ExampleRecursivePortletResponse

Identity Provider Issues `<samlp:Response>` to Web Service Provider via Portlet

This is an ECP SSO response for the Portlet to give to the web site/service. It is "recursively" outfitted with the capability for the WSP to request additional delegation tokens.


```
<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">

    <!-- ECP profile header -->
    <ecp:Response AssertionConsumerServiceURL="https://service.example.com/Shibboleth.sso/SAML2/PAOS"
        S:mustUnderstand="1" S:actor="http://schemas.xmlsoap.org/soap/actor/next"/>

    <!-- 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-9AA9-9B5628D08728</wsa:MessageID>
    <wsa:RelatesTo>uuid:efefefef-aaaa-ffff-cccc-eeeeffffbbbb</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>2008-03-14T17:31:24Z</wsu:Created>
      </wsu:Timestamp>
    </wsse:Security>
  </S:Header>

  <S:Body>
    <samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
        Destination="https://service.example.com/Shibboleth.sso/SAML2/PAOS" ID="
_e71fa15519729e9e3adea5d02b2e38ae"
        InResponseTo="_a02c7e89e77e4871b84349a9db338374" IssueInstant="2008-03-14T17:31:24.781Z" 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-DBBC155DE414" IssueInstant="2008-03-14T17:31:24.781Z">

        <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 WSP -->
          <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">
            E8042FB4-4D5B-48C3-8E14-8EDD852790EE
          </saml:NameID>

          <!-- the bearer authorization is for web SSO by the Portal to the WSP -->
          <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 Address="192.168.10.10" NotOnOrAfter="2008-03-14T17:36:24Z"
                Recipient="https://service.example.com/Shibboleth.sso/SAML2/PAOS"/>
          </saml:SubjectConfirmation>
```

```
          <!-- the HoK authorization is for re-presentation to the IdP by the WSP -->
          <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://service.example.com
/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 WSP and the IdP -->
        <saml:Conditions NotBefore="2008-03-14T17:31:24.781Z" NotOnOrAfter="2008-03-14T18:31:24.781Z">

          <saml:AudienceRestriction>
            <saml:Audience>https://service.example.com/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>
            ...

          <!-- a pointer to the IdP's SSOS and how to contact it -->
          <saml:Attribute Name="urn:liberty:ssos:2006-08" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri">
            <saml:AttributeValue>
              <wsa:EndpointReference xmlns:wsa="http://www.w3.org/2005/08/addressing">
                <wsa:Address>https://idp.example.org/idp/profiles/WSF/SSO</wsa:Address>
                <wsa:Metadata xmlns:disco="urn:liberty:disco:2006-08">
                  <disco:Abstract>ID-WSF Single Sign-On Service</disco:Abstract>
                  <disco:ServiceType>urn:liberty:ssos:2006-08</disco:ServiceType>
                  <disco:ProviderID>http://idp.example.org/idp/shibboleth</disco:ProviderID>
                  <sbf:Framework xmlns:sbf="urn:liberty:sb" version="2.0"/>
                  <disco:SecurityContext>
                    <disco:SecurityMechID>urn:liberty:security:2005-02:ClientTLS:peerSAMLV2</disco:
SecurityMechID>
                    <sec:Token xmlns:sec="urn:liberty:security:2006-08" ref="#_682C46C8-198A-436C-9E0F-
DBBC155DE414" usage="urn:liberty:security:tokenusage:2006-08:SecurityToken"/>
                  </disco:SecurityContext>
                </wsa:Metadata>
              </wsa:EndpointReference>
            </saml:AttributeValue>
          </saml:Attribute>

        </saml:AttributeStatement>

      </saml:Assertion>

    </samlp:Response>
```

```
  </S:Body>

</S:Envelope>
```

Notes

The SOAP exchange with the IdP results in a SAML response to be repackaged into a PAOS response to the WSP by the Portlet. The Portlet is responsible for re-checking that the response location in the `<ecp:Response>` header matches the response location supplied by the WSP in its PAOS request.

Typically the assertion will be encrypted in the response, but for illustrative purposes, it's left unencrypted here.

Obviously the assertion is likely to contain arbitrary attribute information that the WSP can consume directly. The example uses a transient `<saml:NameID>` element for the principal, but this needn't be assumed. If the assertion were left in the clear, then the identifier could be encrypted piecemeal.

The authentication statement is identical to the original SSO assertion, because it reflects the **user's** authentication to the IdP, and not any subsequent delegation.

This final assertion in the chain includes a special condition that identifies the delegate, the Portal, as a transited service between the original client (the browser) and the WSP. If the Portlet is made distinct from the Portal, then the Portlet's entityID would be appended to that condition.

Note the second `<saml:SubjectConfirmation>` and `<saml:Audience>` elements that allow for authentication of the WSP back to the IdP. Typically, the second confirmation will contain the key or certificate of the WSP to tie the assertion to that key.

One of the attributes is not specifically about the user but tells the WSP how it can contact the IdP's IS-WSF Single Sign-On Service using the assertion as an authentication token. The EPR includes the location, the security mechanism, and a pointer to the token to use, in this case the enclosing assertion.

Finally, note the assertion lifetime is set at one hour. The implication is that the assertion is only usable **at the IdP** for that duration. It has no implications for the lifetime of the user's session with the WSP itself. This period can obviously be set as desired.

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`