Authentic 2 - Development #76858

Ne pas utiliser de signature de next_url quand c'est inutile, et limiter leur réutilisation quand c'est utile

21 avril 2023 00:53 - Benjamin Dauvergne

Statut:	Solution proposée	**Début:**	21 avril 2023
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

Dans le faits ça garantit juste que l'URL n'a pas été altéré et qu'elle provient bien de l'IdP:

- mais on peut réutiliser la paire next/next-signature sur une autre URL
- sans limitation dans le temps

Le mieux c'est ne de plus utiliser les signatures là ou c'est possible (jeton) et pour les autres cas de rendre la signature spécifique via un sel (continue et logout).

Demandes liées:

Lié à Authentic 2 - Development #76835: empêcher le contrôle des redirections...	**Solution proposée** 26 avril 2023

Historique

#1 - 21 avril 2023 00:53 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#2 - 21 avril 2023 08:13 - Robot Gitea

- Statut changé de Nouveau à En cours

Benjamin Dauvergne (bdauvergne) a ouvert une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/45
- Titre : WIP: Ne pas permettre la réutilisation des signature de next_url (#76858)
- Modifications : https://git.entrouvert.org/entrouvert/authentic/pulls/45/files

#3 - 21 avril 2023 09:05 - Benjamin Dauvergne

- Lié à Development #76835: empêcher le contrôle des redirections sur les mails d'enregistrement et de réinitialisation de mot de passe ajouté

#4 - 21 avril 2023 09:06 - Benjamin Dauvergne

Rebasé sur #76835.

#5 - 09 novembre 2023 19:59 - Robot Gitea

- Statut changé de En cours à Solution proposée

#6 - 09 novembre 2023 20:05 - Benjamin Dauvergne

- Sujet changé de Ne pas permettre la réutilisation des signature de next_url à Ne pas utiliser de signature de next_url quand c'est inutile, et limiter leur réutilisation quand c'est utile

- Description mis à jour

#7 - 09 novembre 2023 23:08 - Benjamin Dauvergne

Le test test_views_sms_ratelimit[phone-change] a l'air instable.