Ansira

Brand Management

Single Sign-On Specification

SAML – SSO Service Provider Initiated

SAML – Identity Provider Initiated

Contents

1 SSO - Service Provider Initiated

1.1 Introduction

This section describes Service Provider Initiated SAML process between the Ansira (Service Provider) and our client's IdP that will automatically sign-on and sign-off end-users.

1.2 Definitions

1.2.1 End-User

Ansira client user. A person that accesses the Ansira site through a web browser.

1.2.2 Service Provider

Ansira provides a service to the Ansira client through a web browser.

1.2.3 Client's IdP

The service that tracks employees\agents\etc. and authenticates and sends "who is this person" to the Service Provider.

1.3 Checklist between Ansira & IdP

1.3.1 Login Page

i. The end-user can access the Ansira site by visiting the usual login page.
ii. Ansira will communicate with an end-user's IdP to authenticate the end-user.

1.3.2 Service Provider Initiated Bindings

The following are supported by Ansira to communicate with your IdP:

i. urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
ii. iurn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect

1.3.3 Service Provider X509 Certificate sp.cer

Ansira will supply a public X509 certificate to your IdP for the for any authentication.

1.3.4 IdP X509 Certificate IdP.cer

i. If the public X509 certificate is not within the SAML Response, Ansira will need the certificate.
ii. If the public X509 certificate is within the SAML Response, although not required, Ansira would like to receive a Idp.cer from the IdP. Occasionally, an IdP's certificate unexpectedly changes which causes the authentication to fail. Comparing the IdP.cer to the SAML Response quickly resolves this issue.

1.3.5 Ansira Service Provider Name

urn:Ansira:SvPpoc

1.3.6 IdP Provider Name

Example: urn:YourIdPprovidername

1.3.7 IdP Response of UserName

Ansira supports the following two methodologies for communication of the UserName:

i. UserName as the SUBJECT of the SAML Response
ii. UserName as an ATTRIBUTE of the SAML Response

```
1.  <saml:AttributeStatement>
2.      <saml:Attribute Name="AnyNameYouWant_TellUs" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
    format:basic">
3.          <saml:AttributeValue  xsi:type="xs:string">johndoe@yourcompany.com</saml:AttributeValue>
4.      </saml:Attribute>
5.  </saml:AttributeStatement>
```

1.3.8 IdP Response Formats

(See section below for examples)

i. SAML Response General
ii. SAML Response with Signed Assertion
iii. SAML Response with Signed Message
iv. SAML Response with Signed Message & Assertion
v. SAML Response with Encrypted Assertion
vi. SAML Response with Signed & Encrypted Assertion
vii. SAML Response with Signed Message & Encrypted Assertion
viii. SAML Response with Signed Message, Signed & Encrypted Assertion

1.3.9 Encryption Methodologies

(See section below for examples)

i. Ansira supports various encryption methodologies within a SAML Response on various response nodes.

1.3.10 SP Initiated Logout

i. Ansira, as the Service Provider, OPTIONALLY implements SP Initiated Logouts.
ii. Ansira's logout
https://yourcompanyswebsite.Ansira.com/Login/SAMLLogoutAssertion.aspx
iii. Your IdP's logout URL if not included in the metadata.
iv. Ansira supports logout binding Post.
v. After logout,
a. Ansira can redirect the end-user to any URL.
b. Ansira can just display a message informing the end-user that they have been logged-out.

1.4 Support IdP Response Formats

Ansira, as Service Provider, supports 8 Response Formats from your IdP. Below are examples of these formats.

1.4.1 SAML Response General

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="_8e8dc5f69a98cc4c1ff3427e5ce34606fd672f91e6" Version="2.0" IssueInstant="2021-02-04T06:21:48Z" Destination="http://sp.example.com/demo1/index.php?acs" InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685">
    <saml:Issuer>http://idp.example.com/metadata.php</saml:Issuer>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
    <saml:Assertion xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema" ID="_d71a3a8e9fcc45c9e9d248ef7049393fc8f04e5f75" Version="2.0" IssueInstant="2021-02-04T06:21:48Z">
        <saml:Issuer>http://idp.example.com/metadata.php</saml:Issuer>
        <saml:Subject>
            <saml:NameID SPNameQualifier="http://sp.example.com/demo1/metadata.php" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">_ce3d2948b4cf20146dee0a0b3dd6f69b6cf86f62d7</saml:NameID>
            <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData NotOnOrAfter="2031-02-04T06:21:48Z" Recipient="http://sp.example.com/demo1/index.php?acs" InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685"/>
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions NotBefore="2014-07-17T01:01:18Z" NotOnOrAfter="2031-02-04T06:21:48Z">
            <saml:AudienceRestriction>
                <saml:Audience>http://sp.example.com/demo1/metadata.php</saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement AuthnInstant="2021-02-04T06:21:48Z" SessionNotOnOrAfter="2024-07-17T09:01:48Z" SessionIndex="_be9967abd904ddcae3c0eb4189adbe3f71e327cf93">
            <saml:AuthnContext>
                <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml:AuthnContextClassRef>
            </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement>
            <saml:Attribute Name="uid" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                <saml:AttributeValue xsi:type="xs:string">test</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="mail" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                <saml:AttributeValue xsi:type="xs:string">test@example.com</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="eduPersonAffiliation" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                <saml:AttributeValue xsi:type="xs:string">users</saml:AttributeValue>
                <saml:AttributeValue xsi:type="xs:string">examplerole1</saml:AttributeValue>
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

1.4.2 SAML Response with Signed Assertion

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="_8e8dc5f69a98cc4c1ff3427e5ce34606fd672f91e6" Version="2.0" IssueInstant="2021-02-04T06:21:48Z" Destination="http://sp.example.com/demo1/index.php?acs" InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685">
   <saml:Issuer>http://idp.example.com/metadata.php</saml:Issuer>
   <samlp:Status>
      <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
   </samlp:Status>
   <saml:Assertion xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ID="pfx54bf9610-e426-ff27-4247-91058146e34f" Version="2.0" IssueInstant="2021-02-04T06:21:48Z">
      <saml:Issuer>http://idp.example.com/metadata.php</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="#pfx54bf9610-e426-ff27-4247-91058146e34f">
               <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>CcUYp9v9iZVp3PB5mm1QGnMPYS4=</ds:DigestValue>
            </ds:Reference>
         </ds:SignedInfo>
         <ds:SignatureValue>.....a36Q=</ds:SignatureValue>
         <ds:KeyInfo>
            <ds:X509Data>
               <ds:X509Certificate>MIICajCC….==</ds:X509Certificate>
            </ds:X509Data>
         </ds:KeyInfo>
      </ds:Signature>
      <saml:Subject>
         <saml:NameID SPNameQualifier="http://sp.example.com/demo1/metadata.php" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">_ce3d2948b4cf20146dee0a0b3dd6f69b6cf86f62d7</saml:NameID>
         <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData NotOnOrAfter="2031-02-04T06:21:48Z" Recipient="http://sp.example.com/demo1/index.php?acs" InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685" />
         </saml:SubjectConfirmation>
      </saml:Subject>
      <saml:Conditions NotBefore="2014-07-17T01:01:18Z" NotOnOrAfter="2031-02-04T06:21:48Z">
         <saml:AudienceRestriction>
            <saml:Audience>http://sp.example.com/demo1/metadata.php</saml:Audience>
         </saml:AudienceRestriction>
      </saml:Conditions>
      <saml:AuthnStatement AuthnInstant="2021-02-04T06:21:48Z" SessionNotOnOrAfter="2024-07-17T09:01:48Z" SessionIndex="_be9967abd904ddcae3c0eb4189adbe3f71e327cf93">
         <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml:AuthnContextClassRef>
         </saml:AuthnContext>
      </saml:AuthnStatement>
      <saml:AttributeStatement>
         <saml:Attribute Name="uid" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml:AttributeValue xsi:type="xs:string">test</saml:AttributeValue>
         </saml:Attribute>
         <saml:Attribute Name="mail" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml:AttributeValue xsi:type="xs:string">test@example.com</saml:AttributeValue>
         </saml:Attribute>
         <saml:Attribute Name="eduPersonAffiliation" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml:AttributeValue xsi:type="xs:string">users</saml:AttributeValue>
            <saml:AttributeValue xsi:type="xs:string">examplerole1</saml:AttributeValue>
         </saml:Attribute>
      </saml:AttributeStatement>
   </saml:Assertion>
</samlp:Response>
```

1.4.3 SAML Response with Signed Message

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="pfx77ae59c5-d4ec-69a8-2fe9-321ab7629f0c" Version="2.0" IssueInstant="2021-02-04T06:21:48Z" Destination="http://sp.example.com/demo1/index.php?acs" InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685">
   <saml:Issuer>http://idp.example.com/metadata.php</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="#pfx77ae59c5-d4ec-69a8-2fe9-321ab7629f0c">
            <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>stWvC0zvZqTshl9E7CADCQ71GnU=</ds:DigestValue>
         </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>hpunejSXat c=</ds:SignatureValue>
      <ds:KeyInfo>
         <ds:X509Data>
            <ds:X509Certificate>Xp….==</ds:X509Certificate>
         </ds:X509Data>
      </ds:KeyInfo>
   </ds:Signature>
   <samlp:Status>
      <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
   </samlp:Status>
   <saml:Assertion xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ID="_d71a3a8e9fcc45c9e9d248ef7049393fc8f04e5f75" Version="2.0" IssueInstant="2021-02-04T06:21:48Z">
      <saml:Issuer>http://idp.example.com/metadata.php</saml:Issuer>
      <saml:Subject>
         <saml:NameID SPNameQualifier="http://sp.example.com/demo1/metadata.php" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">_ce3d2948b4cf20146dee0a0b3dd6f69b6cf86f62d7</saml:NameID>
         <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData NotOnOrAfter="2031-02-04T06:21:48Z" Recipient="http://sp.example.com/demo1/index.php?acs" InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685" />
         </saml:SubjectConfirmation>
      </saml:Subject>
      <saml:Conditions NotBefore="2014-07-17T01:01:18Z" NotOnOrAfter="2031-02-04T06:21:48Z">
         <saml:AudienceRestriction>
            <saml:Audience>http://sp.example.com/demo1/metadata.php</saml:Audience>
         </saml:AudienceRestriction>
      </saml:Conditions>
      <saml:AuthnStatement AuthnInstant="2021-02-04T06:21:48Z" SessionNotOnOrAfter="2024-07-17T09:01:48Z" SessionIndex="_be9967abd904ddcae3c0eb4189adbe3f71e327cf93">
         <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml:AuthnContextClassRef>
         </saml:AuthnContext>
      </saml:AuthnStatement>
      <saml:AttributeStatement>
         <saml:Attribute Name="uid" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml:AttributeValue xsi:type="xs:string">test</saml:AttributeValue>
         </saml:Attribute>
         <saml:Attribute Name="mail" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml:AttributeValue xsi:type="xs:string">test@example.com</saml:AttributeValue>
         </saml:Attribute>
         <saml:Attribute Name="eduPersonAffiliation" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml:AttributeValue xsi:type="xs:string">users</saml:AttributeValue>
            <saml:AttributeValue xsi:type="xs:string">examplerole1</saml:AttributeValue>
         </saml:Attribute>
      </saml:AttributeStatement>
   </saml:Assertion>
</samlp:Response>
```

1.4.4 SAML Response with Signed Message & Assertion

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="pfxb3f8da88-54f4-5b96-a497-2515b1939271" Version="2.0" IssueInstant="2021-02-04T06:21:48Z" Destination="http://sp.example.com/demo1/index.php?acs" InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685">
   <saml:Issuer>http://idp.example.com/metadata.php</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="#pfxb3f8da88-54f4-5b96-a497-2515b1939271">
            <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>eN+YapmCUMkIIiVdRH3JDB3EkyA=</ds:DigestValue>
         </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>hmbT3TFzi…. =</ds:SignatureValue>
      <ds:KeyInfo>
         <ds:X509Data>
            <ds:X509Certificate>MIICajCC….==</ds:X509Certificate>
         </ds:X509Data>
      </ds:KeyInfo>
   </ds:Signature>
   <samlp:Status>
      <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
   </samlp:Status>
   <saml:Assertion xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ID="pfx9dfdbf38-54ec-b3d3-e3d1-ee4098062ba2" Version="2.0" IssueInstant="2021-02-04T06:21:48Z">
      <saml:Issuer>http://idp.example.com/metadata.php</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="#pfx9dfdbf38-54ec-b3d3-e3d1-ee4098062ba2">
               <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>r108ZSfRzqCW+nq41R6Eb+vMMhA=</ds:DigestValue>
            </ds:Reference>
         </ds:SignedInfo>
         <ds:SignatureValue>HgXB4pS…….+z8=</ds:SignatureValue>
         <ds:KeyInfo>
            <ds:X509Data>
               <ds:X509Certificate>MIICajCCA…. ==</ds:X509Certificate>
            </ds:X509Data>
         </ds:KeyInfo>
      </ds:Signature>
      <saml:Subject>
         <saml:NameID SPNameQualifier="http://sp.example.com/demo1/metadata.php" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">_ce3d2948b4cf20146dee0a0b3dd6f69b6cf86f62d7</saml:NameID>
         <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData NotOnOrAfter="2031-02-04T06:21:48Z" Recipient="http://sp.example.com/demo1/index.php?acs" InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685" />
         </saml:SubjectConfirmation>
      </saml:Subject>
      <saml:Conditions NotBefore="2014-07-17T01:01:18Z" NotOnOrAfter="2031-02-04T06:21:48Z">
         <saml:AudienceRestriction>
            <saml:Audience>http://sp.example.com/demo1/metadata.php</saml:Audience>
         </saml:AudienceRestriction>
      </saml:Conditions>
      <saml:AuthnStatement AuthnInstant="2021-02-04T06:21:48Z" SessionNotOnOrAfter="2024-07-17T09:01:48Z" SessionIndex="_be9967abd904ddcae3c0eb4189adbe3f71e327cf93">
```

1.4.5 SAML Response with Encrypted Assertion

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="_8e8dc5f69a98cc4c1ff3427e5ce34606fd672f91e6" Version="2.0" IssueInstant="2021-02-04T06:21:48Z" Destination="http://sp.example.com/demo1/index.php?acs" InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685">
   <saml:Issuer>http://idp.example.com/metadata.php</saml:Issuer>
   <samlp:Status>
      <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
   </samlp:Status>
   <saml:EncryptedAssertion>
      <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Type="http://www.w3.org/2001/04/xmlenc#Element">
         <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
         <dsig:KeyInfo>
            <xenc:EncryptedKey>
               <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
               <xenc:CipherData>
                  <xenc:CipherValue>s73amKB……=</xenc:CipherValue>
               </xenc:CipherData>
            </xenc:EncryptedKey>
         </dsig:KeyInfo>
         <xenc:CipherData>
            <xenc:CipherValue>5uEbf…….LDs4=</xenc:CipherValue>
         </xenc:CipherData>
      </xenc:EncryptedData>
   </saml:EncryptedAssertion>
</samlp:Response>
```

1.4.6 SAML Response with Signed & Encrypted Assertion

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="_8e8dc5f69a98cc4c1ff3427e5ce34606fd672f91e6" Version="2.0" IssueInstant="2021-02-04T06:21:48Z" Destination="http://sp.example.com/demo1/index.php?acs" InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685">
   <saml:Issuer>http://idp.example.com/metadata.php</saml:Issuer>
   <samlp:Status>
      <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
   </samlp:Status>
   <saml:EncryptedAssertion>
      <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Type="http://www.w3.org/2001/04/xmlenc#Element">
         <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
         <dsig:KeyInfo>
            <xenc:EncryptedKey>
               <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
               <xenc:CipherData>
                  <xenc:CipherValue>kaSQYbEzP…….. =</xenc:CipherValue>
               </xenc:CipherData>
            </xenc:EncryptedKey>
         </dsig:KeyInfo>
         <xenc:CipherData>
            <xenc:CipherValue>L7IuwnESlIR……FzqtoV =</xenc:CipherValue>
         </xenc:CipherData>
      </xenc:EncryptedData>
   </saml:EncryptedAssertion>
</samlp:Response>
```

1.4.7 SAML Response with Signed Message & Encrypted Assertion

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="pfxd1cac2e8-5d55-bc88-4740-c53f543483c7" Version="2.0" IssueInstant="2021-02-04T06:21:48Z" Destination="http://sp.example.com/demo1/index.php?acs" InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685">
   <saml:Issuer>http://idp.example.com/metadata.php</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="#pfxd1cac2e8-5d55-bc88-4740-c53f543483c7">
            <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>aGs0l+UibHi2zmyh3C+ibim9ruk=</ds:DigestValue>
         </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>hfdibVxZa =</ds:SignatureValue>
      <ds:KeyInfo>
         <ds:X509Data>
            <ds:X509Certificate>MIICajC…… ==</ds:X509Certificate>
         </ds:X509Data>
      </ds:KeyInfo>
   </ds:Signature>
   <samlp:Status>
      <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
   </samlp:Status>
   <saml:EncryptedAssertion>
      <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Type="http://www.w3.org/2001/04/xmlenc#Element">
         <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
         <dsig:KeyInfo>
            <xenc:EncryptedKey>
               <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
               <xenc:CipherData>
                  <xenc:CipherValue>s73am……..KB=</xenc:CipherValue>
               </xenc:CipherData>
            </xenc:EncryptedKey>
         </dsig:KeyInfo>
         <xenc:CipherData>
            <xenc:CipherValue>5uEbf…….=</xenc:CipherValue>
         </xenc:CipherData>
      </xenc:EncryptedData>
   </saml:EncryptedAssertion>
</samlp:Response>
```

1.4.8 SAML Response with Signed Message, Signed & Encrypted Assertion

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="pfx33377d24-1f4c-7d92-eead-44034d80df81" Version="2.0" IssueInstant="2021-02-04T06:21:48Z" Destination="http://sp.example.com/demo1/index.php?acs" InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685">
   <saml:Issuer>http://idp.example.com/metadata.php</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="#pfx33377d24-1f4c-7d92-eead-44034d80df81">
            <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>69Qsb1kuEOkdz6v8vqVpBhN2nRM=</ds:DigestValue>
         </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>VxYae....PLTE=</ds:SignatureValue>
      <ds:KeyInfo>
         <ds:X509Data>
            <ds:X509Certificate>MIICa…. ==</ds:X509Certificate>
         </ds:X509Data>
      </ds:KeyInfo>
   </ds:Signature>
   <samlp:Status>
      <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
   </samlp:Status>
   <saml:EncryptedAssertion>
      <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Type="http://www.w3.org/2001/04/xmlenc#Element">
         <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
         <dsig:KeyInfo>
            <xenc:EncryptedKey>
               <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
               <xenc:CipherData>
                  <xenc:CipherValue>kaSQYb……=</xenc:CipherValue>
               </xenc:CipherData>
            </xenc:EncryptedKey>
         </dsig:KeyInfo>
         <xenc:CipherData>
            <xenc:CipherValue>L7IuwnESlIR =</xenc:CipherValue>
         </xenc:CipherData>
      </xenc:EncryptedData>
   </saml:EncryptedAssertion>
</samlp:Response>
```

1.5 Supported IdP Encryption Methodologies

1.5.1 No encryption at all

1.5.2 Supported Key Encryption Method Type Encryption

http://www.w3.org/2001/04/xmlenc#rsa-1_5
http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p

1.5.3 Supported Data Encryption Method Type Encryption

http://www.w3.org/2001/04/xmlenc#tripledes-cbc
http://www.w3.org/2001/04/xmlenc#aes128-cbc
http://www.w3.org/2001/04/xmlenc#aes192-cbc
http://www.w3.org/2001/04/xmlenc#aes256-cbc

1.5.4 Supported Digest Method Type Encryption

http://www.w3.org/2000/09/xmldsig#sha1
http://www.w3.org/2001/04/xmlenc#sha256

1.5.5 Supported Signature Method Type Encryption

http://www.w3.org/2000/09/xmldsig#rsa-sha1
http://www.w3.org/2001/04/xmldsig-more#rsa-sha256

2 SSO - Identity Provider Initiated

2.1 Introduction

Ansira also supports identity provider initiated authentication. In this model Ansira only supports validation of the response from the client site or the client identify provider and there is no communication from Ansira to the client site or identity provider.

The client generates a SAML Response from an identity provider and this is sent as a HTTP POST parameter named SAMLResponse to the Ansira site. If the response received from the client validates against the certificate provided by the client, then the username supplied in the response is used for authentication. SAML version used is 2.0.

2.2 Definitions

2.2.1 Certificate

Ansira will be supplied with the validating certificate, including a separate certificate for stage if necessary. Ansira will also be supplied with a testing environment to validate the configuration. This can be a client hosted web site or standalone tool.

2.2.2 Response parameter

The SAML response parameter in the post parameter is “SAML Response”. This is a base 64 encoded response string sent by the client site.

2.2.3 Username

Username or UserID is the unique identifier that identifies a user within the Ansira system. The field in the SAML response that will be used for the username is configurable and is identified by the client. This is a required field.

2.2.4 Profile attributes

The Ansira implementation allows for user provisioning on-the-fly. A sample request(s) including all the supported attributes must be provided by the client to allow for the Ansira team to engineer translating the data into the Ansira structure.

2.2.5 User profile fields

These are single value fields such as name, email or multi-value fields such as a list of licensed states provided as a comma separated list

2.2.6 Groups

This is the data that is translated into access roles within the Ansira system. A user can belong to multiple groups.

2.2.7 Managers and Approvers

These nodes can contain multiple respective child nodes. In both cases, the values must be a valid loginname of an existing user on the Ansira application. If a supplied manager or approver name is not a valid user, the mapping is ignored.

2.2.8 Location Codes

This is a list of locations identified by their unique identifier that the user has access to. If the location does not exist, the mapping is ignored.

2.2.9 Date & Time

System looks at the AuthnInstant attribute in the saml:AuthnStatement node to compare against the system timestamp with the allowed leeway for the client.

After the user is authenticated, they will pass through from their intranet system into the Ansira system. The Ansira application will need to be opened in a new window. If the user does not exist or if any of the checks above fails the user is redirected to a failure page.

2.3 Create/Update Users

The identity provider model, supports just in time provisioning with the following modes of pass-through

i. Authentication only
ii. Authenticate and Create only
iii. Authenticate, Create and Update if exists.

2.4 Transferring Data

The client will transfer the authentication information to Ansira using the “POST” method with the parameter SAML Response.

The authentication information is transferred to a target URL to be provided by Ansira.
For example, https://PassThroughURL.Ansira.com/Login/PAuthentication.aspx?configSet=SAML

The communication is encrypted using SSL but the SAML Response parameter cannot be encrypted.

2.5 Testing Notes

For testing, the client will provide a testing environment.

Pass-through should be tested for at least one user belonging to each of the user groups that have been configured for pass-through.