ExamplePortletAuthentication

Portlet Forwards `<samlp:AuthnRequest>` to Identity Provider

This is the authentication step for the Liberty variant of ECP SSO between the Portlet and the IdP.

```
<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://portal.example.edu/portlet1/shibboleth"/>

    <!-- WS-Addressing headers with routing information -->
    <wsa:MessageID>uuid:efefefef-aaaa-ffff-cccc-eeeeffffbbbb</wsa:MessageID>
    <wsa:Action>urn:liberty:ssos:2006-08:AuthnRequest</wsa:Action>

    <!-- WS-Security header with timestamp and security token -->
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.
xsd"
        S:mustUnderstand="1">

      <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.
xsd">
        <wsu:Created>2008-03-14T17:31:20Z</wsu:Created>
      </wsu:Timestamp>

      <!-- this is the signed assertion issued for authentication of the Portlet -->
      <saml:Assertion>....</saml:Assertion>

    </wsse:Security>

  </S:Header>

  <S:Body>
    <samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
        AssertionConsumerServiceURL="https://service.example.com/Shibboleth.sso/SAML2/PAOS"
        ID="_a02c7e89e77e4871b84349a9db338374" IssueInstant="2008-03-14T17:31:17Z"
        ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS" Version="2.0">
      <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://service.example.com/shibboleth<
/saml:Issuer>
      <samlp:NameIDPolicy AllowCreate="1"/>
    </samlp:AuthnRequest>
  </S:Body>

</S:Envelope>
```

Notes

This is a repackaging of the request from the WSP in the form of an ID-WSF SOAP message, authenticated by the presence of a SAML assertion in a WS-Security header. The primary Liberty-specific information in the message is the `<sb:Sender>` header, which clearly identifies the Portlet as the invoking system.

The IdP can then establish the right of the Portlet to make the request by ensuring that the subject confirmation of the assertion in the header can be satisfied. This is sufficient to authenticate the Portlet as the subject of the assertion (the user).

The example shown is sufficient for the case of a bearer assertion, or if the Portlet can authenticate with a TLS client certificate. If a digital signature is required, a `<ds:Signature>` would appear in the `<wsse:Security>` header, with references to each SOAP header and the body. Each header would carry a `wsu:Id` attribute to allow it to be referenced. This is a significantly more complex option to implement, with the advantage of not requiring client TLS support on the IdP.

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`