w.c.s. - Development #13177

restriction d'accès à des formulaires selon le mode d'authentification

14 septembre 2016 10:50 - Frédéric Péters

Statut:	Fermé	**Début:**	14 septembre 2016
Priorité:	Haut	**Echéance:**	
Assigné à:	Frédéric Péters	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	

Description

Aujourd'hui on peut restreindre l'accès à "utilisateurs connectés" mais c'est indépendant du type d'authentification, on voudrait pouvoir dire que pour telle démarche, il faut nécessairement s'être identifié par FranceConnect, ou par carte d'identité électronique.

Dans un premier temps ça s'imagine comme étant une série de choix supplémentaires, genre "Utilisateurs connectés via eID", mais ça gagnerait peut-être à être à côté, une série de cases à cocher supplémentaires.

```
----------------------------------
Rôles de l'utilisateur
----------------------------------

Sélectionner les rôles qui pourront accéder à ce formulaire.

 [ Agents traitants      | v ]
 [ ...                   | v ]
 <Ajouter un rôle>

Méthode d'authentification exigée
 [x] eID
 [ ] FranceConnect
```

Cette seconde partie ne s'afficherait évidemment pas quand il n'y a pas de méthodes d'authentification définies.

Mais ça parle ici uniquement de l'accès, mais si on veut appliquer ces restrictions à d'autres moments, genre l'agent pour refuser une demande doit nécessairement être connecté via eID, alors c'est sans doute plus raisonnable au niveau du code de mêler ça sous forme de rôles (pour profiter du "by" déjà présent dans les actions de workflow). Et alors on doit définir un fonctionnement particulier, un formulaire accessible à "Connecté FranceConnect" et "rôle: association", ça demanderait que les deux conditions soient remplies. (alors qu'autrement, c'est un "OU" entre les rôles).

Implications autour du "always_advertise", notamment on veut dans l'API préciser ce qui est nécessaire.

Implications au moment de l'accès à un formulaire auquel on n'a pas droit, page d'info et invitation à se reconnecter sur l'IdP (ForceAuthn=yes + méthode demandée) ?

Demandes liées:

Lié à Plugin FS FranceConnect - Development #13178: Définir un AuthnContext p...	**Nouveau**	**14 septembre 2016**

Révisions associées

Révision 0dc2a83e - 16 janvier 2017 15:39 - Frédéric Péters

general: allow marking form as required a given authentication context (#13177)

Historique

#2 - 14 septembre 2016 11:08 - Benjamin Dauvergne

- Lié à Development #13178: Définir un AuthnContext particulier ajouté

#3 - 16 décembre 2016 20:03 - Frédéric Péters

- Priorité changé de Normal à Haut

#4 - 02 janvier 2017 16:14 - Frédéric Péters

Et lors de l'accès à un formulaire restreint, avoir une page "Niveau d'authent supérieur nécessaire" + bouton "Se reconnecter avec %s" (FranceConnect / eID / etc.).

#5 - 02 janvier 2017 16:17 - Frédéric Péters

Alternativement, si niveau protocole ça ne tient pas dans les échanges avec Authentic, peut-être juste faire une case à cocher "authentication forte requise" et libre interprétation ensuite (le cas d'usage immédiat c'est de toute façon eid ou pas, le cas franceconnect ou ozwillo n'est pas vraiment réel).

#6 - 10 janvier 2017 11:06 - Frédéric Péters

- Fichier 0001-general-allow-marking-form-as-required-a-strong-auth.patch ajouté

- Assigné à mis à Frédéric Péters

- Patch proposed changé de Non à Oui

Voilà un plan minimal mis en place, pour ne pas trop exiger d'authentic, c'est se baser sur sur l'authn context qui est déjà présent dans l'assertion mais dans l'autre sens de simplement afficher un message avec un lien pour l'usager, qui lance un SSO avec ForceAuthn=true, et tant pis si l'usager décide côté authentic de ne pas suivre la méthode qu'on exige, il restera juste bloqué.

En évolution, w.c.s. pourra taper dans RequestedAuthnContext les méthodes souhaitées et il faudrait que les modules d'authentic puissent déclarer les authn context qu'ils prennent en charge, pour ne proposer que les modules pertinents, voire zapper la page de connexion si le module fait juste "proxy".

Côté paramétrage, il y a du côté de l'admin mettre dans le site-options.cfg une option auth-levels, qui prend la liste des authents autorisées, séparées par des virgules (ex: fedict,franceconnect). Il y a ensuite du côté du formulaire la boite de dialogue modifiée comme dans le mockup ascii de la description de ce ticket.

#7 - 10 janvier 2017 11:16 - Benjamin Dauvergne

Le if self.formdef.enable_tracking_codes and data: ressemble à un cavalier programmatique (j'essaie un néologisme informatique dérivé "cavalier législatif").

Ça me parait ok mais juste sur le nommage utiliser level alors qu'il n'y a pas vraiment de notion de niveau m'embête. Peut-être qu'on pourrait rester sur le terme contexte d'authentification et dire authentication_context.

#8 - 10 janvier 2017 11:36 - Frédéric Péters

> Le if self.formdef.enable_tracking_codes and data: ressemble à un cavalier programmatique (j'essaie un néologisme informatique dérivé "cavalier législatif").

En fait il assure que la page qui dit "faut une authent plus forte" n'affiche pas le pavé "code de suivi" (donc tout à fait à propos pour ce patch).

> Ça me parait ok mais juste sur le nommage utiliser level alors qu'il n'y a pas vraiment de notion de niveau m'embête. Peut-être qu'on pourrait rester sur le terme contexte d'authentification et dire authentication_context.

Ou laisser "context" à SAML et utiliser "method" ici ? Mais non parce que method c'est déjà utilisé pour faire la différence entre password et saml dans w.c.s.; je ne suis pas attaché à level mais je préférerais qu'on trouve un mot qui n'est pas utilisé ailleurs. (et si on ne trouve pas, alors va pour context).

#9 - 10 janvier 2017 11:54 - Benjamin Dauvergne

Frédéric Péters a écrit :

> > Le if self.formdef.enable_tracking_codes and data: ressemble à un cavalier programmatique (j'essaie un néologisme informatique dérivé "cavalier législatif").
>
> En fait il assure que la page qui dit "faut une authent plus forte" n'affiche pas le pavé "code de suivi" (donc tout à fait à propos pour ce patch).

Ok, je veux bien un commentaire.

> > Ça me parait ok mais juste sur le nommage utiliser level alors qu'il n'y a pas vraiment de notion de niveau m'embête. Peut-être qu'on pourrait rester sur le terme contexte d'authentification et dire authentication_context.
>
> Ou laisser "context" à SAML et utiliser "method" ici ? Mais non parce que method c'est déjà utilisé pour faire la différence entre password et saml dans w.c.s.; je ne suis pas attaché à level mais je préférerais qu'on trouve un mot qui n'est pas utilisé ailleurs. (et si on ne trouve pas, alors va pour context).

On va finir avec kind ou type et context me va bien, on aura authentication_context_saml et authentication_context, les deux correspondent à la même chose seule change la nomenclature.

#10 - 10 janvier 2017 14:55 - Frédéric Péters

- Fichier 0001-general-allow-marking-form-as-required-a-given-authe.patch ajouté

Va pour context alors; patch à jour. (cette modif + le commentaire suggéré).

Dans la phrase affichée à l'usager, j'ai par contre laissé "authentication level", pour qu'à la traduction on évite un "contexte" qui fait un peu trop technique à mon goût.

#11 - 10 janvier 2017 19:23 - Frédéric Péters

- Fichier 0001-general-allow-marking-form-as-required-a-given-authe.patch ajouté

Avec l'ajout dans la vue du formulaire de l'info sur les contextes demandés.

#12 - 16 janvier 2017 15:38 - Thomas Noël

Ack.

#13 - 16 janvier 2017 15:40 - Frédéric Péters

- Statut changé de Nouveau à Résolu (à déployer)

```
commit 0dc2a83e475c6e4a1af68e90290758132debdef5
Author: Frédéric Péters <fpeters@entrouvert.com>
Date:   Tue Jan 10 10:52:40 2017 +0100

    general: allow marking form as required a given authentication context (#13177)
```

#15 - 23 décembre 2018 14:52 - Frédéric Péters

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

Fichiers

0001-general-allow-marking-form-as-required-a-strong-auth.patch	15,1 ko	10 janvier 2017	Frédéric Péters
0001-general-allow-marking-form-as-required-a-given-authe.patch	15,4 ko	10 janvier 2017	Frédéric Péters
0001-general-allow-marking-form-as-required-a-given-authe.patch	16,5 ko	10 janvier 2017	Frédéric Péters