# Plugin FS FranceConnect - Bug #39789

## scope "profile" refusé

12 février 2020 14:22 - Thomas Noël

| | | | |
|---|---|---|---|
| **Statut:** | Rejeté | **Début:** | 12 février 2020 |
| **Priorité:** | Normal | **Echéance:** | |
| **Assigné à:** | | **% réalisé:** | 0% |
| **Catégorie:** | | **Temps estimé:** | 0:00 heure |
| **Version cible:** | | | |
| **Hors marché:** | Non | **Planning:** | Non |
| **Patch proposed:** | Non | | |

**Description**

Sur une demande de validation :

```
From: Support FranceConnect <support.partenaires@franceconnect.gouv.fr>

Bonjour,

Je vous remercie pour votre email.

Nous n'avons pas pu reproduire l'erreur mentionnée en cliquant sur
"[1]https://connexion-xxxxx.test.entrouvert.org/login/" étant donné que nous
tombons sur un autre problème lié aux scopes.

Impossible de se connecter à FranceConnect : « invalid_scope ».(« Requested
scope "profile openid email". Scope authorized
"email,openid,birthdate,given_name,family_name" »)
```

A priori on ne devait pas demander profile, la doc indique qu'il contient gender (et ici on ne l'a pas)

Extrait de https://partenaires.franceconnect.gouv.fr/fcp/fournisseur-service :

```
Les scopes principaux (identité pivot)

    openid * : l'identifiant technique (sub) de l'utilisateur au format OpenIDConnect sera retourn
é
    gender : le sexe de la personne sera retourné
    birthdate : la date de naissance de la personne sera retourné
    birthcountry : le pays de naissance de la personne sera retourné
    birthplace : la ville de naissance de la personne sera retourné
    given_name : les prénoms de la personne seront retournés
    family_name : le nom de naissance de la personne sera retourné
    email : l'adresse électronique de la personne sera retournée

Les scopes optionnels (information renvoyée si elle est disponible)

    preferred_username : le nom d'usage de la personne sera retourné
    address : l'adresse postale de la personne sera retourné
    phone : le numéro de téléphone de la personne sera retourné

Les "alias"

    identite_pivot : Regroupe les scopes given_name, family_name, preferred_username, birthdate, g
ender, birthplace et birthcountry
    profile : Regroupe les scopes given_name, family_name, preferred_username, birthdate et gender
    birth : Regroupe les scopes birthplace et birthcountry. Permet de récupérer la ville et le dép
artement de naissance de la personne.
<pre>
</pre>
```

## Historique

#### #3 - 12 février 2020 14:24 - Thomas Noël

Note : en cas d'urgence on peut contourner avec "A2_FC_SCOPES": ["email","openid","birthdate","given_name","family_name"] dans le settings.json (la liste autorisée indiquée dans l'erreur FC)

#### #4 - 12 février 2020 14:32 - Thomas Noël

Je pense que FC ne bloquait pas jusqu'à il y a quelques jours quand un des attributs de l'alias "profile" manquait : il renvoyait juste la liste des valeurs dispos.

Il faudrait leur dire de revenir à ce comportement : "profile" doit renvoyer les attributs du profil décidé lors de la demande de liaison FC.

C'est à mon sens beaucoup plus logique. Un avis des camarades compétents ?

#### #5 - 12 février 2020 15:19 - Paul Marillonnet

Thomas Noël a écrit :

> C'est à mon sens beaucoup plus logique. Un avis des camarades compétents ?

Je pense qu'ils ont une lecture plus directe des spécifications OIDC, selon lesquelles la portée profile correspond à ensemble figé de revendications[1], même si oui c'est sans doute moins logique que la solution que tu proposes.

Quant au comportement du serveur lorsque certaines des portées ne lui conviennent pas, c'est hors-spéc OAuth, i.e. carte blanche : « The authorization server MAY fully or partially ignore the scope requested by the client, based on the authorization server policy or the resource owner's instructions » [2].

[1] https://openid.net/specs/openid-connect-core-1_0.html#ScopeClaims

[2] https://tools.ietf.org/html/rfc6749#section-3.3

#### #6 - 12 février 2020 15:40 - Thomas Noël

*- Statut changé de Nouveau à En cours*

#### #8 - 13 février 2020 10:35 - Benjamin Dauvergne

*- Statut changé de En cours à Rejeté*

Il n'y a rien à faire dans authentic.