Security Assertion Markup Language (SAML)

SAML

Security Assertion Markup Language (SAML) is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP).

That is you can use one set of credentials to log into many different websites. It's much simpler to manage one login per user than it is to manage separate logins to email, moodle, library systems, world-wide labs etc.

SAML transactions use Extensible Markup Language (XML) for standardized communications between the identity provider and service providers. SAML is the link between the authentication of a user's identity and the authorization to use a service.

SAML

SAML works by passing information about users, logins, and attributes between the identity provider and service providers.

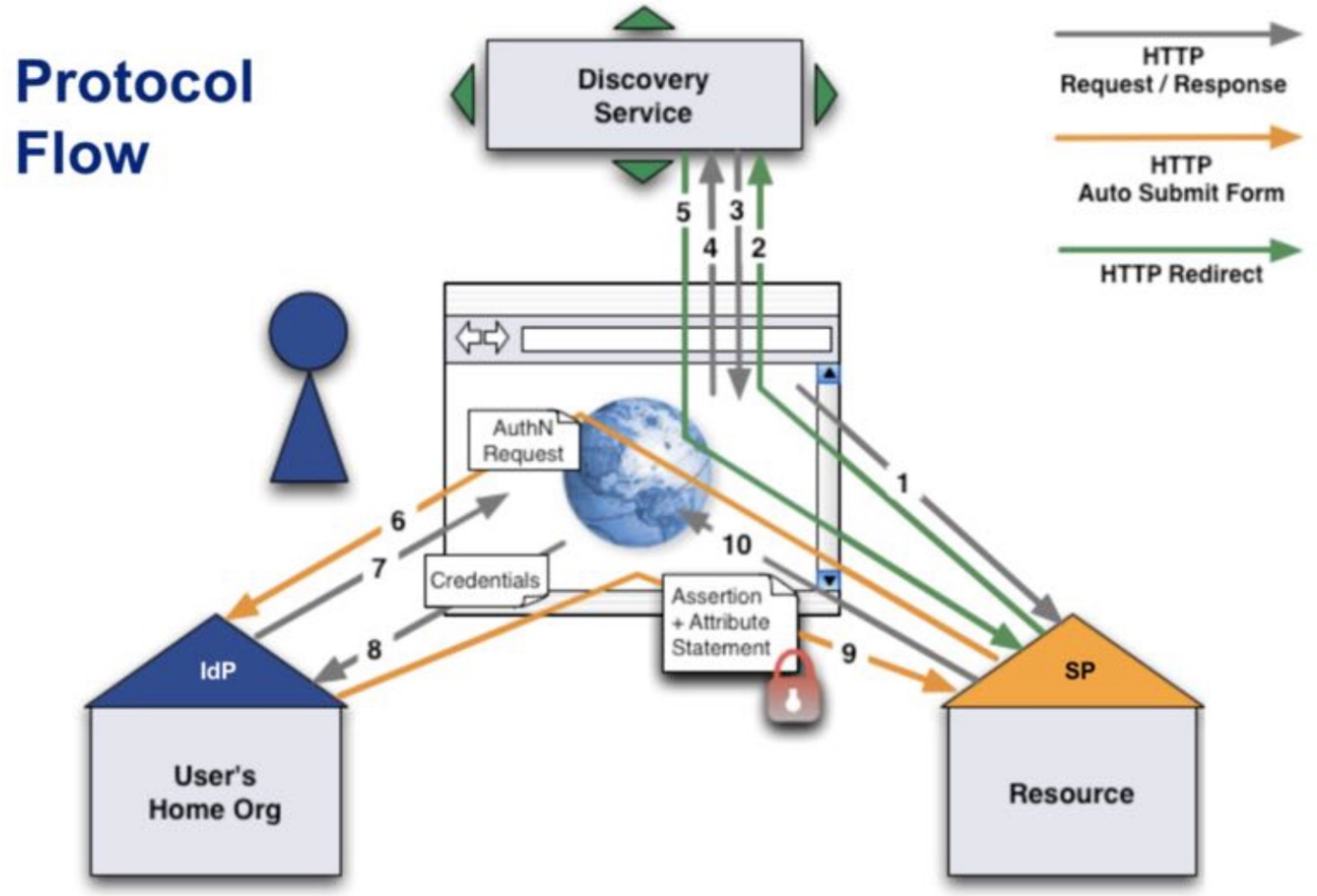
Each user logs in once to Single Sign On with the identify provider, and then the identify provider can pass SAML attributes to the service provider when the user attempts to access those services.

The service provider requests the authorization and authentication from the identify provider.

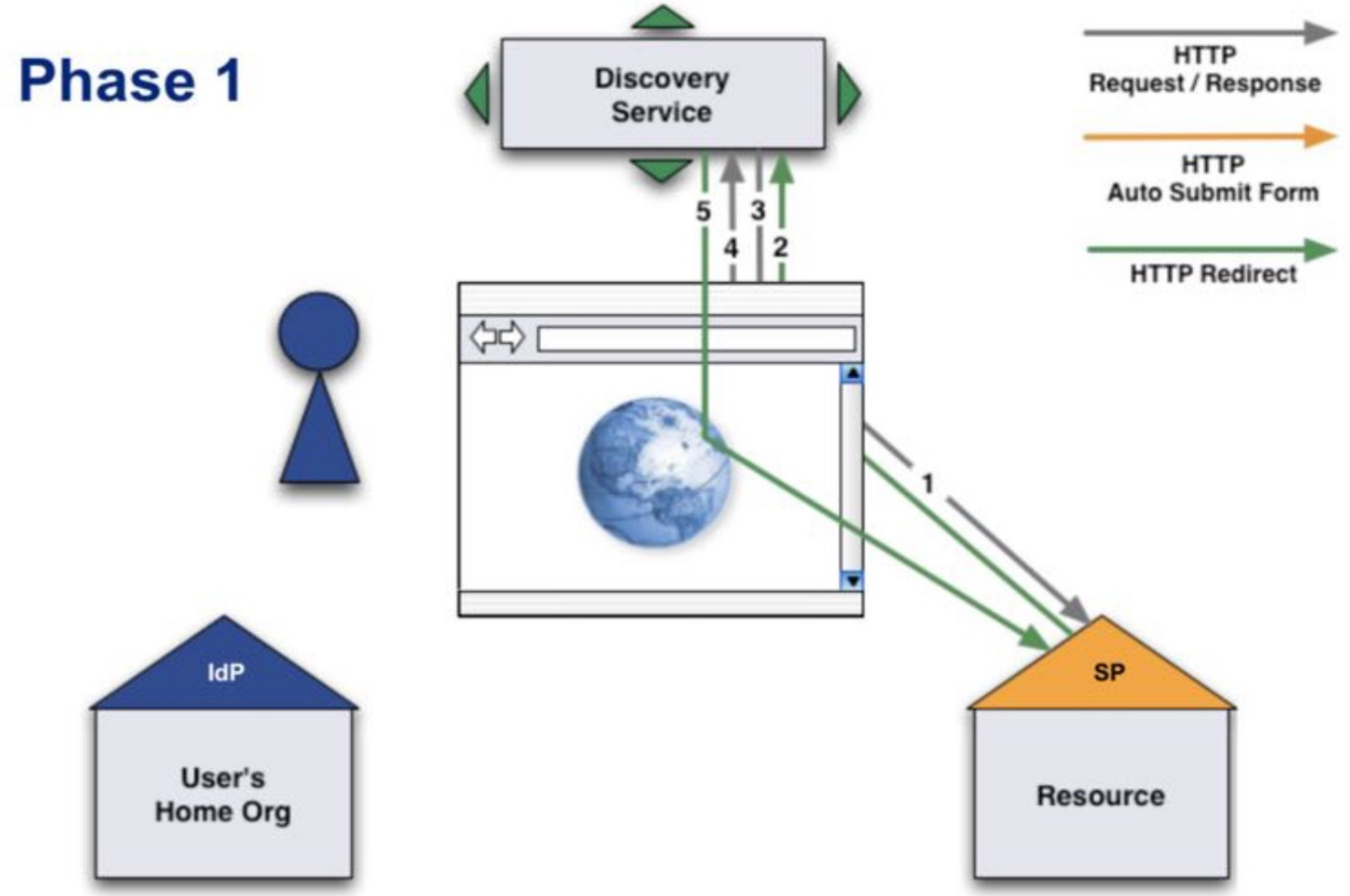
Since both of those systems speak the same language – SAML – the user only needs to log in once.

Each identity provider and service provider need to agree upon the configuration for SAML. Both ends need to have the exact configuration for the SAML authentication to work.

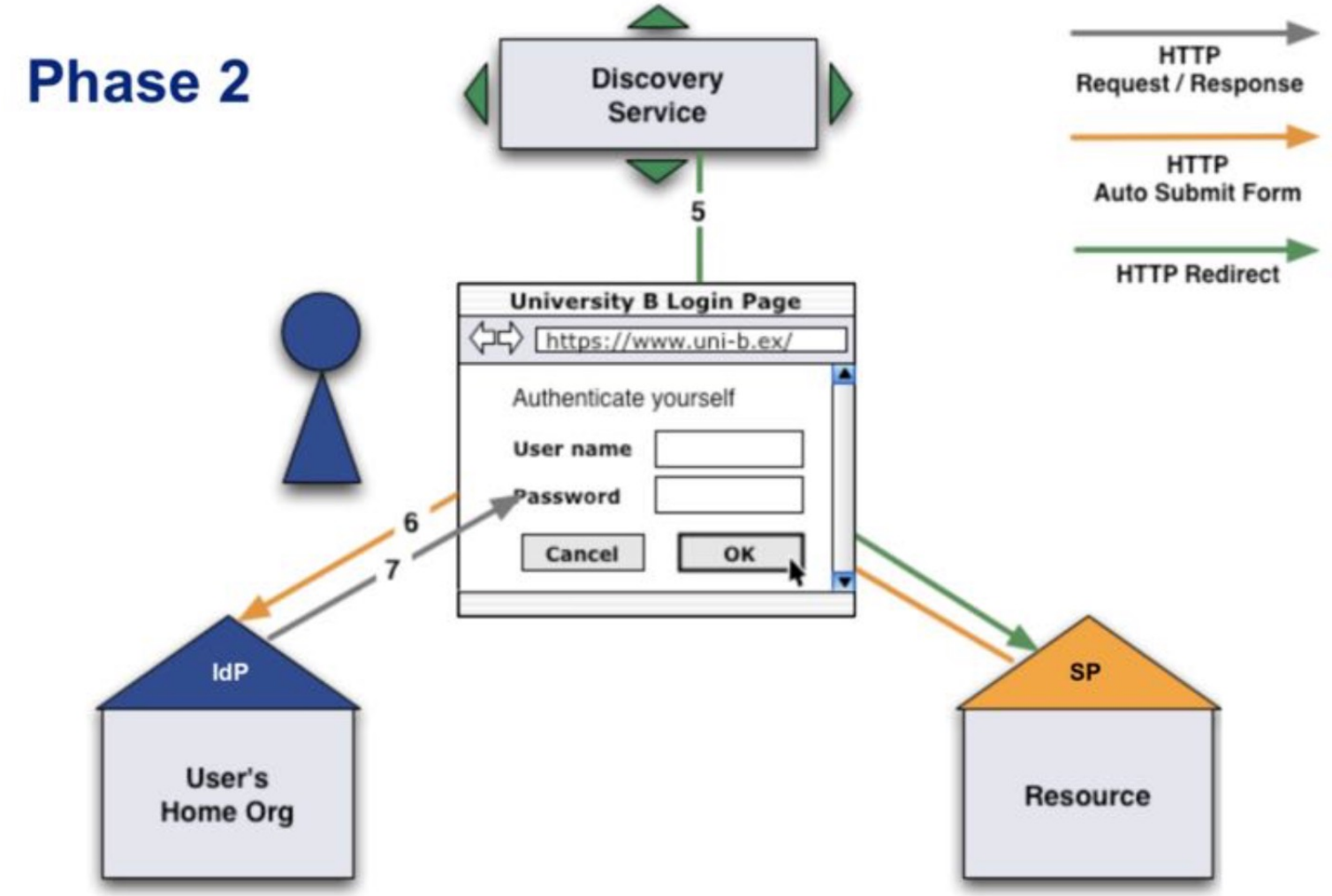
SAML


Protocol Flow
Discovery Service
HTTP Request / Response
HTTP Auto Submit Form
HTTP Redirect
5
3
4
2
AuthN Request
1
6
10
7
Credentials
Assertion + Attribute Statement
8
9
IdP
SP
User's Home Org
Resource

SAML


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

SAML


Phase 2
Discovery Service
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
HTTP Request / Response
HTTP Auto Submit Form
HTTP Redirect

SAML AuthN Request

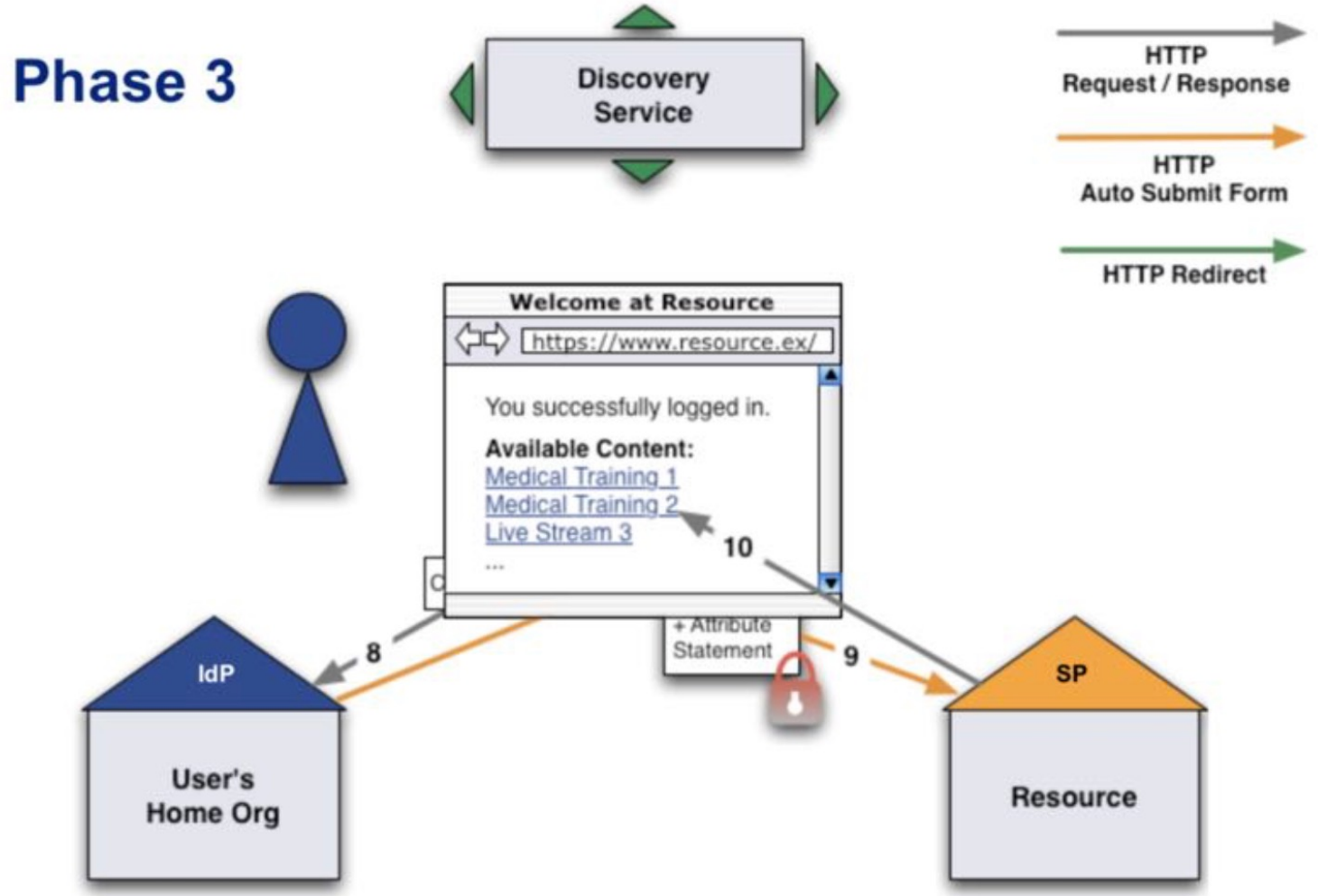
Plain HTML:

```
<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>
```

SAML

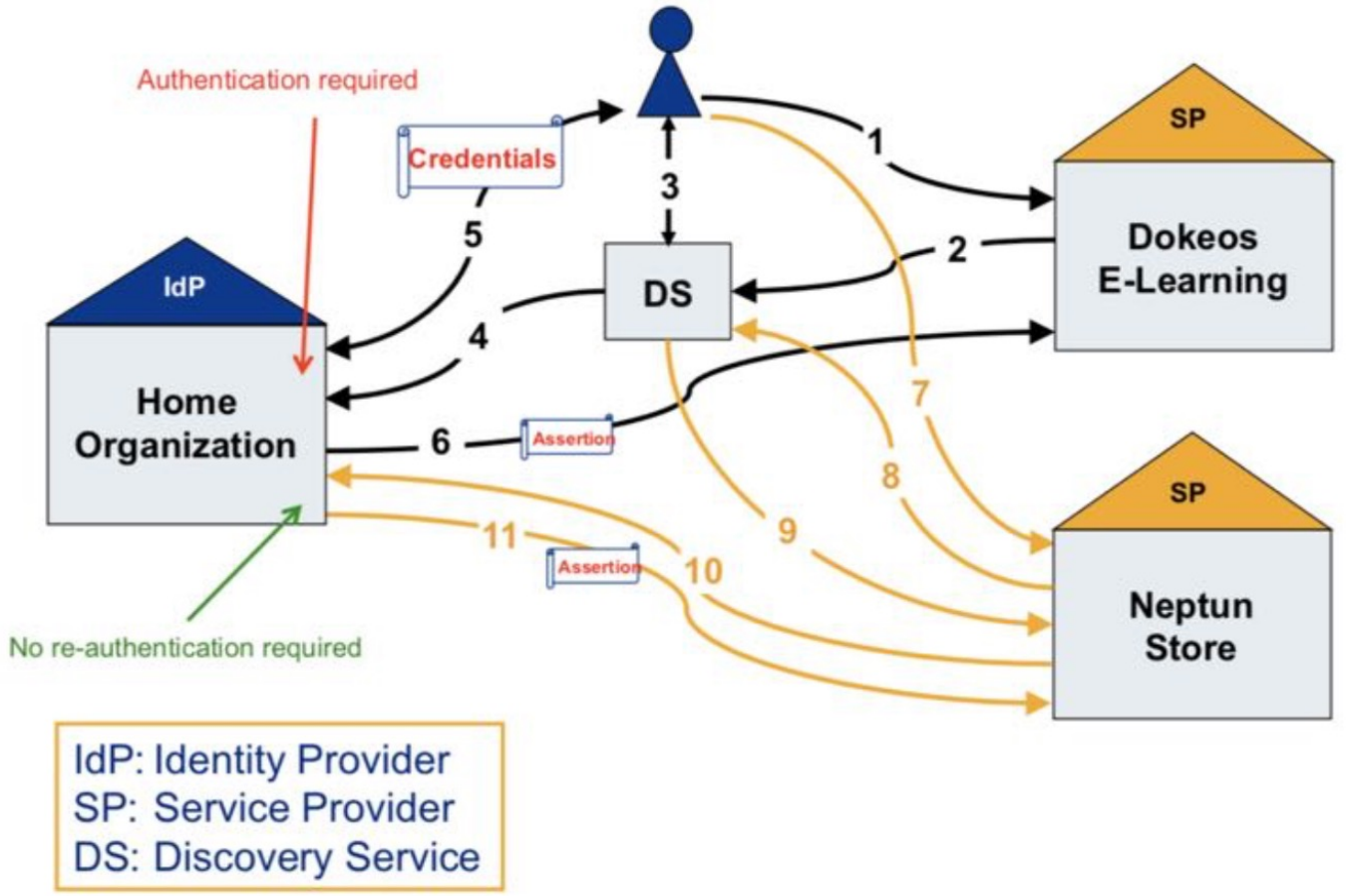

Phase 3
Discovery Service
HTTP Request / Response
HTTP Auto Submit Form
HTTP Redirect
Welcome at Resource
https://www.resource.ex/
You successfully logged in.
Available Content:
Medical Training 1
Medical Training 2
Live Stream 3
...
10
+ Attribute Statement
8
9
IdP
User's Home Org
SP
Resource

SAML

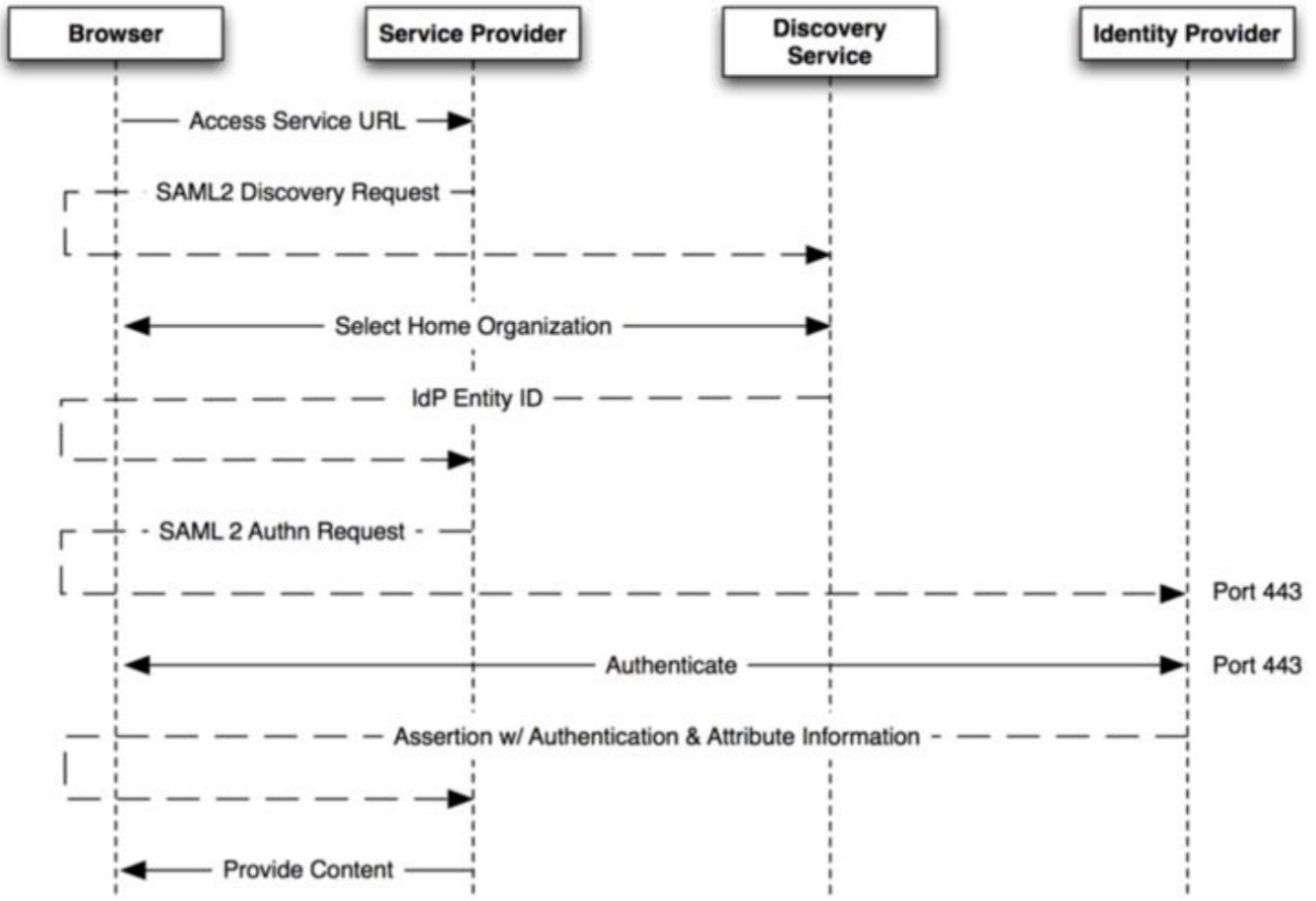
SAML Assertion + Attribute Statement, decrypted (Base64 decoded)

```
<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



SAML


Browser
Service Provider
Discovery Service
Identity Provider
Access Service URL
SAML2 Discovery Request
Select Home Organization
IdP Entity ID
SAML 2 Authn Request
Port 443
Authenticate
Port 443
Assertion w/ Authentication & Attribute Information
Provide Content

Thank You