Configuring a SAML Application with Apple IdMS

What does Apple IdMS support?

- SAML 2.0
  - For Mac and iOS client apps, SAML is supported via an embedded web view for Safari or Chrome.
- SP-Initiated POST-POST binding
- IdP-Initiated POST-POST binding
- Apple IdMS support attributes: FirstName, LastName, email, UniqueID (40 character alphanumeric User ID)

Apple IdMS Metadata

- SAML Testing Environment (UAT) Metadata
  - Entity ID: https://idmsa.apple.com/IDMSWebAuth/SAMLLogin
  - IdP Endpoint: https://idmsac-uat.corp.apple.com/IDMSWebAuth/SAMLLogin
  - IdP Signing Certificate: Refer to the 'SAML Corp Metadata for UAT (Single Cert)' metadata at the end of the file
- SAML Production Environment Metadata
  - Entity ID: https://idmsa.apple.com/IDMSWebAuth/SAMLLogin
  - IdP Endpoint: https://idmsac.corp.apple.com/IDMSWebAuth/SAMLLogin
  - IdP Signing Certificate: Refer to the 'SAML Corp Metadata for Prod (Single Cert)' metadata at the end of the file

Sample Service Provider Metadata

The following data are required from the service provider to configure a SAML integration in the Apple IdMS portal:

- Entity ID: A unique ID for the Service Provider.
- Post back URL: The URL(s) which belong to the Service Provider, where the SAML response will be sent.
- Encryption Certificate: SP certificate used to encrypt the SAML response, sent by the Apple IdP.
- Response attributes: Attributes required by the Service Provider to be sent in the SAML response.
- Authorization Groups: Application groups against which authorization check is done.

Sample SAML Request

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                    ID="ABC"
                    Version="2.0"
                    IssueInstant="2019-06-24T17:21:41Z"
                    AssertionConsumerServiceIndex="0"
                    AttributeConsumingServiceIndex="0"
                    AssertionConsumerServiceURL="ABC"
                    >
    <saml:Issuer>quip</saml:Issuer>
    <samlp:NameIDPolicy AllowCreate="true"
                        Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
                        />
</samlp:AuthnRequest>
```

Sample SAML Response

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
               xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               Destination="ABC"
               ID="A473e2f75-7f2c-4c5c-9329-9cd0988557c0"
               InResponseTo="ABC"
               IssueInstant="2019-06-24T17:21:45.000Z"
               Version="2.0"
               >
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                 Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
                 >AppleSSO</saml:Issuer>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
            <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments" />
            <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
            <Reference URI="#A473e2f75-7f2c-4c5c-9329-9cd0988557c0">
                <Transforms>
                    <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                </Transforms>
                <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
                <DigestValue>yq90ZGtUhrnXagYNfT5rmFZeR8swTN87HzcCLiwzOM0=</DigestValue>
            </Reference>
        </SignedInfo>
        <SignatureValue>ABC</SignatureValue>
        <KeyInfo>
            <X509Data>
                <X509Certificate>ABC=</X509Certificate>
            </X509Data>
        </KeyInfo>
    </Signature>
    <samlp:Status xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <saml2:EncryptedAssertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
        <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                            Id="_fe7828267184de2dae7d34a10fb63438"
                            Type="http://www.w3.org/2001/04/xmlenc#Element"
                            >
            <xenc:EncryptionMethod xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                                   Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"
                                   />
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"
                                    URI="#_a59af520920374e5ed72a72f82c01362"
                                    />
            </ds:KeyInfo>
            <xenc:CipherData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                <xenc:CipherValue>ABC</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedData>
        <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                           Id="_a59af520920374e5ed72a72f82c01362"
                           >
            <xenc:EncryptionMethod xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
```

SAML Corp Metadata for UAT (Single Cert)

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
    <EntityDescriptor xmlns:xsi="https://www.w3.org/2001/XMLSchema-
instance" xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
 entityID="https://idmsa.apple.com/IDMSWebAuth/SAMLLogin">
    <IDPSSODescriptor
        WantAuthnRequestsSigned="false"

protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

        <KeyDescriptor use="signing">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
<ds:X509Certificate>MIIEAjCCAuqgAwIBAgIIf7qScHunBiEwDQYJKoZIhvcNAQELBQ
AwgYUxOzA5BgNVBAMMMkFwcGxlIFNTTyBmb3IgQ2FycmllciBSb290IENlcnRpZmljYXRp
b24gQXV0aG9yaXR5MSQwIgYDVQQLDBtJU1QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxEz
ARBgNVBAoMCkFwcGxlIEluYy4xCzAJBgNVBAYTAlVTMB4XDTIwMDgyMDIxNTQyOVoXDTIy
MDgyMDIxNTQyOVowVDEiMCAGA1UEAwwZc2FtbHNpZ251YXQyMDIwLmFwcGxlLmNvbTEMMA
oGA1UECwwDSVNUMRMwEQYDVQQKDApBcHBsZSBJbmMuMQswCQYDVQQGEwJVUzCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAKm+Um6Y8OIF2t9bjLqZ3tMBPdr406RnUH+nqa
Af7UKRn1RF0jtNDUuELLNq7WObn9ys65EQ0UAJVeNDLHbXJUia8s2TKk/
9twbuP01rLdj7vAj2KMHrol7E8q42cpoeJw+nk++GdSkw1QJf7r/
rP+1pvGLPnvIb7NLaKsOQsI+ZbCwznmSNDdIzLkP8he0tkIu6txh1mqC29mI3e1sRqyFjh
jSgBdqdI+fXrbnUQ9/YkanJzaykQaUIsigcobv/
eWL8hGeqhdqR6xDt0YUrRDfCqer4Tr5W5CUe4AAC4Fx0zMszajLxCyYUG1G62Tvjg27Eok
CAYBGkWix33Z4em8UCAwEAAaOBpTCBojAMBgNVHRMBAf8EAjAAMB8GA1UdIwQYMBaAFA3G
8apLIeyGqdLMPh2+MI4C3edrMEIGCCsGAQUFBwEBBDYwNDAyBggrBgEFBQcwAYYmaHR0cD
ovL29jc3AuYXBwbGUuY29tL29jc3AwMy1zc29hdXRoMDEwHQYDVR0OBBYEFKfIWOicJy73
ZCizpFSvPLJfoJH6MA4GA1UdDwEB/
wQEAwIHgDANBgkqhkiG9w0BAQsFAAOCAQEABv2hmdmfm7XbMUSrQRm8FyTN4k/
sne0ZzlsG+pM5fr8PnrLD+PoRZZFehT6cw9co1Kd98mv4O7kXal8c7p58W/
+J2rBplCrvBi9Ny10W4esTLTMA8o8ilVU5GxHNc1MsyBCdnzYKMcy9eatqoy3Y2EYFjjeR
a1yecIGkT3ymBcklfYvMA6XKK04z+o1o+Ack8NQPsBy+Gph/TORmVRPXML5gznd0+9Hqg/
jOC3mUP/viE2mhOQS8QBrI+8VrsCUwUgPTDSQgzcnkFOVy4A7kRv/
JS3iv5fEwhSu6dNJF64OJpJKpELtiKAv5Th198lzSkj9L0XJ5ilISwX5uC91BUg==</
ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </KeyDescriptor>

        <!-- Supported Name Identifier Formats -->
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:transient</NameIDFormat>

        <!-- AuthenticationRequest Consumer endpoint -->
        <SingleSignOnService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="https://idmsac-uat.corp.apple.com/IDMSWebAuth/
SAMLLogin?CertVersion=v2020"
```

```
            />
        <SingleSignOnService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect"
            Location="https://idmsac-uat.corp.apple.com/IDMSWebAuth/
SAMLLogin?CertVersion=v2020"
            />
    </IDPSSODescriptor>
</EntityDescriptor>
```

SAML Corp Metadata for PROD (Single Cert)

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
    <EntityDescriptor xmlns:xsi="https://www.w3.org/2001/XMLSchema-
instance" xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
 entityID="https://idmsa.apple.com/IDMSWebAuth/SAMLLogin">
    <IDPSSODescriptor
        WantAuthnRequestsSigned="false"

protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

        <KeyDescriptor use="signing">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
<ds:X509Certificate>MIIEATCCAumgAwIBAgIIDSnyDHyWRA8wDQYJKoZIhvcNAQELBQ
AwgYUxOzA5BgNV
BAMMMkFwcGxlIFNTTyBmb3IgQ2FycmllciBSb290IENlcnRpZmljYXRpb24gQXV0
aG9yaXR5MSQwIgYDVQQLDBtJU1QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxEzAR
BgNVBAoMCkFwcGxlIEluYy4xCzAJBgNVBAYTAlVTMB4XDTIwMTExMDIxMTQwNVoX
DTIyMTExMDIxMTQwNVowUzEhMB8GA1UEAwwYc2FtbHNpZ25wcm9kdjEuYXBwbGUu
Y29tMQwwCgYDVQQLDANJU1QxEzARBgNVBAoMCkFwcGxlIEluYy4xCzAJBgNVBAYT
AlVTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA14n0ERTIbMyAVyAK
lXDBZdcfSszWzNbkH+bRJeUfhdwdy8J1bHBK+uX4DWJxUjnoR5diDyApdYS8G3zu
X9py6Lp84P/1QIGm9DrZztXMHi3ICwTVEX1U6F6nL/nctZ34WN2jREZtq9D/Oeaw
gY5uWqwcOlxACXI4kaeapqCIL8/9m0pa4mp+3FNQv7qVS9CtTnVSBD+9SoAJZNJr
rkn8hcKBk7EI8CTZZqGbGOj8uq8UZj+j5+koTFd4vEwGh3PMeQAr69FNstPy7WMq
WftRp8qoGZ4nfK+ZS6gX7Kd0mJK2FQosUYxk6cOWbscT8U5shNhIOxZoDSONMVUU
FfMcoQIDAQABo4GlMIGiMAwGA1UdEwEB/wQCMAAwHwYDVR0jBBgwFoAUDcbxqksh
7Iap0sw+Hb4wjgLd52swQgYIKwYBBQUHAQEENjA0MDIGCCsGAQUFBzABhiZodHRw
Oi8vb2NzcC5hcHBsZS5jb20vb2NzcDAzLXNzb2F1dGgwMTAdBgNVHQ4EFgQUC0Oi
FiGyv/d2mDSdB5bt10LEJ2swDgYDVR0PAQH/BAQDAgeAMA0GCSqGSIb3DQEBCwUA
A4IBAQCXZmYuSYI5UxYqOLXv8Ybqj4LP3ZQaKizdph0Ihs8JbuSgGpe037W9KlAa
BJcrpGO3suQ4nJ27AMc8r0u0emovk1bqDgAMhR69Tag60DjdP+cGs+UdLdzfNWBZ
U5MujB6x+HbeXeN+1tmeD3sZTobj0fZa3o+ifHZeHc+bFEHPXEhh1F/OV+Ed/qd0
ksVlS8u8/Fx8wH3B8bfC7nfcppcYQtxIAuG3QHIUatCZ0Hjh89Q+8OiO/D6aDNYA
mOIqlaI37bxC5lVh+JSYQcry+wG8+NS0fgRWZWk9ZyR2hjfj7VDfyiyu6CDTPh5s
Tqm4tZY57od+5jASv6BqDON/bqZi
</ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </KeyDescriptor>

        <!-- Supported Name Identifier Formats -->
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:transient</NameIDFormat>

        <!-- AuthenticationRequest Consumer endpoint -->
        <SingleSignOnService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="https://idmsac.corp.apple.com/IDMSWebAuth/
SAMLLogin?CertVersion=v2020"
```

```
            />
        <SingleSignOnService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect"
            Location="https://idmsac.corp.apple.com/IDMSWebAuth/
SAMLLogin?CertVersion=v2020"
            />
    </IDPSSODescriptor>
</EntityDescriptor>
```