Collegamento di un SP non federato all'IdP di Ateneo

Il modo più corretto di autenticare utenti universitari sui propri servizi web è quello di federarsi ad IDEM / eduGAIN come resource provider.

Le formalità sul trattamento dei dati personali sono automaticamente assolte dal regolamento di federazione e dalle attività deò gestore della federazione.

Tuttavia, laddove quanto sopra non fosse possibile, riportiamo di seguito le istruzioni per un peering diretto fra SP ed IdP SAML.

Ricordiamo che l'attivazione del collegamento effettivo all'SP in questo caso è subordinata all'espletamento delle formalità richieste dagli uffici universitari in materia di trattamento dei dati personali.

Requisiti sui metadati

Nei metadati DEVONO essere valorizzati:

- ServiceName
- mdui:DisplayName
- mdui:PrivacyStatementURL
- mdui:Logo
- ArtifactResolutionService
- AssertionConsumerService
- RequestedAttribute indicando isRequired="true" se l'attributo è necessario per l'erogazione del servizio.
- possibilmente SingleLogoutService (Single Logout al momento non ancora funzionante sul nostro IdP)

Tutte le url devono essere in https.

Il nostro IdP supporta SOLO SAML 2.0

Esempio di alcune parti dei metadati:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui"
entityID="https://sp-fqdn/shibboleth">
...
  <md:SPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
...
    <AttributeConsumingService index="0">
```

```
        <ServiceName xml:lang="it">Nome del Servizio</ServiceName>
        <ServiceName xml:lang="en">Service Name</ServiceName>
        <ServiceDescription xml:lang="it">Descrizione del
Servizio</ServiceDescription>
        <ServiceDescription xml:lang="en">Service
Description</ServiceDescription>
        <!-- Lista di attributi richiesti -->
        <RequestedAttribute FriendlyName="commonName" Name="urn:oid:2.5.4.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
isRequired="true"/>
        <RequestedAttribute ..... isRequired="true"/>
    </AttributeConsumingService>
...

...
    <md:Extensions>
      <mdui:UIInfo>

        <mdui:DisplayName xml:lang="en">Service Name</mdui:DisplayName>
        <mdui:DisplayName xml:lang="it">Nome del servizio</mdui:DisplayName>

        <mdui:Description xml:lang="en">Service
description</mdui:Description>
        <mdui:Description xml:lang="it">Descrizione del
servizio<mdui:Description>

        <mdui:PrivacyStatementURL
xml:lang="en">https://...</mdui:PrivacyStatementURL>
        <mdui:PrivacyStatementURL
xml:lang="it">https://...</mdui:PrivacyStatementURL>

        <mdui:Logo height="16" width="16"
xml:lang="en">https://...</mdui:Logo>
        <mdui:Logo height="16" width="16"
xml:lang="it">https://...</mdui:Logo>
        <mdui:Logo height="60" width="80"
xml:lang="en">https://...</mdui:Logo>
        <mdui:Logo height="60" width="80"
xml:lang="it">https://...</mdui:Logo>
        <mdui:Logo height="80" width="80"
xml:lang="en">https://...</mdui:Logo>
        <mdui:Logo height="80" width="80"
xml:lang="it">https://...</mdui:Logo>
      </mdui:UIInfo>
    </md:Extensions>
...
  </SPSSODescriptor>
  <Organization>
      <OrganizationName xml:lang="it">Nome
dell'organizzazione</OrganizationName>
      <OrganizationName xml:lang="en">Organization Name</OrganizationName>
```

```
      <OrganizationDisplayName xml:lang="it">Nome
dell'organizzazione</OrganizationDisplayName>
      <OrganizationDisplayName xml:lang="en">Organization
Name</OrganizationDisplayName>
      <OrganizationURL
xml:lang="en">https://organization.url/</OrganizationURL>
  </Organization>
  <!-- contactType può essere uno di technical,administrative,support e
possono esserci più istanze di ContactPerson -->
  <ContactPerson contactType="technical">
    <GivenName>Administrator</GivenName>
    <SurName>Service</SurName>
    <EmailAddress>mailto:username@domain.tld</EmailAddress>
  </ContactPerson>
...
```

Requisiti minimi sul certificato

Public-Key: (2048 bit)

Signature Algorithm: sha256WithRSAEncryption

Entry point

Dichiarare la pagina / le pagine da cui l'utente accede al servizio.

Questo avviene solitamente tramite email/ticket a rete @ units.it

Validazione dei metadati

E' possibile validare i metadati presenti in una url web su https://technical.edugain.org/validator selezionando le lingue *"it"* e *"en"* e *"Metadata URL contains only one entity"*

Le specifiche di SAML 2.0 si trovano su
https://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

Metadati dell'IdP

I metadati dell'IdP sono presenti sul GARR IDEM Registry

Si consiglia di usare tale risorsa come autoritativa per l'aggiornamento degli stessi.

Attributi generalmente disponibili se richiesti

eduPersonAffiliation	Affiliation: Type of affiliation with Home Organization
eduPersonTargetedID	A pseudonomynous ID generated by the IdP that is unique to each SP
eduPersonScopedAffiliation	the affiliation of the user to the organisation concatendated with the domain name of the org (e.g. staff@dcu.ie)
eduPersonPrincipalName	eduPerson per Internet2 and EDUCAUSE see http://www.nmi-edit.org/eduPerson/draft-internet2-mace
surname	Surname or family name
displayName	A single string value indicating the preferred name of a person to be used for display purposes.
givenName	Given name of a person
sAMAccountName	sAMAccountName from Active Directory
schacMotherTongue	Is the language a person learns first. Correspondingly, the person is called a native speaker of the language. Usually a child learns the basics of their first language from their family.
commonName	CommonName
email	E-Mail: Preferred address for e-mail to be sent to this person
telephoneNumber	Business phone number: Office or campus phone number
schacHomeOrganization	Specifies a personÂ´s home organization using the domain name of the organization
schacHomeOrganizationType	Identifies the type of organisation specified in the person's schacHomeOrganization attribute.
schacPersonalUniqueCode	attributes of the following schema: urn:schac:personalUniqueCode:int:esi:units.it:<value> urn:schac:personalUniqueID:it:CF:<value>
schacPersonalUniqueID	Specifies a “legal unique identifier” for the subject it is associated with.
eduPersonEntitlement	Member of: URI (either URL or URN) that indicates a set of rights to specific resources based on an agreement ac

Entity Categories internazionali supportate

- Research and Scholarship Entity Category for IdPs https://refeds.org/category/research-and-scholarship
- Code of Conduct v1 for IdPs http://www.geant.net/uri/dataprotection-code-of-conduct/v1
- SIRTFI https://refeds.org/sirtfi
- European Student Identifier for IdPs https://wiki.geant.org/display/SM/European+Student+Identifier+Entity+Category