Publik - Development #10597

création de compte avec autre chose que name_id_content comme clé de fédération

08 avril 2016 15:36 - Frédéric Péters

Statut:	Nouveau	**Début:**	08 avril 2016
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Club:**	
Planning:			

Description

Pour le moment un SSO avec urn:oasis:names:tc:SAML:2.0:nameid-format:transient va quand même créer un usager dans la base.

Il faudrait que non.

Il faudrait aussi la possibilité de pointer qu'un attribut différent du name_id_content peut en fait servir de clé de fédération.

Par exemple, dans le cas d'un SSO avec le fedict, l'attribut fedid peut servir à ça :


```
{
  "mellon_session": {
    "urn:be:fedict:iam:attr:context": [
      "urn:be:fedict:iam:context:enterprise"
    ],
    "surname": [
      "..."
    ],
    "name_id_name_qualifier": "https://idp.iamfas.int.belgium.be/fas",
    "urn:be:fedict:iam:attr:locale": [
      "fr"
    ],
    "urn:be:fedict:iam:attr:authenticationmethod": [
      "urn:be:fedict:iam:authenticationmethod:eid"
    ],
    "name_id_format": "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
    "name_id_content": "wHrVxs7rgRy22EhKwVVB4IoeqXbw",
    "authn_context_class_ref": "urn:be:fedict:iam:fas:enterprise:eid",
    "issuer": "https://idp.iamfas.int.belgium.be/fas",
    "name_id_sp_name_qualifier": "https://liege-auth.lescommunes.be/accounts/saml/metadata/",
    "egovNRN": [
      "..."
    ],
    "urn:be:fedict:iam:attr:fedid": [
      "..."
    ],
    "authn_instant": "2016-04-08T12:45:11+00:00",
    "session_index": "s2970f11f8ebc89c6063cb1b6afc9ee37ee9e35e11",
    "givenName": [
      "..."
    ]
  }
}
```


Demandes liées:

Lié à Authentic 2 - Development #10605: authentic2-auth-saml: allow using an ...	**Rejeté**	**10 avril 2016**
Lié à django-mellon - Bug #10619: Permettre la fédération à l'aide d'un attri...	**Fermé**	**11 avril 2016**

Historique

#1 - 09 avril 2016 11:16 - Benjamin Dauvergne

Comme je crois que la demande est en rapport avec authentic2, ne pas créer un usager pour du transient est un poil compliqué, Django est de plus en plus incapable d'avoir autre chose qu'un modèle User renvoyé par un module d'authentification, au mieux on pourrait faire des utilisateurs transient nettoyés dès que la session qui les a vu naître disparaît (dans le cron de nettoyage), mais ce serait à construire dans authentic, django-mellon ne fait qu'utiliser le modèle User proposé par l'application qui l'intègre.

Utiliser autre chose que le NameID comme clé de fédération c'est gérable, mais dans le cas du fedict je ne vois pas pourquoi ne pas créer un vrai user dans ce cas, une raison ?

#2 - 09 avril 2016 11:47 - Frédéric Péters

- Sujet changé de création de compte avec nameid transient à création de compte avec autre chose que name_id_content comme clé de fédération

Si, désolé je mélangeais deux choses qui m'arrivaient en même temps. Pour la situation du fedict, il faut bien créer un compte (malgré le transient), et utiliser attributes["urn:be:fedict:iam:attr:fedid"] comme clé de fédération.

#3 - 10 avril 2016 14:34 - Frédéric Péters

(cela étant je viens de créer un authentic2-auth-fedict et je pourrai y mettre du code spécifique, plutôt que complexifier django-mellon et/ou authentic)

#4 - 10 avril 2016 15:51 - Benjamin Dauvergne

- Projet changé de django-mellon à Publik

Je bouge ça dans publik et je lie au ticket #10605.

#5 - 10 avril 2016 15:51 - Benjamin Dauvergne

- Lié à Development #10605: authentic2-auth-saml: allow using an attribute to federate accounts with an IdP sending transient NameIDs ajouté

#6 - 12 avril 2016 11:23 - Benjamin Dauvergne

- Lié à Bug #10619: Permettre la fédération à l'aide d'un attribut si le format de NameID est transient ajouté