Manual setup of SSO config

This doc will be useful even if doing an import using a Federation Metadata XML URL, as the field mappings are not yet importable, and they can be gleaned in the same way as in the manual setup.

The first thing we need is the Metadata XML file. If provided the URL, visit that page to find the details

We need the following from the XML contents:

- An Entity ID
- A login URL
- An x509 certificate
- Field mappings (1 unique, preferably 1 each for email, first name, last name)

An example XML file is in the code block below (from 1 of our Azure active directories), and we can find the above by searching:

- `entityID` - at the top, it is `entityID="https://sts.windows.net/667d9a8d-34fd-4ea9-99a5-b740e26edaac/"`. We copy `https://sts.windows.net/667d9a8d-34fd-4ea9-99a5-b740e26edaac/` (the final forward-slash is important) over to the SSO config
- `SignOnService` - at the bottom, it is `<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://login.microsoftonline.com/667d9a8d-34fd-4ea9-99a5-b740e26edaac/saml2" />`. We copy over `https://login.microsoftonline.com/667d9a8d-34fd-4ea9-99a5-b740e26edaac/saml2`
- `X509Certificate` - near the top, in a truncated form, it is `<ds:X509Certificate>MIIC8DCCAdigAwIBA...</ds:X509Certificate>`. We copy over the MII... value
- `ClaimType` - we have a number of fields here under ClaimType, we want to map 1 that indicates it is unique to `Unique ID` our end, and then 1 each for whichever seems like first name, last name and email. Note that if there is no unique ID field, you could probably specify the email field as the unique ID field. In this instance, we do have a unique ID field, so we set up the field mappings:
  - Unique ID - `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier`
  - First name - `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname`
  - Last name - `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname`
  - Email - `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`

```
<?xml version="1.0" encoding="utf-8"?>
<EntityDescriptor ID="_bdf4eff3-677d-403c-a423-f1f87b0d2e0b"
entityID="https://sts.windows.net/667d9a8d-34fd-4ea9-99a5-b740e26edaac/"
```

```
□xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
□<Signature
□□xmlns="http://www.w3.org/2000/09/xmldsig#">
□□<SignedInfo>
□□□<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
□□□<SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
□□□<Reference URI="#_bdf4eff3-677d-403c-a423-f1f87b0d2e0b">
□□□□<Transforms>
□□□□□<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
□□□□□<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
□□□□</Transforms>
□□□□<DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
□□□□<DigestValue>qVgiVoBjIPqfd5mkAsKdIHvBesKcG/jm3AbuvzSmX6M=</DigestValue>
□□□</Reference>
□□</SignedInfo>
□□<SignatureValue>o3HzUbjf88RoxzNEV6QNhh5jyw+vWtKRxSkqrslORCH0w+P/DW9vG7sYnCjj66lVK7duHb07SBrI
+hAeEXmqEkAW0bSd+dQzXhz3fG8JJOGUaolxg7zJ3K8vDkKFnboKR1XLa60YEPLuCh5ehfg3A8STeE0kp5ky+kvU0BBEkG
ZBKCNEVx0cqZh2m6Wembu2C8xS4Ea/M2R64dnO3/NKYkcxElvYYjS91HJoYc0MWnl2K6xHY8CCxFgqnHsnXHCNnucKZTp8
N4kiM4AxSWTaJw+Pwlh3vPgZNFuQuFhIvkAsLRW8kZzlan/CAYxZ5n3qoJhzjZM31u9gJgihyqSwyw==</SignatureVal
ue>
□□<KeyInfo>
□□□<ds:X509Data
□□□□xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
□□□□<ds:X509Certificate>MIIC8DCCAdigAwIBAgIQeVvBFeMM35dJLAPSmvEdrzANBgkqhkiG9w0BAQsFADA0MTIwMA
YDVQQDEylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMTA3MTYxMzQ0MjhaFw0yNDA3
MTYxMzQ0MjhaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjANBg
kqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7XgcoVwAoh3d4MufKF61mf58inL9sAyCLEC6Rhx+7ZiyT730dK9y+IwvpIU7
c1G0bmfQs51oJ5EdHv+GipDepg4zR8HRlJup9HnSlOhMkaFR+BMsmV19r9rD+beLM+kbNW3/YAISBxGk6OQ0QpNbv0cw6W
Odv7+WfCUFWcU6NbYx12viF3e9HlgXSA6+JoGM3dSIqw1SqE417aCFnTxuGS6b84YKBmlX7Jkr0a5Ekh3JwHqokDMvWmwF
dV8/eSJm4PABqbkLOUih3wMNpdEngx/jilqnD2b26n1TEie0zB0e2F1JINLGtoJh6lFiyrql/Pd6uqLEcBli6vJPC1qo4Q
IDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDnPR2s4jABwzJPB3/W2fDSX60PGGA4HVW9YTxv1CtZVXtG/e8uqLAsjSeOhlB3
TTevhAMxxPn1xx/u0i9RE2j6RMMTFS40omhwZ4+0Go02oV6YDPZPkyPvKdwTD6/TywZ0A8ZVThw0UoO4z9O85Sub3rJvVQ
42cFR5RlKxRgiNvdZ5GVIZ6lZqQWPuq4Z35Iiq3OF131dYWyIglL6aWGh3AjfkqHYFD0ufqK6ZzSZXMd1vthGgzmJGAUv3
B4K0X5V0YSBxQSh8rVcQ5c9Pg/k1Yg/xf9sVgimCLCEYFAn/LhX7Un2W9xOIS/zTscfLW+X/wloaD+PPMNSkpNh0b4O3</
ds:X509Certificate>
□□□</ds:X509Data>
□□</KeyInfo>
□</Signature>
□<RoleDescriptor xsi:type="fed:SecurityTokenServiceType"
protocolSupportEnumeration="http://docs.oasis-open.org/wsfed/federation/200706"
□□xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
□□xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706">
□□<KeyDescriptor use="signing">
□□□<KeyInfo
□□□□xmlns="http://www.w3.org/2000/09/xmldsig#">
□□□□<X509Data>
□□□□□<X509Certificate>MIIC8DCCAdigAwIBAgIQeVvBFeMM35dJLAPSmvEdrzANBgkqhkiG9w0BAQsFADA0MTIwMAYD
VQQDEylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMTA3MTYxMzQ0MjhaFw0yNDA3MT
YxMzQ0MjhaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7XgcoVwAoh3d4MufKF61mf58inL9sAyCLEC6Rhx+7ZiyT730dK9y+IwvpIU7c1
G0bmfQs51oJ5EdHv+GipDepg4zR8HRlJup9HnSlOhMkaFR+BMsmV19r9rD+beLM+kbNW3/YAISBxGk6OQ0QpNbv0cw6WOd
v7+WfCUFWcU6NbYx12viF3e9HlgXSA6+JoGM3dSIqw1SqE417aCFnTxuGS6b84YKBmlX7Jkr0a5Ekh3JwHqokDMvWmwFdV
8/eSJm4PABqbkLOUih3wMNpdEngx/jilqnD2b26n1TEie0zB0e2F1JINLGtoJh6lFiyrql/Pd6uqLEcBli6vJPC1qo4QID
AQABMA0GCSqGSIb3DQEBCwUAA4IBAQDnPR2s4jABwzJPB3/W2fDSX60PGGA4HVW9YTxv1CtZVXtG/e8uqLAsjSeOhlB3TT
evhAMxxPn1xx/u0i9RE2j6RMMTFS40omhwZ4+0Go02oV6YDPZPkyPvKdwTD6/TywZ0A8ZVThw0UoO4z9O85Sub3rJvVQ42
cFR5RlKxRgiNvdZ5GVIZ6lZqQWPuq4Z35Iiq3OF131dYWyIglL6aWGh3AjfkqHYFD0ufqK6ZzSZXMd1vthGgzmJGAUv3B4
K0X5V0YSBxQSh8rVcQ5c9Pg/k1Yg/xf9sVgimCLCEYFAn/LhX7Un2W9xOIS/zTscfLW+X/wloaD+PPMNSkpNh0b4O3</X5
09Certificate>
□□□□</X509Data>
□□□</KeyInfo>
□□</KeyDescriptor>
□□<fed:ClaimTypesOffered>
□□□<auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"
□□□□xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706">
□□□□<auth:DisplayName>Name</auth:DisplayName>
□□□□<auth:Description>The mutable display name of the user.</auth:Description>
□□□</auth:ClaimType>
□□□<auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier"
□□□□xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706">
□□□□<auth:DisplayName>Subject</auth:DisplayName>
□□□□<auth:Description>An immutable, globally unique, non-reusable identifier of the user that is
unique to the application for which a token is issued.</auth:Description>
□□□</auth:ClaimType>
□□□<auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"
□□□□xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706">
□□□□<auth:DisplayName>Given Name</auth:DisplayName>
□□□□<auth:Description>First name of the user.</auth:Description>
□□□</auth:ClaimType>
□□□<auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname"
□□□□xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706">
□□□□<auth:DisplayName>Surname</auth:DisplayName>
□□□□<auth:Description>Last name of the user.</auth:Description>
```

```
□□□</auth:ClaimType>
□□□<auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
□□□□xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706">
□□□□<auth:DisplayName>Email</auth:DisplayName>
□□□□<auth:Description>Email address of the user.</auth:Description>
□□□</auth:ClaimType>
□□</fed:ClaimTypesOffered>
□□<fed:SecurityTokenServiceEndpoint>
□□□<wsa:EndpointReference
□□□□xmlns:wsa="http://www.w3.org/2005/08/addressing">
□□□□<wsa:Address>https://login.microsoftonline.com/667d9a8d-34fd-4ea9-99a5-
b740e26edaac/wsfed</wsa:Address>
□□□</wsa:EndpointReference>
□□</fed:SecurityTokenServiceEndpoint>
□□<fed:PassiveRequestorEndpoint>
□□□<wsa:EndpointReference
□□□□xmlns:wsa="http://www.w3.org/2005/08/addressing">
□□□□<wsa:Address>https://login.microsoftonline.com/667d9a8d-34fd-4ea9-99a5-
b740e26edaac/wsfed</wsa:Address>
□□□</wsa:EndpointReference>
□□</fed:PassiveRequestorEndpoint>
□</RoleDescriptor>
□<RoleDescriptor xsi:type="fed:ApplicationServiceType"
protocolSupportEnumeration="http://docs.oasis-open.org/wsfed/federation/200706"
□□xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
□□xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706">
□□<KeyDescriptor use="signing">
□□□<KeyInfo
□□□□xmlns="http://www.w3.org/2000/09/xmldsig#">
□□□□<X509Data>
□□□□□<X509Certificate>MIIC8DCCAdigAwIBAgIQeVvBFeMM35dJLAPSmvEdrzANBgkqhkiG9w0BAQsFADA0MTIwMAYD
VQQDEylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMTA3MTYxMzQ0MjhaFw0yNDA3MT
YxMzQ0MjhaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7XgcoVwAoh3d4MufKF61mf58inL9sAyCLEC6Rhx+7ZiyT730dK9y+IwvpIU7c1
G0bmfQs51oJ5EdHv+GipDepg4zR8HRlJup9HnSlOhMkaFR+BMsmV19r9rD+beLM+kbNW3/YAISBxGk6OQ0QpNbv0cw6WOd
v7+WfCUFWcU6NbYx12viF3e9HlgXSA6+JoGM3dSIqw1SqE417aCFnTxuGS6b84YKBmlX7Jkr0a5Ekh3JwHqokDMvWmwFdV
8/eSJm4PABqbkLOUih3wMNpdEngx/jilqnD2b26n1TEie0zB0e2F1JINLGtoJh6lFiyrql/Pd6uqLEcBli6vJPC1qo4QID
AQABMA0GCSqGSIb3DQEBCwUAA4IBAQDnPR2s4jABwzJPB3/W2fDSX60PGGA4HVW9YTxv1CtZVXtG/e8uqLAsjSeOhlB3TT
evhAMxxPn1xx/u0i9RE2j6RMMTFS40omhwZ4+0Go02oV6YDPZPkyPvKdwTD6/TywZ0A8ZVThw0UoO4z9O85Sub3rJvVQ42
cFR5RlKxRgiNvdZ5GVIZ6lZqQWPuq4Z35Iiq3OF131dYWyIglL6aWGh3AjfkqHYFD0ufqK6ZzSZXMd1vthGgzmJGAUv3B4
K0X5V0YSBxQSh8rVcQ5c9Pg/k1Yg/xf9sVgimCLCEYFAn/LhX7Un2W9xOIS/zTscfLW+X/wloaD+PPMNSkpNh0b4O3</X5
```

```
09Certificate>
□□□□</X509Data>
□□□</KeyInfo>
□□</KeyDescriptor>
□□<fed:TargetScopes>
□□□<wsa:EndpointReference
□□□□xmlns:wsa="http://www.w3.org/2005/08/addressing">
□□□□<wsa:Address>https://sts.windows.net/667d9a8d-34fd-4ea9-99a5-b740e26edaac/</wsa:Address>
□□□</wsa:EndpointReference>
□□</fed:TargetScopes>
□□<fed:ApplicationServiceEndpoint>
□□□<wsa:EndpointReference
□□□□xmlns:wsa="http://www.w3.org/2005/08/addressing">
□□□□<wsa:Address>https://login.microsoftonline.com/667d9a8d-34fd-4ea9-99a5-
b740e26edaac/wsfed</wsa:Address>
□□□</wsa:EndpointReference>
□□</fed:ApplicationServiceEndpoint>
□□<fed:PassiveRequestorEndpoint>
□□□<wsa:EndpointReference
□□□□xmlns:wsa="http://www.w3.org/2005/08/addressing">
□□□□<wsa:Address>https://login.microsoftonline.com/667d9a8d-34fd-4ea9-99a5-
b740e26edaac/wsfed</wsa:Address>
□□□</wsa:EndpointReference>
□□</fed:PassiveRequestorEndpoint>
□</RoleDescriptor>
□<IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
□□<KeyDescriptor use="signing">
□□□<KeyInfo
□□□□xmlns="http://www.w3.org/2000/09/xmldsig#">
□□□□<X509Data>
□□□□□<X509Certificate>MIIC8DCCAdigAwIBAgIQeVvBFeMM35dJLAPSmvEdrzANBgkqhkiG9w0BAQsFADA0MTIwMAYD
VQQDEylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMTA3MTYxMzQ0MjhaFw0yNDA3MT
YxMzQ0MjhaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7XgcoVwAoh3d4MufKF61mf58inL9sAyCLEC6Rhx+7ZiyT730dK9y+IwvpIU7c1
G0bmfQs51oJ5EdHv+GipDepg4zR8HRlJup9HnSlOhMkaFR+BMsmV19r9rD+beLM+kbNW3/YAISBxGk6OQ0QpNbv0cw6WOd
v7+WfCUFWcU6NbYx12viF3e9HlgXSA6+JoGM3dSIqw1SqE417aCFnTxuGS6b84YKBmlX7Jkr0a5Ekh3JwHqokDMvWmwFdV
8/eSJm4PABqbkLOUih3wMNpdEngx/jilqnD2b26n1TEie0zB0e2F1JINLGtoJh6lFiyrql/Pd6uqLEcBli6vJPC1qo4QID
AQABMA0GCSqGSIb3DQEBCwUAA4IBAQDnPR2s4jABwzJPB3/W2fDSX60PGGA4HVW9YTxv1CtZVXtG/e8uqLAsjSeOhlB3TT
evhAMxxPn1xx/u0i9RE2j6RMMTFS40omhwZ4+0Go02oV6YDPZPkyPvKdwTD6/TywZ0A8ZVThw0UoO4z9O85Sub3rJvVQ42
cFR5RlKxRgiNvdZ5GVIZ6lZqQWPuq4Z35Iiq3OF131dYWyIglL6aWGh3AjfkqHYFD0ufqK6ZzSZXMd1vthGgzmJGAUv3B4
K0X5V0YSBxQSh8rVcQ5c9Pg/k1Yg/xf9sVgimCLCEYFAn/LhX7Un2W9xOIS/zTscfLW+X/wloaD+PPMNSkpNh0b4O3</X5
```

```
09Certificate>
□□□□</X509Data>
□□□</KeyInfo>
□□</KeyDescriptor>
□□<SingleLogoutService Binding="urn: oasis: names: tc: SAML: 2. 0: bindings: HTTP- Redirect"
Location="https: //login. microsoftonline. com/667d9a8d- 34fd- 4ea9- 99a5- b740e26edaac/saml2" />
□□<SingleSignOnService Binding="urn: oasis: names: tc: SAML: 2. 0: bindings: HTTP- Redirect"
Location="https: //login. microsoftonline. com/667d9a8d- 34fd- 4ea9- 99a5- b740e26edaac/saml2" />
□□<SingleSignOnService Binding="urn: oasis: names: tc: SAML: 2. 0: bindings: HTTP- POST"
Location="https: //login. microsoftonline. com/667d9a8d- 34fd- 4ea9- 99a5- b740e26edaac/saml2" />
□</IDPSSODescriptor>
</EntityDescriptor>
```

Revision #1
Created 17 May 2024 07:57:35 by Daniel Jianoran
Updated 12 June 2024 08:12:39 by Daniel Jianoran