Autenticazione SAML su Office365

Francesco Malvezzi

Università di Modena e Reggio nell'Emilia

14 maggio 2015

Office365

- Cloud di Microsoft;
- rende disponibili vari servizi (mail, spazio disco, strumenti di office automation via cloud);
- gli utenti sono in un “active directory” cloud che si chiama “Azure”;
- ha alcune funzionalità SAML2.

Questo scalfisce solo la superficie.

Office365

- Cloud di Microsoft;
- rende disponibili vari servizi (mail, spazio disco, strumenti di office automation via cloud);
- gli utenti sono in un “active directory” cloud che si chiama “Azure”;
- ha alcune funzionalità SAML2.

Questo scalfisce solo la superficie.

Obiettivo

Permettere agli utenti dell'organizzazione di accedere a Office365 con le proprie credenziali:
`https://portal.microsoftonline.com`

Dimostrare la proprità del dominio DNS

- Registrare un dominio di fantasia nella gerarchia `microsoftonline.com`, ad esempio: `idem2015.microsoftonline.com`.
- Associare il vostro nome dominio: Microsoft vi porrà una sfida: un record TXT da aggiungere al vostro DNS.

Creare un utente sul cloud

Anche se l'autenticazione sarà effettuata dal sistema Single Sign On locale [1], gli utenti devono esistere sul cloud, ad esempio con

- il tool Forefront Identity Manager;
- o con chiamate powershell (ad es. `New-MsolUser`).

[1] Microsoft ama il termine "on premise"

Preparare Office365 alla federazione

Per istruire Office365 che deve fare parte di una federazione esiste un comando powershell preciso: `Set-MsolDomainAuthentication`.
I suoi parametri sono:

- nome,
- entityId,
- url del servizio SAML2 POST SSO;
- url di logout,
- chiave pubblica (formato pem);

cioè in pratica i metadati.

Configurazioni di Shibboleth-IdP

A questo punto lo Shibboleth-IdP deve essere pronto a dialogare con Office365:

- aggiungere una sezione apposta al `relying-party.xml`;
- scaricare i metadati da `https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml`.

Nel relying-party.xml:

```
<bean parent="RelyingPartyByName" \
  c:relyingPartyIds="urn:federation:MicrosoftOnline">
  <property name="profileConfigurations">
    <list>
      <bean parent="SAML2.SSO" \
p:encryptAssertions="false"
p:nameIDFormatPrecedence=\
"urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
p:signAssertions="conditional"
p:encryptNameIDs="never" />
    </list>
  </property>
</bean>
```

Rilascio degli attributi

Office365 si aspetta che Shibboleth rilasci:

- `immutableID`: in AD è il guid utente encoded base64, ma è sufficiente che sia un attributo unico (come lo uid) nel formato nameid;
- `UserId`: equivalente allo `eppn`. Personalmente l'ho ricostruito con uno scriptedAttributeDefinition per evitare di usare `eppn` che è un attributo scoped.

Grazie

Grazie per l'attenzione e la pazienza.