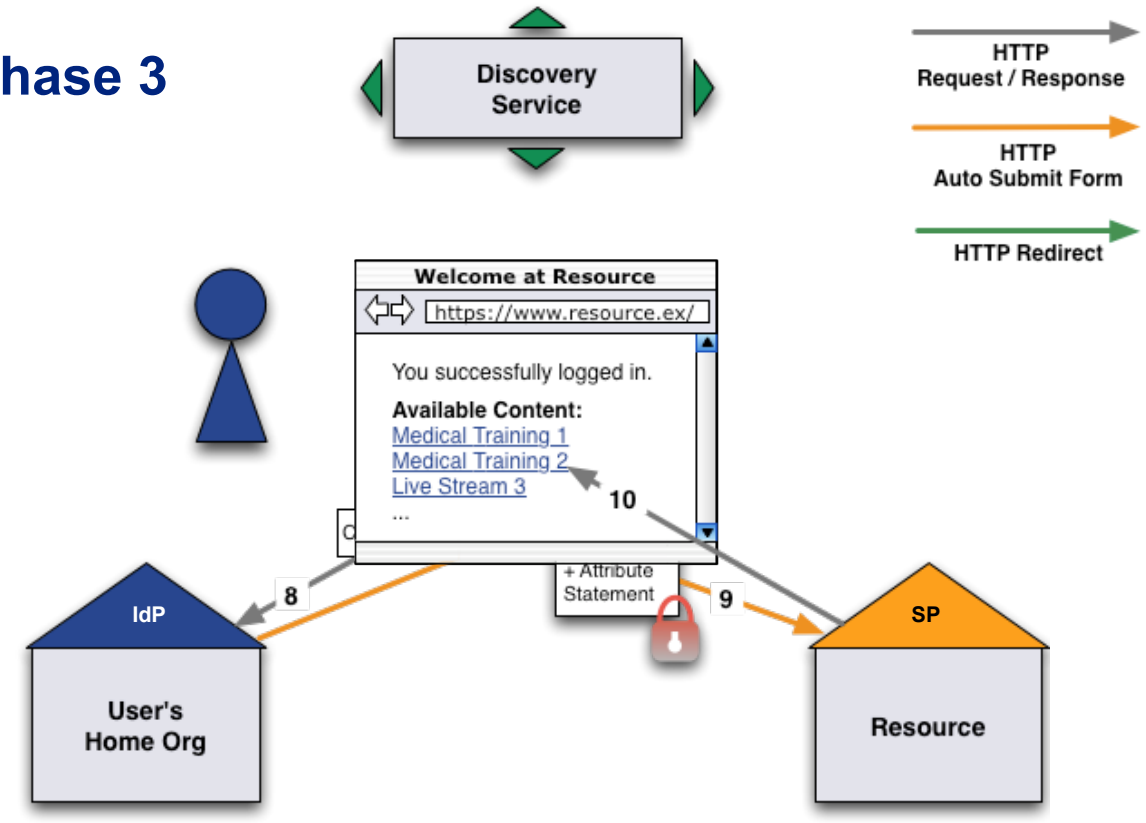
Session initiation and authentication request

⑦ The Identity Provider checks the authentication request. Because the user hasn't yet been authenticated, the Identity Provider sends a redirect to the appropriate login page (usually: Username/Password).

Phase 3

Authentication, attribute statement and access

Phase 3



SAML Assertion + Attribute Statement

Plain HTML

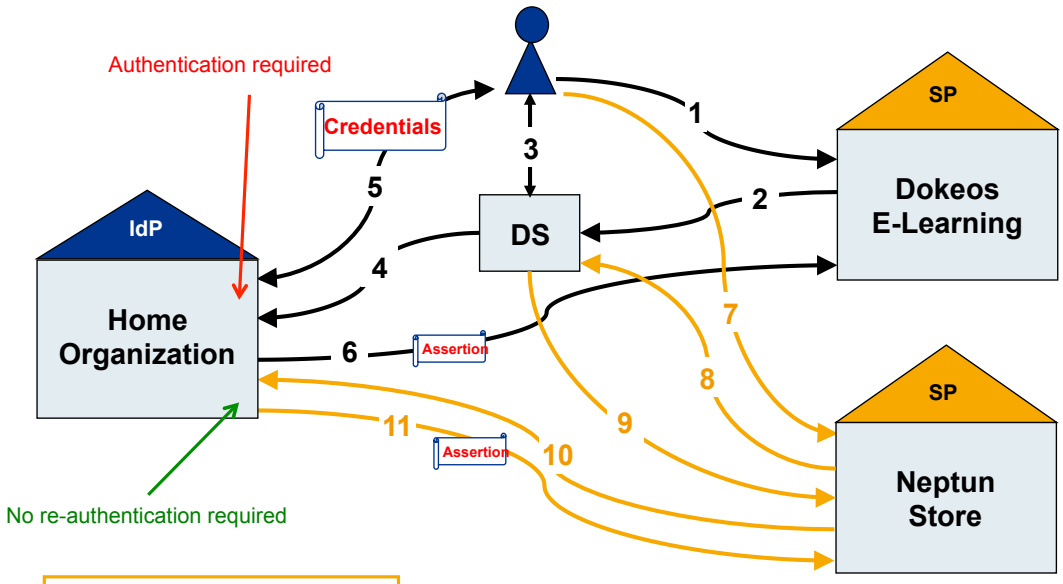
```
<html xml:lang="en">
  <body onload="document.forms[0].submit()">
    <form action="https://aai-demo.switch.ch/Shibboleth.sso/SAML2/POST" method="post">
      <div>
        <input type="hidden" name="RelayState" value="ss:mem:23e3a3b1268acd89dc226bb1ce0d0c6ba7ecf773"/>
        <input type="hidden" name="SAMLResponse"
            value="PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPHNhbWxwO8...
            ...vbj0iW1scDVlc+PC9zYW1scRGLsTgiPz4KPlc3U+"/>
      </div>
    </form>
  </body>
</html>
```

SAML Assertion + Attribute Statement

SAML Assertion + Attribute Statement, decrypted (Base64 decoded)

```
<saml:Assertion ...>
  <saml:Issuer ...>
    https://aai-demo-idp.switch.ch/idp/shibboleth
  </saml:Issuer>
  <saml:Subject ...>
    <saml:NameID ...>
      _e7b68a04488f715cda642fbdd90099f5
    </saml:NameID>
    [...]
  </saml:Subject>
  [...]
  <saml:AuthnStatement ...
      AuthnInstant="2008-02-27T12:20:06.991Z"
      SessionIndex="4m2ETlKYtvbNEmBzVNo3UHLuKSdo3HqTUqAmeZiar94="
      SessionNotOnOrAfter="2008-02-27T12:50:06.991Z">
    [...]
  </saml:AuthnStatement>
  <saml:AttributeStatement ...>
    [...] (Attributes)
  </saml:AttributeStatement>
</saml:Assertion>
```


Accessing multiple SPs



IdP: Identity Provider
SP: Service Provider
DS: Discovery Service

Links

The AAI Demo shows how AAI works.

https://www.switch.ch/aai/demo/

The AAI Attribute Viewer shows which attributes are released by an Identity Provider.

https://attribute-viewer.aai.switch.ch/