Authentic 2 - Development #32372

Gestion des niveaux d'authentification dans le SAML

16 avril 2019 11:58 - Valentin Deniaud

Statut:	Fermé	**Début:**	16 avril 2019
Priorité:	Normal	**Echéance:**	
Assigné à:	Valentin Deniaud	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Mécanique qui doit permettre aux SP de pouvoir gérer l'authentification multifacteur en demandant/recevant un niveau d'authentification spécifique via les assertions SAML.

Ce ticket s'appuie sur et est la suite du gros ticket a2 #32007.

Ticket relié à trois autres (j'ajouterai les liens quand ils seront publiés) :
- Envoi des niveaux d'auth des rôles via le provisionning dans hobo (#32381)
- Gestion symmétrique du SAML dans mellon (#32376)
- Exemple concret d'intégration dans Chrono (#32379)

Ces quatre tickets mis ensembles, voilà un exemple de ce qui marche :
- Créer deux agendas et deux roles.
- Mettre role de visualisation de agenda 1 à role 1 (resp 2).
- Mettre role 2 niveau 2.
- Mettre role 1 et role 2 à un utilisateur.
- Sur le /manage/ de chrono, l'utilisateur peut voir les deux agendas.
- L'utilisateur peut cliquer sur agenda 1 et le voir.
- Quand il clique sur agenda 2, il est redirigé vers a2 pour une montée d'auth, puis il peut voir l'agenda.

(n'est pas encore géré le cas superuser (aka rôle administrateur), mais je vois comment faire et c'est pas très compliqué)

À part ça il y a plein de choses à dire sur l'approche de ce ticket, qui n'est pas hyper sexy.

Comportement attendu : actuellement une brique reçoit des rôles via le provisionning hobo, et les associe à des actions autorisées. Lorsqu'un utilisateur veut faire une action, c'est à la brique de vérifier si il a le rôle qui autorise cette action. Pour introduire le multifacteur, on associe un niveau d'authentification requis à un rôle, qui est connu de la brique via ce même provisionning. Donc en plus de la vérification précédente, une brique va devoir vérifier que le niveau d'authentification de l'utilisateur courant lui donne le droit de faire usage d'un rôle, et sinon demander à a2 une montée d'auth.

Contraintes et prérequis à avoir en tête (pas gravés dans le marbre non plus) :
1. La norme SAML ne dit rien sur le concept de niveau d'authentification, et ne prévoit pas vraiment qu'il y en ait.
2. Comme un niveau dit quelque chose sur l'authentification d'un utilisateur, on doit l'envoyer dans l'attribut AuthnContext de l'assertion SAML (et pas dans une extension random). À fortiori on doit utiliser le sous attribut AuthnContextClassRef, dans lequel on a le droit de mettre une et une seule URI qui va contenir le niveau.
3. On utilise déjà, quoique mollement, l'attribut AuthnContextClassRef pour parler de la méthode d'authentification utilisée (genre password ou certificat SSL).

Idée 1 : on envoie à la fois la méthode d'authentification et le rôle associé dans l'assertion. C'est propre. C'est aussi impossible, voir le point 2 ci-dessus et la mention « une et une seule URI ».

Idée 2 : on envoie pas les niveaux, mais toujours la méthode d'authentification. L'avantage c'est qu'on reste bien dans la norme, mais garder en tête le point 3 ci-dessus, à savoir que c'est une information dont on ne se sert pas au final. Ensuite le SP est responsable d'attribuer un niveau à cette méthode, et de faire sa tambouille. Premièrement, il faudrait mettre plein de code côté SP pour ces logiques d'associations, pour un résultat pas forcément plus propre. Mais le principal problème c'est qu'on a envie de faire l'association méthode/niveau d'auth côté a2, pour centraliser la conf. Donc il faudrait rajouter du provisionning, ça devient compliqué.

Idée 3 (l'heureuse élue) : on envoie la méthode d'authentification uniquement quand un utilisateur s'authentifie à proprement parler (ie passe de pas connecté à connecté, ce qui correspond implicitement à un niveau d'auth de 1). Quand il s'agit de transmettre l'info qu'un utilisateur a un niveau d'auth plus élevé, on envoie ce niveau via une URI à nous de la forme https://entrouvert.org/auth-level/{2,3,4,5}. Avantage, on ne modifie pas le comportement de base, et la logique à mettre en place est relativement simple. Inconvénient, on a un comportement un peu inconsistant, où on se sert d'un même attribut SAML pour envoyer

deux infos un peu différentes selon le contexte (méthode précise sans niveau, puis niveau sans méthode).

Voilà, on en est au stade PoC, il faudra peut-être passer par une PoC de l'idée 2 si la présente est jugée trop sale. Le mieux resterait qu'un gourou SAML ait une idée 4 qui soit grave mieux que celles présentées ici.

Demandes liées:

Lié à Authentic 2 - Development #32786: Authentification multi-facteurs	**Fermé**	**03 mai 2019**

Historique

#1 - 16 avril 2019 13:47 - Valentin Deniaud

- Fichier 0003-utils-record-auth-level-along-with-auth-event.patch ajouté

- Fichier 0004-idp_saml-send-authentication-level-in-SAML-assertion.patch ajouté

- Fichier 0002-auth_oath-record-auth-event-and-move-code-to-utils.patch ajouté

- Fichier 0001-idp_saml-remove-old-code.patch ajouté

- Fichier 0005-idp_saml-handle-authentication-level-increase-reques.patch ajouté

- Patch proposed changé de Non à Oui

#2 - 16 avril 2019 13:48 - Valentin Deniaud

- Tracker changé de Support à Development

#3 - 16 avril 2019 14:33 - Valentin Deniaud

- Description mis à jour

#4 - 23 avril 2019 11:29 - Valentin Deniaud

- Fichier 0007-attributes_ng-limit-user-roles-depending-on-authenti.patch ajouté

- Fichier 0003-auth_oath-record-auth-event-and-move-code-to-utils.patch ajouté

- Fichier 0002-idp_saml-remove-old-code.patch ajouté

- Fichier 0005-idp_saml-send-authentication-level-in-SAML-assertion.patch ajouté

- Fichier 0001-fixup-auth2_multifactor-add-OATH-authentication-fact.patch ajouté

- Fichier 0004-utils-record-auth-level-along-with-auth-event.patch ajouté

- Fichier 0006-idp_saml-handle-authentication-level-increase-reques.patch ajouté

#5 - 23 avril 2019 11:35 - Valentin Deniaud

Le patch 1 est en trop.

Le principal changement est dans le patch 7, le reste c'est juste de la proprification.

Sinon vu la tête que ça prend, il vaudra sûrement mieux ne pas introduire de concept de niveaux d'authentification dans le SAML, de continuer à envoyer juste l'URI de la méthode d'authentification, et d'avoir hobo qui centralise le mapping méthode d'auth <==> niveau.

#6 - 24 avril 2019 11:48 - Valentin Deniaud

- Fichier 0001-attributes_ng-limit-service-roles-depending-on-auth-.patch ajouté

- Statut changé de Nouveau à Solution proposée

#7 - 03 mai 2019 18:29 - Valentin Deniaud

- Lié à Development #32786: Authentification multi-facteurs ajouté

#8 - 16 mai 2019 14:02 - Benjamin Dauvergne

Ce code devient inutile, ce sont des demandes explicite d'avoir des UUIDs de rôles qu'il faut gérer (les détails technique peuvent être réutiliser par contre, c'est peu ou prou les mêmes endroits qui doivent être modifiés coté A2).

#9 - 05 juin 2019 14:36 - Valentin Deniaud

- Statut changé de Solution proposée à Fermé

La nouvelle approche est dans #33708.

Fichiers

0003-utils-record-auth-level-along-with-auth-event.patch	1,82 ko	16 avril 2019	Valentin Deniaud
0004-idp_saml-send-authentication-level-in-SAML-assertion.patch	2,82 ko	16 avril 2019	Valentin Deniaud
0002-auth_oath-record-auth-event-and-move-code-to-utils.patch	1,89 ko	16 avril 2019	Valentin Deniaud
0001-idp_saml-remove-old-code.patch	1,02 ko	16 avril 2019	Valentin Deniaud
0005-idp_saml-handle-authentication-level-increase-reques.patch	4,01 ko	16 avril 2019	Valentin Deniaud
0007-attributes_ng-limit-user-roles-depending-on-authenti.patch	1,19 ko	23 avril 2019	Valentin Deniaud
0003-auth_oath-record-auth-event-and-move-code-to-utils.patch	1,89 ko	23 avril 2019	Valentin Deniaud
0002-idp_saml-remove-old-code.patch	1,02 ko	23 avril 2019	Valentin Deniaud
0005-idp_saml-send-authentication-level-in-SAML-assertion.patch	3,58 ko	23 avril 2019	Valentin Deniaud
0001-fixup-auth2_multifactor-add-OATH-authentication-fact.patch	1000 octets	23 avril 2019	Valentin Deniaud
0004-utils-record-auth-level-along-with-auth-event.patch	1,82 ko	23 avril 2019	Valentin Deniaud
0006-idp_saml-handle-authentication-level-increase-reques.patch	3,52 ko	23 avril 2019	Valentin Deniaud
0001-attributes_ng-limit-service-roles-depending-on-auth-.patch	1,1 ko	24 avril 2019	Valentin Deniaud