Requisitos técnicos para participantes de Unificat

Proveedores de Servicio

Para conectar un servicio a la federación de CSUC, se debe disponer de un componente llamado Proveedor de Servicio (SP) que implemente al menos uno de los siguientes protocolos soportados por la federación:

- SAML 2.0
  - Perfil WebSSO
- SAML 1.1/Shibboleth 1.3
- PAPI
- CAS
- OAuth 2
  - Perfil “Client Credential”
  - Perfil “Implicit”
- OpenID Connect

Se recomienda el uso del protocolo SAML 2.0 siempre que sea posible.

Proveedores de Servicio SAML

La configuración de un Proveedor de Servicio que implementa el protocolo SAML 2 o SAML 1.1 en la federación CSUC se realiza a través del envío de sus metadatos, los cuales deben reflejar los siguientes elementos y atributos en el documento XML:

- `//md:EntityDescriptor/@entityID`: es necesario que exista un elemento `<EntityDescriptor>` cuyo atributo “`entityID`” indique cual es su ID de entidad unívoco en la federación
- `//md:EntityDescriptor/ds:Signature`: es muy recomendable que exista una firma XML que valide el contenido de la descripción de la entidad, de manera que el responsable del Proveedor de Servicio se asegure que la configuración no va a ser alterada
- `//md:EntityDescriptor/md:SPSSODescriptor`: es necesario que contenga un único elemento <SPSSODescriptor> que describa la configuración del Proveedor de Servicio SAML 2

Dentro del elemento `//md:EntityDescriptor/md:SPSSODescriptor` es importante que existan la siguiente información relativa al Proveedor de Servicio:

- /md:KeyDescriptor: es necesario que exista al menos un elemento `<KeyDescriptor>` que especifique el certificado digital para firmar o cifrar mensajes SAML 2
- /md:AssertionConsumerService: es necesario que exista al menos un elemento `<AssertionConsumerService>`

Los espacios de nombre utilizados en las expresiones XPath anteriores son:

- md = urn:oasis:names:tc:SAML:2.0:metadata
- ds = *http://www.w3.org/2000/09/xmldsig#*

Un ejemplo de metadatos para un SP SAML 2:

```
<?xml version="1.0" encoding="utf-8"?>
<md:EntityDescriptor
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  entityID="https://sp.example.org/shibboleth-sp">
  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol urn:oasis:names:tc:
SAML:1.1:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MII…ksFe7Pg=</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>MIICs…Fe7Pg=</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
    <md:NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</md:NameIDFormat>
    <md:AssertionConsumerService index="1" isDefault="true"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://sp.example.org/Shibboleth.sso/SAML2/POST"/>
    <md:AssertionConsumerService index="2"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign"
      Location="https://sp.example.org/Shibboleth.sso/SAML2/POST-SimpleSign"/>
    <md:AssertionConsumerService index="3"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
      Location="https://sp.example.org/Shibboleth.sso/SAML2/Artifact"/>
    <md:AssertionConsumerService index="4"
      Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"
      Location="https://sp.example.org/Shibboleth.sso/SAML/POST"/>
    <md:AssertionConsumerService index="5"
      Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01"
      Location="https://sp.example.org/Shibboleth.sso/SAML/Artifact"/>
  </md:SPSSODescriptor>
  <md:Organization>
    <md:OrganizationName xml:lang="en">Your Service</md:OrganizationName>
    <md:OrganizationDisplayName xml:lang="en">Your Service</md:OrganizationDisplayName>
    <md:OrganizationURL xml:lang="en">http://sp.example.org/</md:OrganizationURL>
  </md:Organization>
  <md:ContactPerson contactType="technical">
    <md:GivenName>Your</md:GivenName>
    <md:SurName>Admin</md:SurName>
    <md:EmailAddress>admin@example.org</md:EmailAddress>
  </md:ContactPerson>
</md:EntityDescriptor>
```

Otros Proveedores de Servicio

La configuración de un Proveedor de Servicio que implementa otro tipo de protocolo, como por ejemplo CAS o PAPI, se realizará enviando los datos de configuración directamente a los administradores de la federación.

Proveedores de Identidad

Requisitos previos

Para conectar un Proveedor de Identidad (IdP) a la federación de CSUC será necesario que implemente el protocolo SAML 2, por lo que es necesario el envío de sus metadatos, y deben cumplir con la *polític a de emisión de atributos* definido para Unificat.

Deben estar acordados quienes son los contactos técnico y administrativo del Proveedor de Identidad, ya que se deben incluir en los metadatos.

Requisitos de los metadatos

Los metadatos deben ser creados conformes al estándar *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0* y además deberán implementar las siguientes extensiones de metadatos SAML 2:

- *SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0*, para que el interfaz de usuario de Unificat muestre información según preferencias de la organización responsable del Proveedor de Identdad
- *SAML V2.0 Metadata Extensions for Shibboleth Version 1.0*, para poder validar los dominios permitidos en determinados atributos "scoped", como por ejemplo eduPersonScopedAffiliation

El documento de metadatos debe reflejar los siguientes elementos y atributos:

- `//md:EntityDescriptor/@entityID`: es necesario que exista un elemento `<EntityDescriptor>` cuyo atributo “`entityID`” indique cual es su ID de entidad unívoco en la federación
- `//md:EntityDescriptor/ds:Signature`: es necesario que exista una firma XML que valide el contenido de la descripción de la entidad, de manera que el responsable del Proveedor de Identidad se asegure que la configuración no va a ser alterada
- `//md:EntityDescriptor/md:Extensions/shibmd`:Scope: es necesario que exista al menos un elemento `<Scope>` indicando el valor permitido para los atributos que utilicen dicha información, como por ejemplo eduPersonScopedAffiliation
- `//md:EntityDescriptor/md:Extensions/mdui:UIInfo`: es necesario que exista un elemento `<UIInfo>` que indique información necesaria por el interfaz de usuario de la federación
- `//md:EntityDescriptor/md:IDPSSODescriptor`: es necesario que contenga un único elemento `<IDPSSODescriptor>` que describa la configuración del Proveedor de Identidad SAML 2
- `//md:EntityDescriptor/md:Organization`: es necesario que contenga un único elemento `<Organization>` que especifique información básica sobre la organización responsable del Proveedor de Identidad SAML 2

- `//md:EntityDescriptor/md:ContactPerson`: es necesario que contenga al menos dos elementos `<ContactPerson>` que indiquen las personas de contacto a nivel técnico y de soporte siendo para ello el valor de su atributo "`contactType`" como "`technical`" y "`support`" respectivamente.

Dentro del elemento `//md:EntityDescriptor/md:IdPSSODescriptor` es importante que existan la siguiente información relativa al Proveedor de Identidad:

- `/md:KeyDescriptor`: es necesario que exista al menos un elemento `<KeyDescriptor>` que especifique el certificado digital para firmar o cifrar mensajes SAML 2
- `/md:NameIDFormat`: es necesario que exista al menos un elemento `<NameIDFormat>` y cuyo valor sea "`urn:oasis:names:tc:SAML:2.0:nameid-format:transient`", ya que el hub de la federación siempre enviará el mensaje solicitando dicho formato para el NameID para las respuestas SAML 2 enviadas por el IdP
- `/md:SingleSignOnService`: es necesario que exista al menos un elemento `<SingleSignOnService>`

Dentro del elemento `//md:EntityDescriptor/mdui:UIInfo` es importante que existan la siguiente información de interfaz de usuario relativa al Proveedor de Identidad:

- `/mdui:DisplayName`: indica el nombre del Proveedor de Identidad a mostrar al usuario en los interfaces de usuario, indicando en su atributo obligatório "`xml:lang`" para qué idioma. Debe existir al menos un elemento `<DisplayName>` y no es posible indicar más de un valor para un mismo idioma. Se recomienda que se emitan valores para los idiomas catalán, inglés y español
- `/mdui:Description`: ofrece una descripción corta del Proveedor de Identidad que será mostrada al usuario en los interfaces de usuario, indicando en su atributo obligatório "`xml:lang`" para qué idioma. Debe existir al menos un elemento `<Description>` y no es posible indicar más de un valor para un mismo idioma. Se recomienda que se emitan valores para los idiomas catalán, inglés y español
- `/mdui:Logo`: indica la localización en formato URI del logo del Proveedor de Identidad, donde se requiere indicar obligatóriamente el alto y el ancho del mismo. Opcionalmente es posible indicar también el idioma, por si se quisiera mostrar un logo diferente en función del idioma del interfaz de usuario, pero debe existir al menos un elemento sin idioma que se utilizará como opcional. Pueden indicarse diferentes elementos `<Logo>` que representen al mismo logo pero con tamaños diferentes, y se deben tener en cuenta las siguientes sugerencias:
  - Se debe utilizar fondo transparente
  - Se debe utilizar el formato PNG siempre que sea posible
  - Se deben utilizar URLs bajo HTTPS, para evitar mensajes de error de determinados navegadores
- `/mdui:InformationURL`: indica una URL con información ampliada a la indicada en la descripción, indicando en su atributo obligatório "`xml:lang`" para qué idioma. Se recomienda que se emitan valores para los idiomas catalán, inglés y español, y se deben tener en cuenta la siguiente sugerencia:
  - Se deben utilizar URLs bajo HTTPS, para evitar mensajes de error de determinados navegadores
- `/mdui:PrivacyStatementURL`: indica una URL con información sobre la privacidad en el tratamiento de la información del usuario en el Proveedor de Identidad, indicando en su atributo

obligatório “`xml:lang`” para qué idioma. Se recomienda que se emitan valores para los idiomas catalán, inglés y español, y se deben tener en cuenta la siguiente sugerencia:

- Se deben utilizar URLs bajo HTTPS, para evitar mensajes de error de determinados navegadores

Los espacios de nombre utilizados en las expresiones XPath anteriores son:

- md = urn:oasis:names:tc:SAML:2.0:metadata
- ds = *http://www.w3.org/2000/09/xmldsig#*
- shibmd = urn:mace:shibboleth:metadata:1.0
- mdui = urn:oasis:names:tc:SAML:metadata:ui

Un ejemplo de metadatos para un IdP SAML 2:

```
<md:EntityDescriptor
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  entityID="http://www.example.com/SAML2/"
  ID="pfx95d1a532-dc6a-c243-fbd8-8499ec0841ab">
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <ds:Reference URI="#pfx95d1a532-dc6a-c243-fbd8-8499ec0841ab">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>b3aPLZjq5DxCDcn/0zXKK1ByRO8=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>YB1Z2exuGJ…zNtxhsw/CqXLdpRg4B+Z44=</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>MIICsDC…lyRLhksFe7Pg=</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </ds:Signature>
  <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:Extensions>
      <shibmd:Scope xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" regexp="false">example.com</shibmd:
Scope>
      <mdui:UIInfo>
        <mdui:DisplayName xml:lang="ca">Nom organització</mdui:DisplayName>
        <mdui:DisplayName xml:lang="es">Nombre organización</mdui:DisplayName>
        <mdui:DisplayName xml:lang="en">Org name</mdui:DisplayName>
        <mdui:Description xml:lang="ca">Servei d'autenticació de l'organització</mdui:Description>
        <mdui:Description xml:lang="es">Servicio de autenticación de la organización</mdui:Description>
        <mdui:Description xml:lang="en">Authentication service organization</mdui:Description>
        <mdui:Logo height="16" width="16">https://www.example.com/resources/images/smalllogo.png</mdui:Logo>
        <mdui:Logo height="97" width="172">https://www.example.com/resources/images/logo.png</mdui:Logo>
        <mdui:InformationURL xml:lang="ca">http://www.example.com</mdui:InformationURL>
        <mdui:InformationURL xml:lang="es">http://www.example.com/es</mdui:InformationURL>
        <mdui:InformationURL xml:lang="en">http://www.example.com/en</mdui:InformationURL>
        <mdui:PrivacyStatementURL xml:lang="ca">http://www.example.com/privacy.html</mdui:
PrivacyStatementURL>
        <mdui:PrivacyStatementURL xml:lang="es">http://www.example.com/es/privacy.html</mdui:
PrivacyStatementURL>
```

```
        <mdui:PrivacyStatementURL xml:lang="en">http://www.example.com/en/privacy.html</mdui:
PrivacyStatementURL>
      </mdui:UIInfo>
    </md:Extensions>
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MII…ksFe7Pg=</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>MIICs…Fe7Pg=</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:SingleLogoutService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="http://www.example.com/SAML2/SLOService.php"/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
    <md:SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="http://www.example.com/SAML2/SSOService.php"/>
    <md:SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="http://www.example.com/SAML2/SSOService.php"/>
  </md:IDPSSODescriptor>
  <md:Organization>
    <md:OrganizationName xml:lang="ca">Nom organització</md:OrganizationName>
    <md:OrganizationDisplayName xml:lang="ca">Nom organització</md:OrganizationDisplayName>
    <md:OrganizationURL xml:lang="ca">http://www.example.com/</md:OrganizationURL>
  </md:Organization>
  <md:ContactPerson contactType="technical">
    <md:GivenName>Your</md:GivenName>
    <md:SurName>Contact</md:SurName>
    <md:EmailAddress>admin@example.com</md:EmailAddress>
  </md:ContactPerson>
  <md:ContactPerson contactType="support">
    <md:GivenName>Your</md:GivenName>
    <md:SurName>Other contact</md:SurName>
    <md:EmailAddress>support@example.com</md:EmailAddress>
  </md:ContactPerson>
</md:EntityDescriptor>
```