ExampleWSPResponse

Portlet Forwards `<samlp:Response>` to Web Service Provider

This is the ECP SSO step between the Portlet and the web site/service.

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

  <S:Header>
    <paos:Response refToMessageID="6c3a4f8b9c2d"
        S:actor="http://schemas.xmlsoap.org/soap/actor/next/" S:mustUnderstand="1"/>

    <!-- equivalent of the RelayState parameter in a browser-based SSO profile -->
    <ecp:RelayState xmlns:ecp="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp"
        S:mustUnderstand="1" S:actor="http://schemas.xmlsoap.org/soap/actor/next">cookie:afcd145</ecp:
RelayState>

  </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>

        </saml:Subject>

        <!-- the conditions apply to all uses, and the assertion is scoped to the WSP -->
        <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: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 <samlp:Response> message from the IdP is wrapped with additional binding information inside a SOAP envelope, the response half of a SOAP exchange, carried in an HTTP response.

The Portlet is responsible for creating the `<paos:Response>` header to correlate the request from the WSP. The original resource at the WSP is recovered from the RelayState header, which is copied from the WSP's request to the response.

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`