Authentic 2 - Support #49699

OIDC : Ajout des code_challenge_methods_supported à la configuration well-known

22 décembre 2020 17:26 - Benjamin Renard

Statut:	Nouveau	**Début:**	22 décembre 2020
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

J'ai fait un test de configuration d'une authentification *OIDC* avec Authentic et un client utilisant la lib *OpenID-Connect-PHP* (https://github.com/jumbojett/OpenID-Connect-PHP) et quand je tente de la configurer en mode *PKCE*, j'ai une erreur m'indiquant que le paramètre *code_challenge_methods_supported* n'est pas fourni dans la configuration *well-known* de l'IDP. Effectivement, ce paramètre semble absent du *JSON* retourné par Authentic sur l'URI */.well-known/openid-configuration*.

Authentic supporte-t-il *PKCE* ? Est-ce le client qui réclame quelques choses hors du standard *OIDC* ?

Historique

#1 - 22 décembre 2020 17:32 - Frédéric Péters

Il n'y a pas de prise en charge de PKCE dans Authentic.

Sur le sujet précédemment Benjamin D. faisait cette réponse :

> Le plus simple est d'utiliser le mode authorization code grant est de laisser la résolution du code à la partie serveur via les crédentiels du client, il est dit que c'est équivalent à PKCE dans le draft (https://tools.ietf.org/html/draft-ietf-oauth-security-topics-11#section-2.1.1).
>
> Aussi dans la même section il y a cette phrase :
> « OpenID Connect clients MAY use the "nonce" parameter of the OpenID Connect authentication request as specified in [OpenID] in conjunction with the corresponding ID Token claim for the same purpose. »
>
> et authentic gère bien le paramètre nonce, il vous suffit donc de générer un nonce sur la partie serveur de votre client et vérifier que celui-ci correspond lors de la consommation de l'id token. Pour le diagramme de séquence :

Error executing the **plantuml** macro (Missing partial wiki_external_filter/_macro_image with {:locale=>[:fr, :en], :formats=>[:pdf], :variants=>[], :handlers=>[:raw, :erb, :html, :builder, :ruby, :rsb]}. Searched in: * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/redmine_tags/app/views" * "/usr/share/redmine/plugins/redmine_entrouvert/app/views" * "/usr/share/redmine/plugins/plantuml/app/views" * "/usr/share/redmine/plugins/localizable/app/views" * "/usr/share/redmine/app/views")

> Ce mécanisme interdit le rejeu (si tant est qu'une interception soit possible dans ce diagramme).

#2 - 01 février 2021 17:40 - Benjamin Renard

Frédéric Péters a écrit :

> Il n'y a pas de prise en charge de PKCE dans Authentic.
>
> Sur le sujet précédemment Benjamin D. faisait cette réponse :

Désolé du délai de réponse, j'avais zappé… Merci pour ton retour et pour les précisions de Benjamin. C'était juste un test, donc pas de souci pour moi ici. J'espère n'avoir pas à traiter de cas ou PKCE soit un impératif, mais jusqu'ici, dans les intégrations qu'on a eut à faire, l'application cliente ne gérait que le mode implicite/natif de toutes manières.

Si le cas ce présent, j'essayerai de me rappeler l'existence de cette explication de Benjamin.