

# Single-Sign-On

CrowdComms currently supports SSO via the SAML2 standard. This is an enterprise-grade industry standard to allow users to authenticate between Identity Providers (IDPs) and Service Providers (SPs). The CrowdComms platform is a Service Provider and examples of IDPs include Microsoft Active Directory, OneLogin, Okta and others.

- [FREQUENTLY ASKED QUESTIONS](#)
- [INTRODUCTION](#)
- [SAML2](#)
- [Shared SSO between apps](#)
- [Manual setup of SSO config](#)

# FREQUENTLY ASKED QUESTIONS

**Q:** Do all the delegates still need to be registered on the site as usual?

**A:** No if they're logging in via their company's directory. With SSO, the user's basic information such as First name, Last name, Email, and Phone number will be auto-populated in the event app.

**Q:** My event will consist of delegates from my own company and speakers from outside the company, can I still use SSO?

**A:** Yes, delegates from within the company who has been authenticated will be able to utilise the SSO function. The speakers from outside the company will be able to log in to the event app using their username and password.

**Q:** Not everyone in my company's Active Directory will be invited to my company's event, can I still use SSO and tailor only the relevant people to have access to the event app?

**A:** Yes, once your business IT contact has set up the SAML2, you can work with them to decide who from your company should get delegate access to the event app.

# INTRODUCTION

## SINGLE SIGN-ON (SSO)

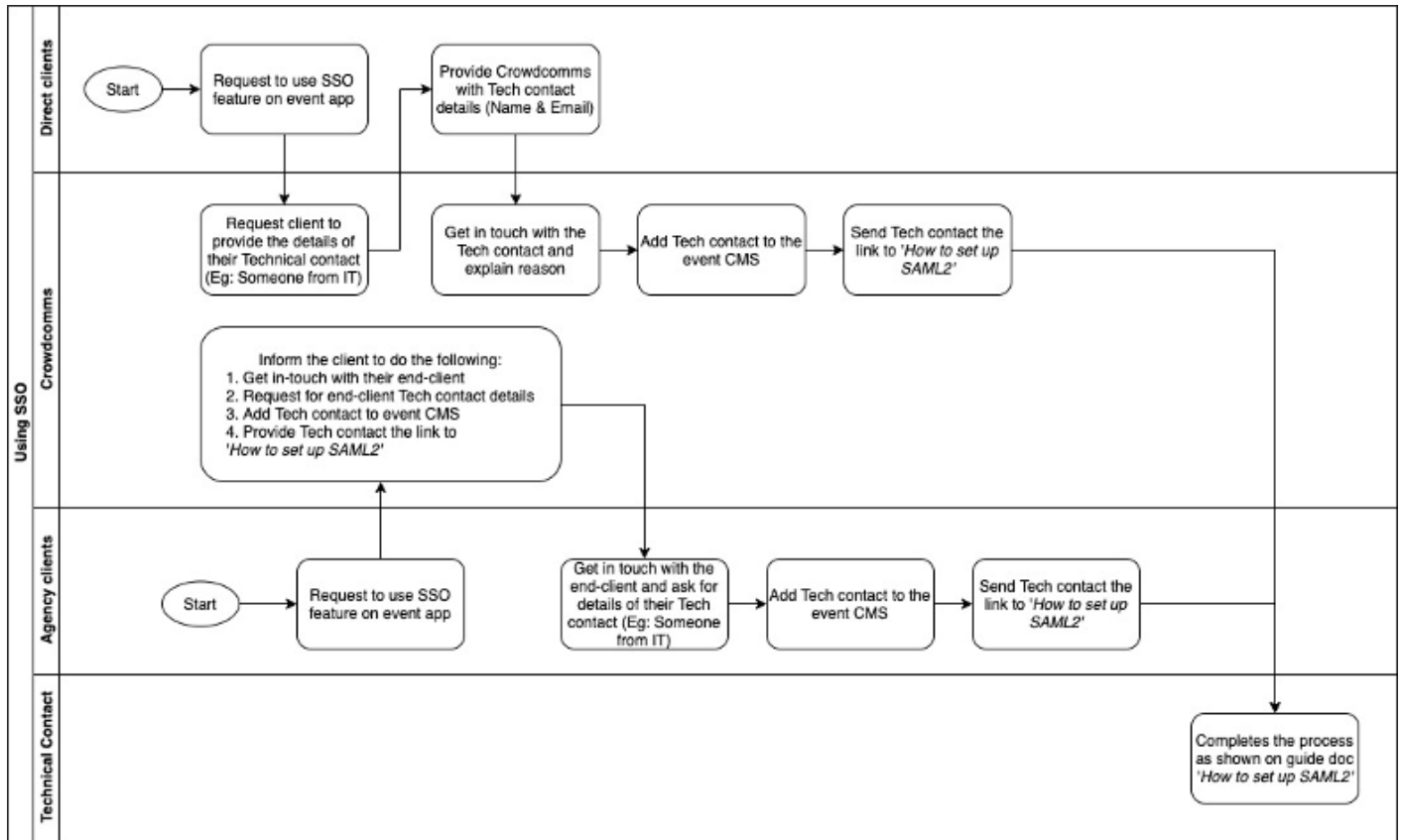
Single sign-on (SSO) is an authentication process that allows a user to use one set of login credentials, for example, a username and password, to access multiple applications.

## PURPOSE

SSO helps clients and their users with the challenge of maintaining the different credentials for different applications separately which streamlines the process of signing on without the need to re-enter the password. With SSO end-users time and efforts get minimized as they don't need to constantly sign in and out separately into multiple applications.

## PROCESS

Setting up SSO must be done by the client's IT department or technical personal. The setup will involve authenticating the Identity Prover (IDP) i.e., the client with the Service Provider (SP) i.e., Crowdcomms event platform.



# SAML2

How **does SSO work**? **SSO works** based upon a trust relationship set up between an application, known as the service provider, and an identity provider, like OneLogin. ... In **SSO**, this identity data takes the form of tokens that contain identifying bits of information about the user like a user's email address or a username.

## How to set up saml2-compatible identity providers

### *Manual Set Up*

- Log into CMS
- Select App
- Click on "Settings"
- Click on "Authentication" and then "Single Sign On"
- Click on "Add Provider"
- Check the "Manual Set Up" option
- Fill in; "Provider Name"
- Copy the "Issuer URL" into the "SAML Entity I.D" in CMS
- Copy the "SAML2 Endpoint" into the "SSO Login URL" field in CMS
- Copy the "Certificate" into the required field in CMS
- Fill in the "Unique ID" field in CMS under field mapping
- Click "Save changes" in CMS

### Setup Type

Choose between setting up your provider manually or via importing IDP metadata.

☒ Manual Setup



Set up all of your fields from scratch

☐ Import IDP Metadata XML



Import XML metadata to automatically configure your provider

### Manual Setup

Manually configure your SAML Identity providers

Provider Name \*

SAML Entity ID \*

SSO Login URL \*

Group


Automatically add users who sign in with SSO to this group

☐ Sign SP auth requests?

☐ Allow identity providers to create new profiles in the app

x509 Certificate \*

x509 certificate should be Base64 encoded

 Save changes

## Import IDP Metadata XML

Required details:

- Entity ID: <https://saml.crowdcomms.com>
- Reply URL: <https://api.crowdcomms.com/complete/saml/> Note: this needs to be summit-api for apps using the Summit environment, and dlt-api for apps using the Deloitte environment. Deloitte apps using the main environment should still use just api.

Using the above you should be able to import your metadata with the following steps:

- Fill in; "Provider Name"
- Return to IDP and copy the Metadata URL

- Copy the link into the CMS field "Metadata URL"
- Insert a name into the "Unique User I.D" field (for example; NameId) - this is based on the field mapping the client sets up. They will map their Active Directory fields to potentially something shorter, eg their ID field could be mapped to 'uniqueid', and so instead of filling in NameId here, you'd fill in uniqueid
- Click Save in CMS
- Copy the "Relay State URL" into the Configuration TAB
- Copy the "Audience" into the Configuration TAB
- Copy the "Recipient" into the Configuration TAB

## ← Create Auth Provider

### 🔧 Setup Type

Choose between setting up your provider manually or via importing IDP metadata.

☐ Manual Setup



Set up all of your fields from scratch

☒ Import IDP Metadata XML



Import XML metadata to automatically configure your provider

### 📄 Import IDP Setup

If your IDP supplies an XML metadata document, import it here to setup SSO on your app.

Identity Provider Name \*

Metadata URL \*

Entity ID Override

This field is only required if you need to override the SAML2 entity ID

☐ Allow identity providers to create new profiles in the app


### 🖼️ Display Options

Configure how your auth provider will appear on the login page.

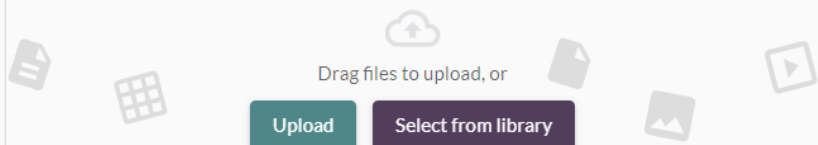
Login Text

If left blank, this field defaults to 'Login with {{provider name}}'

0 / 256

 Login Provider Logo

☐ Crop image



## ***Branding the Login Page with SSO***

The Front End Login page can be branded with unique text and/or with a logo in the "Display Options" section of the "Edit Auth Provider" page




### Display Options

Configure how your auth provider will appear on the login page.

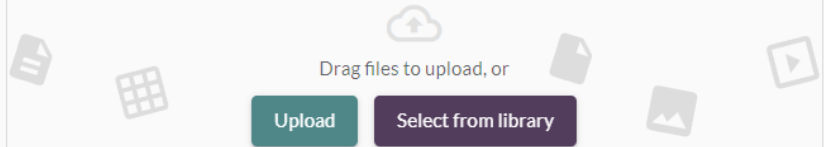
Login Text

If left blank, this field defaults to 'Login with {{provider name}}'

0 / 256

 Login Provider Logo

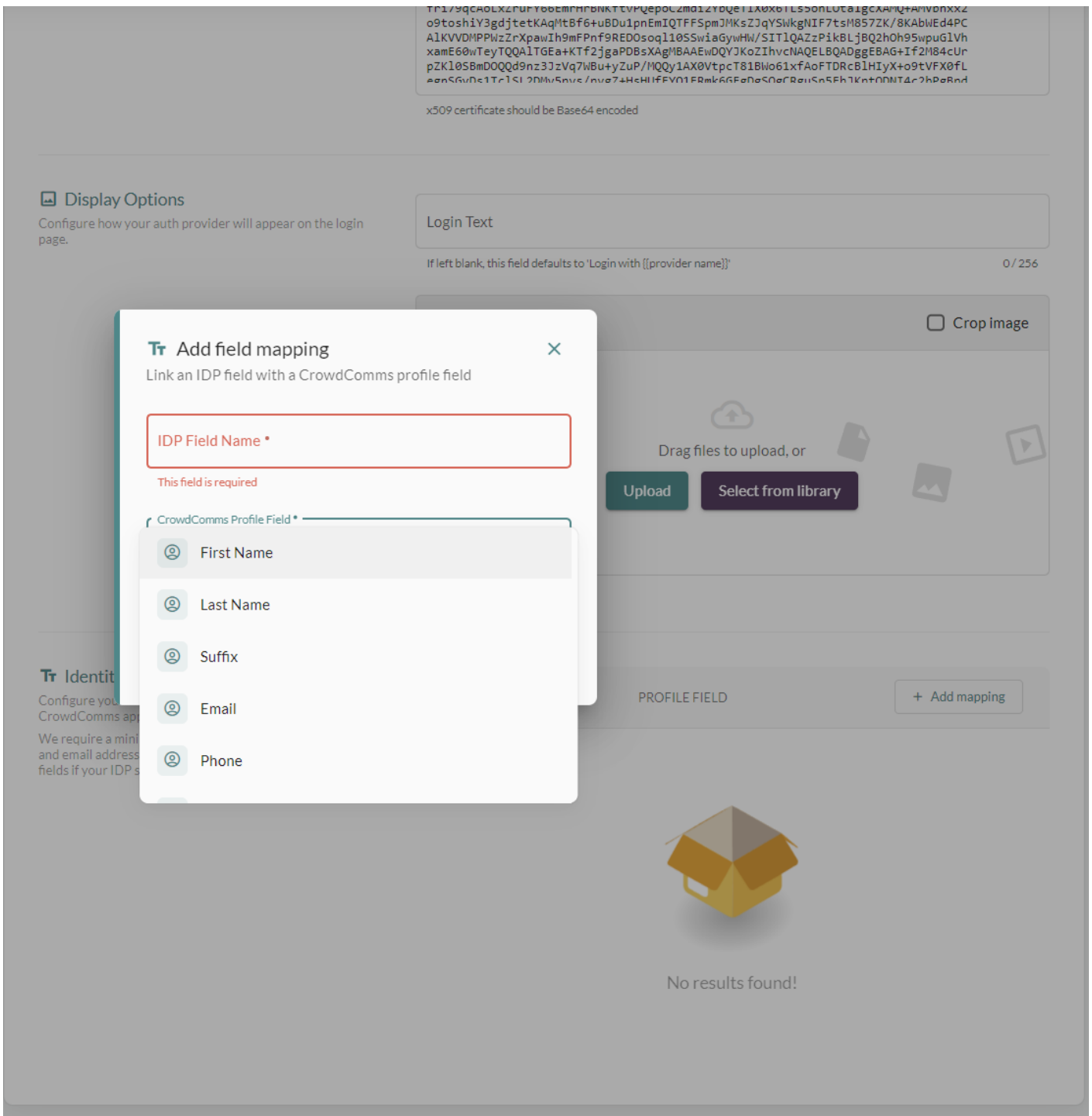
☐ Crop image



- Upload the image you wish to add to the login page
- Type the text you would like to appear (For Example... "Please log in")
- Click Save

## ***Field Mapping***

- Click on "Edit Provider" to edit the SSO you set up in the previous step
- Scroll down and click on "Add Mapping"



- Enter each field mapping and click "Save". Again these are based on the field mappings the client sets up. We take the output of their mapping, and map it to a profile field in our own system
- Click Save

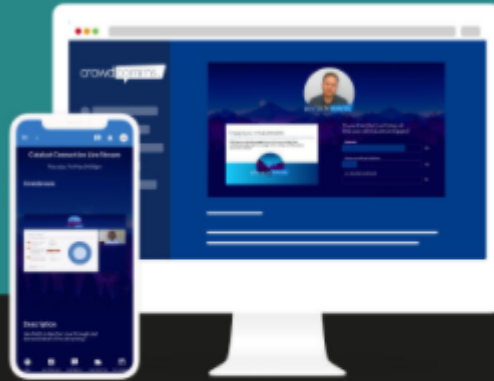
## ***Logging into Front End***

- Open up Front End of App

# Event Tech Solutions

LIVE

crowdcomms.



## Log In

Please enter your email address

Email Address\*

Select Language

English (English)

CONFIRM

## Login with Training Material



Sign In

- Click on "Sign In"
- Enter your credentials
- At this point, if any more User information is required then a screen will appear for the user to fill them in (for example; first name), otherwise, you will receive a "Success Screen" before FE loads up
- As this is the first time the User will of logged in, they will receive the company privacy message to accept or decline
- The user is now logged into the App



# Shared SSO between apps

When setting up SSO for a client's active directory, you normally need to provide them with an Entity ID from our platform in the form of ``https://saml.crowdcomms.com/<unique identifier>``. That unique identifier is specific per app. What this means is that clients can only access 1 app per active directory, and they typically re-create and re-populate new active directories if they have multiple apps with us.

There is now capability to share an active directory among multiple apps:

- Let the client choose any entity ID as long as it starts with ``https://saml.crowdcomms.com/`` eg ``https://saml.crowdcomms.com/dlt``
- Have them set that as our Entity ID in their active directory
- Fill that suffix in in the 'Entity ID Suffix Override' field in the App Settings in the CMS

We provide the choice because clients may decide they want multiple Active Directories that are shared for whatever reason. So we may have ``dlt1``, ``dlt2``, etc that are linked to multiple apps each

# 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+dQzXhz3fG8JJ0GUaoLxgzJ3K8vDkKFnbokR1XLa60YEPLuCh5ehfg3A8STeE0kp5ky+kVU0BBEKg  
ZBKCNEx0cqZh2m6Wembu2C8xS4Ea/M2R64dnO3/NKYkcxElvYYjS91HJoYc0MWhl2K6xHY8CCxFggqHsnXHCNnucKZTp8  
N4kiM4AxSWTaJw+Pwlh3vPgZNfuQuFhIvkAsLRW8kZzlAn/CAYxZ5n3qoJhzjZM3lu9gJgihyqSwy==</SignatureVal  
ue>  
      <KeyInfo>  
        <ds:X509Data  
          xmlns:ds="http://www.w3.org/2000/09/xmldsig#">  
            <ds:X509Certificate>MIIC8DCCAdigAwIBAgIQeVvBFEMM35dJLAPSmvEdrzANBgkqhkiG9w0BAQsFADA0MTIwMA  
YDVQQDEylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMTA3MTYxMzM0MjhaFw0yNDAA3  
MTYxMzM0MjhaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRLcmF0ZWQgU1NPIENlc nRpZmljYXRlMIIBIjANBg  
kqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAT7XgcOVwAoh3d4MuFKF61mf58inL9sAyCLEC6RhX+7ZiyT730dK9y+IwvpIU7  
c1G0bmFqs51oJ5EdHv+GipDepg4zR8HRljUp9HnSlOhMkaFR+BMsMv19r9rD+beLM+kbNW3/YAISBxGk60Q0QpNbV0cw6W  
OdV7+WfCUFWcU6NbYx12viF3e9HlgXSA6+JoGM3dSIqw1SqE417aCFnTxuGS6b84YKBmlX7Jkr0a5Ekh3JwHqokDMvWmWf  
dv8/eSJm4PABqbKL0Ui h3WMnpdEngx/jilqnD2b26n1TEie0zB0e2F1JINLGtoJh6lFiyrql/Pd6uqLEcBli6vJPC1qo4Q  
IDAQABMA0GCsqGSib3DQEBcwIAA4IBAQNPR2s4jABwzJPB3/W2fDSX60PGGA4HVW9YT xv1CtZVXTG/e8uqLASjSe0hlB3  
TTevhAMxxPnlxx/u0i9RE2j6RMMTFs40omhwZ4+0Go02oV6YDPZPKypVkdWTd6/TywZ0A8ZVThw0Uo04z9085Sub3rJvVQ  
42cFR5RlKxRginvdZ5GVI Z6LzQqWPuq4Z35Iiq30F131dYWYIgLL6awGh3AjfkqHYFD0ufqK6ZzSZXMd1vthGgzmJGAUV3  
B4K0X5V0YSBXQSh8rVcQ5c9Pg/k1Yg/xf9sVgimCLCEYFAn/LhX7Un2W9x0IS/zTscfLW+X/wload+PPMNskpNh0b403</  
ds:X509Certificate>  
          </ds:X509Data>  
        </KeyInfo>  
      </Signature>  
    <RoleDescriptor xsi:type="fed:SecurityTokenServiceType"  
protocolSupportEnumeration="http://docs.oasis-open.org/ws-fed/federation/200706"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```

<?xml:namespace prefix="fed" http://docs.oasis-open.org/ws-fed/federation/200706">
  <KeyDescriptor use="signing">
    <KeyInfo
      <?xml:namespace prefix="http://www.w3.org/2000/09/xmldsig#">
        <X509Data>
          <X509Certificate>MIIC8DCCAdigAwIBAgIQeVvBFEMM35dJLAPSmvEdrzANBgkqhkiG9w0BAQsFADA0MTIwMAYD
          VQQDEylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMTA3MTYxMzQ0MjhaFw0yNDA3MT
          YxMzQ0MjhaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRLcmF0ZWQgU1NPIENlcnpZmljYXRlMIIBIjANBgkq
          hkiG9w0BAQEFAA0CAQ8AMIIBCgKCAQEAA7XgcoVwAoh3d4MufKF61mf58inL9sAyCLEC6RhX+7ZiyT730dK9y+IwvpIU7c1
          G0bmfQs51oJ5EdHv+GipDepg4zR8HRLJup9HnSl0hMkaFR+BMsmV19r9rD+beLM+kbNW3/YAISBxGk60Q0QpNbv0cw6W0d
          v7+WfCUFWcU6NbYx12viF3e9HlgXSA6+JoGM3dSIqw1SqE417aCFnTxuGS6b84YKBmLX7Jkr0a5Ekh3JwHqokDMvWmWfDV
          8/eSJm4PABqbkL0Uih3WMNpdEngx/jilqnD2b26n1TEie0zB0e2F1JINLGoJh6lFiyrl/Pd6uqLEcBli6vJPC1qo4QID
          AQABMA0GCSqGSIb3DQEBwJAA4IBAQDnPR2s4jABwzJPB3/W2fDSX60PGGA4HVW9YTxxv1CtZVXtG/e8uqLAsjSe0h1B3TT
          evhAMxxPn1xx/u0i9RE2j6RMMTF540omhWZ4+0Go02oV6YDPZPkyPvKdwTD6/TywZ0A8ZVThw0Uo04z9085Sub3rJvVQ42
          cFR5RlKxRgiNvdZ5GVIz6lZqQWPuq4Z35Iiq30F131dYWyIglL6aWgh3AjfkqHYFD0ufqK6ZzSZXMd1vthGgzmJGAUv3B4
          K0X5V0YSBxQSh8rVcQ5c9Pg/k1Yg/xf9sVgimCLCEYfAn/LhX7Un2W9x0IS/zTscfLW+X/wloaD+PPMNSkpNh0b403</X5
          09Certificate>
        </X509Data>
      </KeyInfo>
    </KeyDescriptor>
    <fed:ClaimTypesOffered>
      <auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"
        <?xml:namespace prefix="http://docs.oasis-open.org/ws-fed/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"
        <?xml:namespace prefix="http://docs.oasis-open.org/ws-fed/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"
        <?xml:namespace prefix="http://docs.oasis-open.org/ws-fed/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"
        <?xml:namespace prefix="http://docs.oasis-open.org/ws-fed/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
VQQDEylNaWNYb3NvZnQgQXp1cmUgRmVhZG9wIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMTA3MTYxMzQ0MjhaFw0yNDA3MT
YxMzQ0MjhaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVYZSBGZWRLcmF0ZWQgU1NPIENlcnpZmljYXRlMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAA7XgcoVwAoh3d4MufKF61mf58inL9sAyCLEC6RhX+7ZiyT730dK9y+IwvpIU7c1
G0bmfQs51oJ5EdHv+GipDepg4zR8HRLJup9HnSl0hMkaFR+BMsmV19r9rD+beLM+kbNW3/YAISBxGk60Q0QpNbvcw6W0d
v7+WfCUFWcU6NbYx12viF3e9HlgXSA6+JoGM3dSIqw1SqE417aCfnTxuGS6b84YKBmlX7Jkr0a5Ekh3JwHqokDMvWmwFdV
8/eSJm4PABqbKLOUih3WMNpdEngx/jilqnD2b26n1TEie0zB0e2F1JINLGoJh6lFiyqL/Pd6uqLEcBli6vJPC1qo4QID
AQABMA0GCSqGSIb3DQEBcwJAA4IBAQNPR2s4jABwzJPB3/W2fDSX60PGGA4HVW9YTxv1CtZVXtG/e8uqLAsjSe0hLB3TT
evhAMxxPn1xx/u0i9RE2j6RMMTFS40omhwZ4+0Go02oV6YDPZPKyPvKdwTD6/TywZ0A8ZVThwUo04z9085Sub3rJvVQ42
cFR5RlKxRgiNvdZ5GVIZ6LZqQWPuq4Z35Iiq30F131dYWyIgl6aWgh3AjfkqHYFD0ufqK6ZzSZXMd1vthGgzmJGAUv3B4
K0X5V0YSBxQSh8rVcQ5c9Pg/k1Yg/xf9sVgimCLCEYFAn/LhX7Un2W9x0IS/zTscfLW+X/wloaD+PPMNSkpNh0b403</X5
```

```
<?xml version="1.0" encoding="UTF-8"?>
<X509Certificate>
  <X509Data>
    <KeyInfo>
      <KeyDescriptor>
        <fed: TargetScopes>
          <wsa: EndpointReference>
            <?xml 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>
            <?xml 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>
            <?xml 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>
            <?xml xmlns="http://www.w3.org/2000/09/xmldsig#">
              <X509Data>
                <X509Certificate>MIIC8DCCAdigAwIBAgIQeVvBFEMM35dJLAPSmvEdrzANBgkqhkiG9w0BAQsFADA0MTIwMAYD
                VQQDEylNaWNYb3NvZnQgQXplcmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMTA3MTYxMzQ0MjhaFw0yNDA3MT
                YxMzQ0MjhaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVvZSBGZWRLcmF0ZWQgU1NPIENlcnpZmljYXRlMIIBIjANBgkq
                hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7XgcoVwAoh3d4MufKF61mf58inL9sAyCLEC6RhX+7ZiyT730dK9y+IwplIU7c1
                G0bmFQs51oJ5EdHv+GipDepg4zR8HRLJup9HnS10hMkaFR+BMsmV19r9rD+beLM+kbNW3/YAISBXGk60Q0QpNbvcw6W0d
                v7+WfCUFWcU6NbYx12viF3e9HlgXSA6+JoGM3dSIqw1SqE417aCFnTxuGS6b84YKBmLX7Jkr0a5EKH3JwHqokDMvWmwFdV
                8/eSJm4PABqbKLOUih3wMNPdEngx/jilqnD2b26n1TEie0zB0e2F1JINLGtoJh6lFiyrqL/Pd6uqLEcBli6vJPC1qo4QID
                AQABMA0GCSqGSIb3DQEBCwIAA4IBAQNPR2s4jABwzJPB3/W2fDSX60PGGA4HVW9YTxv1CtZVXtG/e8uqLAsjSeOhLB3TT
                evhAMxxPn1xx/u0i9RE2j6RMMTF540omhwZ4+0Go02oV6YDPZPKyPvKdwTD6/TywZ0A8ZVThw0Uo04z9085Sub3rJvVQ42
                cFR5RlKxRgiNvdZ5GVIz6LZqQPuq4Z35Iiq30F131dYWyIglL6aWGh3AjfkqHYFD0ufqK6ZzSZXMd1vthGgzMJGAUv3B4
                K0X5V0YSBxQSh8rVcQ5c9Pg/k1Yg/xf9sVgimCLCEYFAn/LhX7Un2W9x0IS/zTscfLW+X/wload+PPMNSkpNh0b403</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>