Configurazione base di un IdP

Connessione con un SP

Nunzio Napolitano <nunzio.napolitano@uniparthenope.it> - *Università PARTHENOPE, CTS*

Agenda

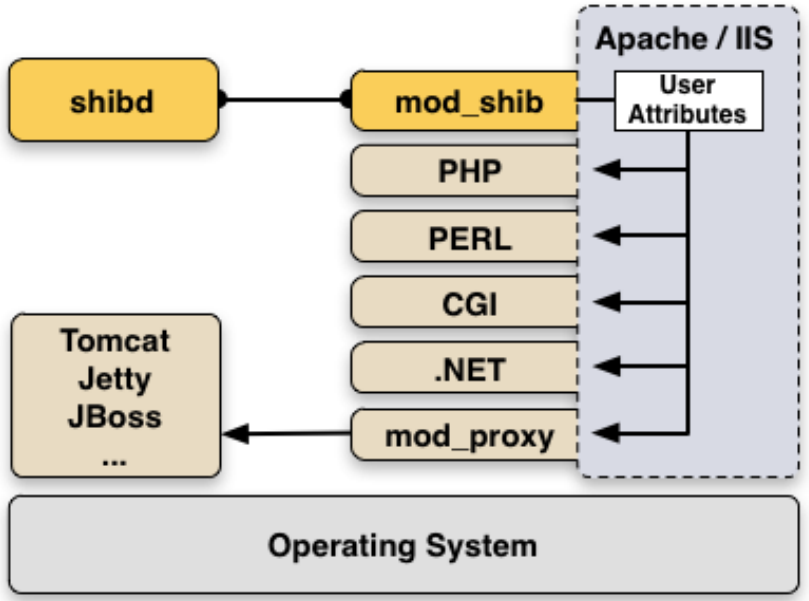
- Panoramica su SP
- Configurazione metadati
  - Test di funzionamento
- Rilascio attributi
  - Configurazione attribute-**release**.xml
  - Configurazione attribute-**filter**.xml
  - Test di funzionamento

Impostiamo l’ambiente di lavoro

ansible-playboook playbook.yml -i hosts -e '{"pre_t": 2}'

Nunzio Napolitano <nunzio.napolitano@uniparthenope.it> - *Università PARTHENOPE, CTS*

Shibboleth SP



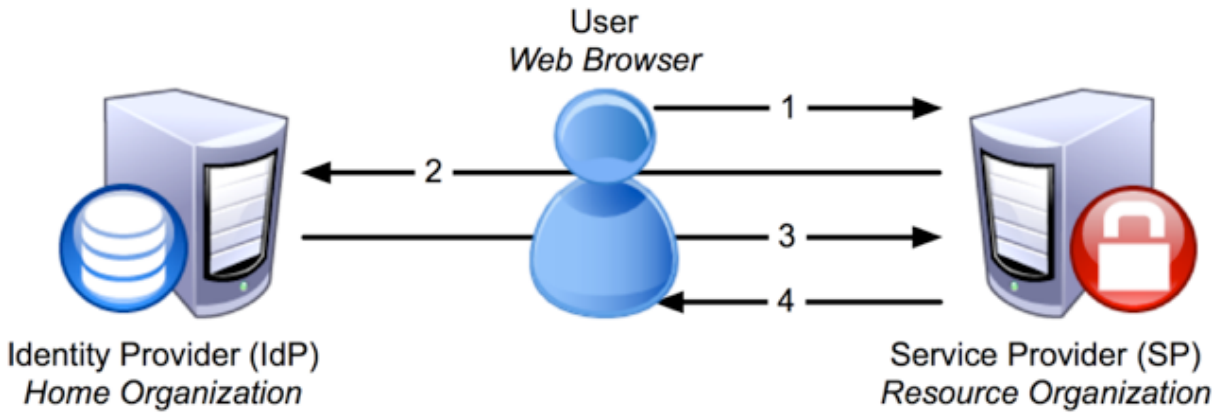
Shibboleth Service Provider è composto da

- 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. jetty) devono operare con Apache or IIS come front-end

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.

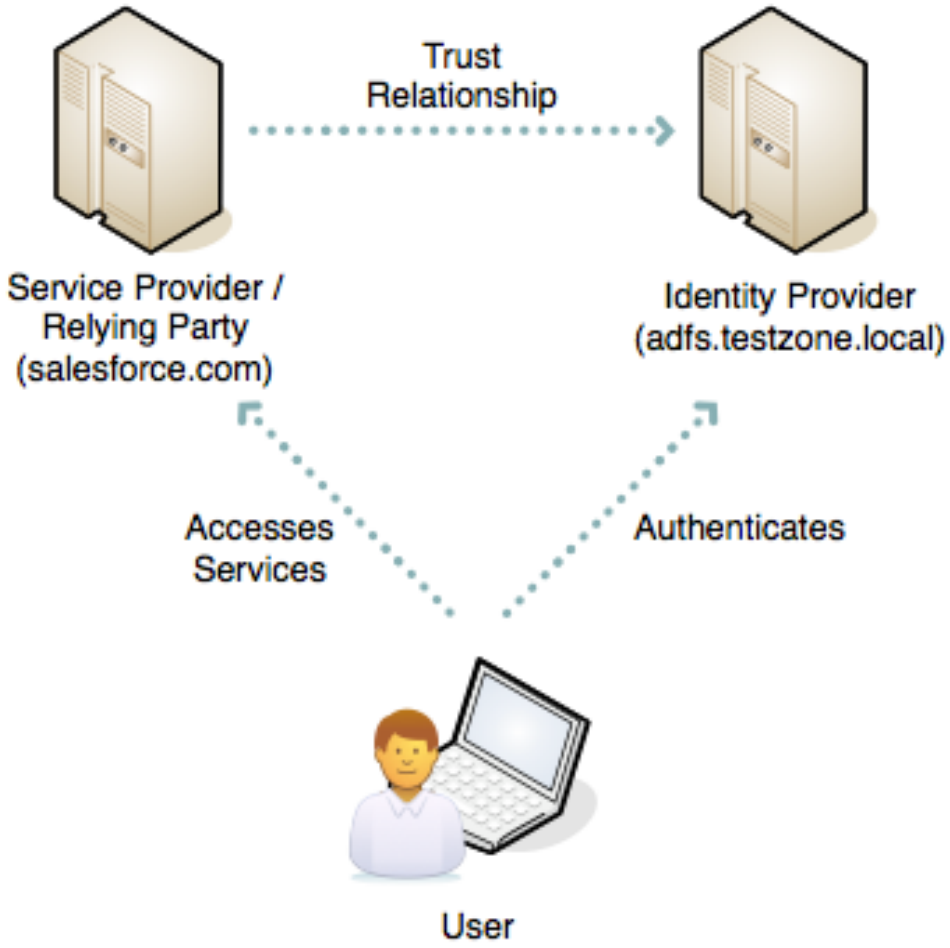
4.The **SP verifies the IdP's response** and sends the request through to the resource

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

Nunzio Napolitano <nunzio.napolitano@uniparthenope.it> - *Università PARTHENOPE, CTS*

Trust relationship

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

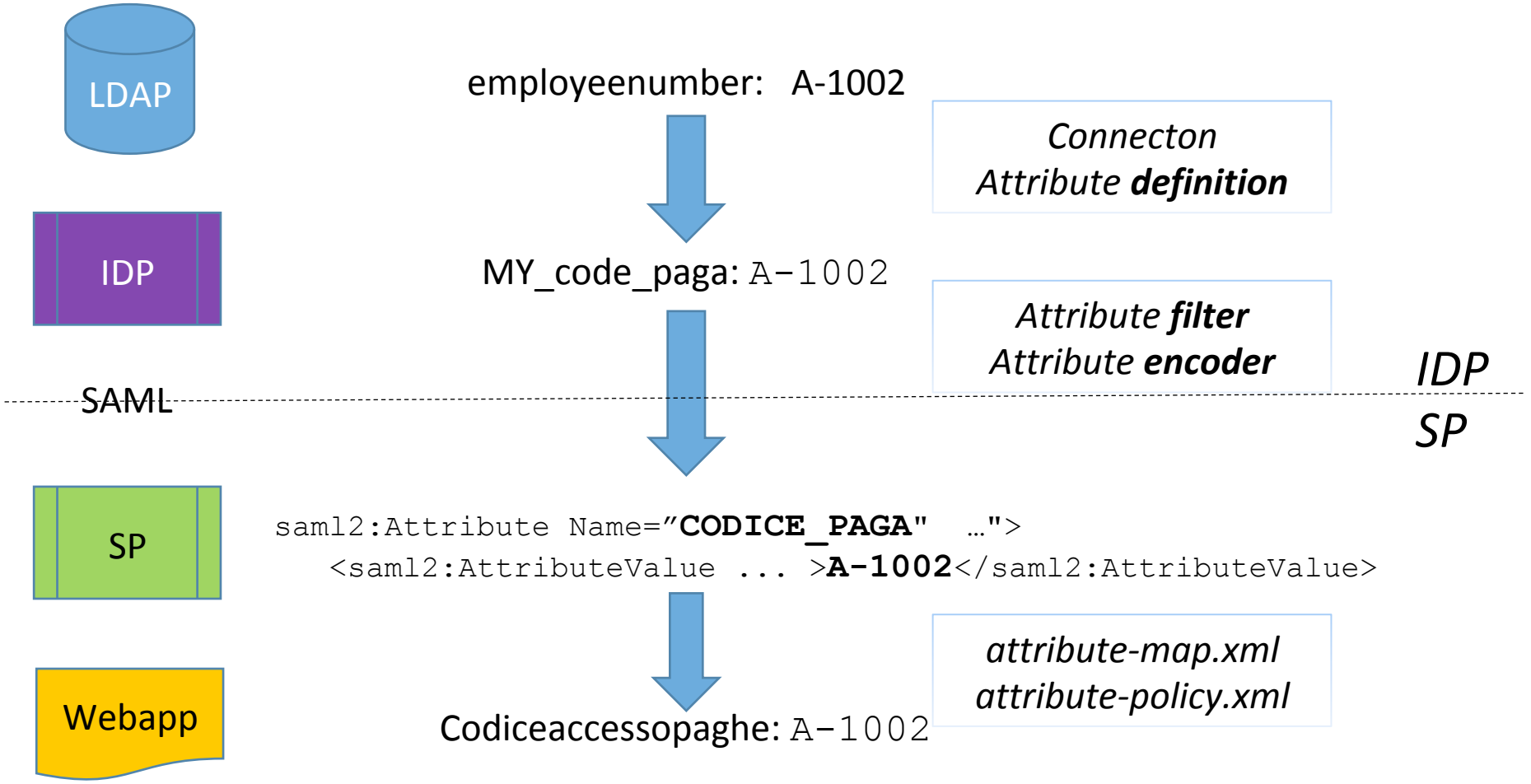


Nunzio Napolitano <nunzio.napolitano@uniparthenope.it> - *Università PARTHENOPE, CTS*

Esercizio 1 – set dei metatadati

1. Verifica (**non**) funzionamento (https://sp.example.org/secure)
2. 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`** (`service shibd restart`)
3. Verifica (**non**) funzionamento (https://sp.example.org/secure)
4. 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`
   - Reload dei metadati run-time
     - `cd /opt/shibboleth-idp/bin`
     - `./reload-service.sh -id shibboleth.MetadataResolverService -u http://localhost:8080/idp`
5. Verifica funzionamento (https://sp.example.org/secure)

Passaggio attributi – end to end



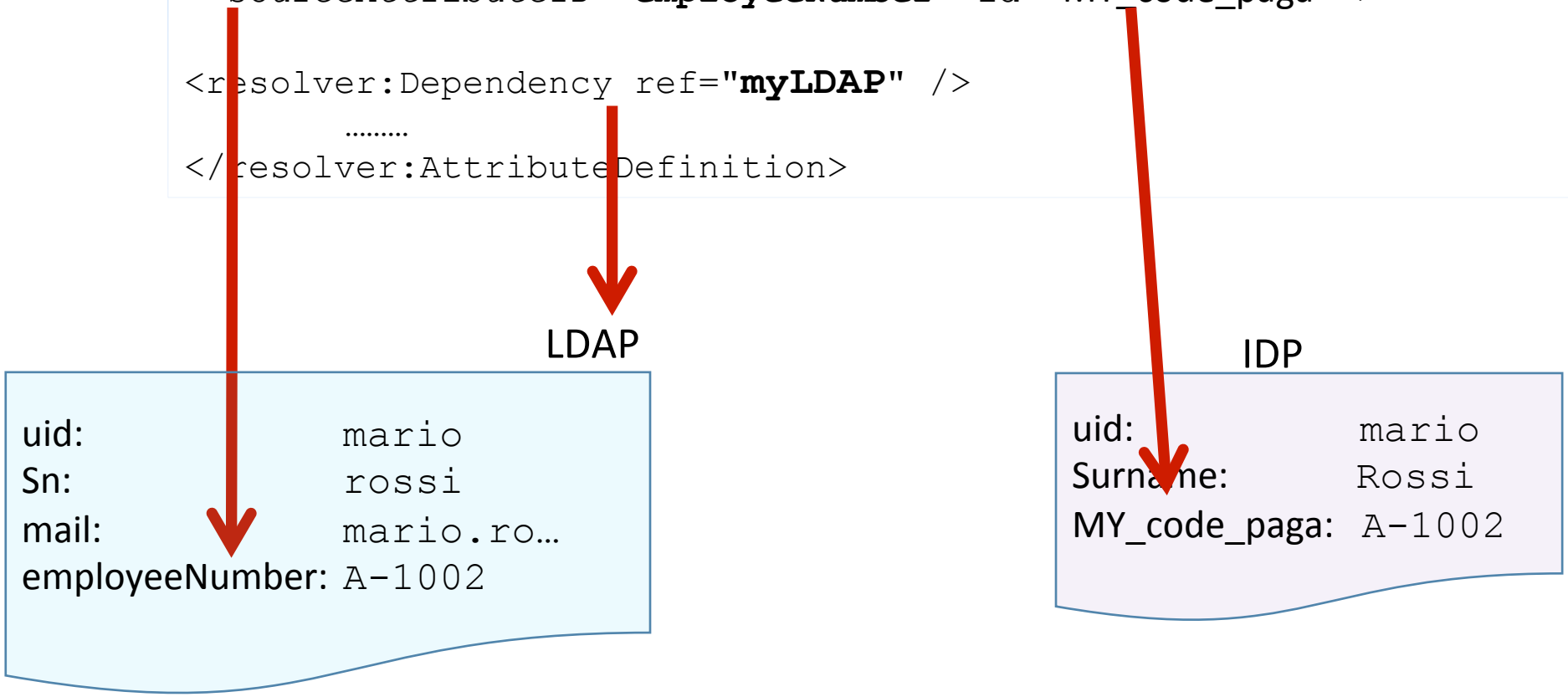
Nunzio Napolitano <nunzio.napolitano@uniparthenope.it> - *Università PARTHENOPE, CTS*

Definizione dell'attibuto

Attribute-resolver.xml

```
<resolver:AttributeDefinition  xsi:type="ad:Simple"
  sourceAttributeID="employeeNumber" id="MY_code_paga" >

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



Codifica SAML dell'attributo

Attribute-resolver.xml

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

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

saml2:Assertion

```
….
<saml2:Attribute
   FriendlyName="codice X servizio paghe" Name="CODICE_PAGA"  …">
   <saml2:AttributeValue ... xsi:type="xs:string">A-1002</saml2:AttributeValue>
 </saml2:Attribute>
```


Nunzio Napolitano <nunzio.napolitano@uniparthenope.it> - *Università PARTHENOPE, CTS*

Esercizio 2 – parte 1 *configurazione attributi*

- Configurazione attribute-**release**.xml
  - Copia `attribute-resolver-full.xml` in `attribute-resolver.xml`
  - Decommentare le definizioni degli attributi e il dataconnector MyLdap
  - Definire il seguente attributo custom:
    - Id: **`MY_code_paga`**
    - Attributo Ldap di origine: **`employeeNumber`**
    - SAML name: **`CODICE_PAGA`**
    - SAML friendly name **`Codice X servizio paghe`**

- Reload della configurazione

```
curl -sk https://localhost/idp/profile/admin/reload-service?
id=shibboleth.MetadataResolverService
```

Esercizio 2 – Verifica intermedia

https://sp.example.org/secure/index.php

Mario / mariopw2018

Maria / mariapw2018

Pino / pinopw2018

Pina / pinapw2018

Check attributi

Verifica degli attributi disponibili alla applicazione finale

Staus	Requirement	Required value	SAML2 attribute name	Environment Variable	Value
	Required		MY_PAGA_CODE	codiceaccessopaghe	
	Required	@example.org	urn:oid:0.9.2342.19200300.100.1.3	mail	
	Optional		miaOrganizzazione:adGroup	ActiveDir_group	
	Optional		miaOrganizzazione:adMail	Additional_mail	
	Optional		urn:oid:2.5.4.3	cn	
	Optional		urn:oid:2.16.840.1.113730.3.1.241	displayName	
	Optional		urn:oid:1.3.6.1.4.1.5923.1.1.1.7	entitlement	

Nunzio Napolitano <nunzio.napolitano@uniparthenope.it> - *Università PARTHENOPE, CTS*

Esercizio 2 – parte 2 *rilascio attributi*

- Configurazione attribute-**filter**.xml
  - Edit file `attribute-filter.xml` per aggiungere il rilascio dei seguenti attributi:

```
uid
commonName
displayName
Surname
givenName
mail
edupersonaffiliation
edupersonascopedaffiliation
MY_code_paga
```

- Reload della configurazione

```
curl -sk https://localhost/idp/profile/admin/reload-service?
id=shibboleth.AttributeFilterResources
```

Esercizio 2 – Verifica finale

`https://sp.example.org/secure/index.php`

Check attributi

Verifica degli attributi disponibili alla applicazione finale

Staus	Requirement	Required value	SAML2 attribute name	Environment Variable	Value
	Required		MY_PAGA_CODE	codiceaccessopaghe	A-1002
	Required	@example.org	urn:oid:0.9.2342.19200300.100.1.3	mail	maria.verdi@example.org
	Optional		urn:oid:2.5.4.42	givenName	Maria
	Optional		urn:oid:2.5.4.4	sn	Verdi
	Optional		miaOrganizzazione:adGroup	ActiveDir_group	
	Optional		urn:oid:1.3.6.1.4.1.25178.1.2.10	schacHomeOrganizationType	
	Not needed	staff	urn:oid:1.3.6.1.4.1.5923.1.1.1.9	affiliation	student@example.org member@example.org

Nunzio Napolitano <nunzio.napolitano@uniparthenope.it> - *Università PARTHENOPE, CTS*

Speriamo vi sia piaciuto….

…..e tutto abbia funzionato!!!

Domande???

Se qualcosa fosse andato storto…

ansible-playboook playbook.yml -i hosts -e '{"pre_t": 3}'

Nunzio Napolitano <nunzio.napolitano@uniparthenope.it> - *Università PARTHENOPE, CTS*