

## Authentic 2 - Development #27540

### idp\_oidc: déterminer si claims dont la valeur est absente doivent être absent ou à null

24 octobre 2018 07:32 - Benjamin Dauvergne

<b>Statut:</b>	Fermé	<b>Début:</b>	24 octobre 2018
<b>Priorité:</b>	Bas	<b>Echéance:</b>	
<b>Assigné à:</b>	Benjamin Dauvergne	<b>% réalisé:</b>	0%
<b>Catégorie:</b>		<b>Temps estimé:</b>	0:00 heure
<b>Version cible:</b>		<b>Planning:</b>	
<b>Patch proposed:</b>	Oui		

#### Description

C'est une chose dont je me suis aperçu en ajoutant le test OIDC pour le nouveau type d'attribut image ([#26022](#)), si un claim pointe sur un attribut absent du dictionnaire produit par attributes\_ng alors je ne produit pas le claim:

```
# src/authentic2_idp_oidc/utils.py
```

```
def create_user_info(client, user, scope_set, id_token=False):
    '''Create user info dictionnary'''
    user_info = {
        'sub': make_sub(client, user)
    }
    attributes = get_attributes({
        'user': user, 'request': None, 'service': client,
        '__wanted_attributes': client.get_wanted_attributes()})
    for claim in client.oidcclaim_set.filter(name__isnull=False):
        if not set(claim.get_scopes()).intersection(scope_set):
            continue
        if not claim.value in attributes: # <-- ICI
            continue
        user_info[claim.name] = normalize_claim_values(attributes[claim.value])
        # check if attribute is verified
        if claim.value + ':verified' in attributes:
            user_info[claim.value + '_verified'] = True
    hooks.call_hooks('idp_oidc_modify_user_info', client, user, scope_set, user_info)
    return user_info
```

Je me demande si ce ne serait pas plus agréable pour les consommateurs que le claim soit toujours présent (déjà ça rend mon test plus propre, au lieu d'un .get() je peux faire un []) mais avec une valeur None/null.

#### Révisions associées

##### Révision ce1b7964 - 19 mars 2019 15:32 - Benjamin Dauvergne

idp\_oidc: use force\_bytes/text and six.text\_type instead of smart\_bytes and unicode (#27540)

Just some cleaning, not really related to #27540.

##### Révision 6964b0cc - 19 mars 2019 15:32 - Benjamin Dauvergne

idp\_oidc: export claim even if source attribute is absent (fixes #27540)

#### Historique

##### #1 - 08 novembre 2018 14:41 - Benjamin Dauvergne

- Tracker changé de Support à Development

##### #2 - 08 novembre 2018 14:47 - Benjamin Dauvergne

- Priorité changé de Normal à Bas

##### #3 - 08 novembre 2018 14:47 - Benjamin Dauvergne

- Assigné à Benjamin Dauvergne supprimé

**#4 - 22 novembre 2018 12:48 - Benjamin Dauvergne**

- Assigné à mis à Benjamin Dauvergne

**#5 - 22 novembre 2018 12:48 - Benjamin Dauvergne**

- Fichier 0001-idp\_oidc-use-force\_bytes-text-and-six.text\_type-inst.patch ajouté
- Fichier 0002-idp\_oidc-export-claim-even-if-source-attribute-is-ab.patch ajouté
- Statut changé de Nouveau à Solution proposée
- Patch proposed changé de Non à Oui

Tous les claims déclarés sont désormais à null aucune valeur n'est trouvée via les attributs.

Si plusieurs mapping génère des valeurs on garde la dernière différente de None.

J'ai du modifier un test provenant de [#23643](#) qui testait systématiquement l'absence de preferred\_username car ce n'était pas le but de ce test (le but étant que cela fonctionne pour un utilisateur sans username, ce qui est toujours le cas).

**#6 - 18 mars 2019 11:01 - Benjamin Dauvergne**

- Fichier 0001-idp\_oidc-use-force\_bytes-text-and-six.text\_type-inst.patch ajouté
- Fichier 0002-idp\_oidc-export-claim-even-if-source-attribute-is-ab.patch ajouté

Rebasé.

**#7 - 19 mars 2019 12:20 - Paul Marillonnet**

- Projet changé de Authentic 2 à Site Publik
- Statut changé de Solution proposée à Information nécessaire

Hmm, on s'éloigne des recommandations dans les spéc :/

Cf [https://openid.net/specs/openid-connect-core-1\\_0.html#UserInfoResponse](https://openid.net/specs/openid-connect-core-1_0.html#UserInfoResponse)

```
If a Claim is not returned, that Claim Name SHOULD be omitted from the JSON object representing the Claims; it SHOULD NOT be present with a null or empty string value.
```

Et c'est vrai qu'on aurait plus de moyen de discerner un attribut présent mais valant null, et l'absence de cet attribut. Si c'est simplement pour pouvoir faire un dict[key] à la place de dict.get(key) dans les tests je ne pense pas que ça vaille la peine d'enfreindre cette recommandation.

Est-ce que je passe à côté de quelque chose d'important sur ce patch ?

**#8 - 19 mars 2019 12:21 - Paul Marillonnet**

- Projet changé de Site Publik à Authentic 2

(oops, mauvaise manip' de ma part, je replace le ticket dans le projet a2)

**#9 - 19 mars 2019 13:59 - Benjamin Dauvergne**

Tu as raison, je modifie.

**#10 - 19 mars 2019 14:03 - Benjamin Dauvergne**

- Statut changé de Information nécessaire à Solution proposée

Benjamin Dauvergne a écrit :

Tu as raison, je modifie.

Je n'ai pas la même lecture finalement, cette phrase fait suite à celle-ci :

For privacy reasons, OpenID Providers MAY elect to not return values for some requested Claims.

Et donc "not returned" ça ne veut pas dire absence du claim, ça veut dire refus de l'IdP de renvoyer le claim et ça c'est pris en compte; en fait on ne

refuse jamais actuellement, on va refuser l'autorisation complète, donc le cas n'arrivant la phrase que tu cites ne s'applique pas pour moi. Ainsi le RP peut faire la différence entre un refus et une absence.

**#11 - 19 mars 2019 14:22 - Paul Marillonnet**

- Statut changé de Solution proposée à Solution validée

Oui, complètement, mauvaise lecture de ma part.  
Ack.

**#12 - 19 mars 2019 15:51 - Benjamin Dauvergne**

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

```
commit 6964b0cc8283381528f3c92a58db12e041d5b3c4
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date: Thu Nov 22 12:37:29 2018 +0100
```

```
idp_oidc: export claim even if source attribute is absent (fixes #27540)
```

```
commit ce1b796473cbdabcf025e5be9266e999ef17f5b1
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date: Thu Nov 22 12:34:11 2018 +0100
```

```
idp_oidc: use force_bytes/text and six.text_type instead of smart_bytes and unicode (#27540)
```

```
Just some cleaning, not really related to #27540.
```

**#13 - 19 mars 2019 15:55 - Benjamin Dauvergne**

- % réalisé changé de 0 à 100

Appliqué par commit [authentic2|6964b0cc8283381528f3c92a58db12e041d5b3c4](#).

**#14 - 19 mars 2019 23:46 - Benjamin Dauvergne**

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

- % réalisé changé de 100 à 0

**Fichiers**

---

0001-idp_oidc-use-force_bytes-text-and-six.text_type-inst.patch	2,79 ko	22 novembre 2018	Benjamin Dauvergne
0002-idp_oidc-export-claim-even-if-source-attribute-is-ab.patch	2,31 ko	22 novembre 2018	Benjamin Dauvergne
0001-idp_oidc-use-force_bytes-text-and-six.text_type-inst.patch	2,79 ko	18 mars 2019	Benjamin Dauvergne
0002-idp_oidc-export-claim-even-if-source-attribute-is-ab.patch	2,31 ko	18 mars 2019	Benjamin Dauvergne