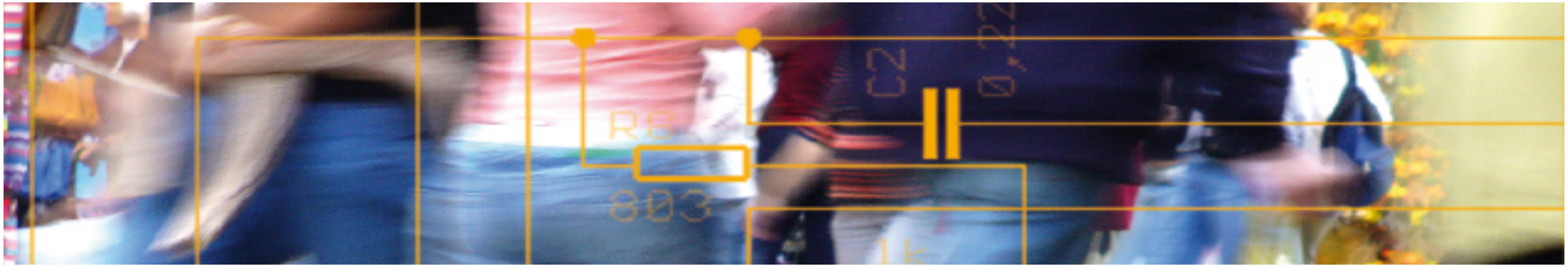
AAI Login Demo



SWITCH

Daniel Lutz
aai@switch.ch

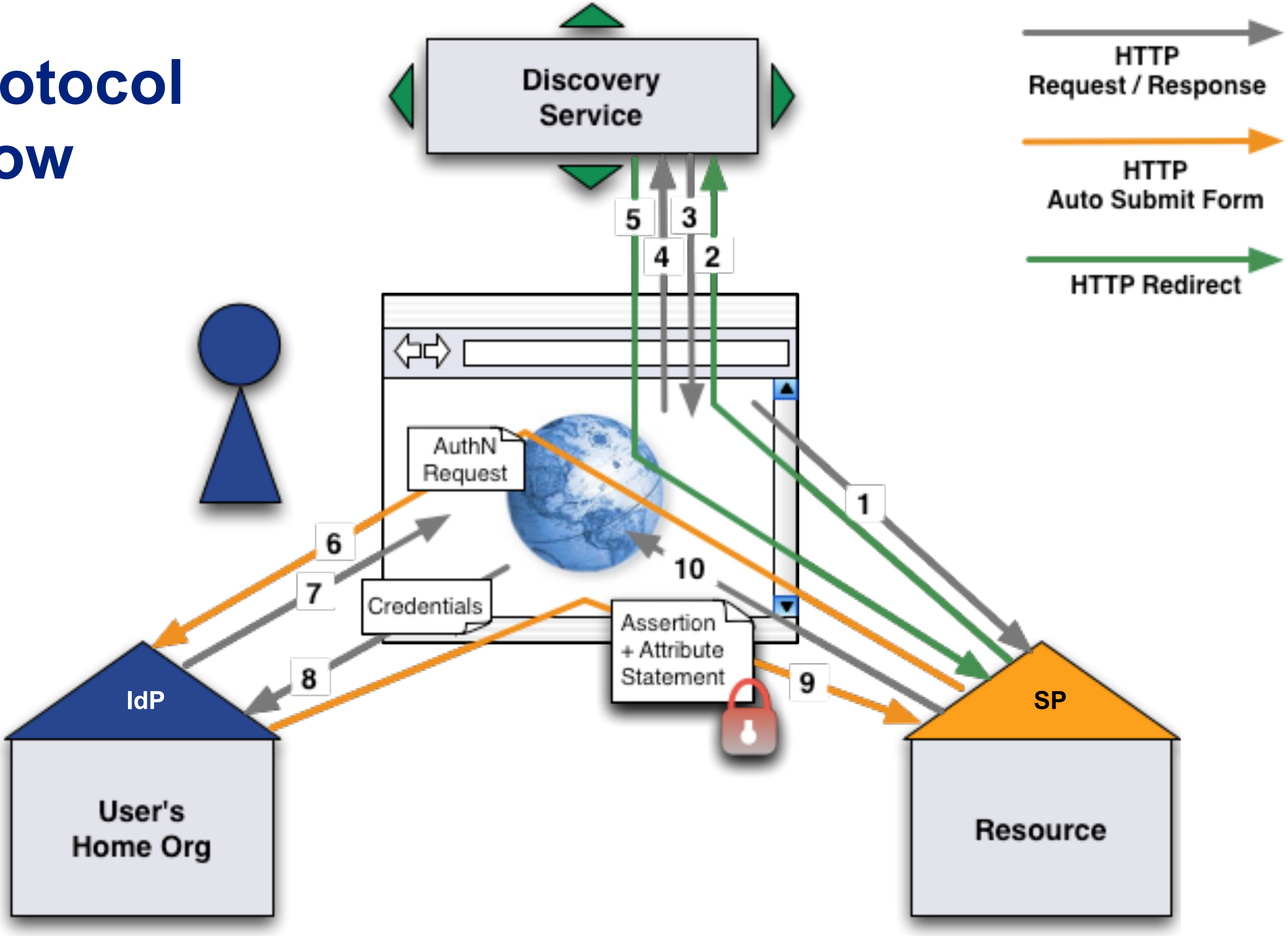
SWITCHaai Introduction Course
Bern, 1. March 2013

Agenda

- Illustration of protocol flow
  SAML2, Web Browser SSO

- Live demonstration

Protocol Flow

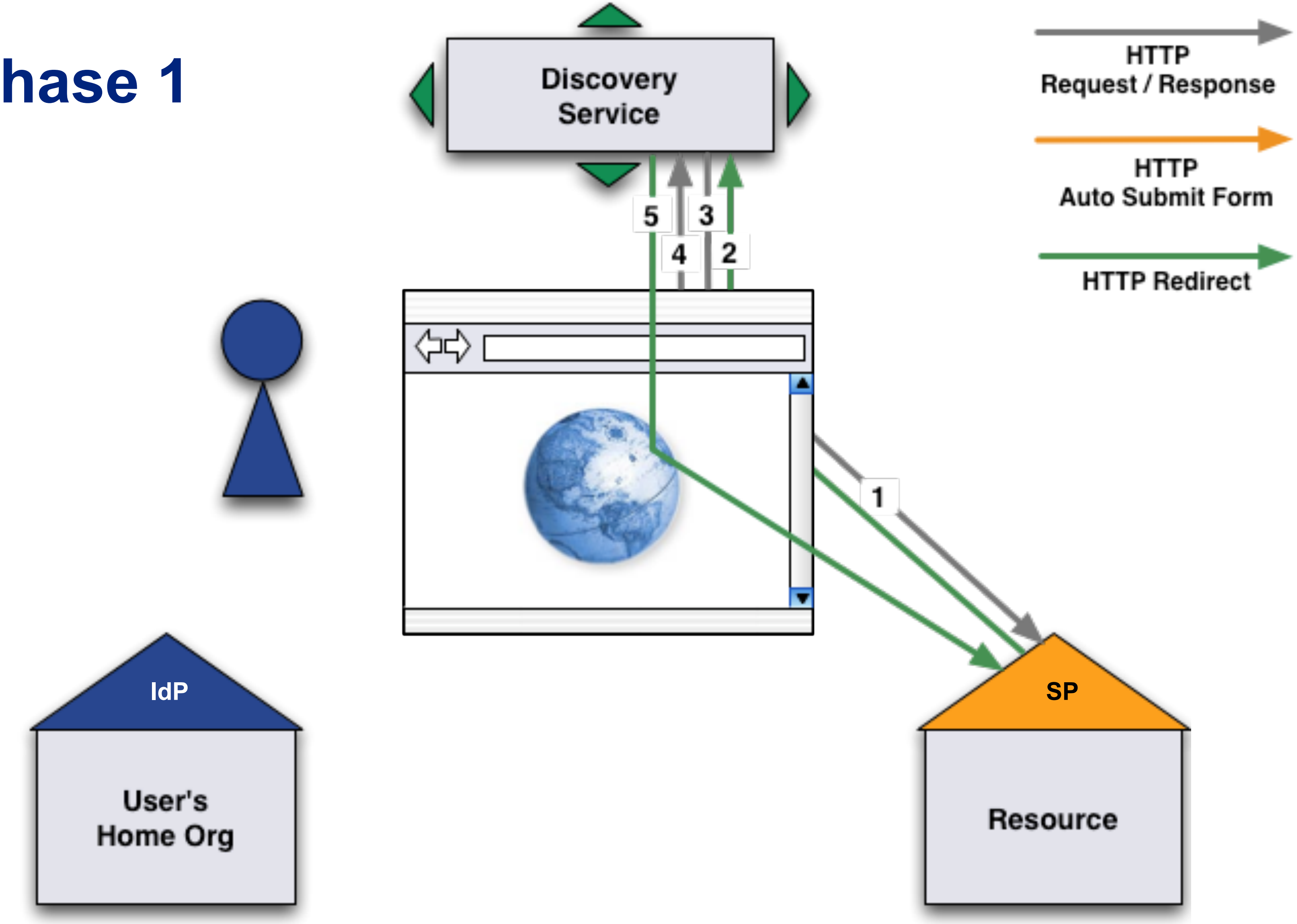


http://www.switch.ch/aai/demo/

Phase 1

First access to the Service Provider and Identity Provider discovery

Phase 1


Discovery Service
5
4
3
2
1
IdP
User's Home Org
SP
Resource
HTTP Request / Response
HTTP Auto Submit Form
HTTP Redirect

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.

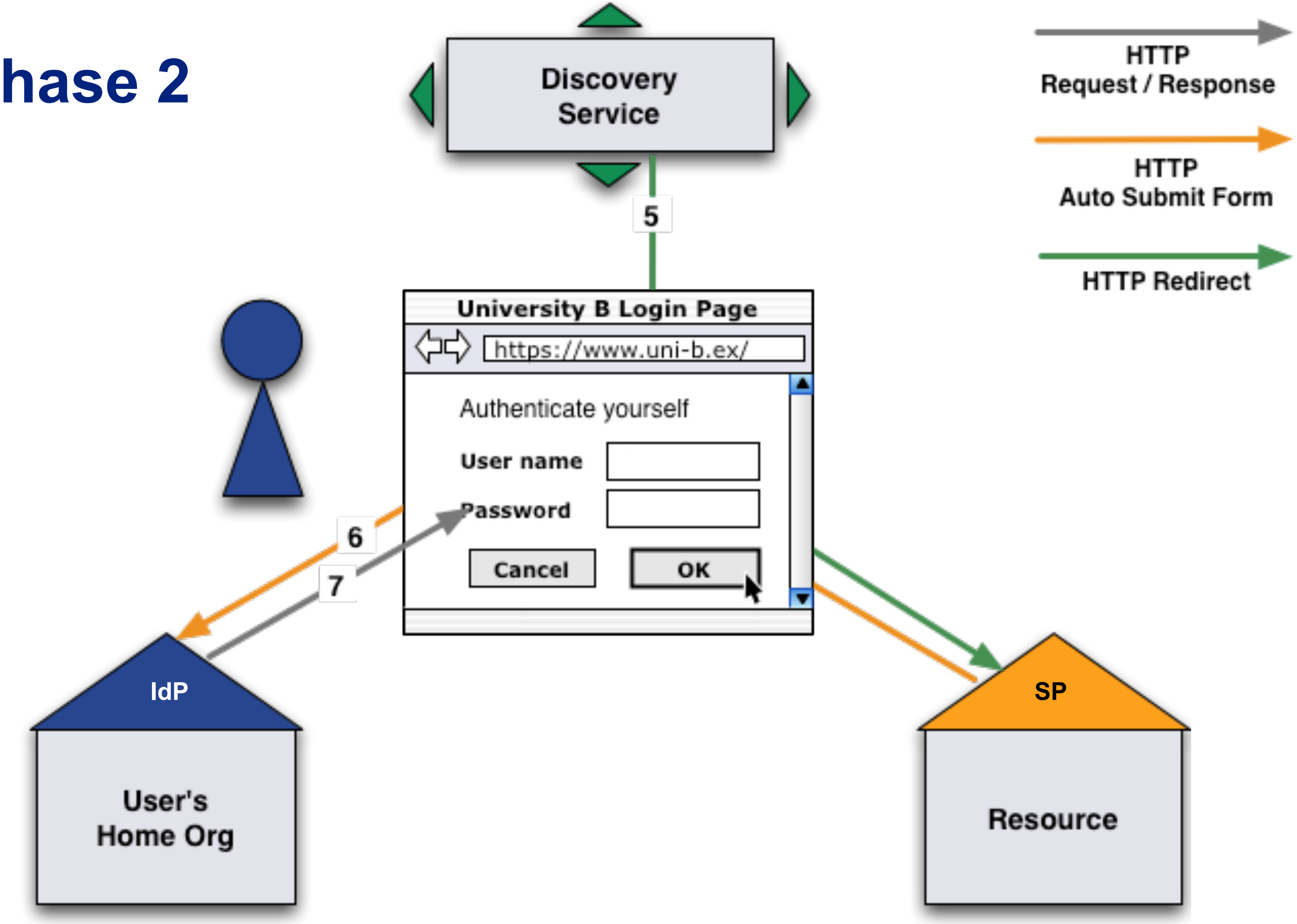
④ On the Discovery Service page, the user submits the Identity Provider selection.

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


Discovery Service
HTTP Request / Response
HTTP Auto Submit Form
HTTP Redirect
5
University B Login Page
https://www.uni-b.ex/
Authenticate yourself
User name
Password
Cancel
OK
6
7
IdP
User's Home Org
SP
Resource

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.

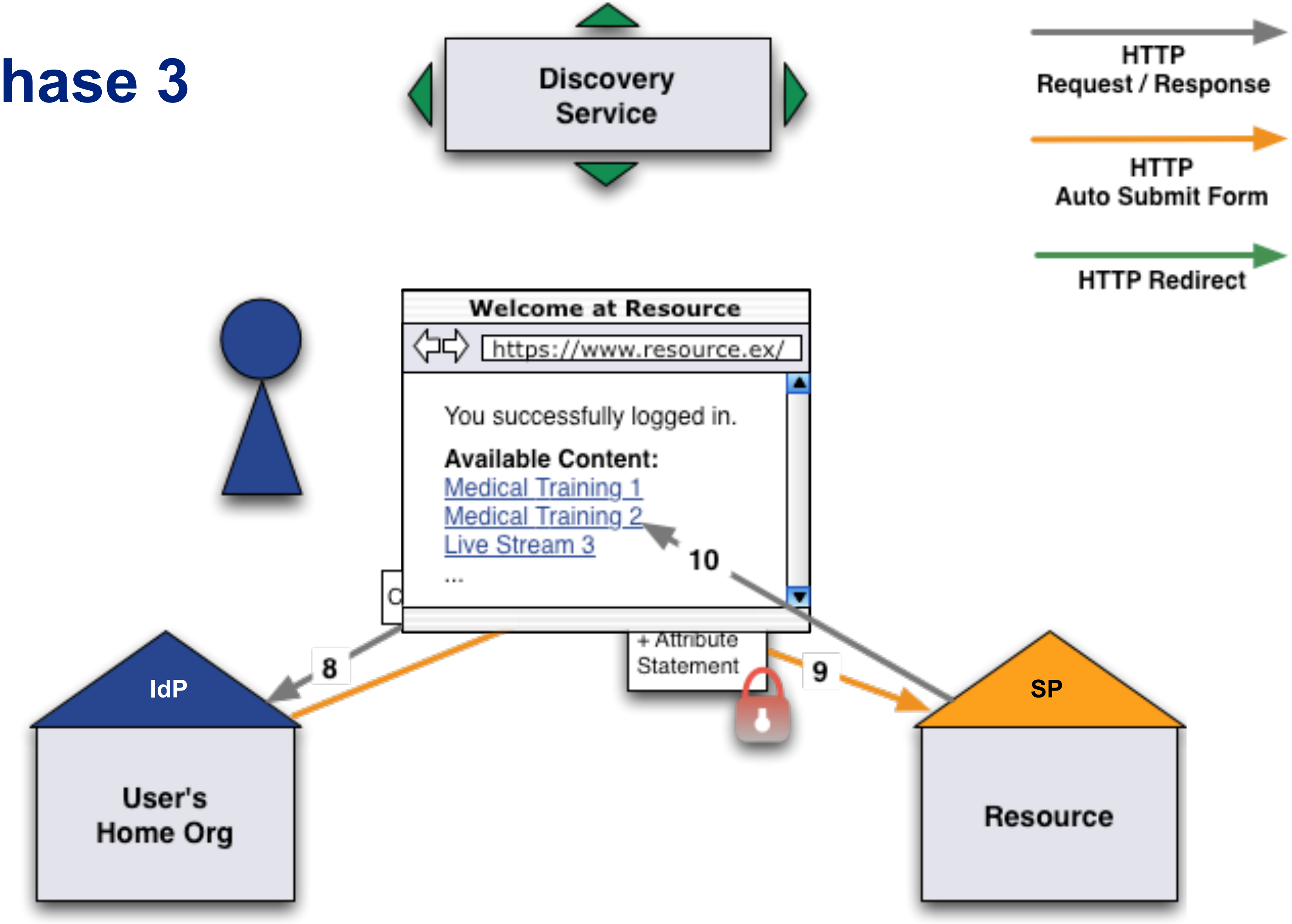
Session initiation and authentication request

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



Welcome at Resource

https://www.resource.ex/

You successfully logged in.

Available Content:

Medical Training 1

Medical Training 2

Live Stream 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>
```

Authentication, attribute statement and access

⑧ The user types his username and password credentials and submits them to the Identity Provider.

⑨ The Identity Provider verifies the credentials. If authentication succeeds, the IdP issues an assertion for the SP and returns it within an auto-submit-post-form to the browser.

The web browser immediately posts the SAML Assertion to the Service Provider with use of Javascript automatically.

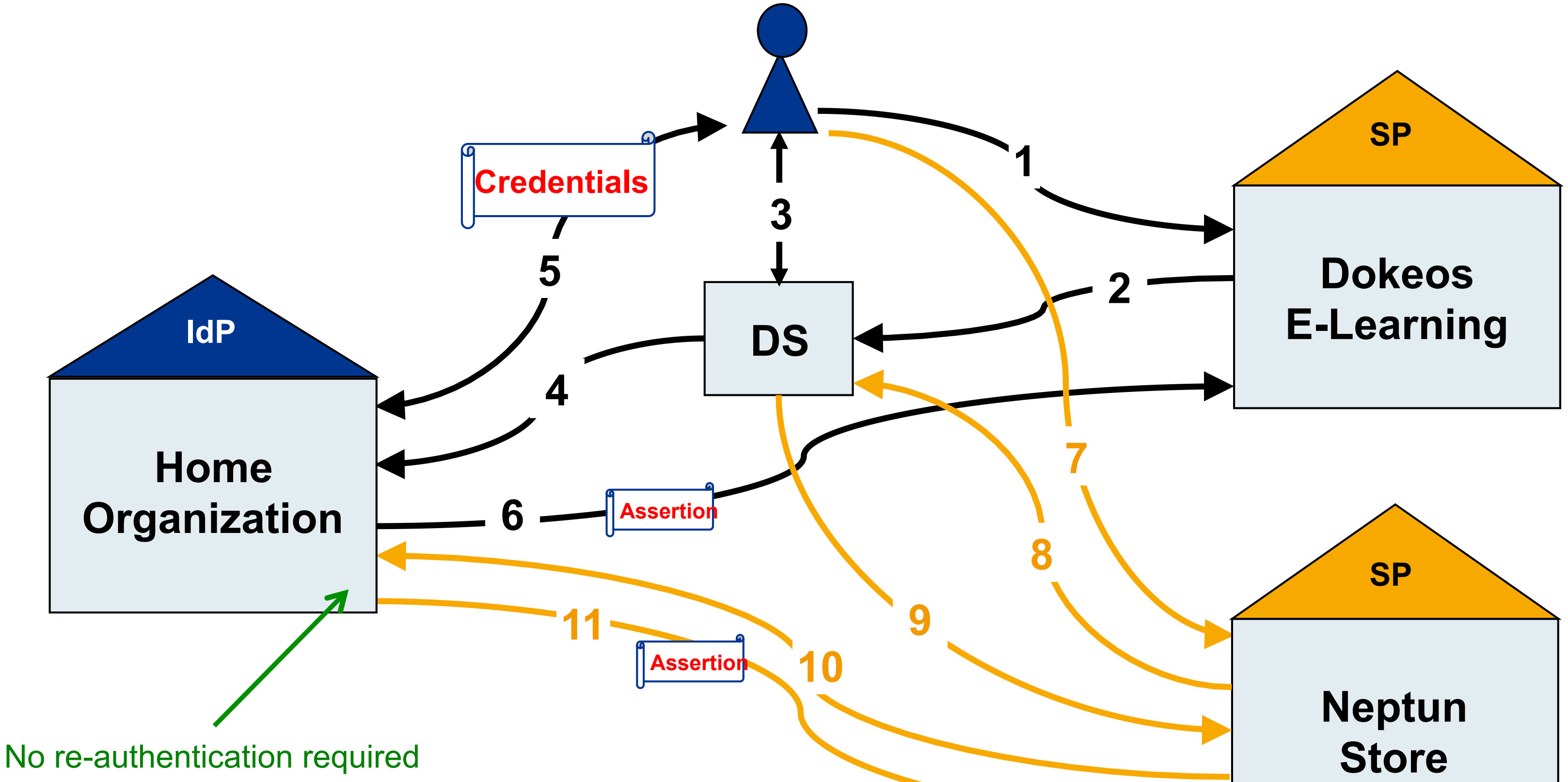
The Service Provider processes the SAML assertion including the authentication and attribute statements.

Authentication, attribute statement and access

⑩ Finally, the Service Provider starts a new session for the user and redirects the user to the previously requested resource.

Now, the user is authenticated and gets access to the resource depending on the access rules configured for the resource.

Accessing multiple SPs



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

Live Demo

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

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://av.aai.switch.ch/