Authentic 2 - Bug #53754

authentification forcée (ForceAuthn) SAML après un SSO vers un IdP SAML

04 mai 2021 21:25 - Frédéric Péters

Statut:	Nouveau	**Début:**	04 mai 2021
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

On part d'un SP qui lance un SSO vers Authentic en passant ForceAuthn (parce qu'on demande à l'usager de se réauthentifier), l'usager clique sur une méthode d'authentification SAML, ça fait SSO puis ça revient dans sso_after_process_request qui fait

```
    did_auth = find_authentication_event(request, nonce) is not None
...
    if not passive and (user.is_anonymous or (force_authn and not did_auth)):
        logger.debug('login required')
        return need_login(request, login, nid_format, service)
```

et on se trouve là avec force_authn à True (ok logique) et did_auth à False, ce qui surprend et amène à ce que la mire de connexion soit à nouveau proposée.

find_authentication_event ne trouve pas d'événement attaché au nonce en question, parce que l'événement enregistré, ce qui se fait dans src/authentic2_auth_saml/adapters.py se fait ainsi :

```
    def auth_login(self, request, user):
        utils.login(request, user, 'saml')
```

c'est-à-dire sans associer de nonce à cette authentification.

Pour un IdP OIDC, ça semble par contre ok, (src/authentic2_auth_oidc/views.py)

```
            login(request, user, 'oidc', nonce=nonce)
```

Demandes liées:

Lié à django-mellon - Development #55953: conserver un nonce et pouvoir deman...	**Fermé**	**03 août 2021**

Historique

#2 - 04 août 2021 18:32 - Benjamin Dauvergne

- Lié à Development #55953: conserver un nonce et pouvoir demander le flag forceAuthn sur la vue login, et pouvoir certifier au login qu'ils ont été conservés ajouté

#3 - 04 août 2021 18:32 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#4 - 12 janvier 2022 19:30 - Benjamin Dauvergne

- Assigné à Benjamin Dauvergne supprimé