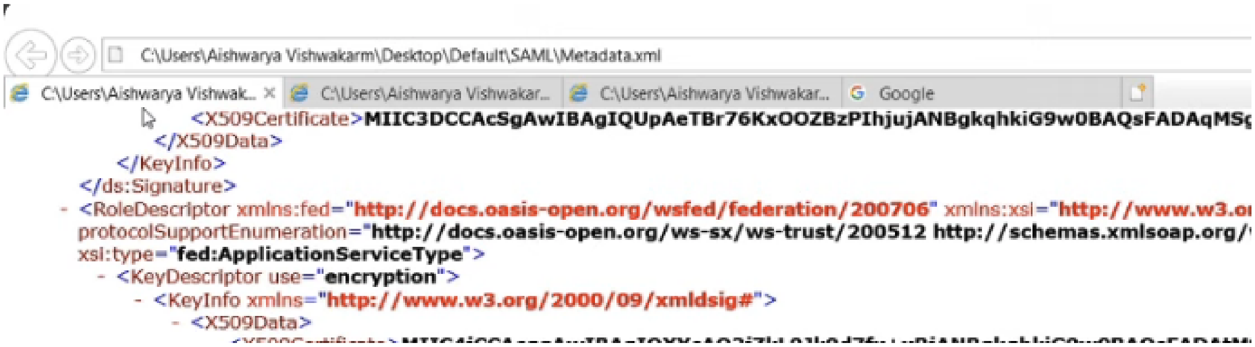
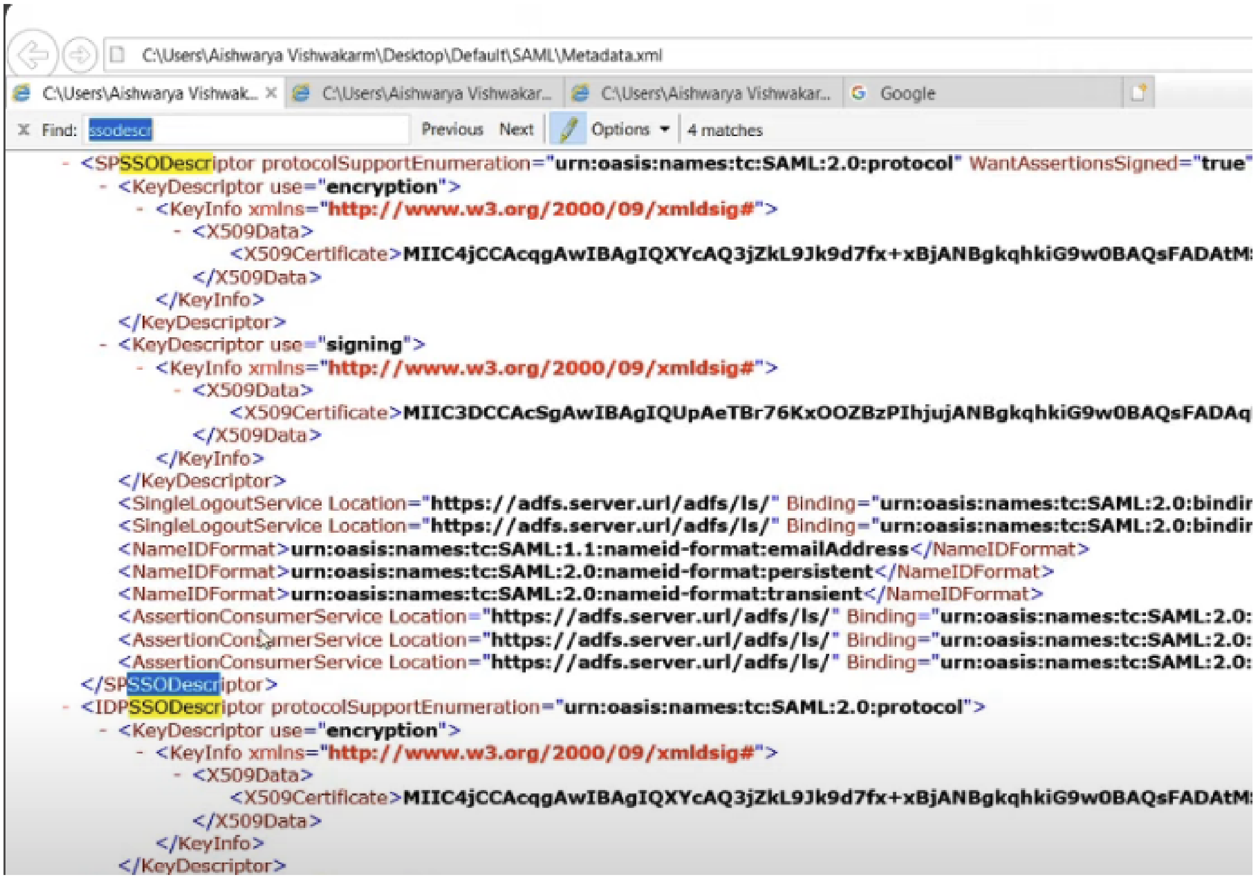

C:\Users\Aishwarya Vishwakarm\Desktop\Default\SAML\Metadata.xml
C:\Users\Aishwarya Vishwak... ×
C:\Users\Aishwarya Vishwakar...
C:\Users\Aishwarya Vishwakar...
Google

```
          <X509Certificate>MIIC3DCCAcSgAwIBAgIQUpAeTBr76KxOOZBzPIhjujANBgkqhkiG9w0BAQsFADAqMS
        </X509Data>
      </KeyInfo>
    </ds:Signature>
  - <RoleDescriptor xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706" xmlns:xsi="http://www.w3.o
    protocolSupportEnumeration="http://docs.oasis-open.org/ws-sx/ws-trust/200512 http://schemas.xmlsoap.org/
    xsi:type="fed:ApplicationServiceType">
    - <KeyDescriptor use="encryption">
      - <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        - <X509Data>
```

Metadata xml : It can be SP or IDP. entity id signing certificates and endpoints - we should be interested in this.

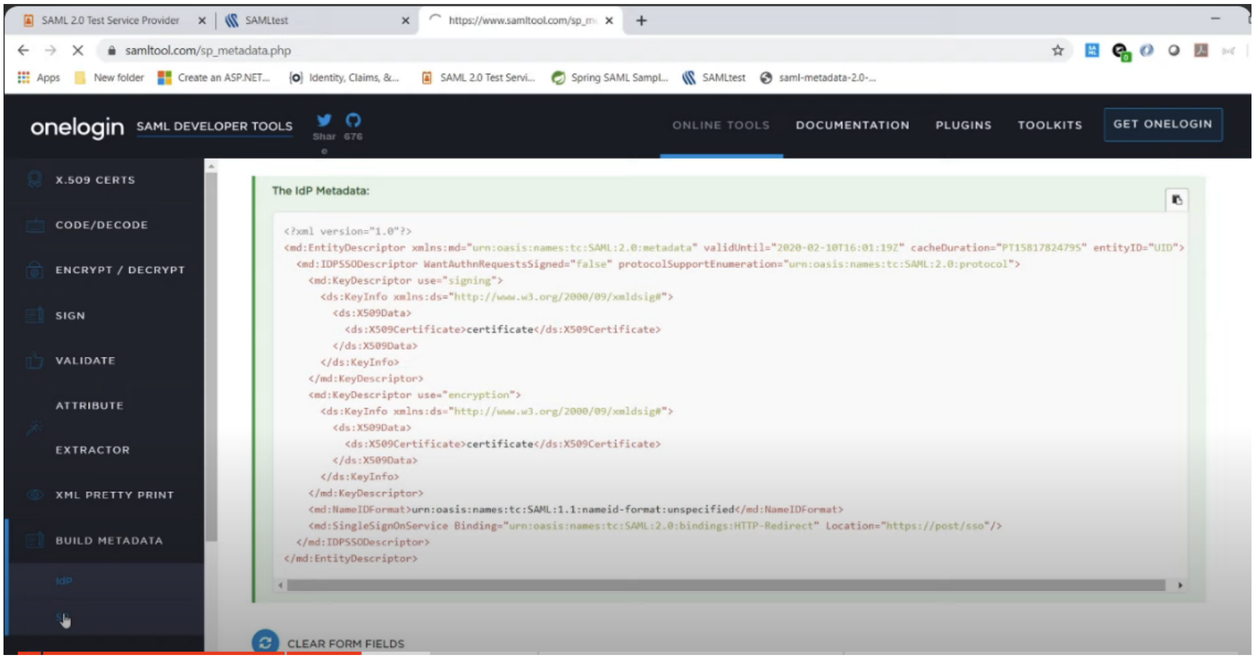
Endpoint - In sp ACS (AssertionConsumerService Location). In the IDP SingleSingOnService location.

How to find metadata xml is related to sp or idp. Search for the SSODescriptor tag. In idp we only find IDPSSODescriptor tag. In sp we find both SPSSODescriptor and IDPSSODescriptor tags


C:\Users\Aishwarya Vishwakarm\Desktop\Default\SAML\Metadata.xml
C:\Users\Aishwarya Vishwak... ×
C:\Users\Aishwarya Vishwakar...
C:\Users\Aishwarya Vishwakar...
Google
× Find: ssodescr
Previous
Next
Options ▾
4 matches

```
  - <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true"
    - <KeyDescriptor use="encryption">
      - <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        - <X509Data>
            <X509Certificate>MIIC4jCCAcqgAwIBAgIQXYcAQ3jZkL9Jk9d7fx+xBjANBgkqhkiG9w0BAQsFADAtM
          </X509Data>
        </KeyInfo>
      </KeyDescriptor>
    - <KeyDescriptor use="signing">
      - <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        - <X509Data>
            <X509Certificate>MIIC3DCCAcSgAwIBAgIQUpAeTBr76KxOOZBzPIhjujANBgkqhkiG9w0BAQsFADAq
          </X509Data>
        </KeyInfo>
      </KeyDescriptor>
      <SingleLogoutService Location="https://adfs.server.url/adfs/ls/" Binding="urn:oasis:names:tc:SAML:2.0:bindir
      <SingleLogoutService Location="https://adfs.server.url/adfs/ls/" Binding="urn:oasis:names:tc:SAML:2.0:bindir
      <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
      <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat>
      <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
      <AssertionConsumerService Location="https://adfs.server.url/adfs/ls/" Binding="urn:oasis:names:tc:SAML:2.0:
      <AssertionConsumerService Location="https://adfs.server.url/adfs/ls/" Binding="urn:oasis:names:tc:SAML:2.0:
      <AssertionConsumerService Location="https://adfs.server.url/adfs/ls/" Binding="urn:oasis:names:tc:SAML:2.0:
    </SPSSODescriptor>
  - <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    - <KeyDescriptor use="encryption">
      - <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        - <X509Data>
            <X509Certificate>MIIC4jCCAcqgAwIBAgIQXYcAQ3jZkL9Jk9d7fx+xBjANBgkqhkiG9w0BAQsFADAtM
          </X509Data>
        </KeyInfo>
      </KeyDescriptor>
```

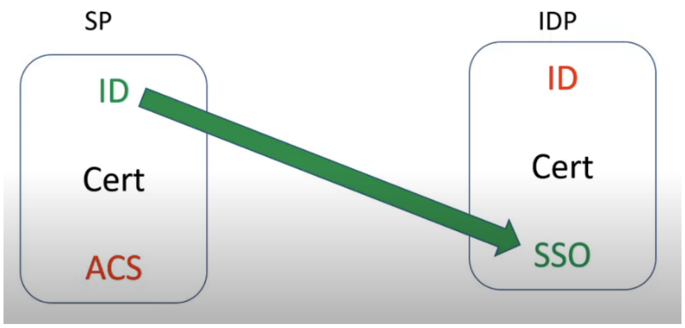
We can create sp and idp files using samltool.com as shown below.



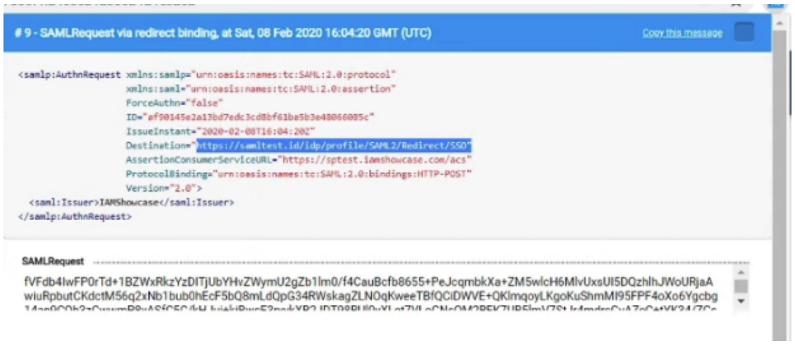
The IdP Metadata:

```
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2020-02-10T16:01:19Z" cacheDuration="PT1581782479S" entityID="UID">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>certificate</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:KeyDescriptor use="encryption">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>certificate</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://post/sso"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

SAML Request - it is a request made by SP to IDP. it contains endpoints that are shared in meta-data file.



In SAML request it is going to destination - SSO url of IDP

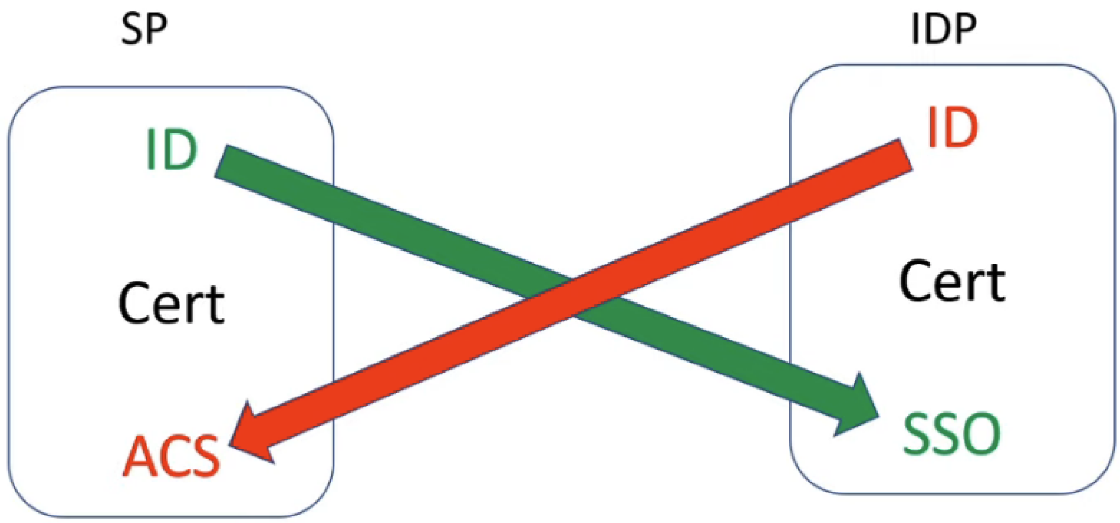


9 - SAMLRequest via redirect binding, at Sat, 08 Feb 2020 16:04:20 GMT (UTC)

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                    ForceAuthn="false"
                    ID="af90145e2a13bd7edc3cd8bf61ba5b3e48066085c"
                    IssueInstant="2020-02-08T16:04:20Z"
                    Destination="https://samltest.id/idp/profile/SAML2/Redirect/SSO"
                    AssertionConsumerServiceURL="https://sptest.iamshowcase.com/acs"
                    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                    Version="2.0">
  <saml:Issuer>IAMShowcase</saml:Issuer>
</samlp:AuthnRequest>
```

SAMLRequest

```
fVFdb4IwFP0rTd+1BZWxRkzYzDITjUbYHvZWymU2gZb1lm0/f4CauBcfb8655+PeJcqmbkXa+ZM5wlcH6MlvUxsUI5DQzhlhJWoURjaA
wiuRpbutCKdctM56q2xNb1bub0hEcF5bQ8mLdQpG34RWskagZLNOqKweeTBfQCiDWVE+QKlmqoyLKgoKuShmMI95FPF4oXo6Ygcbg
```



Simplest explanation of overall picture.