Authentic 2 - Bug #72507

idp_oidc : recueillir le consentement ou la sélection de profil de l'usager même lors d'un SSO passif (prompt=none)

15 décembre 2022 16:55 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	15 décembre 2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Paul Marillonnet	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

La requête part avec prompt=none et si un compte avec profil est connecté, alors elle revient toujours avec l'erreur "consent_required".

Un premier souci de forme c'est que l'erreur devrait être "account_selection_required" dans ce cas.

Ensuite je pense changer le prompt=none envoyé en mode passif par prompt=select_account et l'interpréter d'une manière qui n'est peut-être pas celle voulu par la spéc (ça n'est pas très clair) :

```
select_account
    The Authorization Server SHOULD prompt the End-User to select a user account. This enables an End-User who has multiple accounts at the Authorization Server to select amongst the multiple accounts that they might have current sessions for. If it cannot obtain an account selection choice made by the End-User, it MUST return an error, typically account_selection_required.
```

Je compte l'interpréter ainsi :

- si on est connecté permettre la sélection et le consentement,
- sinon retourner l'erreur select_account_required

Coté auth_oidc au retour il faut ignorer cette erreur et continuer (actuellement on reste bloqué sur une message d'alerte).

Demandes liées:

Lié à Authentic 2 - Development #27135: Déléguer l'authentification passive à...	**Fermé**	**09 octobre 2018**
Lié à Authentic 2 - Development #72538: auth_oidc : gérer les erreurs OP de s...	**Fermé**	**16 décembre 2022**

Révisions associées

Révision c5b67aaa - 20 décembre 2022 11:52 - Paul Marillonnet

idp_oidc: get user profile selection or consent even when prompt=none (#72507)

Historique

#2 - 15 décembre 2022 16:55 - Benjamin Dauvergne

- Lié à Development #27135: Déléguer l'authentification passive à la vue de login si aucune session n'est ouverte ajouté

#3 - 16 décembre 2022 10:06 - Paul Marillonnet

- Statut changé de Nouveau à En cours

- Assigné à mis à Paul Marillonnet

Ok, en effet, je regarde.

#4 - 16 décembre 2022 10:10 - Paul Marillonnet

- Sujet changé de Le SSO passif via OIDC est incompatible avec le support des profils (personnes morales) à idp_oidc : le SSO passif via OIDC est incompatible avec le support des profils (personnes morales)

Ce ticket pour la partie fournisseur, et j'en crée un second pour la partie auth_oidc.

#5 - 16 décembre 2022 10:15 - Paul Marillonnet

- Lié à Development #72538: auth_oidc : gérer les erreurs OP de sélection de profil requise lors d'un tentative d'authn en prompt=none ajouté

#6 - 16 décembre 2022 11:01 - Paul Marillonnet

- Fichier 0001-idp_oidc-profile-selection-error-when-prompt-none-72.patch ajouté

- Statut changé de En cours à Solution proposée

- Patch proposed changé de Non à Oui

Il me semble que faire comme ceci ici suffirait, à condition de gérer cette erreur côté auth_oidc (ce sera #72538).

Pour moi prompt=none et prompt=select_account ce sont deux options incompatibles, je pense que le cas select_account n'a pas besoin d'être géré pour le problème identifié ici.

D'ailleurs dans la gestion des personnes morales dans Publik, authentic client oidc n'a pas connaissance des multiples profils de l'usager côté fournisseur (c'est transparent du point de vue du RP OIDC).
Côté idp_oidc, s'attendre à recevoir un prompt=select_account ça veut dire qu'on modifie ce postulat, ce serait l'objet d'un autre ticket je pense, pas en lien avec le problème sur l'authn passive de ce ticket ci.

#7 - 16 décembre 2022 11:29 - Paul Marillonnet

(s/select_account_required/account_selection_required et s/SelectAccountRequired/AccountSelectionRequired/ dans la branche, pour se conformer aux specs.)

#8 - 16 décembre 2022 11:35 - Benjamin Dauvergne

J'aurai du me l'assigner mais j'ai commencé en fait. Mais pas le coté idp_oidc donc on pourra merge nos deux codes, c'est bon.

#9 - 16 décembre 2022 11:45 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> Pour moi prompt=none et prompt=select_account ce sont deux options incompatibles, je pense que le cas select_account n'a pas besoin d'être géré pour le problème identifié ici.

Oui on ne peut pas mettre les deux c'est certain, none doit toujours être seul d'après la spec, par contre on peut combiner login/consent/select_account. La sémantique de chacun si on est connecté ou pas n'est par contre vraiment pas claire. "The Authorization Server SHOULD prompt the End-User to select a user account." mais est-ce qu'il should prompt the user for login ? for consent ? Who knows...

> D'ailleurs dans la gestion des personnes morales dans Publik, authentic client oidc n'a pas connaissance des multiples profils de l'usager côté fournisseur (c'est transparent du point de vue du RP OIDC).
> Côté idp_oidc, s'attendre à recevoir un prompt=select_account ça veut dire qu'on modifie ce postulat, ce serait l'objet d'un autre ticket je pense, pas en lien avec le problème sur l'authn passive de ce ticket ci.

On va revenir à la base :

- on déclenche un SSO passif si on a une forte présomption (via des cookies sur domaine commun, genre sur ".grandlyon.com") qu'une session ouverte existe sur un IdP connu,
- sur un SSO passif deux résultats, soit on s'est trompé et ça revient tout de suite avec une erreur,
- soit une session est effectivement ouverte et on procède à la connexion sans aucune interaction avec l'utilisateur.

Dans le cas personne moral on se retrouve dans une situation bâtarde, on a une session ouverte, mais si la gestion des personnes morales est active pour le compte, on doit procéder à une interaction avec l'utilisateur pour choisir le bon profil (et c'est actif en recette pour Toodego dont dépend le portail SAU d'aide aux usagers, sujet de tous les tickets sur l'authentification passive dans le projet GLC).

On a le choix entre rendre impossible l'authent passive pour les comptes avec plusieurs profils ou accepter une interaction dans ce cas (et finalement je pense que passer de 'none' à 'select_account' dans le code auth_oidc n'a pas vraiment d'importance, je retire ce point). Donc au final quand on reçoit prompt=none :

- est-ce qu'on affiche quand même consentement + sélection de profil ou est-ce qu'on retourne une erreur ? Je penche pour la première solution même si elle n'est pas fidèle à la spéc, elle correspond au comportement qu'on souhaite pour les usagers, si ça pose souci dans le futur on pourra en faire une option du service, mais dans l'immédiat je dirai de faire comme ça par défaut.

#10 - 16 décembre 2022 12:29 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> On va revenir à la base :
>
> - on déclenche un SSO passif si on a une forte présomption (via des cookies sur domaine commun, genre sur ".grandlyon.com") qu'une session ouverte existe sur un IdP connu,

- sur un SSO passif deux résultats, soit on s'est trompé et ça revient tout de suite avec une erreur,
- soit une session est effectivement ouverte et on procède à la connexion sans aucune interaction avec l'utilisateur.

Dans le cas personne moral on se retrouve dans une situation bâtarde, on a une session ouverte, mais si la gestion des personnes morales est active pour le compte, on doit procéder à une interaction avec l'utilisateur pour choisir le bon profil (et c'est actif en recette pour Toodego dont dépend le portail SAU d'aide aux usagers, sujet de tous les tickets sur l'authentification passive dans le projet GLC).

On a le choix entre rendre impossible l'authent passive pour les comptes avec plusieurs profils ou accepter une interaction dans ce cas (et finalement je pense que passer de 'none' à 'select_account' dans le code auth_oidc n'a pas vraiment d'importance, je retire ce point). Donc au final quand on reçoit prompt=none :

- est-ce qu'on affiche quand même consentement + sélection de profil ou est-ce qu'on retourne une erreur ? Je penche pour la première solution même si elle n'est pas fidèle à la spéc, elle correspond au comportement qu'on souhaite pour les usagers, si ça pose souci dans le futur on pourra en faire une option du service, mais dans l'immédiat je dirai de faire comme ça par défaut.

Ah oui ok, je comprends mieux, merci. J'ai écrit le patche en n'ayant envisagé que cette seconde solution, je ne comprenais pas le dilemme ici.
Je n'envisageais même pas d'amener à une interaction consentement + sélection profil dans le cas où prompt=none, de peur que ça pète des trucs (genre ces écrans de sélection qui s'affichent de façon intempestive à l'usager pour les services partenaires GLCPro/Asso à venir, avec une autre implémentation client OIDC etc.). J'étais resté sur la ligne « prompt=none -> jamais d'interaction quelle qu'elle soit » et j'avoue ne pas connaître les implications d'une dérogation à cette règle, côté implémentation OIDC des partenaires GLC notamment.

#11 - 16 décembre 2022 12:32 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> côté implémentation OIDC des partenaires GLC notamment.

Il faudrait vérifier mais je suis quasiment sûr qu'on est les seuls à utiliser ça.

PS: voilà, vérifié il n'y a personne qui s'en sert actuellement:

```
$ sudo zgrep authorize moncompte-access.log* | grep authorize | wc
 671490 15579660 473372084
bdauvergne@glc.node1.prod:/var/log/nginx$ sudo zgrep authorize moncompte-access.log* | grep authorize | grep p
rompt | wc
      0       0       0
```

#12 - 16 décembre 2022 12:58 - Paul Marillonnet

- Statut changé de Solution proposée à En cours

Ok, merci d'avoir vérifié, je modifie mon patch ici (et il me semble que celui de #72538 reste pertinent, pour une implémentation client OIDC propre, même s'il n'est plus lié à la façon dont on corrige le problème ici).

#13 - 19 décembre 2022 10:18 - Paul Marillonnet

- Fichier 0001-idp_oidc-prompt-for-user-profile-selection-even-when.patch ajouté

- Statut changé de En cours à Solution proposée

Voilà, nouvelle version du patch.

#14 - 20 décembre 2022 10:33 - Benjamin Dauvergne

Il faut aussi laisser s'afficher le formulaire de consentement en cas de prompt=none, le cas d'usage SAU la personne n'est possiblement jamais venu sur le portail Toodego et donc n'a pas de consentement, prompt=none ne doit arrêter le processus que sur un besoin de login.

#15 - 20 décembre 2022 12:04 - Paul Marillonnet

- Fichier 0001-idp_oidc-get-user-profile-selection-or-consent-even-.patch ajouté

Benjamin Dauvergne a écrit :

> Il faut aussi laisser s'afficher le formulaire de consentement en cas de prompt=none, le cas d'usage SAU la personne n'est possiblement jamais venu sur le portail Toodego et donc n'a pas de consentement, prompt=none ne doit arrêter le processus que sur un besoin de login.

Ok, donc ça change des choses au delà du support des profils personnes morales.

#16 - 20 décembre 2022 12:04 - Paul Marillonnet

- Sujet changé de idp_oidc : le SSO passif via OIDC est incompatible avec le support des profils (personnes morales) à idp_oidc : recueillir le consentement ou la sélection de profil de l'usager même lors d'un SSO passif (prompt=none)

#17 - 20 décembre 2022 12:16 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> Ok, donc ça change des choses au delà du support des profils personnes morales.

Oui, je ne vois pas d'autre solution pour rendre le service qu'on veut rendre ou alors il faut utiliser une autre valeur pour prompt (en inventer une ou supposer que select_account veut dire cela, ce qui était ma première idée).

#18 - 20 décembre 2022 12:22 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

#19 - 20 décembre 2022 12:33 - Paul Marillonnet

- Statut changé de Solution validée à Résolu (à déployer)

```
commit c5b67aaae1be3642d0e53069862b36aa5e4010fe
Author: Paul Marillonnet <pmarillonnet@entrouvert.com>
Date:   Fri Dec 16 10:12:06 2022 +0100

    idp_oidc: get user profile selection or consent even when prompt=none (#72507)
```

#20 - 23 décembre 2022 10:14 - Transition automatique

- Statut changé de Résolu (à déployer) à Solution déployée

#21 - 26 février 2023 04:42 - Transition automatique

Automatic expiration

Fichiers

0001-idp_oidc-profile-selection-error-when-prompt-none-72.patch	3,99 ko	16 décembre 2022	Paul Marillonnet
0001-idp_oidc-prompt-for-user-profile-selection-even-when.patch	4,04 ko	19 décembre 2022	Paul Marillonnet
0001-idp_oidc-get-user-profile-selection-or-consent-even-.patch	5,76 ko	20 décembre 2022	Paul Marillonnet