Authentic 2 - Support #36965

auth_oidc : prise en charge des ID Tokens chiffrés

15 octobre 2019 18:05 - Paul Marillonnet

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

Description

Avec des informations supplémentaires lors de l'enregistrement d'un fournisseur, dans le même esprit que pour la signature : déclarer des algos de chiffrement supportés par le fournisseur, et ajouter les clés publiques de déchiffrement au jwks de l'objet de fournisseur distant dans les modèles.

Idéalement, refuser tout ID Token en clair lorsque le fournisseur associé a été enregistré comme envoyant des jetons chiffrés (Cf les spécs[1] : "If encryption was negotiated with the OP at Registration time and the ID Token is not encrypted, the RP SHOULD reject it.")

[1] https://openid.net/specs/openid-connect-core-1_0.html#IDTokenValidation

Historique

#1 - 15 octobre 2019 18:08 - Paul Marillonnet

- Statut changé de Nouveau à Information nécessaire

- Assigné à mis à Paul Marillonnet

Je vais relire la doc pour comprendre si un fournisseur qui chiffre ses jetons attend aussi nécessairement qu'on présente un jeton d'accès chiffré lors de l'appel à l'endpoint UserInfo. Auquel cas ça complique un peu l'affaire.

#2 - 15 octobre 2019 18:13 - Benjamin Dauvergne

- Priorité changé de Normal à Bas

Pour l'instant je n'ai jamais croisé de JWT chiffré (OIDC imposant TLS c'est rare, mais ça pourrait servir pour les utiliser comme jeton vraiment opaque, encore que... comme c'est signé à destination du RP un IDtoken retourné à l'OP ne pourra pas être déchiffré, même avec un chiffrement symétrique, à moins que le destinataire soit dans l'entête, bon c'est un peu flou pour moi).