SSO Technical Requirements

Before configuring Core SSO, the following requirements must be met:

1. A valid Identity Provider (IdP) must be configured with the SAML 2.0 Web Browser profile in accordance with the SAML 2.0 OASIS standard and must provide a valid IdP metadata file containing:
    a. X509 RSA 2048 bits Public Certificate (RFC 5280) ( ).
    b. **EntityId** ( ).
    c. **SingleSignOnService** URL with HTTP Redirect Binding ( ).
    d. **NameIDFormat** in `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`.
2. IdP must communicate using HTTP over TLS [RFC 2818].
3. A SHA-256 signature in the metadata, response, and/or assertion.

EXAMPLE

```
entityID="https://idp/saml/metadata/622342">

        MIIEFzCCAv…

    urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
```

4. Certificates must have at least a three-year expiry and should be valid a minimum of 8 months before expiring.
5. The RCS profile requires at least the message or the assertion to be signed.
6. The username used for the assertion subject statement should be the user's primary email address.

> The username should be identical to the email address used to register the user in Core.