

Installare un Service Provider

Davide Vaghetti <davide.vaghetti@garr.it>

Università degli Studi Roma Tre, 07-10-2019

Workshop GARR 2019 "Net Makers"

Agenda

- Installazione e configurazione di Shibboleth Service Provider 3.04
- Protezione di una Location
- Configurazione con IdP locale
- Registrazione in Federazione di Test
- Configurazione del Discovery Service
- Configurazione dei metadata della Federazione di Test

Shibboleth Service Provider

Shibboleth Service Provider permette di abilitare il single sign on basato su SAML e l'autenticazione federata tramite integrazione nativa con i web server Apache e IIS.



Shibboleth®

Installazione

Verifica della versione di Shibboleth SP che verra' installata

```
$ apt-cache showpkg libapache2-mod-shib
```

```
Package: libapache2-mod-shib
```

```
Versions:
```

```
3.0.4+dfsg1-1 (/var/lib/apt/lists/deb.debian.org_[...])
```

Installare il modulo per Apache2 e le dipendenze

```
$ sudo apt-get install libapache2-mod-shib make
```

Cosa e' stato installato?

Tre pacchetti principali

```
libapache2-mod-shib  # modulo e file di configurazione per apache2
shibboleth-sp-common # file HTML, XSD e di configurazione per shibd
shibboleth-sp-utils  # utilities e demone shibd
```

Diamo uno sguardo più da vicino

```
$ dpkg -L libapache2-mod-shib
$ dpkg -L shibboleth-sp-common
$ dpkg -L shibboleth-sp-utils
```

File e directory

`/etc/shibboleth` # File di configurazione per il demone *shibd*
shibboleth2.xml file di configurazione principale di *shibd*
attribute-map.xml definizione degli attributi

`/var/log/shibboleth` # File di log
shibd.log log generali del processo
transaction.log, log delle singole transazioni

`/var/cache/shibboleth` # Cache dei metadata

Status

Per verificare lo stato di *shibd*

```
sudo shibd -t
```

Mancano le chiavi per signing e encryption

```
sudo shibd -t
```

```
[..]
```

```
2019-10-04 12:04:25 ERROR XMLTooling.CredentialResolver.Chaining : caught exception  
processing embedded CredentialResolver element: Unable to load private key from file  
(/etc/shibboleth/sp-signing-key.pem).
```

```
[..]
```

```
2019-10-04 12:04:25 ERROR XMLTooling.CredentialResolver.Chaining : caught exception  
processing embedded CredentialResolver element: Unable to load private key from file  
(/etc/shibboleth/sp-encrypt-key.pem).
```

```
[..]
```


Chiavi e certificati

Creiamo le coppie chiavi certificati per signing e encryption

```
$ sudo /usr/sbin/shib-keygen -n sp-signing -e https://sp<NUM>.aai-test.garr.it
$ sudo /usr/sbin/shib-keygen -n sp-encrypt -e https://sp<NUM>.aai-test.garr.it
# File creati: $ ls /etc/shibboleth/*.pem
# I certificati così creati hanno una durata di 10 anni e sono RSA a 3072 bit
(man shib-keygen)
```

Verifichiamo le informazioni contenute nei certificati

```
$ openssl x509 -in /etc/shibboleth/sp-encrypt-cert.pem -noout -text
$ openssl x509 -in /etc/shibboleth/sp-signing-cert.pem -noout -text
```

shibboleth2.xml: entityID e https

Aprire il file /etc/shibboleth/shibboleth2.xml

```
$ sudo vim /etc/shibboleth/shibboleth2.xml
```

Impostate l'entityID

[...]

```
<ApplicationDefaults entityID="https://sp-<NUM>.aai-test.garr.it/shibboleth"
```

[...]

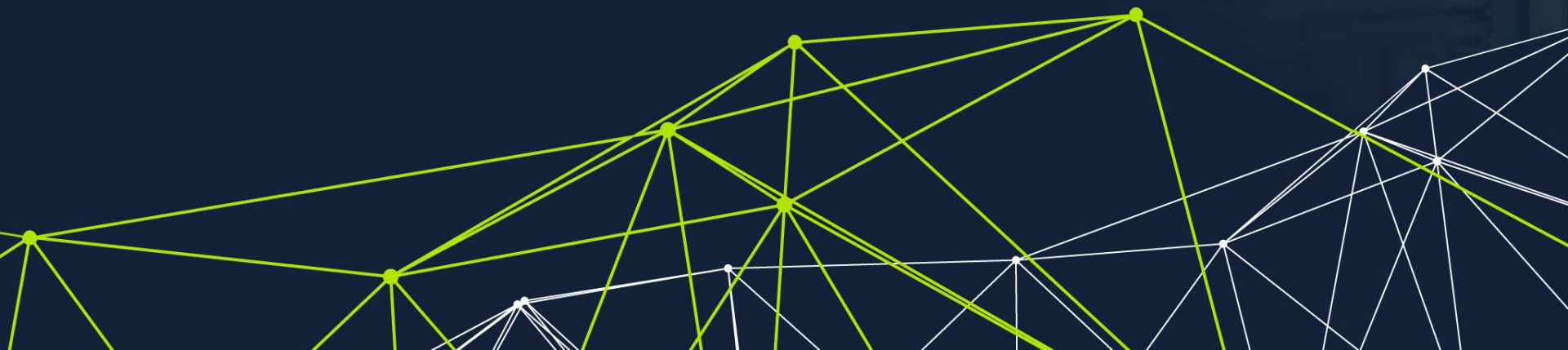
Forzare https su cookie e handler

[...]

```
<Sessions lifetime="28800" timeout="3600" relayState="ss:mem"  
    checkAddress="false" handlerSSL="true" cookieprops="https">
```

[...]

Configuriamo un IdP locale



IdP locale: metadata e entityID

Scarichiamo i metadata

```
$ cd /etc/shibboleth  
$ sudo wget https://idp-wsgarr19.aai-test.garr.it/idp/shibboleth -O idp-wsgarr19.xml
```

Configuriamo l'IdP in *shibboleth2.xml*

```
$ vim /etc/shibboleth/shibboleth2.xml  
  
[...]  
<SSO entityID="https://idp-wsgarr19.aai-test.garr.it/idp/shibboleth"  
    SAML2  
</SSO>  
[...]  
<MetadataProvider type="XML" validate="true" path="idp-wsgarr19.xml"/>  
[...]
```

Verifichiamo la configurazione e riavviamo *shibd*

```
$ sudo shibd -t  
  
$ sudo service shibd restart
```

Verifichiamo il funzionamento del Service Provider

Location /Shibboleth.sso

Login

<https://sp-<NUM>.aai-test.garr.it/Shibboleth.sso/Login>

Logout

<https://sp-<NUM>.aai-test.garr.it/Shibboleth.sso/Logout>

Status (solo da localhost)

<https://sp-<NUM>.aai-test.garr.it/Shibboleth.sso/Status>

Session

<https://sp-<NUM>.aai-test.garr.it/Shibboleth.sso/Session>

Metadata

<https://sp-<NUM>.aai-test.garr.it/Shibboleth.sso/Metadata>

Discovery Feed

<https://sp-<NUM>.aai-test.garr.it/Shibboleth.sso/DiscoFeed>

Proteggiamo una directory di Apache2

Verifichiamo che /docs sia accessibile senza autenticazione

(BROWSER) `https://sp-<NUM>.aai-test.garr.it/docs`

Configuriamo l'autenticazione per la *Location*

```
$ sudo vim /etc/apache2/site-available/sp-<NUM>.aai-test.garr.it.conf
```

```
[..]  
    <Location /docs>  
        AuthType shibboleth  
        ShibRequestSetting requireSession true  
        Require valid-user  
    </Location>  
</VirtualHost>  
[..]
```

Accesso autenticato

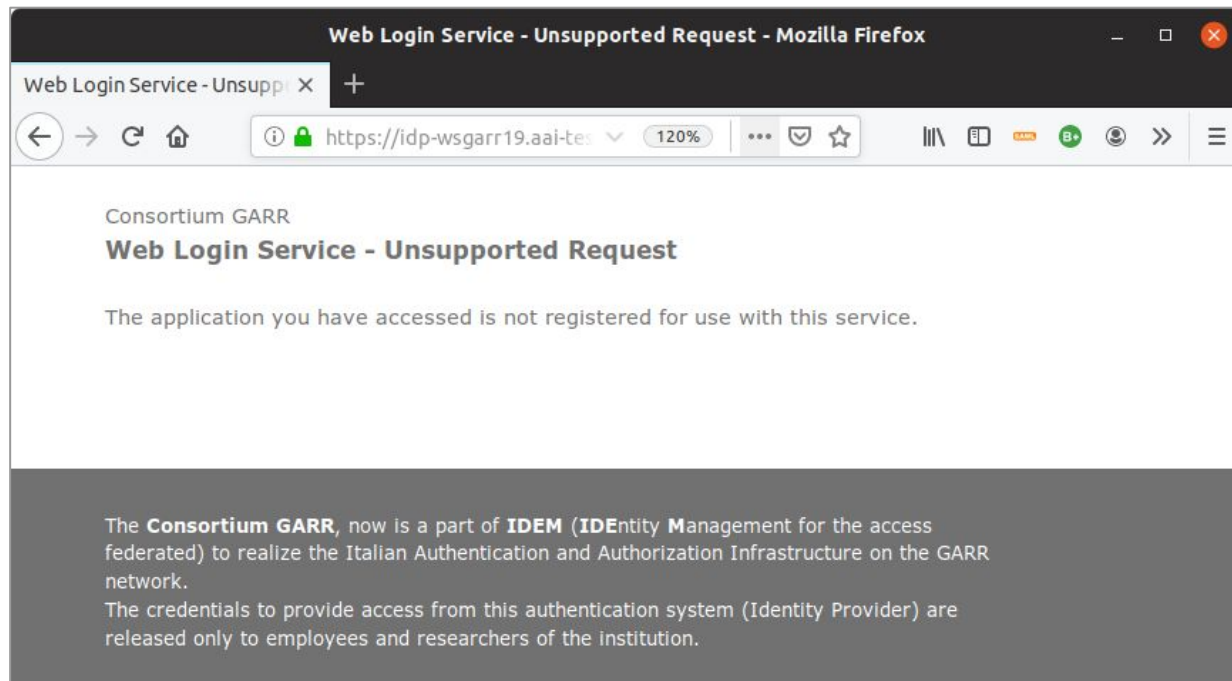
Attiviamo la nuova configurazione

```
$ sudo service apache2 reload
```

Verifichiamo che /docs sia accessibile **previa autenticazione**

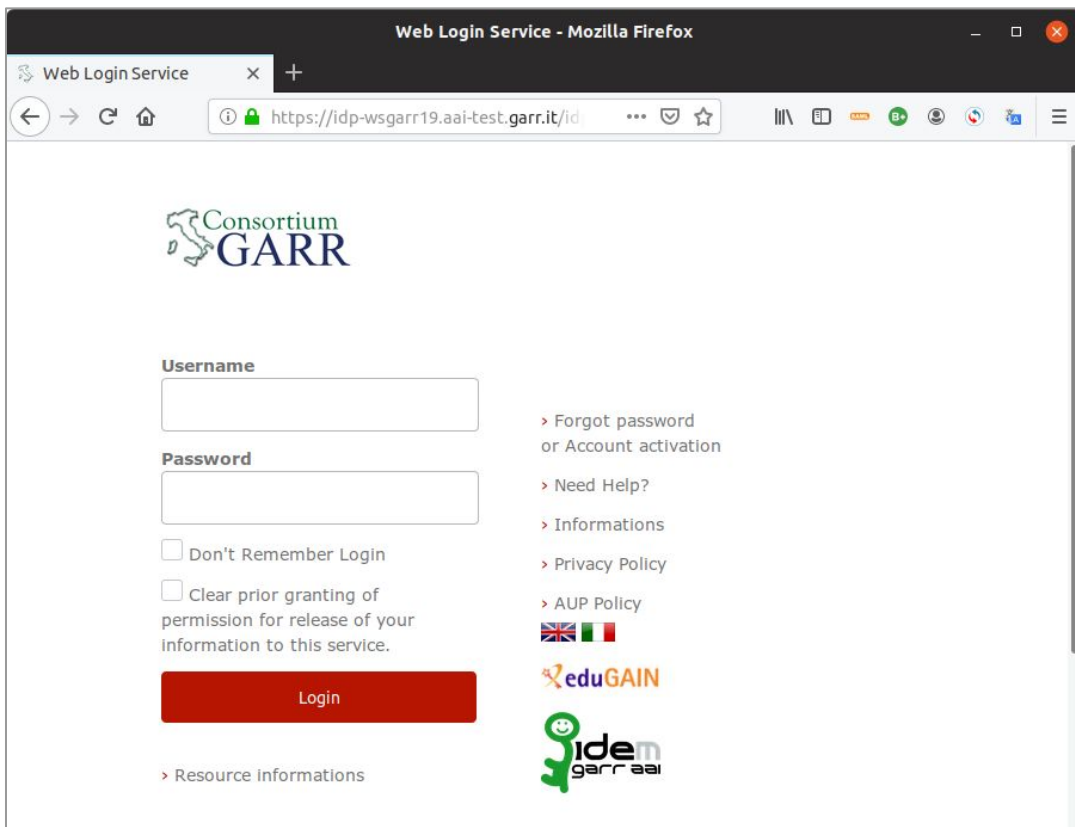
(BROWSER) <https://sp-<NUM>.aai-test.garr.it/docs>

Redirezione sull'IdP configurato



Il nostro Service
Provider è sconosciuto
per l'Identity Provider
--- mancano i
metadata.

Scambiati i metadata... riproviamo



Web Login Service - Mozilla Firefox

Web Login Service

https://idp-wsgarr19.aai-test.garr.it/id

Consortium GARR

Username

Password

☐ Don't Remember Login

☐ Clear prior granting of permission for release of your information to this service.

Login

> Forgot password or Account activation

> Need Help?

> Informations

> Privacy Policy

> AUP Policy

eduGAIN

idem garr aai

> Resource Informations

Il nostro Service Provider questa volta viene correttamente riconosciuto dall'Identity Provider e veniamo rediretti alla pagina di login.

Cosa succede dietro il browser...

```
$ sudo tail -f /var/log/shibboleth/transaction.log /var/log/shibboleth/shibd.log
```

```
==> /var/log/shibboleth/transaction.log <==
```

```
2019-10-05 07:33:06|Shibboleth-TRANSACTION.AuthnRequest|||https://idp-wsgarr19.aai-test.garr.  
it/idp/shibboleth|||||urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect|||||
```

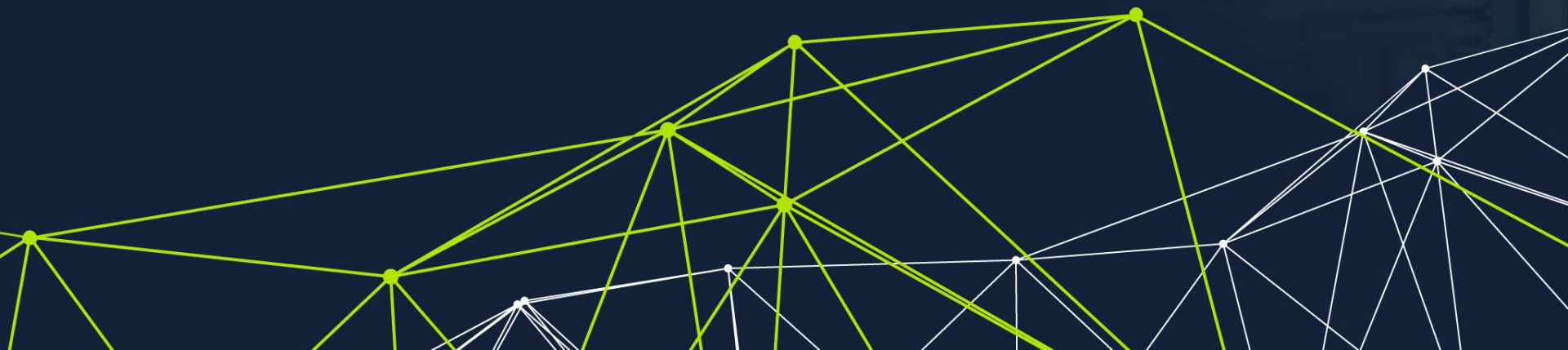
```
2019-10-05 07:33:24|Shibboleth-TRANSACTION.Login|_|_cc5a0cd7795043569d3164c8b12e025d|https://i  
dp-wsgarr19.aai-test.garr.it/idp/shibboleth|_9db55daff56ad792530d443fbb90293c|urn:oasis:names  
:tc:SAML:2.0:ac:classes:PasswordProtectedTransport|2019-10-05T07:33:23|AAdzZWNyZXQxuHg9H3Hed  
SQ1rFcdPj5kaFX/mhb6LIw1ZvZvKJn/vNNp+MC5pI/b9wGVk0J4q77kHu1TMOPDZuRdYXA+hMcn4GsPmB7bjlNPnenaLO  
VeqDhQD2ocAXYDMJbMQNm4HfyrU/qTnyB4I/3L5s4b+RkzjJQgMAKZ|urn:oasis:names:tc:SAML:2.0:bindings:H  
TTP-POST||urn:oasis:names:tc:SAML:2.0:status:Success||Mozilla/5.0 (X11; Linux x86_64)  
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36|79.49.202.16
```

```
2019-10-05 07:43:10|Shibboleth-TRANSACTION.AuthnRequest|||https://idp-wsgarr19.aai-test.garr.  
it/idp/shibboleth|||||urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect|||||
```

```
==> /var/log/shibboleth/shibd.log <==
```

```
2019-10-05 07:43:10|Shibboleth-TRANSACTION.AuthnRequest|||https://idp-wsgarr19.aai-test.garr.  
it/idp/shibboleth|||||urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect|||||
```

Registriamo il SP in federazione di Test



Copiamo i metadata del nostro SP

Recuperiamo i metadata:

(BROWSER) <https://sp-<NUM>.aai-test.garr.it/Shibboleth.sso/Metadata>

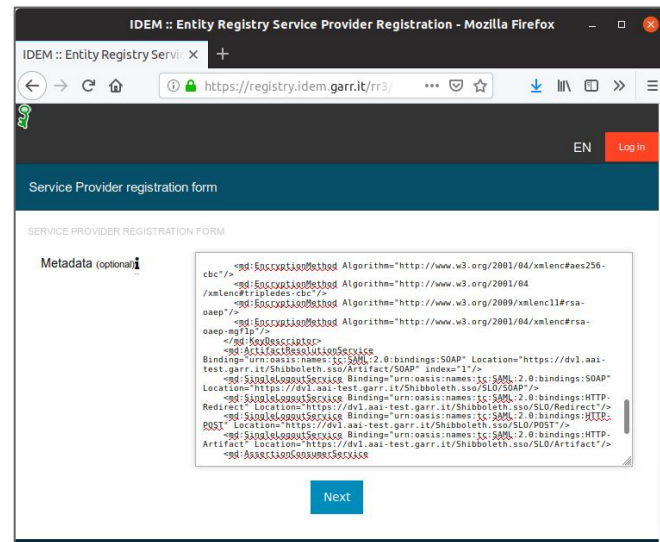
Salviamoli e copiamo il contenuto nella clipboard

apriamo il file con un editor

selezioniamo tutto il contenuto

CTRL-C

(BROWSER) <https://registry.idem.garr.it>



Popoliamo *General* e *Organization*

IDEM :: Entity Registry - Mozilla Firefox

IDEM :: Entity Registry

https://registry.idem.garr.it/rr3/

EN Log in

Service Provider registration form - advanced mode

SERVICE PROVIDER REGISTRATION FORM

General Organization Contacts UI Information SAML Certificates Required Attributes

Federation i

IDEM Test Federation

Your contact details

Given name

Surname

Email

Contact phone

Start over Save draft Register

IDEM :: Entity Registry - Mozilla Firefox

IDEM :: Entity Registry

https://registry.idem.garr.it/rr3/prc

EN Log in

Service Provider registration form - advanced mode

SERVICE PROVIDER REGISTRATION FORM

General Organization Contacts UI Information SAML Certificates Required Attributes

Name of organization

Abkhaz (ab) Add in new language

Displayname of organization

English (en) Add in new language

URL to information about organization

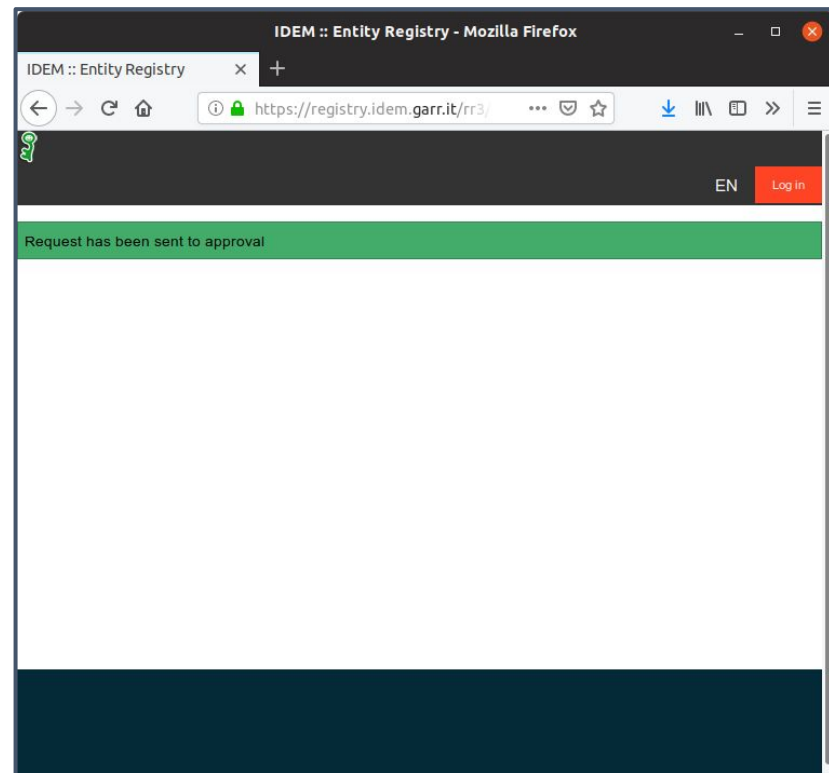
English (en) Add in new language

Start over Save draft Register

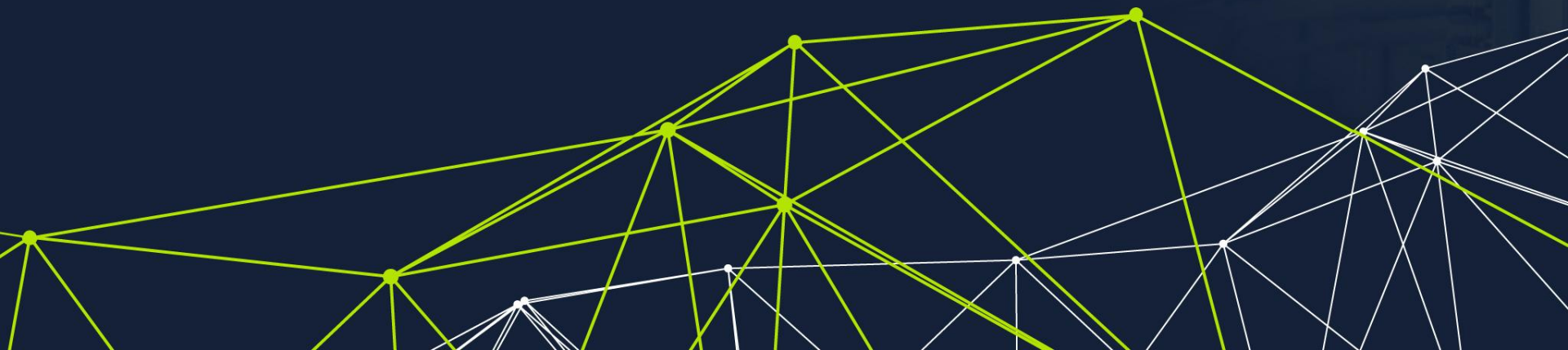
Inviando la richiesta di registrazione

Il tipico workflow prevede la registrazione del Service Provider via web-form e l'invio di una mail <idem-help@garr.it> per richiedere l'approvazione da parte del Servizio IDEM GARR AAI.

Una volta ricevuta la conferma dell'approvazione, i metadata del nostro SP saranno distribuiti nella federazione di Test.



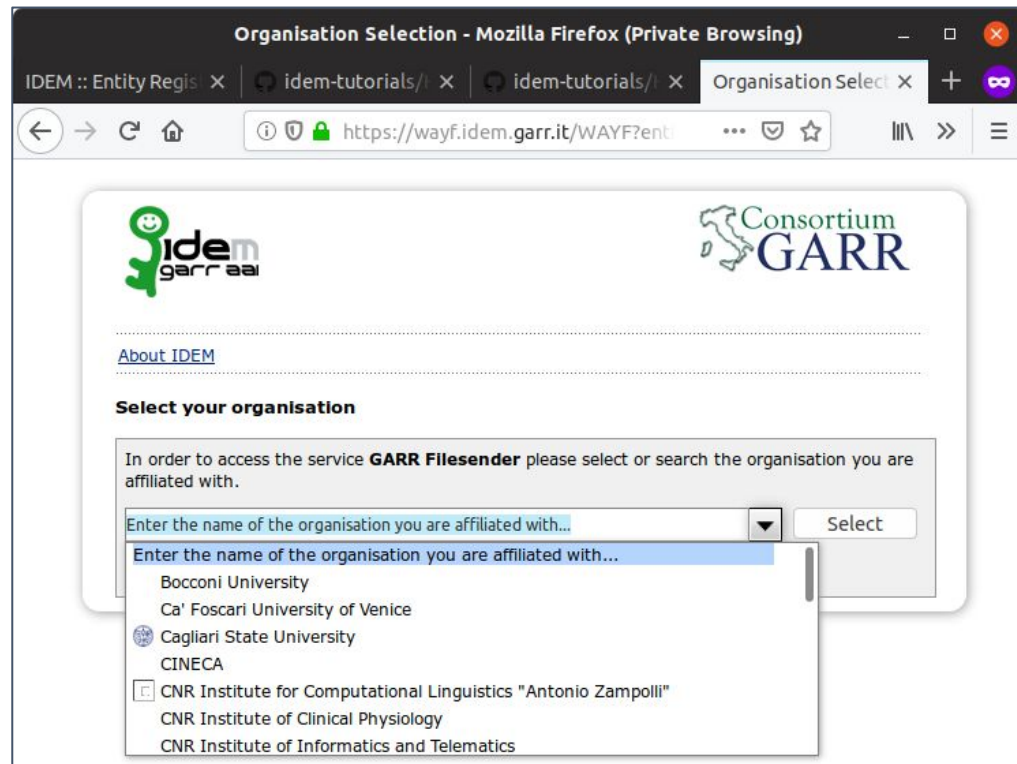
Installiamo il Discovery Service



Discovery service

Per attivare l'autenticazione con gli IdP della federazione di Test ci dobbiamo dotare di un *Discovery Service*, cioè il servizio che ci permette di scegliere dinamicamente ed in tempo reale l'IdP con cui autenticarci.

Il *Discovery Service* può essere locale, ad esempio Shibboleth EDS, o remoto, ad esempio il WAYF di IDEM.



Installiamo un discovery service locale

Scarichiamo e installiamo Shibboleth EDS

```
$ cd /usr/local/src ; sudo wget https://shibboleth.net/downloads\  
/embedded-discovery-service/1.2.2/shibboleth-embedded-ds-1.2.2.tar.gz  
$ sudo tar xfvz shibboleth-embedded-ds-1.2.2.tar.gz  
$ cd shibboleth-embedded-ds-1.2.2 ; sudo make install
```

Verifichiamo cosa è stato installato

```
$ cd /etc/shibboleth-ds  
  
$ ls -la
```

Configuriamo la *returnWhiteList* del EDS

```
$ sudo vim /etc/shibboleth-ds/idpselect_config.js  
[...]  
this.returnWhiteList = [  
"^https://\\/sp-<NUM>\\.aai-test\\.garr\\.it\\/Shibboleth\\.sso\\/Login.*$" ];  
[...]
```

Abilitiamo la configurazione per Apache2

```
$ sudo cp shibboleth-ds.conf /etc/apache2/conf-available  
$ sudo a2enconf shibboleth-ds  
$ sudo service apache2 reload
```

Abilitiamo il discovery service nel service provider

Modifichiamo il tag SSO in shibboleth2.xml

```
$ sudo vim /etc/shibboleth/shibboleth2.xml
```

[...]

```
<SSO discoveryProtocol="SAMLDS"
```

```
discoveryURL="https://dv1.aai.test.garr.it/shibboleth-ds">
```

```
SAML2
```

```
</SSO>
```

[...]

...e carichiamo i metadata di federazione

Aggiungiamo un *MetadataProvider*

```
$ cd /etc/shibboleth
```

```
$ sudo wget https://md.idem.garr.it/certs/idem-signer-20220121.pem -O idem-sign-cert.pem
```

```
$ sudo vim /etc/shibboleth/shibboleth2.xml
```

[...]

```
<MetadataProvider type="XML"
    url="http://md.idem.garr.it/metadata/idem-test-metadata-sha256.xml"
    backingFilePath="idem-test-metadata-sha256.xml"
    maxRefreshDelay="7200">
  <MetadataFilter type="Signature" certificate="idem-sign-cert.pem" verifyBackup="false"/>
  <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000" />
</MetadataProvider>
```

[...]

Accesso autenticato con un IdP di federazione

Attiviamo la nuova configurazione

```
$ sudo service apache2 reload
```

```
$ sudo service shibd restart
```

Accediamo alla location protetta (/docs)

(BROWSER) <https://sp-<NUM>.aai-test.garr.it/docs>

Fine

Domande?

Davide Vaghetti (davide.vaghetti@garr.it)

Marco Malavolti (marco.malavolti@garr.it)