Table of Contents

Overview ................................................................................................................................................................... 3
Configuring OIF as an IdP in Adobe Sign....................................................................................................... 3
Configuring Adobe Sign as a SP in OIF ........................................................................................................... 5
Verifying Email Address as NameID Format ................................................................................................ 9
Overview

Adobe Sign can support Security Assertion Markup Language (SAML) single sign-on (SSO) using external identity providers (IdPs) such as Oracle Identity Federation (11g). This document describes the steps for configuring Adobe Sign, acting as the SAML consumer or service provider (SP), to use OIF. This document also provides suggested steps for configuring OIF, however, please contact your OIF system administrator before making any configuration changes to your OIF Server. Before proceeding, please see the Adobe Sign Single Sign On Using SAML Guide, which describes the SAML set up process and provides detailed information on the SAML Settings in Adobe Sign.

Configuring OIF as an IdP in Adobe Sign

Your organization’s instance of OIF needs to be configured within Adobe Sign as the external SAML Identity Provider (IdP). As an administrator for your Adobe Sign Account, navigate to SAML Setting in Adobe Sign as an (Account | Account Settings | SAML Settings).

You will need metadata information from your OIF IdP configuration. Typically, the metadata for the OIF is available as an XML content at: http://<hostname>:<managedserverport>/fed/idp/metadata. Please contact your OIF administrator to gather the relevant. You will need the following configuration information.

- **Entity ID/Issuer URL**—The entityId attribute on EntityDescriptor element
- **Logout URL/SLO Endpoint**—When someone logs out of Adobe Sign, this URL is called to log them out of the IdP as well.
- **Login URL/SSO Endpoint**—The Location attribute on SingleSignOnService element
- **IdP Certificate**—Certificate information under the element EntityDescriptor -> IDPSSODescriptor -> KeyDescriptor use="signing"
This information should be configured in the appropriate fields in the Adobe Sign SAML configuration. See image below:
Configuring Adobe Sign as a SP in OIF

Once the OIF SAML configuration is complete within the Adobe Sign UI, the next step is to configure Adobe Sign as a Service Provider within OIF. The information required for configuring Adobe Sign within OIF is available on the Adobe Sign SAML Service Provider (SP) information section under Account | Account Settings | SAML Settings.
The metadata description for Adobe Sign is shown below:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:mdns="http://mdns.org/2002/06/metadata/ns"
xmlns:mdext="urn:oasis:names:tc:SAML:metadata:extension"
xmlns:ns10="urn:oasis:names:tc:SAML:profiles:v1metadata"
xmlns:mdnl="urn:oasis:names:tc:SAML:2:0:assertion"
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute" ID="id-mC-OgDSjU-8rnJaELW8wJ7TH78Y3GYRmNW43BdsfasA" cacheDuration="P30D" entityID="http://echosign.com" validUntil="2023-08-23T05:43:11Z">
  <md:SPSSODescriptor
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor
        use="signing">
      <dsig:KeyInfo>
        <dsig:X509Data>
          <dsig:X509Certificate>
            MIIDVjCCAj6gAwIBAgIETgKFaDANBgkqhkiG9w0BAQUFADBtMQswCQYDVQQGEwJVUjEVMBMGA1UEChMKVjEAAAAA
          </dsig:X509Certificate>
        </dsig:X509Data>
      </dsig:KeyInfo>
    </md:KeyDescriptor>
    <md:AssertionConsumerService
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="SP assertion consume URL" index="1" isDefault="true"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

You must customize this metadata description and change the highlighted section in the XML to match the URL for your account. The Assertion Consumer URL for your specific account is shown in SAML Settings (see above).

The steps for completing the configuration in OIF are as follows:

1. Go to the Federations configuration screen on the OIF Administration panel.
2. Create a new federation profile

3. Create a new Service Provider (SP) listing for Adobe Sign
Import the Adobe Sign SP configuration XML or manually create the SP listing using the provider information from the Adobe Sign SAML settings.

4. Complete the configuration. Adobe Sign will appear as a new Service Provider listing in the OIF list of SPs.
Verifying Email Address as NameID Format

Adobe Sign uses email address as the unique user identifier. Before testing the single sign-on one last step is the ensure that the email address field is mapped to the appropriate user attribute within OIF and that email address is enabled as a valid NameID format. See images below: