Authentic 2 - Development #61130

protéger les jetons signing.dumps() en confidentialité

26 janvier 2022 16:29 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	26 janvier 2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Ça fait écho à #60624, nos jetons sont protégés en intégrité mais pas en confidentialité, ça ne coûte rien d'ajouter le chiffrement AES implémenté dans a2 par dessus.

Révisions associées

Révision 2d93d95f - 04 février 2022 10:13 - Benjamin Dauvergne

misc: move authentic2.crypto to authentic2.utils.crypto (#61130)

Révision 0795cbeb - 04 février 2022 10:13 - Benjamin Dauvergne

utils: add dumps/loads for confidentiality protected tokens (#61130)

Révision f72d1d3b - 04 février 2022 10:13 - Benjamin Dauvergne

misc: use new signing.dumps/loads implementation (#61130)

Historique

#1 - 26 janvier 2022 22:01 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#2 - 26 janvier 2022 22:01 - Benjamin Dauvergne

- Fichier 0002-misc-use-new-signing.dumps-loads-implementation-6113.patch ajouté

- Fichier 0001-utils-add-dumps-loads-for-confidentiality-protected-.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#3 - 26 janvier 2022 22:01 - Benjamin Dauvergne

J'ai fait en sorte que ça ressemble à la sortie de signing.dumps() pour ne pas casser les regexp du routage d'URL, du base64url séparé par des caractères ':'.

#4 - 27 janvier 2022 08:01 - Frédéric Péters

Comme pylint pointe de ce côté je serais pour un commentaire sur le src/authentic2/crypto.py pointant que tout est importé dans un module là pour compatibilité avec les imports existants.

J'aurais aussi séparé "déplacer le ficher" et "ajouter des méthodes dedans".

#5 - 27 janvier 2022 08:02 - Frédéric Péters

- Statut changé de Solution proposée à En cours

(mais même en ne divisant pas le commit ça m'irait, après les corrections pylint).

#6 - 27 janvier 2022 08:40 - Benjamin Dauvergne

- Fichier 0002-utils-add-dumps-loads-for-confidentiality-protected-.patch ajouté

- Fichier 0001-misc-move-authentic2.crypto-to-authentic2.utils.cryp.patch ajouté

- Fichier 0003-misc-use-new-signing.dumps-loads-implementation-6113.patch ajouté

- Statut changé de En cours à Solution proposée

Ok.

#7 - 03 février 2022 14:52 - Paul Marillonnet

- Statut changé de Solution proposée à Solution validée

Nickel, rien à redire, d'accord avec le découpage des commits de cette nouvelle version.

Si on peut juste retirer l'octet en trop dans le commentaire de 0001 (et donc le plagiat inintentionnel au connecteur cryptor de passerelle) qui me perturbe, c'est bon pour moi !

#8 - 04 février 2022 10:13 - Benjamin Dauvergne

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

```
commit f72d1d3b2a02cff8c4a71558145f77b0261d1988
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Wed Jan 26 16:56:03 2022 +0100

    misc: use new signing.dumps/loads implementation (#61130)

commit 0795cbeb8962a45f1303a8cde67ba2cc5ce21839
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Wed Jan 26 16:48:20 2022 +0100

    utils: add dumps/loads for confidentiality protected tokens (#61130)

commit 2d93d95fc5e270728cdaab795751f1374b22515a
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Thu Jan 27 08:27:38 2022 +0100

    misc: move authentic2.crypto to authentic2.utils.crypto (#61130)
```

#9 - 05 février 2022 15:16 - Transition automatique

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

#10 - 10 avril 2022 04:42 - Transition automatique

Automatic expiration

Fichiers

0002-misc-use-new-signing.dumps-loads-implementation-6113.patch	16,2 ko	26 janvier 2022	Benjamin Dauvergne
0001-utils-add-dumps-loads-for-confidentiality-protected-.patch	18,2 ko	26 janvier 2022	Benjamin Dauvergne
0002-utils-add-dumps-loads-for-confidentiality-protected-.patch	5,29 ko	27 janvier 2022	Benjamin Dauvergne
0001-misc-move-authentic2.crypto-to-authentic2.utils.cryp.patch	15,8 ko	27 janvier 2022	Benjamin Dauvergne
0003-misc-use-new-signing.dumps-loads-implementation-6113.patch	16,2 ko	27 janvier 2022	Benjamin Dauvergne