Ubilogin WSIDP 4.0

Message Exchange Example

1. Overview

This document describes the SOAP messages exchanged by the Ubilogin WSIDP with the other parties Web Service Provider (WSP) and Web Service Client (WSC). There are two different kinds of messages: Oasis Open SAML 2.0 messages and Liberty Alliance ID-WSF 2.0 messages. All the messages are transferred through the WSC.

2. Successful Message Exchange

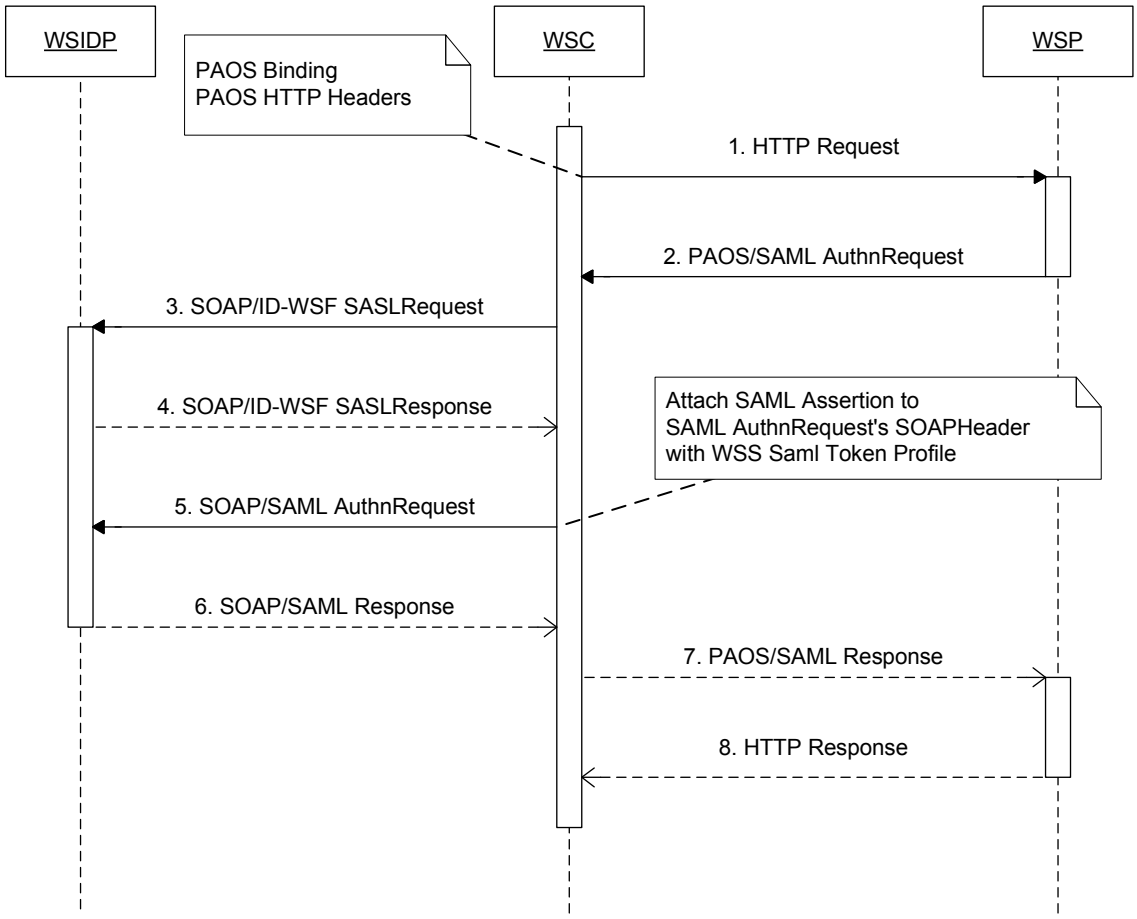

Figure 1. SAML and ID-WSF message exchange sequence.

The first and last messages in Figure 1—the HTTP request made by WSC to WSP (1.) and the respective HTTP response (8.)—are specific to the application protocol between WSC and WSP and is thus omitted in this document. The first HTTP request must have the PAOS HTTP headers as specified by the [SAML-Bindings] document. For other normative documents, see the chapter 3. References.

The message examples presented in this chapter are the following:

1. The PAOS reply from WSP to WSC containing SAML AuthnRequest (message 2 in figure 1).
2. The ID-WSF SASLRequest from WSC to WSIDP (message 3 in figure 1)
3. The ID-WSF SASLResponse from WSIDP to WSC (message 4 in figure 1)
4. The SAML AuthnRequest from WSC to WSIDP (message 5 in figure 1)
5. The SAML Response from WSIDP to WSC (message 6 in figure 1)
6. The SAML Response from WSC to WSP (message 7 in figure 1)

The response messages presented in this chapter are all result of a successful authentication and authorization.

In the examples the entityid of the WSP is *"https://service.com/sp1"* and the entityid of the WSIDP is *"https://identityprovider.com/wsidp"*. The XML signature value inside the *<ds:SignatureValue>* element is removed due to XML pretty printing.

SAML Bindings

The following sequence diagram represents the SAML messages sent between the WSC, WSP and WSIDP. It illustrates the use of PAOS Binding between the WSC and WSP and the use of SOAP Binding between the WSC and WSIDP.

The information boxes contain the following information for each sent message:

- Used SAML Binging (SOAP/PAOS)
- Mandatory HTTP Headers
- Mandatory SOAP Header elements
- Optional SOAP header elements are enclosed in brackets

Not all of the mentioned attributes and sub-elements are required in the ecp:Request, paos:Request, and paos:Response elements. For more specific information refer to [SAML-Profiles, pages 21-26].

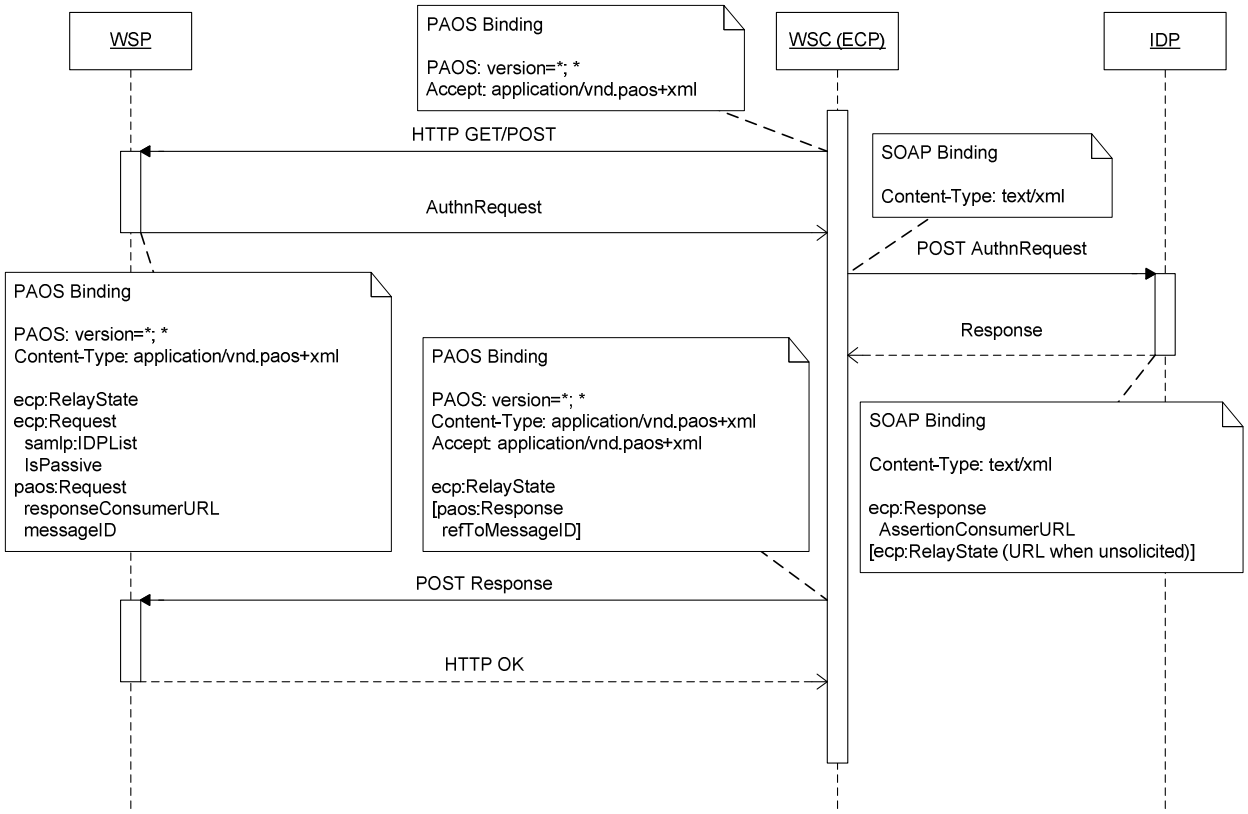

Figure 2. The SAML Bindings, HTTP headers and SOAP headers used in the authentication procedure.

2.1. WSP to WSC: AuthnRequest

Listing 1. The WSP sends a SAML AuthnRequest inside a PAOS response to WSC.

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

  <SOAP-ENV:Header>

    <paos:Request xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" SOAP-
ENV:actor="http://schemas.xmlsoap.org/soap/actor/next" SOAP-ENV:mustUnderstand="1"
responseConsumerURL="https://service.com/sp1/AssertionConsumer"
service="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp"
xmlns:paos="urn:liberty:paos:2003-08"/>

    <ecp:Request xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" SOAP-
ENV:actor="http://schemas.xmlsoap.org/soap/actor/next" SOAP-ENV:mustUnderstand="1"
xmlns:ecp="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp">

      <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://service.com/sp1</saml:Issuer>

      <samlp:IDPList xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">

        <samlp:IDPEntry
Loc="https://identityprovider.com/wsidp/saml2/SingleSignOnService"
ProviderID="https://identityprovider.com/wsidp"/>

      </samlp:IDPList>

    </ecp:Request>
```

```
    <ecp:RelayState xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" SOAP-
ENV:actor="http://schemas.xmlsoap.org/soap/actor/next" SOAP-ENV:mustUnderstand="1"
xmlns:ecp="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp">8e002b2b26680bc6</ecp:RelaySt
ate>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <samlp:AuthnRequest xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="https://service.com/sp1/AssertionConsumer"
Destination="https://identityprovider.com/wsidp/saml2/SingleSignOnService"
ID="_597003ad4d80008390a71481c6a9fe364930ccdf" IssueInstant="2007-06-29T07:12:01.113Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Version="2.0">
      <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://service.com/sp1</saml:Issuer>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <ds:Reference URI="#_597003ad4d80008390a71481c6a9fe364930ccdf">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>VFSDui+AZ+fi0c+53/0QoVjpwJs=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>LcCh…</ds:SignatureValue>
      </ds:Signature>
      <samlp:Scoping>
        <samlp:IDPList>
          <samlp:IDPEntry
Loc="https://identityprovider.com/wsidp/saml2/SingleSignOnService"
ProviderID="https://identityprovider.com/wsidp"/>
        </samlp:IDPList>
        <samlp:RequesterID>https://service.com/sp1</samlp:RequesterID>
      </samlp:Scoping>
    </samlp:AuthnRequest>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

2.2. WSC to WSIDP: SASLRequest

The message must contain the SOAPAction HTTP header with the value “urn:liberty:sa:2006-08:SASLRequest” or the empty value “” including the quotation marks. This is specified in chapter 4.2 of [WS-AddressingSOAP].

Listing 2. *Here the WSIDP authenticates to the WSIDP with ID-WSF Authentication service using the PLAIN SASL mechanism and the credentials “user” and “pass”.*

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header>
    <wsa:Action xmlns:wsa="http://www.w3.org/2005/08/addressing" SOAP-
ENV:actor="http://schemas.xmlsoap.org/soap/actor/next" SOAP-
ENV:mustUnderstand="1">urn:liberty:sa:2006-08:SASLRequest</wsa:Action>
    <sbf:Framework xmlns:sbf="urn:liberty:sb" SOAP-
ENV:actor="http://schemas.xmlsoap.org/soap/actor/next" SOAP-ENV:mustUnderstand="1"
version="2.0"/>
    <wsa:MessageID xmlns:wsa="http://www.w3.org/2005/08/addressing" SOAP-
ENV:actor="http://schemas.xmlsoap.org/soap/actor/next" SOAP-
ENV:mustUnderstand="1">urn:uuid:5f5cfda9-4566-4d02-83b3-5876732aea68</wsa:MessageID>
    <wsa:ReplyTo xmlns:wsa="http://www.w3.org/2005/08/addressing">
      <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
    </wsa:ReplyTo>
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-secext-1.0.xsd" SOAP-
ENV:actor="http://schemas.xmlsoap.org/soap/actor/next" SOAP-ENV:mustUnderstand="1">
      <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-utility-1.0.xsd">
        <wsu:Created>2007-06-29T07:12:02.223Z</wsu:Created>
      </wsu:Timestamp>
    </wsse:Security>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <sa:SASLRequest mechanism="PLAIN" xmlns:sa="urn:liberty:sa:2006-08">
      <sa:Data>AHVzZXIxAHVzZXIx</sa:Data>
    </sa:SASLRequest>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

2.3. WSIDP to WSC: SASLResponse

Listing 3. The authentication succeeds and the WSIDP returns a SAML assertion along in the SASLResponse.

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header>
    <wsa:Action xmlns:wsa="http://www.w3.org/2005/08/addressing" SOAP-
ENV:actor="http://schemas.xmlsoap.org/soap/actor/next" SOAP-
ENV:mustUnderstand="1">urn:liberty:sa:2006-08:SASLResponse</wsa:Action>
```

```
    <sbf:Framework xmlns:sbf="urn:liberty:sb" SOAP-
ENV:actor="http://schemas.xmlsoap.org/soap/actor/next" SOAP-ENV:mustUnderstand="1"
version="2.0"/>

    <wsa:MessageID xmlns:wsa="http://www.w3.org/2005/08/addressing" SOAP-
ENV:actor="http://schemas.xmlsoap.org/soap/actor/next" SOAP-
ENV:mustUnderstand="1">urn:uuid:a9598ac4-f6e6-417a-9718-5d2a986b4672</wsa:MessageID>

    <wsa:RelatesTo xmlns:wsa="http://www.w3.org/2005/08/addressing" SOAP-
ENV:actor="http://schemas.xmlsoap.org/soap/actor/next" SOAP-
ENV:mustUnderstand="1">urn:uuid:5f5cfda9-4566-4d02-83b3-5876732aea68</wsa:RelatesTo>

    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-secext-1.0.xsd" SOAP-
ENV:actor="http://schemas.xmlsoap.org/soap/actor/next" SOAP-ENV:mustUnderstand="1">

      <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-utility-1.0.xsd">

        <wsu:Created>2007-06-29T07:12:05.801Z</wsu:Created>

      </wsu:Timestamp>

    </wsse:Security>

  </SOAP-ENV:Header>

  <SOAP-ENV:Body>

    <sa:SASLResponse serverMechanism="PLAIN" xmlns:sa="urn:liberty:sa:2006-08">

      <lu:Status code="OK" xmlns:lu="urn:liberty:util:2006-08"/>

      <wsa:EndpointReference xmlns:wsa="http://www.w3.org/2005/08/addressing">

        <wsa:Address>https://identityprovider.com/wsidp/saml2/SingleSignOnService
</wsa:Address>

        <wsa:Metadata>

          <disco:ServiceType xmlns:disco="urn:liberty:disco:2006-08">
urn:oasis:names:tc:SAML:2.0:protocol</disco:ServiceType>

          <disco:ProviderID xmlns:disco="urn:liberty:disco:2006-08">
https://identityprovider.com/wsidp</disco:ProviderID>

          <sbf:Framework version="2.0" xmlns:sbf="urn:liberty:sb"/>

          <disco:SecurityContext xmlns:disco="urn:liberty:disco:2006-08">

            <disco:SecurityMechID>
urn:liberty:security:2006-08:TLS:Bearer</disco:SecurityMechID>

            <sec:Token usage="urn:liberty:security:tokenusage:2006-08:SecurityToken"
xmlns:sec="urn:liberty:security:2006-08">

              <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="_ca679bbe58dc2a0cbb6109c42ef9f3ac13b86bd2" IssueInstant="2007-06-29T07:12:05.754Z"
Version="2.0">

                <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://identityprovider.com/wsidp</saml:Issuer>

                <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

                  <ds:SignedInfo>

                    <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

                    <ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

                    <ds:Reference URI="#_ca679bbe58dc2a0cbb6109c42ef9f3ac13b86bd2">

                      <ds:Transforms>
```



```
                        <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
                      </ds:Transforms>
                      <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                      <ds:DigestValue>JZ/FWXSSSaApyyCTYHxGjM8mjWk=</ds:DigestValue>
                    </ds:Reference>
                  </ds:SignedInfo>
                  <ds:SignatureValue>Owei… </ds:SignatureValue>
                </ds:Signature>
                <saml:Subject>
                  <saml:NameID>dGhpcy1pcy1hLWZpY3Rpb25hbC1uYW1laWQtZGF0YQo=
</saml:NameID>
                  <saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                    <saml:SubjectConfirmationData NotOnOrAfter="2007-06-
29T07:22:05.754Z" Recipient="https://identityprovider.com/wsidp"/>
                  </saml:SubjectConfirmation>
                </saml:Subject>
                <saml:Conditions NotBefore="2007-06-29T07:12:05.754Z"
NotOnOrAfter="2007-06-29T08:12:05.754Z">
                  <saml:AudienceRestriction>
                    <saml:Audience>https://identityprovider.com/wsidp</saml:Audience>
                  </saml:AudienceRestriction>
                </saml:Conditions>
                <saml:AuthnStatement AuthnInstant="2007-06-29T07:12:05.285Z">
                  <saml:SubjectLocality/>
                  <saml:AuthnContext>
                    <saml:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</saml:AuthnContextClassRef>
                  </saml:AuthnContext>
                </saml:AuthnStatement>
              </saml:Assertion>
            </sec:Token>
          </disco:SecurityContext>
        </wsa:Metadata>
      </wsa:EndpointReference>
    </sa:SASLResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

2.4. WSC to WSIDP: AuthnRequest

Listing 4. The WSC encloses the SAML assertion in the wsse:Security SOAP header of the AuthnRequest and forwards the AuthnRequest message to the WSIDP.

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header>
    <Security xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd">
      <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="_ca679bbe58dc2a0cbb6109c42ef9f3ac13b86bd2" IssueInstant="2007-06-29T07:12:05.754Z"
Version="2.0">
        <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://identityprovider.com/wsidp</saml:Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"/>
            <ds:Reference URI="#_ca679bbe58dc2a0cbb6109c42ef9f3ac13b86bd2">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <ds:DigestValue>JZ/FWXSSSaApyyCTYHxGjM8mjWk=</ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>Owei… </ds:SignatureValue>
        </ds:Signature>
        <saml:Subject>
          <saml:NameID>dGhpcy1pcy1hLWZpY3Rpb25hbC1uYW1laWQtZGF0YQo=</saml:NameID>
          <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData NotOnOrAfter="2007-06-29T07:22:05.754Z"
Recipient="https://identityprovider.com/wsidp"/>
          </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions NotBefore="2007-06-29T07:12:05.754Z" NotOnOrAfter="2007-06-
29T07:13:05.754Z">
          <saml:AudienceRestriction>
            <saml:Audience>https://identityprovider.com/wsidp</saml:Audience>
          </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement AuthnInstant="2007-06-29T07:12:05.285Z">
```

```
          <saml:SubjectLocality/>
          <saml:AuthnContext>
            <saml:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</saml:AuthnContextClassRef>
          </saml:AuthnContext>
        </saml:AuthnStatement>
      </saml:Assertion>
    </Security>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <samlp:AuthnRequest xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="https://service.com/sp1/AssertionConsumer"
Destination="https://identityprovider.com/wsidp/saml2/SingleSignOnService"
ID="_597003ad4d80008390a71481c6a9fe364930ccdf" IssueInstant="2007-06-29T07:12:01.113Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Version="2.0">
      <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://service.com/sp1</saml:Issuer>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <ds:Reference URI="#_597003ad4d80008390a71481c6a9fe364930ccdf">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>VFSDui+AZ+fi0c+53/0QoVjpwJs=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>LcCh…</ds:SignatureValue>
      </ds:Signature>
      <samlp:Scoping>
        <samlp:IDPList>
          <samlp:IDPEntry
Loc="https://identityprovider.com/wsidp/saml2/SingleSignOnService"
ProviderID="https://identityprovider.com/wsidp"/>
        </samlp:IDPList>
        <samlp:RequesterID>https://service.com/sp1</samlp:RequesterID>
      </samlp:Scoping>
    </samlp:AuthnRequest>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

2.5. WSIDP to WSC: Response

Listing 5. The WSIDP accepts the AuthnRequest from the WSP and responds with a successful SAML Response.

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

  <SOAP-ENV:Header>

    <ecp:Response xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
AssertionConsumerServiceURL="https://service.com/sp1/AssertionConsumer"
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
S:actor="http://schemas.xmlsoap.org/soap/actor/next" S:mustUnderstand="1"
xmlns:ecp="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp"/>

  </SOAP-ENV:Header>

  <SOAP-ENV:Body>

    <samlp:Response xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://service.com/sp1/AssertionConsumer"
ID="_08a30797189f2a1e77b586cea75831617501c773"
InResponseTo="_597003ad4d80008390a71481c6a9fe364930ccdf" IssueInstant="2007-06-
29T07:12:07.066Z" Version="2.0">

      <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://identityprovider.com/wsidp</saml:Issuer>

      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

        <ds:SignedInfo>

          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>

          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

          <ds:Reference URI="#_08a30797189f2a1e77b586cea75831617501c773">

            <ds:Transforms>

              <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>

              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

            </ds:Transforms>

            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

            <ds:DigestValue>hFuthkuJZcKfIm9fpFwIXzf2d3U=</ds:DigestValue>

          </ds:Reference>

        </ds:SignedInfo>

        <ds:SignatureValue>Vrbk… </ds:SignatureValue>

      </ds:Signature>

      <samlp:Status>

        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>

      </samlp:Status>

      <saml:Assertion ID="_9558e408fafe00cbaa95a04783fcc89a58771492"
IssueInstant="2007-06-29T07:12:07.066Z" Version="2.0">

        <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://identityprovider.com/wsidp</saml:Issuer>

        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

          <ds:SignedInfo>
```

```
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"/>
            <ds:Reference URI="#_9558e408fafe00cbaa95a04783fcc89a58771492">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <ds:DigestValue>b8r3f27+dCWDF3hI6YMTxdKISkg=</ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>QW0E…</ds:SignatureValue>
        </ds:Signature>
        <saml:Subject>
          <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName" NameQualifier="ldap://localhost/dc=identityprovider,
dc=com">uid=user,ou=Persons,dc=identityprovider,dc=com</saml:NameID>
          <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData
InResponseTo="_597003ad4d80008390a71481c6a9fe364930ccdf" NotOnOrAfter="2007-06-
29T07:22:07.066Z" Recipient="https://service.com/sp1/AssertionConsumer"/>
          </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions NotBefore="2007-06-29T07:12:07.066Z" NotOnOrAfter="2007-06-
29T07:22:07.066Z">
          <saml:AudienceRestriction>
            <saml:Audience>https://service.com/sp1</saml:Audience>
          </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement AuthnInstant="2007-06-29T07:12:05.254Z"
SessionNotOnOrAfter="2007-06-29T07:22:07.066Z">
          <saml:SubjectLocality/>
          <saml:AuthnContext>
            <saml:AuthnContextDeclRef>https://identityprovider.com/wsidp/saml2/names/
ac/password.1</saml:AuthnContextDeclRef>
          </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement>
          <saml:Attribute Name="role">
            <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">manager
</saml:AttributeValue>
          </saml:Attribute>
```



```
        </saml:AttributeStatement>
      </saml:Assertion>
    </samlp:Response>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

2.6. WSC to WSP: Response

Listing 6. The WSC encloses the <ecp:RelayState> header in the SOAP message and forwards the Response to the WSP.

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header>
    <ecp:RelayState xmlns:ecp="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" SOAP-
ENV:actor="http://schemas.xmlsoap.org/soap/actor/next" SOAP-
ENV:mustUnderstand="1">8e002b2b26680bc6</ecp:RelayState>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <samlp:Response xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://service.com/sp1/AssertionConsumer"
ID="_08a30797189f2a1e77b586cea75831617501c773"
InResponseTo="_597003ad4d80008390a71481c6a9fe364930ccdf" IssueInstant="2007-06-
29T07:12:07.066Z" Version="2.0">
      <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://identityprovider.com/wsidp</saml:Issuer>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <ds:Reference URI="#_08a30797189f2a1e77b586cea75831617501c773">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>hFuthkuJZcKfIm9fpFwIXzf2d3U=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>Vrbk… </ds:SignatureValue>
      </ds:Signature>
      <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
      </samlp:Status>
```

```
      <saml:Assertion ID="_9558e408fafe00cbaa95a04783fcc89a58771492"
IssueInstant="2007-06-29T07:12:07.066Z" Version="2.0">
        <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://identityprovider.com/wsidp</saml:Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"/>
            <ds:Reference URI="#_9558e408fafe00cbaa95a04783fcc89a58771492">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <ds:DigestValue>b8r3f27+dCWDF3hI6YMTxdKISkg=</ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>QW0E…</ds:SignatureValue>
        </ds:Signature>
        <saml:Subject>
          <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName" NameQualifier="ldap://localhost/dc=identityprovider,
dc=com">uid=user,ou=Persons,dc=identityprovider,dc=com</saml:NameID>
          <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData
InResponseTo="_597003ad4d80008390a71481c6a9fe364930ccdf" NotOnOrAfter="2007-06-
29T07:22:07.066Z" Recipient="https://service.com/sp1/AssertionConsumer"/>
          </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions NotBefore="2007-06-29T07:12:07.066Z" NotOnOrAfter="2007-06-
29T07:22:07.066Z">
          <saml:AudienceRestriction>
            <saml:Audience>https://service.com/sp1</saml:Audience>
          </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement AuthnInstant="2007-06-29T07:12:05.254Z"
SessionNotOnOrAfter="2007-06-29T07:22:07.066Z">
          <saml:SubjectLocality/>
          <saml:AuthnContext>
            <saml:AuthnContextDeclRef>https://identityprovider.com/wsidp/saml2/names/
ac/password.1</saml:AuthnContextDeclRef>
          </saml:AuthnContext>
        </saml:AuthnStatement>
```

```
        <saml:AttributeStatement>
          <saml:Attribute Name="role">
            <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">manager
</saml:AttributeValue>
          </saml:Attribute>
        </saml:AttributeStatement>
      </saml:Assertion>
    </samlp:Response>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

3. References

[ID-WSF] Liberty ID-WSF Authentication, Single Sign-On, and Identity Mapping Services Specification

http://www.projectliberty.org/liberty/content/download/871/6189/file/liberty-idwsf-authn-svc-v2.0.pdf

[ID-WSF-SOAP] Liberty ID-WSF SOAP Binding Specification

http://www.projectliberty.org/liberty/content/download/897/6267/file/liberty-idwsf-soap-binding-v2.0.pdf

[PAOS] Liberty Reverse HTTP Binding for SOAP Specification

http://www.projectliberty.org/liberty/content/download/2008/13941/file/liberty-paos-v1.0.pdf

[SAML-Bindings] Bindings for the OASIS Security Assertion Markup Language (SAML)

http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf

[SAML-Core] Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML)

http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[SAML-Meta] Metadata for the OASIS Security Assertion Markup Language (SAML)

http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

[SAML-Profiles] Profiles for the OASIS Security Assertion Markup Language (SAML)

http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

[WS-AddressingSOAP] Web Services Addressing 1.0 - SOAP Binding

http://www.w3.org/TR/ws-addr-soap/

[WSS-SAML] Web Services Security: SAML Token Profile

http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0.pdf

[XMLSig] XML-Signature Syntax and Processing

http://www.w3.org/TR/xmldsig-core/

4. Contact Information

Ubisecure Solutions, Inc.

www.ubisecure.com
info@ubisecure.com
support@ubisecure.com

<firstname.lastname>@ ubisecure.com

Tekniikantie 14
FIN-02150 Espoo, FINLAND

tel. +358-9-2517 7250
fax +358-9-2517 7070

Registered in Espoo, Finland
reg. nr. FI17487214

About Ubisecure

Ubisecure Solutions, Inc. is a leading partner in providing advanced authentication and authorization solutions for Internet, Intranet and Extranet services. Ubisecure provides application developers, integrators, solution providers and end-user organizations with IT-security software solutions that maximize the competitive advantage of its customers. The Ubisecure product line consists of Ubilogin solutions for authentication and Web Single Sign On access to Internet and Intranet/Extranet services, Ubipass VPN-authentication and Ubisignature electronic signatures. Ubisecure provided authentication utilizes ordinary GSM handsets, challenge-response SMS-messages, one-time passwords in Java-phones, smart cards, Windows Integrated Authentication as well as various third party vendor services and products. Ubisecure has offices in Finland and Sweden.

For more information, visit Ubisecure 's web site at www.ubisecure.com

