



www.cnrs.fr

RETOUR D'EXPERIENCE : SHIBBOLISER DES APPLICATIONS

Roland Dirlwanger
CNRS – Délégation Aquitaine-Limousin



P. 2

SOMMAIRE

- | Les prérequis

- | Adapter une application existante :
 - | Cas d'une application locale : CNRS-Hebdo
 - | Cas d'une application open-source : OTRS

- | Conclusion

- | Quelques liens utiles



www.cnrs.fr

RETOUR D'EXPERIENCE : SHIBBOLISER DES APPLICATIONS

Roland Dirlewanger
CNRS – Délégation Aquitaine-Limousin

Les prérequis ...



P. 4

Les prérequis

- | S'assurer que l'établissement dispose d'un Identity Provider (IdP)
- | Vérifier que la gestion de comptes de l'application est compatible avec les attributs de l'IdP :
 - | Exemple : l'IdP renvoie des uid ? Des adresses méls ?
- | Configurer SSL dans Apache
 - | Obtenir un certificat de serveur émis par une autorité de certification reconnue par les clients de l'application (CNRS, TCS)
- | Mettre en place un Service Provider (SP)



P. 5

Mettre en place un Service Provider

- | Une documentation très bien faite !
 - | <https://federation.renater.fr/docs/installation>
 - | Cliquer sur « Support ... de la formation Shibbolisation d'application »

- | Les grandes lignes, sur Linux
 - | Installation des 5 RPMS disponibles sur le site de Internet2
 - | Obtention des certificats
 - | Configuration Apache et Shibboleth
 - | Test dans le cadre de fédération Éducation-Recherche de test
 - | Déclaration dans la fédération Éducation-Recherche

- | Compter une bonne journée !
 - | ... si tout ce passe bien



P. 6

Mettre en place un Service Provider

- | Ce qui peut vous faire perdre du temps :
 - | « Zapper » un élément de la doc !
 - | Il n'y a pas les RPMs pour votre distribution sur le site de Internet2
 - OK pour CentOS 5, RHEL 4 et 5, SLE 10 et 11, openSuse
 - Pas pour Fedora
- | Recompiler les RPMs en Fedora 10
 - | Les RPMS se recompilent facilement mais xmltooling a besoin d'être adapté (me contacter pour plus d'infos)
 - Il appelle la libcurl avec des paramètres de chiffrement spécifiques à OpenSSL alors que libcurl s'appuie sur NSS3.
 - Message d'erreur :

```
(59) Unknown cipher in list: ALL:!aNULL:!LOW:!EXPORT:!SSLv2
```



www.cnrs.fr

RETOUR D'EXPERIENCE : SHIBBOLISER DES APPLICATIONS

Roland Dirlewanger
CNRS – Délégation Aquitaine-Limousin

Adapter une application locale ...



P. 8

Adapter une application locale : CNRS-Hebdo

- | L'application est CNRS-Hebdo (Linux, Apache, Postgres, PHP)
 - | Lettre hebdomadaire du CNRS avec une édition par Délégation
 - Permet de mutualiser les actualités de niveau national, régional ou local
 - Génère la lettre et l'envoi à tous les personnels de la DR (CNRS ou non CNRS, permanents ou non permanents)
 - Utilisateurs = services communication des DR
 - | Hébergée par les délégations elles-mêmes ou à la DR Aquitaine-Limousin
- | Authentification
 - | Auparavant : authentification par certificat
 - | Objectif : authentification via Janus (IdP du CNRS)



P. 9

Adapter une application locale : CNRS-Hebdo

| Le contexte :

| Éléments favorables :

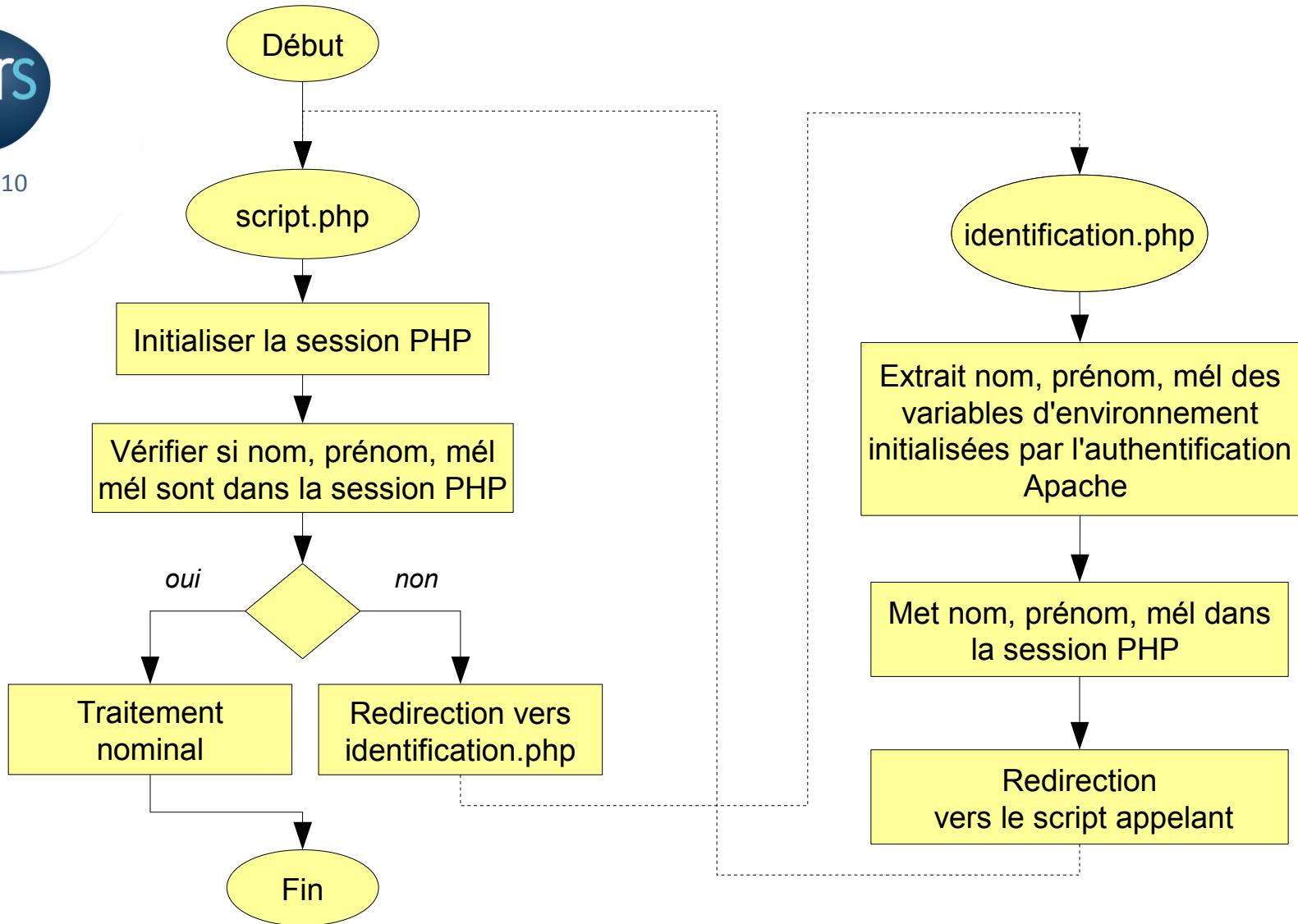
- C'est l'auteur de l'application qui effectue la shibbolisation
- C'est le serveur Apache qui est en charge de l'authentification :
 - dispose de la liste des utilisateurs autorisés
 - donne accès ou pas à l'application selon le certificat de l'utilisateur
 - passe les attributs nom, prénom, adresse mél issus du certificat

| Éléments défavorables :

- Fedora 10 donc pas de RPMs pour Shibboleth
- Première installation sur le site



L'authentification dans CNRS-Hebdo





Passer d'une authentification par certificat à shibboleth Les modifications dans la configuration d'Apache

| Authentification par certificat

conf.d/ssl.conf contient :

```
<Location "/Hebdo/identification.php">
  SSLVerifyClient optional
  SSLOptions      +FakebasicAuth
  AuthType        Basic
  AuthName        "CNRS-Hebdo"
  AuthUserFile    conf/passwd_ssl
  require         valid-user
</Location>
```

conf/passwd_ssl contient :

La liste des DN des certificats des
utilisateurs autorisés

```
/C=FR/.../emailAddress=user1@domain1.fr
/C=FR/.../emailAddress=user2@domaine2.fr
/C=FR/.../emailAddress=user3@domaine3.fr
```

| Authentification Shibboleth

La directive <Location> est transférée
dans conf.d/shib.conf

conf.d/shib.conf contient :

La liste des adresses méls des utilisateurs
autorisés

```
<Location /Hebdo/identification.php>
  AuthType shibboleth
  ShibRequestSetting requireSession 1
  require user user1@domain1.fr
  require user user2@domaine2.fr
  require user user3@domaine2.fr
</Location>
```



P. 12

Passer d'une authentification par certificat à shibboleth Les modifications dans le code de l'application

- | Seul le script identification.php est impacté

- | Les modifs consistent à :
 - | Détecter si on est dans une authentification par certificat ou par Shibboleth
 - Dans le premier cas : conserver le code qui initialise les noms, prénoms et l'adresse mél à partir des variables `SSL_S_CLIENT_S_DN_*`
 - Dans le second cas : initialiser les noms, prénoms à partir des variables `cn`, `givenName`, `mail`

- | Durée de l'opération : 5 minutes !



www.cnrs.fr

RETOUR D'EXPERIENCE : SHIBBOLISER DES APPLICATIONS

Roland Dirlewanger
CNRS – Délégation Aquitaine-Limousin

Adapter une application tierce ...



P. 14

Adapter une application tierce : OTRS

- | L'application est OTRS (Linux, Apache,MySQL, Perl)
 - | Système de gestion d'incidents : www.otrs.org
 - | Déployé dans la plupart des délégations du CNRS à l'initiative de la Délégation Rhône-Auvergne (DR7, Lyon) pour le suivi des contrats de service
 - | La DR de Lyon propose un ensemble de modifications pour une authentification par certificat et création automatiques de comptes



P. 15

Adapter une application tierce : OTRS

| Le contexte :

| Éléments favorables :

- Deuxième SP installé sur le site
- RPMs de Shibboleth disponibles (CentOS4)
- Possibilité de capitaliser sur les adaptations de Lyon pour les certificats

| Éléments défavorables :

- Application inconnue par la personne qui effectue shibbolisation
- Culture Perl un peu ancienne



P. 16

Adapter une application locale : OTRS Installation et configuration de Shibboleth

- | Grandement facilitée par le fait que c'est le deuxième SP !

- | Les étapes :
 - | Demande du certificat TCS pour le nouvel SP
 - | Installation de shibboleth via les RPMs disponibles
 - | Recopie et adaptation de la configuration du premier SP
 - | Déclaration auprès de la fédération d'identité

- | Coût total : une à deux heures



P. 17

Adapter une application locale : OTRS Configuration de Shibboleth

- | /etc/shibboleth2

- | Adaptation de la configuration d'un SP existant

- | /etc/httpd/conf.d/shib.conf :

- | Configure l'authentification Shibboleth pour le répertoire qui contient les deux interfaces utilisateurs :

```
<Location /otrs/>  
    AuthType shibboleth  
    ShibRequestSetting requireSession 1  
    require valid-user  
</Location>
```



Adapter une application locale : OTRS Adaptation du code de OTRS

- | En fait, OTRS permet de définir ses propres « backends » d'authentification
 - | Sont des modules Perl
 - Un module pour l'authentification des « clients », un pour les « agents »
 - Définissent trois méthodes : `new`, `GetOptions` et `Auth`
 - | Se déclarent et se paramètrent dans `Kernel/Config.pm` via les variables de configuration :
 - `$Self->{'AuthModule'}` pour l'authentification des agents
 - `$Self->{'Customer::AuthModule'}` pour celle des clients
 - `$Self->{'AuthModule::NomDuModule::paramètre'}` pour les paramètres



Adapter une application locale : OTRS Adaptation du code de OTRS

| Écriture du module d'authentification Shibboleth.pm

| Les méthodes sont simples à implémenter

- GetOption et new sont sur le même modèle dans tous les backends
- Auth renvoie l'identifiant de l'utilisateur ou null

| Rajout de la création automatique de compte configurable via le paramètre

```
AuthModule::Shibboleth::AutoCreateCustomerAccount
```

| Configuration d'OTRS dans Config/Kernel.pm :

```
$Self->{'AuthModule'} = 'Kernel::System::Auth::Shibboleth';  
$Self->{'Customer::AuthModule'} = 'Kernel::System::Auth::Shibboleth';  
$Self->{'AuthModule::Shibboleth::AutoCreateCustomerAccount'} = '1';
```



www.cnrs.fr

RETOUR D'EXPERIENCE : SHIBBOLISER DES APPLICATIONS

Roland Dirlewanger
CNRS – Délégation Aquitaine-Limousin

Conclusion ...



P. 21

Adapter une application à Shibboleth Facile ? pas facile ?

- | Pas de règle absolue
- | Un investissement initial
 - | Pour s'appropriier les notions de Shibboleth
 - | Pour créer le premier SP du site
- | La difficulté pour adapter une application dépend de l'application elle-même
 - | Cas faciles :
 - Applications sans rôles pour les utilisateurs où l'authentification est déléguée au serveur WWW (cas de CNRS-Hebdo)
 - Applications dont le code prévoit d'origine l'utilisation de greffons d'authentification (cas de OTRS)



www.cnrs.fr

RETOUR D'EXPERIENCE : SHIBBOLISER DES APPLICATIONS

Roland Dirlewanger
CNRS – Délégation Aquitaine-Limousin

Quelques liens utiles ...



P. 23

Un script très utile

| printenv.php qui permet d'afficher les variables d'environnement retournées par le serveur Apache :

```
<?php
    Header("Content-Type: text/plain");

    print_r($_SERVER);
?>
```



P. 24

Documentation utile

- | Rendre compatible une application avec Shibboleth
<https://federation.renater.fr/docs/fiches/shibbolisation>
- | Guides d'installation de Shibboleth – Installer un SP Shibboleth
<https://federation.renater.fr/docs/installation>
- | Mise en oeuvre d'un serveur Apache utilisant les certificats issus de l'IGC du CNRS
<http://www.cnrs.fr/aquitaine-limousin/spip.php?article622>