Authentic 2 - Development #65743

SLO OIDC : avec iss et sid, pourrait-on tenter le logout en "backchannel"

29 mai 2022 23:32 - Thomas Noël

Statut:	Rejeté	**Début:**	29 mai 2022
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

Actuellement le SLO se passe en frontoffice avec des iframe qui chargent des URLs.

Aujourd'hui ces URL contiennent les informations (iss/sid) qui permettent de retrouver la session à tuer.

Ne pourrait-on pas renforcer le logout en faisant en sorte que Authentic appelle lui-même ces URLs ? ("en backchannel")

Je dis "renforcer" parce que le chargement des iframe, surtout sur des domaines tiers, c'est mort.

Historique

#1 - 30 mai 2022 10:42 - Benjamin Dauvergne

Donc utiliser les URLs frontchannel pour du backchannel ? Oui pourquoi pas, mais il faudrait que ce soit optionnel parce que le frontchannel "classique" en iframe est utilisé à certains endroits où ça marche (parce que même domaine parent) et ensuite il y a une spec pour le backchannel qui bien sûr n'a aucun rapport (il faut placer iss, sid dans un json web-token et poster ça)[1].

[1]: https://openid.net/specs/openid-connect-backchannel-1_0.html

#3 - 30 mai 2022 12:25 - Thomas Noël

- Statut changé de Nouveau à Rejeté

Ok, je rejette, il faudrait plutôt implémenter https://openid.net/specs/openid-connect-backchannel-1_0.html

#4 - 30 mai 2022 12:41 - Benjamin Dauvergne

Pour moi la solution c'est d'implémenter frontchannel comme il faut, et de dire aux gens que si les cookies ne passent pas bien alors il faut se baser sur iss/sid, le faire en backchannel n'apporte rien de plus, si la notif via navigateur ne passe pas, le POST en backchannel peut lui aussi échouer pour diverses raisons (ça timeout, le réseau est tombé, whatever...). Comme la personne était encore sur le site du RP (SP en SAML) 2s avant, on peut penser qu'ouvrir une page dans une iframe dans son navigateur devrait marcher.