

Paramétrer connexion à serveur de qualification Scenari

Table des matières

Introduction	3
1. Formulaire service provider et modifications shibboleth	4
1.1. Remplir le formulaire de Service Provider	4
1.2. Modifications à apporter à ID Shibboleth établissement	5
2. Tester l'accès au serveur de qualification	8

Introduction

Pour que les fournisseurs d'identités et le service scenari puissent interagir ensemble, il faut qu'ils aient une connaissance mutuelle réciproque, dite relation de confiance.

Cette connaissance se base sur des fichiers de métadonnées.

Nous allons dans cette partie établir une telle relation entre notre IdP Shibboleth et le service scenari de kelis, en leur faisant chacun charger les métadonnées de l'autre: on parle de **relation bilatérale directe**.



A noter...

Que dans un premier temps, on travaille sur un serveur dit de « qualification » pour tester toutes les opérations de paramétrage.

Une fois toutes les procédures validées, on passera sur un serveur de production où il suffira de répéter ces procédures.

1. Formulaire service provider et modifications shibboleth

1.1. Remplir le formulaire de Service Provider

Les informations obligatoires du formulaire

1. PRÉSENTATION

NOM (français et anglais)

Scenari

URL du service

<https://groupeinsa.scenari.eu/~static/fr-FR/home.xhtml#>

Catégorisation

service à portée nationale

2. RESPONSABLES et CONTACTS

informations sur responsable INSA

Langue = français

responsable = mel.responsable@insa-ville.fr

organisme = INSA Ville

mails des contacts technique et mail contact sécurité

3. FEDERATIONS

Fédération de test

Oui

Fédération éducation recherche

non (impossible)

EduGain

non (impossible)

Fédération de qualification

non (impossible)

4. ATTRIBUTS

Liste des attributs

1. "mail"
2. "uid"
3. "displayName"
4. "surname"
5. "givenName"
6. "schacHomeOrganization"
7. "eduPersonPrimaryAffiliation"

5. INFORMATIONS TECHNIQUES

URL métadonnées

<https://groupeinsa-qua.scenari.ovh/chain/public/u/saml/GetManifest>

Entity ID

<https://groupeinsa-qua.scenari.ovh/chain>

point d'accès SAML

(chargé automatiquement)

Certificat X509 SAML

(chargé automatiquement)

Certificat de chiffrement

Uploader le fichier certificat_chiffrement_kelis.crt (cf. certificat_chiffrement_kelis) récupéré en étape 1 (archive à dézipper)

1.2. Modifications à apporter à ID Shibboleth établissement

Modifications IDP shibboleth INSA Rouen Normandie

Basée sur les modifications apportées à IDP shibboleth de l'INSA de Rouen Normandie pour configurer une relation de confiance avec le serveur scenari de qualification de Kelis

1. Fichier idp.properties

Section à intégrer au fichier /opt/shibboleth-idp/conf/metadata-providers.xml

```
<MetadataProvider id="KELIS"
    xsi:type="FileBackedHTTPMetadataProvider"
    metadataURL="https://groupeinsa-qua.scenari.ovh/chain/public/u/saml/GetManifest"
    backingFile="/opt/shibboleth-idp/metadata/kelis-metadata.xml">
</MetadataProvider>
```

Ligne à décommenter

Ligne idp.encryption.optional = true décommentée

Ceci a été désactivé pour le test. Il faut faire un retour à Kelis pour qu'ils signent leur métadonnées (Manifest)



Remarque

Ici le fichier kelis-metadata.xml est la copie en locale du fichier de métadonnées "Manifest".

2. Fichier saml-nameid.xml

Dé-commenter la section suivante

```
<!-- Uncommenting this bean requires configuration in saml-nameid.properties. -->
<ref bean="shibboleth.SAML2PersistentGenerator" /> <bean
parent="shibboleth.SAML2AttributeSourcedGenerator" p:omitQualifiers="true"
p:format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress" p:attributeSourceIds="#{
{'mail'}}" />
```



vision en mode code

```
<!-- Uncommenting this bean requires configuration in saml-
nameid.properties. -->
<ref bean="shibboleth.SAML2PersistentGenerator" />
<bean parent="shibboleth.SAML2AttributeSourcedGenerator"
p:omitQualifiers="true"
p:format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
p:attributeSourceIds="#{ {'mail'}}" />
```

3. Fichier attribute-filter.xml

Ajouter les informations suivantes

```
<!-- ScenariKelis -->
<AttributeFilterPolicy id="https://groupeinsa-qua[https://groupeinsa-qua/]scenari.ovh/chain">
<PolicyRequirementRule xsi:type="Requester" value="https://groupeinsa-qua[https://groupeinsa-qua/]scenari.ovh/chain" /> <AttributeRule attributeID="mail"> <PermitValueRule xsi:type="ANY" />
</AttributeRule> <AttributeRule attributeID="uid"> <PermitValueRule xsi:type="ANY" />
</AttributeRule> <AttributeRule attributeID="displayName"> <PermitValueRule xsi:type="ANY" />
</AttributeRule> <AttributeRule attributeID="surname"> <PermitValueRule xsi:type="ANY" />
</AttributeRule> <AttributeRule attributeID="givenName"> <PermitValueRule xsi:type="ANY" />
</AttributeRule> <AttributeRule attributeID="schacHomeOrganization"> <PermitValueRule
xsi:type="ANY" /> </AttributeRule> <AttributeRule attributeID="eduPersonPrimaryAffiliation">
<PermitValueRule xsi:type="ANY" /> </AttributeRule> </AttributeFilterPolicy>
```



vision en mode code

```

<!-- ScenariKells -->
<AttributeFilterPolicy id="https://groupeinsa-qua.scenari.ovh/chain">
  <PolicyRequirementRule xsi:type="Requester" value="https://groupeinsa-
qua.scenari.ovh/chain" />
  <AttributeRule attributeID="mail">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
  <AttributeRule attributeID="uid">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
  <AttributeRule attributeID="displayName">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
  <AttributeRule attributeID="surName">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
  <AttributeRule attributeID="givenName">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
  <AttributeRule attributeID="schacHomeOrganization">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
  <AttributeRule attributeID="eduPersonPrimaryAffiliation">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
</AttributeFilterPolicy>

```

4. A titre d'exemple, télécharger les IDP Shibboleth Rouen et Strasbourg configurés

Rouen

<https://shibboleth.insa-rouen.fr/idp/shibboleth>

Strasbourg

<https://ssotest.insa-strasbourg.fr/idp/shibboleth>

2. Tester l'accès au serveur de qualification

Transfert information à Kelis et tests

L'objectif final est de vérifier que la connexion au serveur scenari (de qualification) fonctionne via les identifiants de connexion de l'établissement/ Pour ce faire, il va falloir renseigner et envoyer l'URL des métadonnées de l'établissement et créer/envoyer un compte test pour que Kelis puisse vérifier le bon fonctionnement de la connexion.

1. Transfert url des metadonnées de l'INSA ville x

Récupérer et transmettre à url des metadonnées de l'INSA ville x à nadir.kesraoui@insa-rouen.fr et lefleuri@insa-toulouse.fr qui transmettront à Kelis (et gèrent la coordination avec Kelis).



URL métadonnées INSA Rouen

<https://shibboleth.insa-rouen.fr/idp/shibboleth>

2. Création d'un compte test

Créer un compte test dont l'identifiant est une adresse mail, afin d'éviter d'éventuels problèmes homonymie complète de prénom / nom entre 2 établissements différents (cas de figure rencontré lors des tests Rouen/Strasbourg)



Truc & astuce

Utiliser le mail plutôt que Prénom Nom (le DisplayName de l'annuaire INSA).



Remarque

Seul impact pour l'utilisateur : il voit son pseudo affiché dans l'interface donc son mail.

3. Envoi compte test pour test par Kelis

Afin de finaliser/valider la procédure de connexion pour l'établissement, l'éditeur Kelis va tester de son côté l'accès via le compte test créé.

Envoyer les identifiants et MDP à nadir.kesraoui@insa-rouen.fr et lefleuri@insa-toulouse.fr qui transmettront à Kelis (et gèrent la coordination avec Kelis).

4. Validation de la procédure

nadir.kesraoui@insa-rouen.fr et lefleuri@insa-toulouse.fr font part des retours sur les tests de connexion, avec soit modifications éventuelles à apporter ou validation.