Séminaire EOLE
Dijon
20-21 Octobre 2009

Eole SSO

Sommaire

- Présentation du projet
- Fonction de fédération
- Mise en œuvre
- Exemple d'utilisation
- Informations utiles

Présentation du projet

- Motivations
  - Single Sign On : saisie de mot de passe unique.
  - Fédérer l'authentification d'un ensemble d'applications.
  - Maîtrise du produit pour son adaptation en fonction des besoins et de l'évolution du système d'information.
- Fonctionnalités
  - Support de plusieurs protocoles pour faciliter l'intégration des applications (CAS / SAML / OpenID).
  - Fonctions de contrôle des attributs transmis
  - Possibilité de fédération avec d'autres produits grâce au protocole SAML

Fonction de fédération

- Intérêt
  - Déléguer l'authentification de l'utilisateur à son établissement d'origine
  - Propager des informations sur l'utilisateur en choisissant les attributs envoyés au fournisseur de service
- Fonctionnement
  - Utilisation du protocole SAML version 2 pour propager les informations (protocole utilisé par de nombreux autres produits).
  - Gestion du mode fournisseur d'identité et fournisseur de services

Mise en œuvre

- Établissement d'un lien de confiance
  - Échange de fichiers de méta-données entre les 2 entités
  - Les méta-données du service Eole-SSO sont disponibles sur l'url : https://adresse_serveur:8443/saml/metadata
  - Placer les méta-données de l'entité partenaire dans /usr/share/sso/metadata (la prise en compte nécessite un redémarrage du service)

Mise en œuvre

- Mise en place du contrôle d'attributs (fournisseur d'identité)
  - Création d'un fichier d'association de filtre dans /usr/share/sso/app_filters/local_apps.ini

```
[saml_seshat_mon_acad]
port=8443
baseurl=/saml/acs
scheme=https
addr=serveur_seshat.ac-mon_acad.fr
typeaddr=dns
filter=federation
```

  - Création d'un fichier de filtre d'attributs (federation.ini)

```
[utilisateur]
uid=uid
rne=rne
```

Mise en œuvre

- Définition de jeu d'attributs de fédération (fournisseur de services)
  - Des jeux de correspondance d'attributs peuvent être définis pour chaque fournisseur d'identité.

```
[urn:fi:ac-dijon:et-collège TestEole:1.0]
codeRne=rne
cn=cn
```

- Configuration des attributs requis (fournisseur de services)

```
<AttributeConsumingService index="1" isDefault="true">
  <ServiceName xml:lang="en-us">EoleSSO Attribute Set</ServiceName>
  <ServiceDescription xml:lang="en-us">Liste des attributs pour "EoleSSO"</ServiceDescription>
  <RequestedAttribute FriendlyName="Identifiant établissement" Name="coderne"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/>
  <RequestedAttribute FriendlyName="Identifiant utilisateur local" Name="uid"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true"/>
  <RequestedAttribute FriendlyName="Code civilité" Name="codecivilite"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="false"/>
</AttributeConsumingService>
```

Exemple d'utilisation

- Fédération entre 2 serveurs Eole-SSO et FIM
  - Fournisseur d'identité : Scribe 1 (établissement) hébergeant un portail web.
  - Fournisseur de services/d'identité : Scribe 2 (académique)
  - Fournisseur de services : Serveur FIM académique
  - Des liens de fédération sont configurés entre les serveurs Scribe 1 et Scribe 2, ainsi qu'entre Scribe 2 et FIM.
  - Un utilisateur connecté sur Scribe 1 et étant reconnu dans le référentiel des serveurs Scribe 2 et FIM peut accéder à des ressources protégées par FIM (portail ARENB).

Informations utiles

- Page wiki Eole SSO : http:/eole.orion.education.fr/wiki/index.php/EoleSSO
- Page sur l'expérimentation SSO/FIM : http:/eole.orion.education.fr/wiki/index.php/EoleSSOFim
- Le projet CAS : http://www.ja-sig.org/products/cas/
- Oasis / Spécifications SAML : http://www.oasis-open.org/specs/index.php#saml
- OpenID : http://openid.net http://www.openidfrance.fr

Merci de votre attention