Authentic 2 - Bug #36966

auth_oidc: pouvoir émettre des requêtes signées

15 octobre 2019 18:10 - Benjamin Dauvergne

Statut:	Nouveau	**Début:**	15 octobre 2019
Priorité:	Bas	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

La requête d'autorisation doit être encodé dans un JWT passé dans un paramètre request, voir la spec.

Historique

#1 - 16 octobre 2019 15:51 - Paul Marillonnet

- Assigné à mis à Paul Marillonnet

#2 - 22 juin 2020 17:44 - Paul Marillonnet

En fait, c'est même dans une RFC à part. Voir par exemple https://tools.ietf.org/html/rfc7523#page-4 :

```
   The following example demonstrates an access token request with a JWT
   as an authorization grant (with extra line breaks for display
   purposes only):

     POST /token.oauth2 HTTP/1.1
     Host: as.example.com
     Content-Type: application/x-www-form-urlencoded

     grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Ajwt-bearer
     &assertion=eyJhbGciOiJFUzI1NiIsImtpZCI6IjE2In0.
     eyJpc3Mi[...omitted for brevity...].
     J9l-ZhwP[...omitted for brevity...]
```

#3 - 22 juin 2020 17:45 - Paul Marillonnet

<HS>D'ailleurs, l'autre moitié de cette RFC traite de l'authentification du client à l'aide d'un JWT, qui est peut-être quelque chose qui pourrait nous intéresser aussi, à voir.</HS>

#4 - 22 juin 2020 17:50 - Benjamin Dauvergne

- Priorité changé de Normal à Bas

Paul Marillonnet a écrit :

> <HS>D'ailleurs, l'autre moitié de cette RFC traite de l'authentification du client à l'aide d'un JWT, qui est peut-être quelque chose qui pourrait nous intéresser aussi, à voir.</HS>

Mouais...

Par contre pour les requêtes signé ça n'a qu'un seul usage : pouvoir respecter le flag forçant à une réauthentification ou une session avec une certaine fraîcheur, on a le même problème en SAML, si les requêtes d'authentification ne sont pas signés n'importe qui peut générer une requête sans flag de ré-authentification (l'idtoken ne contient pas l'information comme quoi l'utilisateur s'est réauthentifié).

#5 - 22 juillet 2020 15:21 - Paul Marillonnet

- Fichier 0001-auth_oidc-support-signed-authz-requests-through-jwt-.patch ajouté

- Tracker changé de Support à Bug

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

On pourrait faire quelque chose comme ça.

#6 - 25 août 2020 10:54 - Benjamin Dauvergne

- Statut changé de Solution proposée à Nouveau

Tu n'as pas du tout implémenté les requêtes signées, tu t'es trompé de spec : https://openid.net/specs/openid-connect-core-1_0.html#JWTRequests

#7 - 07 septembre 2020 14:28 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> Tu n'as pas du tout implémenté les requêtes signées, tu t'es trompé de spec :
> https://openid.net/specs/openid-connect-core-1_0.html#JWTRequests

J'ai implémenté les requêtes signées au sens de la RFC OAuth que je cite plus haut (la 7523).
Je pense qu'on est pas loin de ce qui ce que spécifie le passage de la doc OIDC que tu mentionnes ici. Je vais regarder ça.

#8 - 07 septembre 2020 14:49 - Benjamin Dauvergne

Désolé d'en remettre une couche mais ça n'a actuellement aucun intérêt.

#9 - 07 septembre 2020 15:23 - Paul Marillonnet

Ok, je laisse ça de côté.

#10 - 07 septembre 2020 15:23 - Paul Marillonnet

- Assigné à Paul Marillonnet supprimé

#11 - 07 septembre 2020 15:25 - Frédéric Péters

Pour quelqu'un·e qui repasserait ici dans plusieurs mois, si ça va vite pour l'écrire, il manque quoi dans ton patch par rapport à la description du ticket ?

(mais si c'est le ticket en lui-même qui n'a aucun intérêt, rejetons-le plutôt, non ?).

#12 - 07 septembre 2020 15:34 - Paul Marillonnet

Frédéric Péters a écrit :

> Pour quelqu'un·e qui repasserait ici dans plusieurs mois, si ça va vite pour l'écrire, il manque quoi dans ton patch par rapport à la description du ticket ?

Des règles de spécifiques de présence de certains paramètres dans la requête au sens OAuth et/ou dans le JWT, et la syntaxe du paramètre claims qui permet de déclarer le caractère essentiel ou non des revendications.

> (mais si c'est le ticket en lui-même qui n'a aucun intérêt, rejetons-le plutôt, non ?).

J'ai l'impression qu'on peut rejeter, oui.

#13 - 08 septembre 2020 10:47 - Benjamin Dauvergne

- Assigné à mis à Paul Marillonnet

Frédéric Péters a écrit :

> Pour quelqu'un·e qui repasserait ici dans plusieurs mois, si ça va vite pour l'écrire, il manque quoi dans ton patch par rapport à la description du ticket ?
>
> (mais si c'est le ticket en lui-même qui n'a aucun intérêt, rejetons-le plutôt, non ?).

Je me rends compte que j'ai du l'écrire sur un autre ticket : ça n'a aucune intérêt actuellement parce que je ne connais pas un seul client OIDC qui émette des requêtes signées (ce qui ne veut pas dire qu'aucune lib pour implémenter OIDC ne le gère, il y en a certainement, mais la fonctionnalité n'est vraiment pas courante voir invisible dans les faits, ce qui n'est pas le cas coté SAML pour les requêtes signées ou chiffrées (ça n'est pas courant mais ça arrive régulièrement quand on se confronte à des implémentations exotiques ou configurées exotiquement par exemple Shibboleth).

#14 - 08 septembre 2020 15:39 - Benjamin Dauvergne

- Assigné à Paul Marillonnet supprimé

Fichiers

0001-auth_oidc-support-signed-authz-requests-through-jwt-.patch	17,5 ko	22 juillet 2020	Paul Marillonnet