ExamplePortalResponse

Identity Provider Issues <samlp:Response> to Portal

This is the SOAP response to the Portal with the assertion it will hand off to the Portlet.

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">

  <S:Header xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:sbf="urn:liberty:sb" xmlns:sb="urn:liberty:
sb:2006-08">

    <!-- ID-WSF defined headers -->
    <sbf:Framework version="2.0"/>
    <sb:Sender providerID="https://idp.example.edu/idp/shibboleth"/>

    <!-- WS-Addressing headers with routing information -->
    <wsa:MessageID>uuid:071BCD36-FE77-470D-9AA9-9B5628D0873A</wsa:MessageID>
    <wsa:RelatesTo>uuid:efefefef-aaaa-ffff-cccc-eeeeffffcccc</wsa:RelatesTo>
    <wsa:Action>urn:liberty:ssos:2006-08:Response</wsa:Action>

    <!-- WS-Security header with timestamp -->
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.
xsd">
      <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.
xsd">
        <wsu:Created>2008-03-14T17:25:30Z</wsu:Created>
      </wsu:Timestamp>
    </wsse:Security>

  </S:Header>

  <S:Body>
    <samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="_e71fa15519729e9e3adea5d02b2e38af"
        InResponseTo="_a02c7e89e77e4871b84349a9db338374" IssueInstant="2008-03-14T17:25:30Z" Version="2.0">

      <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://idp.example.edu/idp/shibboleth<
/saml:Issuer>
      <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
      </samlp:Status>

      <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0"
          ID="_682C46C8-198A-436C-9E0F-DBBC155DE415" IssueInstant="2008-03-14T17:25:30Z">

        <saml:Issuer>https://idp.example.edu/idp/shibboleth</saml:Issuer>
        <ds:Signature>...</ds:Signature> <!-- signature elided -->

        <saml:Subject>

          <!-- the identifier is scoped between the IdP and the Portlet -->
          <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">
            E8042FB4-4D5B-48C3-8E14-8EDD852790FF
          </saml:NameID>

          <!-- the first confirmation is for the portal -->
          <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
                https://portal.example.edu/shibboleth
            </saml:NameID>
            <saml:SubjectConfirmationData NotOnOrAfter="2008-03-14T17:30:30Z"
                Recipient="http://www.w3.org/2005/08/addressing/role/anonymous"/>
          </saml:SubjectConfirmation>

          <!-- the second confirmation is for the portlet back to the IdP -->
          <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
            <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
                https://portal.example.edu/portlet1/shibboleth
            </saml:NameID>
```

```
            <saml:SubjectConfirmationData xsi:type="saml:KeyInfoConfirmationDataType"
              <ds:KeyInfo>...<ds:KeyInfo>
            </saml:SubjectConfirmationData>
          </saml:SubjectConfirmation>

        </saml:Subject>

        <!-- the conditions apply to all uses, and the assertion is scoped to the Portlet and IdP -->
        <saml:Conditions NotBefore="2008-03-14T17:25:30Z" NotOnOrAfter="2008-03-14T18:25:30Z">
          <saml:AudienceRestriction>
            <saml:Audience>https://portal.example.edu/portlet1/shibboleth</saml:Audience>
            <saml:Audience>https://idp.example.edu/idp/shibboleth</saml:Audience>
          </saml:AudienceRestriction>

          <saml:Condition xsi:type="del:DelegationRestrictionType" xmlns:del="urn:oasis:names:tc:SAML:2.0:
conditions:delegation">
            <del:Delegate>
              <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
               https://portal.example.edu/shibboleth
              </saml:NameID>
            </del:Delegate>
          </saml:Condition>

        </saml:Conditions>

        <saml:AuthnStatement AuthnInstant="2008-03-14T17:21:24.781Z" SessionIndex="_682C46C8-198A-436C-9E0F-
DBBC155DE414">
          <saml:SubjectLocality Address="192.168.1.1"/>
          <saml:AuthnContext>
            <saml:AuthnContextClassRef>
              urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
            <saml:AuthnContextClassRef>
          </saml:AuthnContext>
        </saml:AuthnStatement>

        <saml:AttributeStatement>
            ...
        </saml:AttributeStatement>

      </saml:Assertion>

    </samlp:Response>
  </S:Body>

</S:Envelope>
```

Notes

The token returned in this step is really intended to be used by the Portlet in subsequent SSO operations with services to authenticate to the IdP as the user.

To model the hand-off between the Portal, which is asking for the assertion, and the Portlet, I'm using a "bearer" confirmation method that identifies the Recipient (the allowed delivery location) as the WS-Addressing anonymous URL, which implies "self". This is the best way I can think of to limit the bearer semantic to the local hand-off, without compromising the security between the Portlet and the IdP. Essentially, nothing should accept such a bearer assertion other than the Portlet itself (because we code it to do so).

The other noteworthy extension is the additional condition that identifies the Portal as a delegate, so that the subsequent assertions issued to the Portlets will include the Portal as the first link in the delegation chain.

For the purposes of these examples, assume the following:

- Identity Provider EntityID
  - `https://idp.example.edu/idp/shibboleth`
- Identity Provider Browser SSO Service URL
  - `https://idp.example.edu/idp/profile/SAML2/Redirect/SSO`
- Portal Resource URL
  - `https://portal.example.edu/`
- Portal EntityID
  - `https://portal.example.edu/shibboleth`
- Portal Assertion Consumer Service URL

    - `https://portal.example.edu/Shibboleth.sso/SAML2/POST`

- Portlet EntityID
    - `https://portal.example.edu/portlet1/shibboleth`

- Web Service Provider Resource URL
    - `https://service.example.com/orderstatus`
- Web Service Provider EntityID
    - `https://service.example.com/shibboleth`
- Web Service Provider Assertion Consumer Service URL
    - `https://service.example.com/Shibboleth.sso/SAML2/PAOS`