ALLEGATO 1

Integrazione con sistema “IMS-SPID Regione Basilicata” tramite SP Shibboleth

Ver.Documento 1.3
22.03.2017

INFRASTRUTTURA

Server : 172.18.17.249

S.O. Centos

Servizi **Apache** e **Shibboleth**

Le cartelle su cui intervenire per le configurazioni sono

per Apache:
/etc/httpd/conf.d

Per Shibboleth
/**etc/shibboleth**

I file su cui intervenire sono:

Per Apache

i file conf legati agli url pubblicati:
es. sic.regione.basilicata.it.conf

Per Shibboleth
shibboleth2.xml

Virtual Host.

Analizziamo come esempio l'applicazione collegata al dominio **sic.regione.basilicata.it.conf**

```
“
<VirtualHost 172.18.17.249:80>

    DocumentRoot "/var/www/html/sic.regione.basilicata.it"
    ServerName sic.regione.basilicata.it
    ServerAlias sic.regione.basilicata.it

    ErrorLog logs/sic.regione.basilicata.it_error_log
    TransferLog logs/sic.regione.basilicata.it_access_log
    LogLevel warn


    ProxyRequests Off
    ProxyTimeout 3600
    ProxyPreserveHost On
    ProxyVia On
“
```

Questa sezione è standard Apache.
Quella che segue è la parte relativa ad un proxypass utilizzando shibboleth integrato con spid.

```
    ########S_P_I_D##########
    <Location /giunta>
    “
        AuthType shibboleth
        ShibRequestSetting applicationId sic.regione.basilicata.it-giunta
        ShibRequestSetting requireSession 1
        ShibUseHeaders On
        require valid-user
    ”
```

Le clausole evidenziate sono obbligatorie se si usa shibboleth.
In particolare **ShibRequestSetting applicationId** deve contenere il giusto riferimento al file shibboleth2.xml presente sotto la cartella /etc/shibboleth
Come evidenziato da Maurizio Colucci, è buona norma che **l'applicationId** faccia riferimento al path della location. (sic.regione…..-giunta)
infine chiudere con la chiamata standard del proxypass.

```
        ProxyPass http://172.18.17.153:7777/giunta
    </Location>
```

Questa logica va ripetuta su tutte le location desiderate .

```
    <Location /spid>
        AuthType shibboleth
        ShibRequestSetting applicationId sic.regione.basilicata.it-spid
        ShibRequestSetting requireSession 1
        ShibUseHeaders On
        require valid-user
        ProxyPass http://172.18.17.153:7777/spid
    </Location>
```

Se un path non rientra sotto spid non va indicato nulla.

```
    <Location /i>
        ProxyPass http://172.18.17.153:7777/i/
    </Location>
```

altro esempio

```
    <Location /sic2>
        AuthType shibboleth
```

```
        ShibRequestSetting applicationId sic.regione.basilicata.it-sic2
        ShibRequestSetting requireSession 1
        ShibUseHeaders On
        require valid-user

        ProxyPass http://localhost:8080/sic2
    </Location>
    ########################

</VirtualHost>
```

infine chiudere con il tag normale di apache per i virtual host.

Al termine delle modifiche bisogna riavviare i servizi Apache
/etc/init.d/httpd restart ed accertarsi che siano effettivamente partiti.

Dopo aver creato il file di configurazione per il VirtualHost con le chiamate shibboleth è obbligatorio intervenire sul file shibboleth2.xml

SHIBBOLETH2.XML

Vi sono sezioni che devono essere modificate o aggiunte per ogni path integrato con spid pubblicato nei file di VirtualHost

Da non modificare

“

```
<SPConfig xmlns="urn:mace:shibboleth:2.0:native:sp:config"
   xmlns:conf="urn:mace:shibboleth:2.0:native:sp:config"
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
   xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
   clockSkew="180">


   <RequestMapper type="Native">

     <RequestMap applicationId="default">
```

“

Sezione da aggiornare

Bisogna creare un tag HOST NAME per ogni virtual host pubblicato.

```
        <Host name="sic.regione.basilicata.it">
```

Bisogna creare un applicationId per ogni path pubblicato nel file di configurazione del virtualhost che richieda l’autenticazione shibboleth.

```
            <Path name="giunta" applicationId="sic.regione.basilicata.it-giunta" authType="shibboleth" requireSession="true"/>

            <Path name="spid" applicationId="sic.regione.basilicata.it-spid" authType="shibboleth" requireSession="true"/>

            <Path name="sic2" applicationId="sic.regione.basilicata.it-sic2" authType="shibboleth" requireSession="true"/>
          </Host>
```

Come indicato in precedenza, è buona regola indicare nel applicationId il dominio e il path sottoposto all’autenticazione (*Path = Giunta, ApplicationId=sic.regione.basilicata.it-giunta*)

Altro esempio.

```
          <Host name="vte.regione.basilicata.it" >
            <Path Name= “vte” applicationId="vte.regione.basilicata.it-vte" authType="shibboleth" requireSession="true"/>
            <Path Name= “portal” applicationId="vte.regione.basilicata.it-portal" authType="shibboleth" requireSession="true"/>
          </Host>

     </RequestMap>
   </RequestMapper>
```

Il valore associato al tag ApplicationDefaults entityID NON HA valore significativo nella ns. configurazione, quindi quello che è riportato non è legato esplicitamente all’url indicato. Maurizio mi dice semplicemente che non deve essere vuoto.

```
  <ApplicationDefaults entityID="https://sic.regione.basilicata.it/shibboleth"
                       REMOTE_USER="eppn persistent-id targeted-id">

      <Sessions lifetime="28800" timeout="3600" relayState="ss:mem"
              checkAddress="false" handlerSSL="false" cookieProps="http">

         <SSO entityID="https://spid.regione.basilicata.it/idp-discovery">
           SAML2 SAML1
         </SSO>

         <Logout>SAML2 Local</Logout>

         <Handler type="MetadataGenerator" Location="/Metadata" signing="false"/>
         <Handler type="Status" Location="/Status" acl="127.0.0.1 ::1"/>
```

```
    <Handler type="Session" Location="/Session" showAttributeValues="true"/>
    <Handler type="DiscoveryFeed" Location="/DiscoFeed"/>
</Sessions>

<Errors supportContact="root@localhost"
    helpLocation="/about.html"
    styleSheet="/shibboleth-sp/main.css"/>

<MetadataProvider type="XML" validate="true" file="metadata-discovery.xml"/>

<AttributeExtractor type="XML" validate="true" reloadChanges="false" path="attribute-map.xml"/>

<AttributeResolver type="Query" subjectMatch="true"/>

<AttributeFilter type="XML" validate="true" path="attribute-policy.xml"/>

<CredentialResolver type="File" key="sp-key.pem" certificate="sp-cert.pem"/>

<!--
<ApplicationOverride id="admin" entityID="https://admin.example.org/shibboleth"/>
→
```

La sezione ApplicationOverride va replicata per ogni path (location) del file virtual host.

```
<ApplicationOverride id="sic.regione.basilicata.it-giunta" entityID="https://sic.regione.basilicata.it/giunta/shibboleth">
```

Questa è una chiamata importante per il logout di shibolett.
Per la logout bisognerà richiamare un url così composto: **Dominio/ valore dell'handlerURL/logout**

```
<Sessions lifetime="28800" timeout="3600" relayState="ss:mem"
      checkAddress="false" handlerURL="/giunta/Shibboleth.sso" handlerSSL="false" cookieProps="http">

    <SSO entityID="https://spid.regione.basilicata.it/idp-discovery">
      SAML2 SAML1
    </SSO>

    <Logout>SAML2 Local</Logout>

    <Handler type="MetadataGenerator" Location="/Metadata" signing="false"/>
    <Handler type="Status" Location="/Status" acl="127.0.0.1 ::1"/>
    <Handler type="Session" Location="/Session" showAttributeValues="true"/>
    <Handler type="DiscoveryFeed" Location="/DiscoFeed"/>

</Sessions>

</ApplicationOverride>
```

Altro Esempio.

```
  <ApplicationOverride id="sic.regione.basilicata.it-sic2" entityID="https://sic.regione.basilicata.it/sic2/shibboleth">

<Sessions lifetime="28800" timeout="3600" relayState="ss:mem"
      checkAddress="false" handlerURL="/sic2/Shibboleth.sso" handlerSSL="false" cookieProps="http">

    <SSO entityID="https://spid.regione.basilicata.it/idp-discovery">
      SAML2 SAML1
    </SSO>

    <Logout>SAML2 Local</Logout>
    <Handler type="MetadataGenerator" Location="/Metadata" signing="false"/>
    <Handler type="Status" Location="/Status" acl="127.0.0.1 ::1"/>
    <Handler type="Session" Location="/Session" showAttributeValues="true"/>
    <Handler type="DiscoveryFeed" Location="/DiscoFeed"/>

</Sessions>

</ApplicationOverride>
```

```
    </ApplicationDefaults>

    <SecurityPolicyProvider type="XML" validate="true" path="security-policy.xml"/>
    <ProtocolProvider type="XML" validate="true" reloadChanges="false" path="protocols.xml"/>

</SPConfig>
```

Al termine riavviare i servizi Shibboleth
/etc/init.d/shibd restart
verificando l'avvenuto riavvio.

Infine bisognerà collegarsi all'url dominio/valore location sottoposto a shibboleth/Shibboleth.sso/Metadata.
Esempio: sic.regione.basilicata.it/giunta/Shibboleth.sso/Metadata

Questo scaricherà un file Metadata che dovremo inviare a COLUCCI / PUBLISYS per la pubblicazione su SPID/IMS

Nel metadata sotto riportato sono incluse **tutte** le combinazioni certificati/root. Si noti che il valore di *entityID* deve corrispondere all'*entityId* nella rispettiva stanza *SessionInitiator* entro *ApplicationDefaults* (ovvero *ApplicationOverride* se sono censite più applicazioni) del file *shibboleth2.xml*.

https://spid.regione.basilicata.it/metadata/idp/idp-metadata.xml

Mappatura degli attributi utente

Il server Shibboleth SP è in grado di ricevere i messaggi SAML prodotti dall'infrastruttura di autenticazione o Identity Provider utilizzato e di estrarre da essi gli attributi relativi agli utenti autenticati. Tali attributi vengono quindi inseriti in altrettanti header HTTP, per consentire al Service Provider di accedervi ed utilizzarli.
Per definire le corrispondenze tra gli attributi presenti nei messaggi SAML e gli header HTTP prodotti, è necessario intervenire sul file "*/etc/shibboleth/attribute-map.xml*", oggetto di questa sezione. In tale file sono definite una serie di regole di mappatura come la seguente [14]:

```
<Attribute name="NOME_ATTRIBUTO_SAML" id="NOME_HEADER_HTTP" nameFormat="SAML_ATTRIBUTE_NAME_FORMAT">
        <AttributeDecoder xsi:type="StringAttributeDecoder"/>
</Attribute>
```

https://spid.regione.basilicata.it/metadata/idp/attribute-map.xml