La Fédération d'identité Education Recherche

Sans peine

emmanuel.courcelle@inp-toulouse.fr

Le mésocentre CALMIP

Une **Unité Mixte** de Service (UMS 3667)

Au service de la communauté E.S.R.
de la **région Occitanie**

Ses atouts :

- Proximité
- Production (stabilité et performance)
- Multi-thématique

Attribution des ressources

Pas de comptes ouverts au fil de l'eau

Les comptes sont attribués :

- Par un **comité d'experts** des différentes thématiques scientifiques
- Au cours de deux **sessions annuelles :**
  - La session A à l'automne
  - La session B au printemps

Gestion des **R**essources et **A**ttributions pour les **M**ésocentres de **C**alcul

On demande plusieurs types d'informations :

- Description du projet **scientifique**
- Description **technique** du code utilisé
- Liste de **collaborateurs**
- Demandes de **formation**

Tout se passe en ligne :

- **Demandes** de ressources
- **Répartition** des dossiers entre experts
- **Expertise** des demandes

Pourquoi utiliser la F.E.R. ?

Pas d'authentification jusqu'à la fin 2015 !

- Besoin de **confidentialité**
- Nécessité de prévoir **plusieurs rôles** :
  - Demandeur
  - Expert
  - Président du Comité (répartit des dossiers entre experts)
  - Administrateur de l'application
- Utilisateurs = Chercheurs ou Ingénieurs de l'ESR

Périmètre inclus dans celui de la F.E.R.

La Fédération d'Identités Enseignement Recherche

Un cadre de confiance :

- Mise en commun des **informations d'identité** provenant de administrations des établissements
- Les établissements signent une charte

Un cadre technique :

- **Normalisation** qui repose sur http(s)
  - **SAML** : Security Assertion Markup Language
- Une **application** largement utilisée : **shibboleth**
- Des **services** d'authentification
-  Ne fonctionne que pour les applications Web !

Plusieurs fédérations

Fédération de **Tests**

- Opérée par Renater, utile en période de dev

Fédération de **Production**

- Opérée par Renater

Fédération Internationale **EduGAIN**

- Opérée par Terena

IDP et SP

IDP = Identity Provider

- Fournisseur d'identités
- Maintient et fournit l'identité des utilisateurs
- Vérifie l'authentification de la personne

SP = Service Provider

- Fournit un service ayant besoin d'authentification
- Utilise les IdP de la fédération pour authentifier ses utilisateurs

Les attributs

On peut demander les attributs dont on a besoin

- Adresse mail, nom, prénom, etc.

La demande se fait sur le guichet Renater

-  Elle doit être justifiée

Aussi dans les fichiers de configuration

L'attribut par défaut : **eppn**

- **`eduPersonPrincipalName`**

`Prenom.nom@cnrs.fr`

Les comptes CRU, un IDP particulier

Permet d'ouvrir des comptes de manière automatique

- Utile en cas de problème
- Utile pour authentifier des personnes non ESR

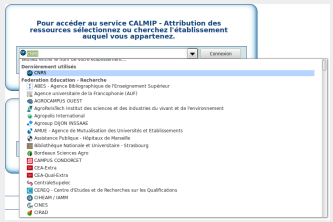
La confiance n'est plus là !

→ Les comptes CRU sont **par défaut** dans la fédération de tests

→ **On doit les demander** explicitement dans la fédération de production

Le processus d'authentification

Avec le wayf standard



wayf

Idp cnrs

SP calmip

`login.php`
Non authentifié

`login.php`
authentifié
`REMOTE_USER`

Idp inpt

Idp crous

Idp ...

Session php

Les choix fondamentaux

Identifier par **`eppn`**

-  Qui connaît son eppn ?

Accepter et encadrer les **comptes CRU**

-  Utile en cas de problème sur un IdP
-  Permet de gérer les cas « compliqués »
-  Signaler aux admins un nouvel utilisateur CRU

Ouverture de comptes **automatique**

Faire un **`wayf`** « maison »

En pratique...

Prérequis : Deux serveurs (**test, prod)** avec apache en https

Installer Shibboleth (**`apt-get`**)

Configurer Shibboleth (entityId, attributs, metadonnées, CRU)

```
<ApplicationDefaults entityID="https://monsite.fr"
 REMOTE_USER="eppn ...">
```

Configurer Apache :

```
<Location "/role/public/login.php">
    AuthType shibboleth
    ShibRequestSetting requireSession 1
    ShibRequestSetting applicationId default
    Require shibboleth
</Location>
```

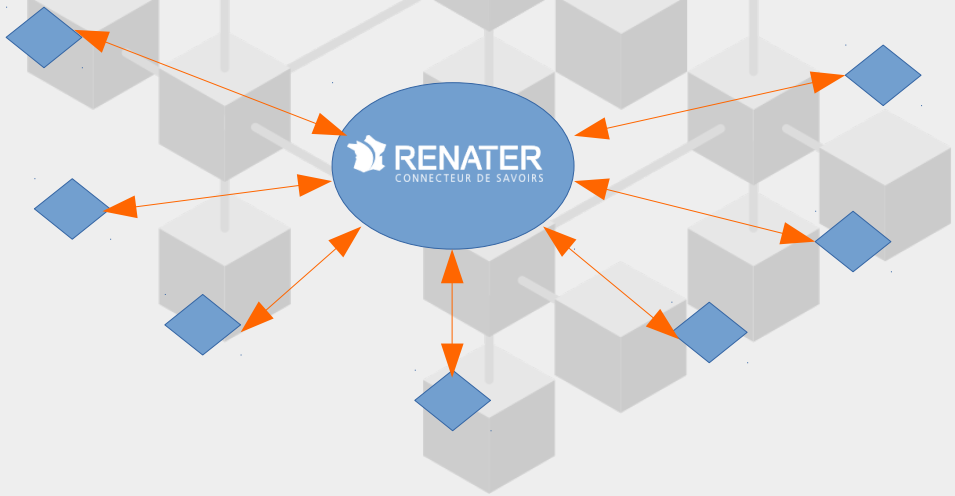
En pratique...

Établir le dialogue avec renater pour échanger les métadonnées

- Générer un certificat autosigné
- Vérifier que ça marche :
  `https : //monsite.fr/Shibboleth.sso/Metadata`
- Télécharger le certificat de renater
- Télécharger le fichier de métadonnées de la Fédération

Le fichier de métadonnées de la fédération est quotidiennement téléchargé par Schibboleth

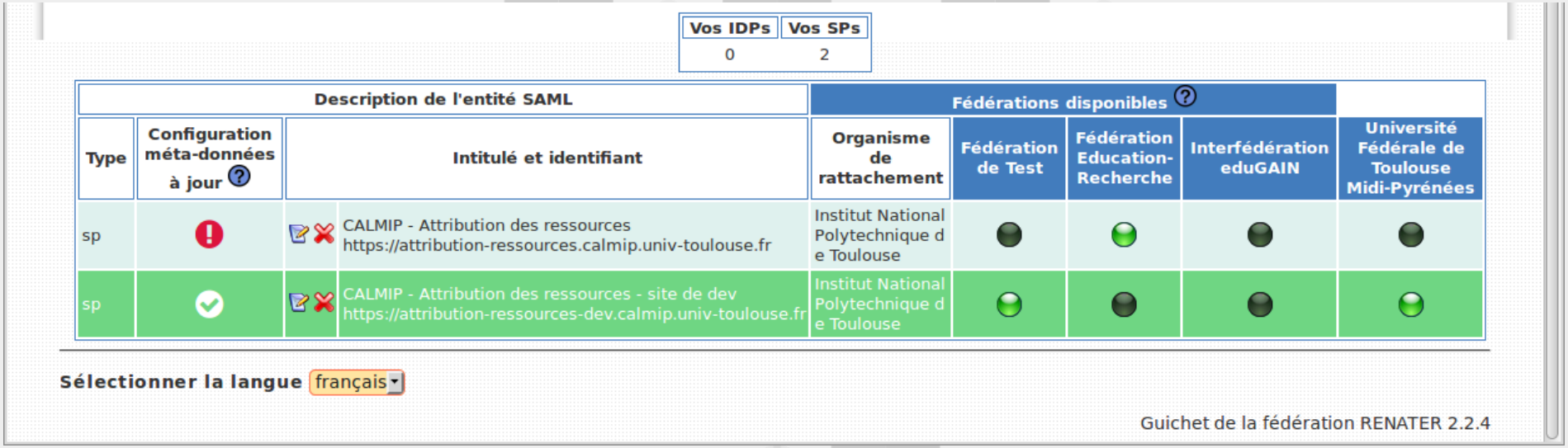
IDP ou SP



En pratique...

Enregistrer ses SP sur le guichet de Renater :
`https://federation.renater.fr/registry`

Il faut être connecté en utilisant… la F.E.R



Vos IDPs	Vos SPs
0	2

Description de l'entité SAML				Fédérations disponibles			
Type	Configuration méta-données à jour	Intitulé et identifiant	Organisme de rattachement	Fédération de Test	Fédération Education-Recherche	Interfédération eduGAIN	Université Fédérale de Toulouse Midi-Pyrénées
sp	!	CALMIP - Attribution des ressources https://attribution-ressources.calmip.univ-toulouse.fr	Institut National Polytechnique de Toulouse	●	●	●	●
sp	✓	CALMIP - Attribution des ressources - site de dev https://attribution-ressources-dev.calmip.univ-toulouse.fr	Institut National Polytechnique de Toulouse	●	●	●	●

Sélectionner la langue français

Guichet de la fédération RENATER 2.2.4

Le guichet Renater

Permet d'enregistrer son SP sur une fédération :

Fédération de test

- On commence par là !
-  Très peu d'IdP fonctionnent !
-  On clique et on est intégré

Fédération de **Production**

-  La tutelle doit valider

Fédération **EduGain** (Internationale)

… et c’est tout !

Pour essayer, mettre dans login.php :

```
<?php
echo "<pre>"; print_r($_SERVER); echo "</pre>";
```

Aller à l’URL:

https://monsite.fr/login.php

La réponse :

```
[eppn] => xxxxx@sac.cru.fr
[mail] => emmanuel.courcelle@yyyy.fr
…
[REMOTE_USER] => xxxxx@sac.cru.fr
```

Les choix importants

Identifier par **`eppn`**

-  Qui connaît son eppn ?

Accepter et encadrer les **comptes CRU**

-  Utile en cas de problème sur un IdP
-  Permet de gérer les cas « compliqués »
-  Signaler aux admins un nouvel utilisateur CRU

Ouverture de comptes **automatique**

Faire un **`wayf`** « maison »

Le workflow complet

Création de compte automatique

```
Cliquer sur Connexion → redirection sur votre IdP
$eppn = $_SERVER['REMOTE_USER']
if ($eppn est dans la base)
then
  Imprimer Bienvenue
else
  Formulaire d'entrée de mail → $mail
  if ($mail est dans la base)
  then
    Associer $eppn au compte correspondant
    Imprimer Bienvenue
  else
    Créer un compte
    Associer $mail et $eppn à ce compte
    Imprimer Bienvenue
  endif
  if ($eppn est un CRU)
    Envoyer une notification à admin
  endif
endif
```

Un utilisateur peut avoir plusieurs eppn !

Les choix importants

Identifier par **`eppn`**

-  Qui connaît son eppn ?

Accepter et encadrer les **comptes CRU**

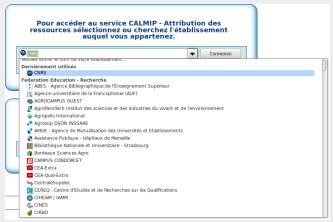
-  Utile en cas de problème sur un IdP
-  Permet de gérer les cas « compliqués »
-  Signaler aux admins un nouvel utilisateur CRU

Ouverture de comptes **automatique**

Faire un **`wayf`** « maison »

Le processus d'authentification

Avec le wayf « maison »



wayf

ldp cnrs

SP calmip

`wayf.php`
Non authentifié

`login.php`
authentifié
`REMOTE_USER`

Idp inpt

Idp crous

Idp ...

Session php

Trouver l'URL des IDP

Sélectionner l'IDP à partir du wayf standard

Lire l'**`acces.log`** d'apache :

x.x.x.x - - [...] `GET /Shibboleth.sso/Login?target=https://monappliweb.fr/login.php&`**`providerId=https://shibboleth.xxx.fr/idp/shibboleth`**

...ou lire le fichier de metadata

Conclusion...

La F.E.R., mais **c'est très simple ...**

- Renater organise des formations
- Votre DSI peut vous aider
- Vous pouvez me contacter

… ça marche très bien

… et merci à l'INPT pour ses machines virtuelles très efficaces !