# EoleSSO - Tâche #14106

Scénario # 14102 (Terminé (Sprint)): Suite de l'implémentation d'OpenID / France Connect dans EoleSSO

## Définir / implémenter la notion de déconnexion lors d'une authentification faite via OpenID Connect

19/11/2015 17:13 - Bruno Boiget

| | | | |
|---|---|---|---|
| **Statut:** | Fermé | **Début:** | 19/11/2015 |
| **Priorité:** | Normal | **Echéance:** | |
| **Assigné à:** | Bruno Boiget | **% réalisé:** | 100% |
| **Version cible:** | sprint 2016 10-12 - Equipe MENESR | **Temps estimé:** | 8.00 heures |
| | | **Temps passé:** | 24.50 heures |

**Description**

2 aspects sont à considérer pour la déconnexion :

- fermeture de la session EoleSSO en cas de déconnexion de la session OpenID
- fermeture de la session OpenID en cas de déconnexion de la sessino EoleSSO
  - avec demande à l'utilisateur ?
  - option activable au niveau de gen_config, ou à considérer comme une préférence utilisateur ?

**Demandes liées:**

| | | |
|---|---|---|
| Lié à EoleSSO - Tâche #13853: Etudier les possiblités de déconnexion après co... | **Fermé** | **02/11/2015** |

### Révisions associées

**Révision 3320d907 - 10/03/2016 18:14 - Bruno Boiget**

Suite de la gestion du logout

- correction de l'enregistrement de l'association avec l'utilisateur local
- implémentation du suivi des déconnexions en cours pour OpenID

ref #14106 @4h

**Révision e6742d10 - 14/03/2016 18:01 - Bruno Boiget**

Correction de la déconnexion avec France Connect

- stockage du paramètre id_token reçu à la connexion
- envoi en tant que 'id_token_hint' à la déconnexion

ref #14106 @4h

**Révision c01f9128 - 15/03/2016 17:36 - Bruno Boiget**

Permière version fonctionnelle gérant la déconnexion

- stockage des id_token/access_token pour les transmettre au logout
- confirmation/déconnexion spécifique pour certains providers (google, ...)

ref #14106

**Révision c1322fe6 - 17/03/2016 16:13 - Bruno Boiget**

Suite de la gestion du logout

- correction de l'enregistrement de l'association avec l'utilisateur local
- implémentation du suivi des déconnexions en cours pour OpenID

ref #14106 @4h

**Révision a61f2503 - 17/03/2016 16:13 - Bruno Boiget**

Correction de la déconnexion avec France Connect

- stockage du paramètre id_token reçu à la connexion
- envoi en tant que 'id_token_hint' à la déconnexion

ref #14106 @4h

**Révision 95f0f841 - 17/03/2016 16:13 - Bruno Boiget**

Permière version fonctionnelle gérant la déconnexion

- stockage des id_token/access_token pour les transmettre au logout
- confirmation/déconnexion spécifique pour certains providers (google, ...)

ref #14106

**Révision f961909d - 21/03/2016 15:43 - Bruno Boiget**

Ajout de traductions supplémentaire + fichier manquant

ref #14106 @30m

## Historique

**#1 - 08/03/2016 18:03 - Bruno Boiget**

*- Statut changé de Nouveau à En cours*

**#2 - 08/03/2016 18:04 - Bruno Boiget**

*- Assigné à mis à Bruno Boiget*

*- Restant à faire (heures) changé de 8.0 à 4.0*

**#3 - 10/03/2016 18:18 - Bruno Boiget**

*- Statut changé de En cours à Nouveau*

*- Assigné à Bruno Boiget supprimé*

*- % réalisé changé de 0 à 80*

*- Restant à faire (heures) changé de 4.0 à 2.0*

**#4 - 10/03/2016 18:27 - Bruno Boiget**

La chaîne de déconnexion est fonctionnelle, mais le paramêtre 'id_token_hint' fourni à la déconnexion ne semble pas convenir à France Connect.

A première vue, le token passé contient un paramêtre 'aud': [u'cd7de882541d7fc760fd888bd29b985c577ec98a42b764ca0e03d8a4caf44262'] qui correspond au client_id déclaré, mais la déconnexion échoue avec ce message :

```
client cd7de882541d7fc760fd888bd29b985c577ec98a42b764ca0e03d8a4caf44262 does not exist
```

En remplaçant dans l'url utilisée la valeur de id_token_hint par le token renvoyé par France Connect lors de l'authentification, la déconnexion semble se dérouler correctement.

Ce paramêtre initial ne peut pas être intercepté par EoleSSO (appel http en backend effectué par la librairie pyoidc). On pourrait éventuellement dérivé la classe du client fourni pour récupérer et stocker le jeton fourni afin de le rejouer à la déconnexion.

Voir si il n'y a pas des corrections à ce sujet sur des versions plus récentes de la librairie (mais problème de compatibilité avec la librairie python-crypto du système).

Voir aussi comment cela est géré dans la librairie Openid de Django, qui utilise également pyoidc : https://github.com/marcanpilami/django-oidc

#### #5 - 14/03/2016 09:38 - Scrum Master

*- Statut changé de Nouveau à En cours*

#### #6 - 14/03/2016 09:39 - Scrum Master

*- Assigné à mis à Bruno Boiget*

#### #7 - 15/03/2016 09:42 - Scrum Master

*- Statut changé de En cours à Résolu*

#### #8 - 15/03/2016 17:33 - Bruno Boiget

*- % réalisé changé de 80 à 100*

*- Restant à faire (heures) changé de 2.0 à 0.5*

Après test de versions plus récentes de la librairie (en utilisant python virtualenv), la déconnexion ne passe toujours pas en générant un 'id_token_hint' au format jwt (en repartant des paramètres de l'id_token initial), et l'authentification demande des corrections supplémentaires (France Connect à l'air de refuser qu'un paramètre 'state' soit passé dans la requête access_token_request, alors que le client l'ajoute automatiquement).

La solution retenue pour l'instant est de garder la version 0.7.6 de pyoidc et de Surcharger la classe Client de pyoidc pour stocker les id_token et access_token reçus à l'authentification.

- Dans le cas 'standard' (France Connect) Le 'token_id' initial est renvoyé en tant que 'token_id_hint' lors de la déconnexion.
  - cf http://openid.net/specs/openid-connect-frontchannel-1_0.html#RPLogout
- certains fournisseurs (google, microsoft, facebook) n'ont à priori pas d'implémentation du single logout tel que défini dans les récents drafts openid connect.
  - solutions alternative proposée : demande à l'utilisateur si il souhaite fermer sa session auprès du fournisseur, et redirection vers des URLs spécifiques en fonction du provider
  - cf http://stackoverflow.com/questions/16946798/logout-from-external-login-service-gmail-facebook-using-oauth/17127549#17127549

Revoir la configuration Creole pour les différents cas possibles : cf demande #14108

**#9 - 30/03/2016 10:02 - Scrum Master**

*- Statut changé de Résolu à Fermé*

*- Restant à faire (heures) changé de 0.5 à 0.0*