Authentic 2 - Development #26253

Fournisseur OIDC : support des signatures ECDSA

08 septembre 2018 16:11 - Paul Marillonnet

Statut:	Fermé	**Début:**	08 septembre 2018
Priorité:	Bas	**Echéance:**	
Assigné à:	Paul Marillonnet	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

En particulier l'algo ES256, qui apparaît en 'Recommended+' dans la RFC.
(cf https://tools.ietf.org/html/rfc7518#section-3)

Demandes liées:

Lié à Authentic 2 - Development #31862: authn OIDC : vérifier la signature de...	**Fermé**	**29 mars 2019**

Révisions associées

Révision ab59ef13 - 10 avril 2020 14:51 - Paul Marillonnet

idp_oidc: add ecdsa support (#26253)

Historique

#1 - 11 septembre 2018 17:04 - Benjamin Dauvergne

Oui ce serait bien, les clés sont plus courtes (mais sinon on s'en fout un peu, le mode HMAC est 100x plus simple à utiliser et dans l'absolu bien plus rapide).

#2 - 11 septembre 2018 17:13 - Paul Marillonnet

- Assigné à mis à Paul Marillonnet

- Priorité changé de Normal à Bas

#3 - 08 novembre 2018 14:41 - Benjamin Dauvergne

- Tracker changé de Support à Development

#4 - 29 mars 2019 18:19 - Paul Marillonnet

- Fichier 0001-WIP-oidc-support-ec-signature-for-rp-and-idp-modules.patch ajouté

- Statut changé de Nouveau à En cours

Un patch WIP pour donner une idée de l'allure que prennent les choses.
Le patch concerne à la fois les modules IdP et RP (je découperai en deux patches pour la relecture).
Pour l'instant seul la partie IdP est testée. Je reviens dès que j'ai les tests pour la partie RP.

#5 - 29 mars 2019 18:37 - Paul Marillonnet

- Lié à Development #31862: authn OIDC : vérifier la signature de l'ID Token reçu ajouté

#6 - 09 avril 2020 09:51 - Paul Marillonnet

- Fichier 0001-idp_oidc-add-ecdsa-support-26253.patch ajouté

- Statut changé de En cours à Solution proposée

- Patch proposed changé de Non à Oui

#7 - 09 avril 2020 10:52 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

#8 - 10 avril 2020 14:58 - Paul Marillonnet

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

```
commit ab59ef131294808a9d1ef59327ed924d91af00b9
Author: Paul Marillonnet <pmarillonnet@entrouvert.com>
Date:   Sat Apr 4 10:35:02 2020 +0200

    idp_oidc: add ecdsa support (#26253)
```

#9 - 17 avril 2020 15:16 - Frédéric Péters

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

Fichiers

0001-WIP-oidc-support-ec-signature-for-rp-and-idp-modules.patch	9,67 ko	29 mars 2019	Paul Marillonnet
0001-idp_oidc-add-ecdsa-support-26253.patch	9,99 ko	09 avril 2020	Paul Marillonnet