Requisits tècnics per participants d'Unificat

Proveïdors de Servei

Per a connectar un servei a la federació de CSUC, s'ha de disposar d'un component anomenat Proveïdor de Servei (SP) que implementi almenys un dels següents protocols suportats per la federació:

- SAML 2.0
  - Perfil WebSSO
- SAML 1.1/Shibboleth 1.3
- PAPI
- CAS

Es recomana l'ús del protocol SAML 2.0 sempre que sigui possible.

Proveïdors de Servei SAML

La configuració d'un Proveïdor de Servei que implementa el protocol SAML 2 o SAML 1.1 en la federació CSUC es realitza a través de l'enviament de les seves metadades, els quals han de reflectir els següents elements i atributs en el document XML:

- `//md:EntityDescriptor/@*entityID`: és necessari que existeixi un element `<EntityDescriptor>` l'atribut del qual `entityID` indiqui com és el seu ID d'entitat unívoc en la federació.
- `//md:EntityDescriptor/*ds:Signature`: és necessari que existeixi una signatura XML que validi el contingut de la descripció de l'entitat, de manera que el responsable del Proveïdor de Servei s'asseguri que la configuració no serà alterada (com a mínim en sha256).
- `//md:EntityDescriptor/*md:SPSSODescriptor`: és necessari que contingui un únic element `<SPSSODescriptor>` que descrigui la configuració del Proveïdor de Servei SAML 2.

Dins de l'element `//md:EntityDescriptor/*md:SPSSODescriptor` és important que existeixin la següent informació relativa al Proveïdor de Servei:

- `/md:KeyDescriptor`: és necessari que existeixi almenys un element `<KeyDescriptor>` que especifiqui el certificat digital per a signar i xifrar missatges SAML 2.

- `/md:AssertionConsumerService`: és necessari que existeixi almenys un element `<AssertionConsumerService>`.

Dins de l'element `//md:EntityDescriptor/*mdui:UIInfo` és important que existeixin la següent informació d'interfície d'usuari relativa al Proveïdor de Servei:

- `/mdui:DisplayName`: indica el nom del Proveïdor de Servei a mostrar a l'usuari en les interfícies d'usuari, indicant en el seu atribut obligatori `xml:lang` per a quin idioma. Ha d'existir almenys un element `<DisplayName>` i no és possible indicar més d'un valor per a un mateix idioma. Es recomana que s'emetin valors per als idiomes català, anglès i espanyol.
- `/mdui:Description`: ofereix una descripció curta del Proveïdor de Servei que serà mostrada a l'usuari en les interfícies d'usuari, indicant en el seu atribut obligatori `xml:lang` per a quin idioma. Ha d'existir almenys un element `<Description>` i no és possible indicar més d'un valor per a un mateix idioma. Es recomana que s'emetin valors per als idiomes català, anglès i espanyol.
- `/mdui:Logo`: indica la localització en format URI del logo del Proveïdor de Servei, on es requereix indicar obligatóriamente l'alt i l'ample d'aquest. Opcionalment és possible indicar també l'idioma, per si es volgués mostrar un logo diferent en funció de l'idioma de la interfície d'usuari, però ha d'existir almenys un element sense idioma que s'utilitzarà com a opcional. Poden indicar-se diferents elements `<Logo>` que representin al mateix logo però amb grandàries diferents, i s'han de tenir en compte els següents suggeriments:
  - S'ha d'utilitzar fons transparent.
  - S'ha d'utilitzar el format PNG sempre que sigui possible.
  - S'han d'utilitzar URLs sota HTTPS, per a evitar missatges d'error de determinats navegadors.
- `/mdui:InformationURL`: indica una URL amb informació ampliada a la indicada en la descripció, indicant en el seu atribut obligatori `xml:lang` per a quin idioma. Es recomana que s'emetin valors per als idiomes català, anglès i espanyol, i s'han de tenir en compte el següent suggeriment:
  - S'han d'utilitzar URLs sota HTTPS, per a evitar missatges d'error de determinats navegadors.
- `/mdui:PrivacyStatementURL`: indica una URL amb informació sobre la privacitat en el tractament de la informació de l'usuari en el Proveïdor de Servei, indicant en el seu atribut obligatori `xml:lang` per a quin idioma. Es recomana que s'emetin valors per als idiomes català, anglès i espanyol, i s'han de tenir en compte el següent suggeriment:
  - S'han d'utilitzar URLs sota HTTPS, per a evitar missatges d'error de determinats navegadors.

Els espais de nom utilitzats en les expressions XPath anteriors són:

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

Un exemple de metadades per a 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:Extensions>
      <mdui:UIInfo>
        <mdui:DisplayName xml:lang="ca">Servei</mdui:DisplayName>
        <mdui:DisplayName xml:lang="es">Servicio</mdui:DisplayName>
        <mdui:DisplayName xml:lang="en">Service</mdui:DisplayName>
        <mdui:Description xml:lang="ca">Descripció del servei</mdui:Description>
        <mdui:Description xml:lang="es">Descripción del servicio</mdui:Description>
        <mdui:Description xml:lang="en">Service description</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: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>
```

Altres Proveïdors de Servei

La configuració d'un Proveïdor de Servei que implementa un altre tipus de protocol, com per exemple CAS o PAPI, es realitzarà enviant les dades de configuració directament als administradors de la federació.

Proveïdors d'Identitat

Requisits de les metadades

Les metadades han de ser creats conformes a l'estàndard *Metadata for the OASI Security Assertion Markup Language (SAML) V2.0* i a més hauran d'implementar les següents extensions de metadades SAML 2:

- *SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0*, perquè la interfície d'usuari d'Unificat mostri informació segons preferències de l'organització responsable del Proveïdor de Identitat.
- *SAML V2.0 Metadata Extensions for Shibboleth Version 1.0*, per a poder validar els dominis permesos en determinats atributs "scoped", com per exemple `eduPersonScopedAffiliation`.

El document de metadades ha de reflectir els següents elements i atributs:

- `//md:EntityDescriptor/@*entityID`: és necessari que existeixi un element `<EntityDescriptor>` l'atribut del qual `entityID` indiqui com és el seu ANEU d'entitat unívoc en la federació.
- `//md:EntityDescriptor/*ds:Signature`: és necessari que existeixi una signatura XML que validi el contingut de la descripció de l'entitat, de manera que el responsable del Proveïdor d'Identitat s'asseguri que la configuració no serà alterada (com a mínim en sha256).
- `//md:EntityDescriptor/*md:Extensions/*shibmd:Scope`: és necessari que existeixi almenys un element `<Scope>` indicant el valor permès per als atributs que utilitzin aquesta informació, com per exemple `eduPersonScopedAffiliation.`
- `//md:EntityDescriptor/*md:Extensions/*mdui:UIInfo`: és necessari que existeixi un element `<UIInfo>` que indiqui informació necessària per la interfície d'usuari de la federació.
- `//md:EntityDescriptor/*md:IDPSSODescriptor`: és necessari que contingui un únic element `<IDPSSODescriptor>` que descrigui la configuració del Proveïdor d'Identitat SAML 2.
- `//md:EntityDescriptor/*md:Organization`: és necessari que contingui un únic element `<Organization>` que especifiqui informació bàsica sobre l'organització responsable del Proveïdor d'Identitat SAML 2.
- `//md:EntityDescriptor/*md:ContactPerson`: és necessari que contingui almenys dos elements `<ContactPerson>` que indiquin les persones de contacte a nivell tècnic i de suport sent per a això el valor del seu atribut `contactType` com `technical` i `support` respectivament.

Dins de l'element `//md:EntityDescriptor/*md:IdPSSODescriptor` és important que existeixin la següent informació relativa al Proveïdor d'Identitat:

- `/md:KeyDescriptor`: és necessari que existeixi almenys un element `<KeyDescriptor>` que especifiqui el certificat digital per a signar i xifrar missatges SAML 2.
- `/md:NameIDFormat`: és necessari que existeixi almenys un element `<NameIDFormat>` i el valor del qual sigui `urn:oasi:names:tc:SAML:2.0:nameid-*format:transient`, ja que el hub de la federació sempre enviarà el missatge sol·licitant aquest format per al NameID per a les respostes SAML 2 enviades pel IdP.
- `/md:SingleSignOnService`: és necessari que existeixi almenys un element `<SingleSignOnService>.`

Dins de l'element `//md:EntityDescriptor/*mdui:UIInfo` és necessari que existeixin la següent informació d'interfície d'usuari relativa al Proveïdor d'Identitat:

- `/mdui:DisplayName`: indica el nom del Proveïdor d'Identitat a mostrar a l'usuari en les interfícies d'usuari, indicant en el seu atribut obligatori `xml:lang` per a quin idioma. Ha d'existir almenys un element `<DisplayName>` i no és possible indicar més d'un valor per a un mateix idioma. Es recomana que s'emetin valors per als idiomes català, anglès i espanyol.
- `/mdui:Description`: ofereix una descripció curta del Proveïdor d'Identitat que serà mostrada a l'usuari en les interfícies d'usuari, indicant en el seu atribut obligatori `xml:lang` per a quin idioma. Ha d'existir almenys un element `<Description>` i no és possible indicar més d'un valor per a un mateix idioma. Es recomana que s'emetin valors per als idiomes català, anglès i espanyol.
- `/mdui:Logo`: indica la localització en format URI del logo del Proveïdor d'Identitat, on es requereix indicar obligatóriamente l'alt i l'ample d'aquest. Opcionalment és possible indicar també l'idioma, per si es volgués mostrar un logo diferent en funció de l'idioma de la interfície d'usuari, però ha d'existir almenys un element sense idioma que s'utilitzarà com a opcional. Poden indicar-se diferents elements `<Logo>` que representin al mateix logo però amb grandàries diferents, i s'han de tenir en compte els següents suggeriments:
  - S'ha d'utilitzar fons transparent.
  - S'ha d'utilitzar el format PNG sempre que sigui possible.
  - S'han d'utilitzar URLs sota HTTPS, per a evitar missatges d'error de determinats navegadors.
- `/mdui:InformationURL`: indica una URL amb informació ampliada a la indicada en la descripció, indicant en el seu atribut obligatori `xml:lang` per a quin idioma. Es recomana que s'emetin valors per als idiomes català, anglès i espanyol, i s'han de tenir en compte el següent suggeriment:
  - S'han d'utilitzar URLs sota HTTPS, per a evitar missatges d'error de determinats navegadors.
- `/mdui:PrivacyStatementURL`: indica una URL amb informació sobre la privacitat en el tractament de la informació de l'usuari en el Proveïdor d'Identitat, indicant en el seu atribut obligatori `xml:lang` per a quin idioma. Es recomana que s'emetin valors per als idiomes català, anglès i espanyol, i s'han de tenir en compte el següent suggeriment:
  - S'han d'utilitzar URLs sota HTTPS, per a evitar missatges d'error de determinats navegadors.

Els espais de nom utilitzats en les expressions XPath anteriors són:

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

Un exemple de metadades per a 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>
```