Nunzio Napolitano (Università degli Studi di Napoli '***PARTHENOPE***')

IdP configurazione base

Connessione con un SP

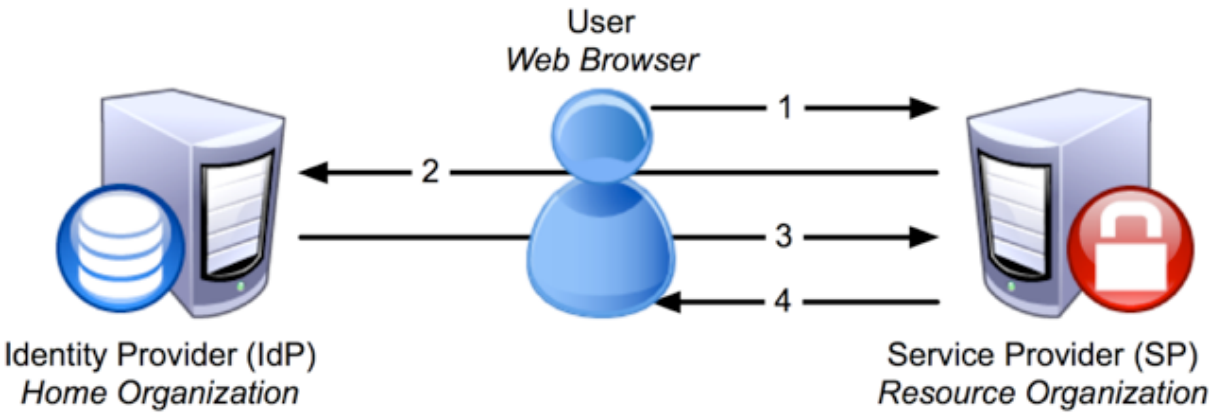
Consortium GARR

Agenda

- Panoramica su SP
- Configurazione metadati
- Test di funzionamento
- Configurazione attribute-**release**.xml
- Configurazione attribute-**filter**.xml
- Test di funzionamento

Nunzio Napolitano *(Università PARTHENOPE)*
nunzio.napolitano@uniparthenope.it

Quadro di insieme



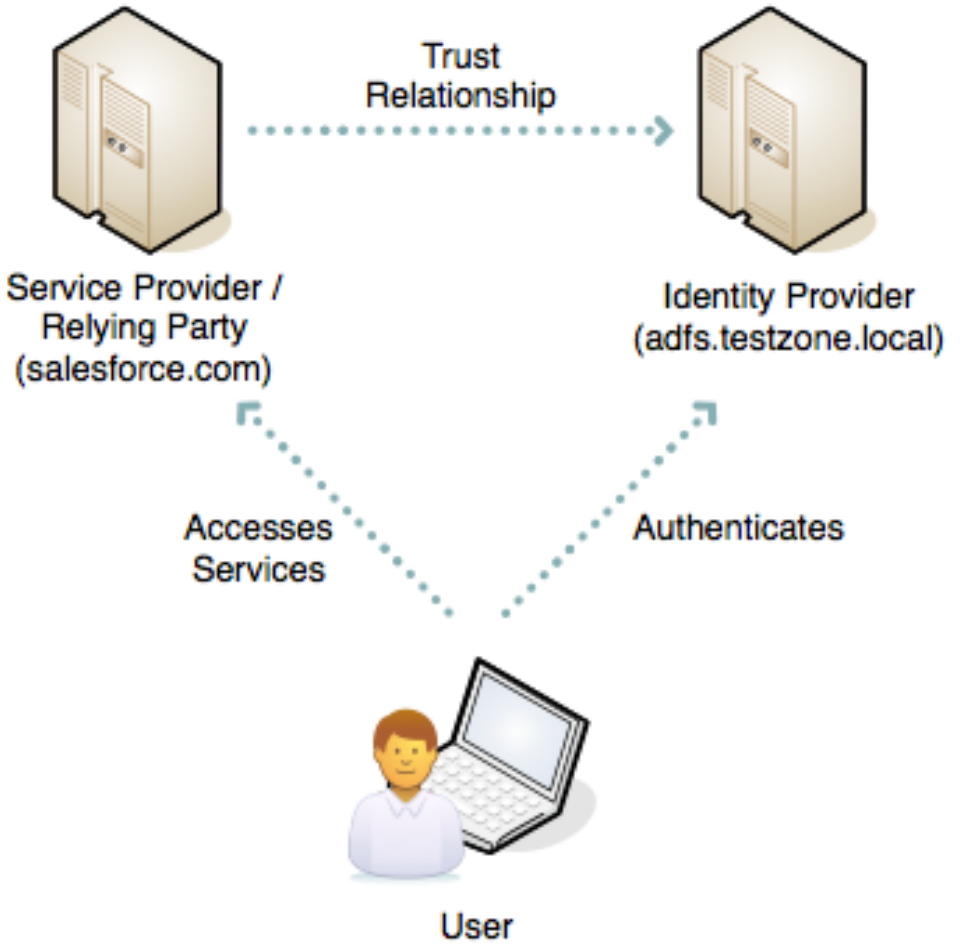
1.The SP detects the user attempting to **access restricted content** within the resource.
2.The SP generates an **authentication request**, then sends the request, and the user, to the user's IdP.
3.The **IdP authenticates** the user, then sends the **authentication response**, and the user, back to the SP.
4.The **SP verifies the IdP's response** and sends the request through to the resource

https://wiki.shibboleth.net/confluence/display/SHIB2/NewUnderstandingShibboleth

Nunzio Napolitano *(Università PARTHENOPE)*
nunzio.napolitano@uniparthenope.it

Trust relationship

La fiducia reciproca fra IdP ed SP si ottiene attraverso i **metadati**



Nunzio Napolitano *(Università PARTHENOPE)*
nunzio.napolitano@uniparthenope.it

Esercizio 1 – set dei metatadati

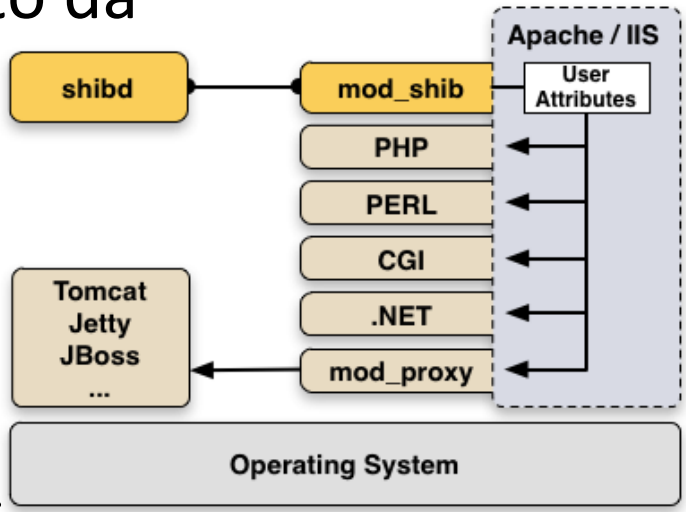
- Verifica (non) funzionamento (https://sp.example.org/secure)
- Aggiunta metadati Idp al SP
  - `Curl -k https://idp.example.org/idp/shibboleth -o /etc/shibboleth/metadata/idp.example.org-metadata.xml`
  - Restart servizio **`shibd`**
- Aggiunta metadati SP al IdP
  - `Curl -k https://sp.example.org/Shibboleth.sso/Metadata -o /opt/shibboleth-idp/metadata/sp.example.org-metadata.xml`
  - Modifica file `/opt/shibboleth-idp/conf/metadata-providers.xml`
  - Restart servizio **`tomcat7`**
- Verifica funzionamento (https://sp.example.org/secure)

Nunzio Napolitano *(Università PARTHENOPE)*
nunzio.napolitano@uniparthenope.it

Shibboleth SP

Shibboleth Service Provider è composto da

- mod_shib (Apache /IIS)
- Demone SHIBD



Caratteristiche

- Proteggere l'accesso con «Require»
- Attributi utente accessibili nell'ambiente del web server da tutte le applicazioni (PHP, Perl, .Net, ASP, CGI, ...) es. $_SERVER['mail'].
- Servlet container, (es. Tomcat) devono operare con Apache or IIS come front-end

Nunzio Napolitano *(Università PARTHENOPE)*
nunzio.napolitano@uniparthenope.it

Definizione dell'attibuto

Attribute-resolver.xml

```
<resolver:AttributeDefinition  xsi:type="ad:Simple"
  sourceAttributeID="uid" id="ORG_srvX_code" >

<resolver:Dependency ref="myLDAP" />
        ……
</resolver:AttributeDefinition>
```

Nunzio Napolitano *(Università PARTHENOPE)*
nunzio.napolitano@uniparthenope.it

Codifica SAML dell'attributo

Attribute-resolver.xml

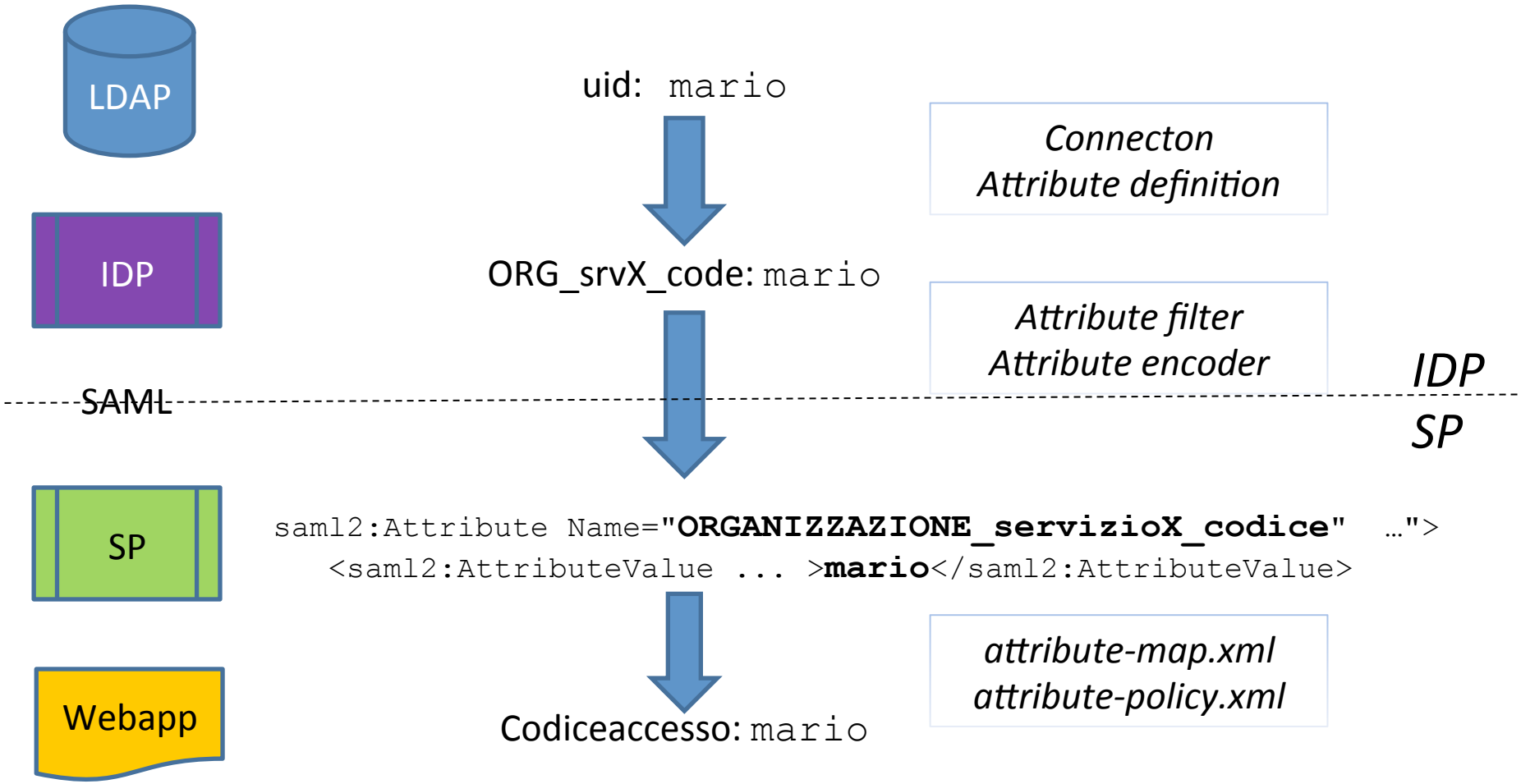
```
<resolver:AttributeDefinition
   ……
<resolver:Dependency ref="myLDAP" />

<resolver:AttributeEncoder xsi:type="enc:SAML2String"
  name="ORGANIZZAZIONE_servizioX_codice"
  friendlyName= "codice servizio X"
  encodeType="false" />
</resolver:AttributeDefinition>
```

saml2:Assertion

```
….
<saml2:Attribute
   FriendlyName="codice servizio X" Name="ORGANIZZAZIONE_servizioX_codice"  …">
   <saml2:AttributeValue ... xsi:type="xs:string">mario</saml2:AttributeValue>
 </saml2:Attribute>
```


Nunzio Napolitano *(Università PARTHENOPE)*
nunzio.napolitano@uniparthenope.it

Passaggio attributi – *end to end*



Nunzio Napolitano *(Università PARTHENOPE)*
nunzio.napolitano@uniparthenope.it

Esercizio 2 – rilascio attributi

- Configurazione attribute-**release**.xml
  - Copia `attribute-resolver-full.xml` in `attribute-resolver.xml`
  - Scommentare le definizioni degli attributi
  - Definire il seguente attributo custom:
    - Id: **`ORG_srvX_code`**
    - Attributo Ldap di origine: **`uid`**
    - SAML encoding: **`ORGANIZZAZIONE_servizioX_codice`**
- Configurazione attribute-**filter**.xml
  - Edit file `attribute-filter.xml` per aggiungere il rilascio dei seguenti attributi:

    `commonName displayName surname givenName ORG_srvX_code`
- Restart servizio
- Verifica finale

Nunzio Napolitano *(Università PARTHENOPE)*
nunzio.napolitano@uniparthenope.it

Speriamo vi sia piaciuto….

…..e tutto abbia funzionato!!!

Nunzio Napolitano *(Università PARTHENOPE)*
nunzio.napolitano@uniparthenope.it