Hobo - Development #43121

saml : générer des clés 2048 bits

20 mai 2020 02:13 - Thomas Noël

Statut:	Fermé	**Début:**	20 mai 2020
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Actuellement (hobo/agent/common/management/commands/hobo_deploy.py) on fait :

- KEY_SIZE = 1024
- DAYS = 3652

Révisions associées

Révision e9506e6f - 17 juillet 2020 07:24 - Thomas Noël

hobo_deploy: increase SAML keys size from 1024 to 2048 bits (#43121)

Historique

#2 - 20 mai 2020 09:25 - Benjamin Dauvergne

On va juste monter à 2048; ça sort d'où ce 4096 ?

Je cite l'ANSSI :

> Pour une protection des communications jusqu'en 2030, les clés RSA doivent avoir une taille minimale de 2048 bits, et les clés ECDSA doivent avoir une taille min-imale de 256 bits. Pour ECDSA, les courbes éprouvées retenues sontsecp256r1,secp384r1,secp521r1, ainsi quebrainpoolP256r1,brainpoolP384r1etbrainpoolP512r1. Pour RSA, l'exposant de la clé publique doit être supérieur ouégal à216+ 1.

#3 - 20 mai 2020 09:34 - Benjamin Dauvergne

Pour les performances c'est à la fois négligeable comme souvent la crypto, et beaucoup plus lent :

```
$ openssl speed rsa2048 rsa4096
                  sign    verify    sign/s verify/s
rsa 2048 bits 0.000781s 0.000024s   1280.6  42466.3
rsa 4096 bits 0.005391s 0.000085s    185.5  11827.4
```

#5 - 16 juin 2020 11:57 - Thomas Noël

- Sujet changé de saml : générer des clés 4096 bits à saml : générer des clés 2048 bits

#6 - 17 juin 2020 17:58 - Thomas Noël

- Fichier 0001-hobo_deploy-increase-SAML-keys-size-from-1024-to-204.patch ajouté

- Statut changé de Nouveau à Solution validée

- Patch proposed changé de Non à Oui

#8 - 17 juillet 2020 07:24 - Frédéric Péters

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

```
commit e9506e6fd0d6e6d3ba5891190b2e1214ff3c81c0
Author: Thomas NOEL <tnoel@entrouvert.com>
Date:   Wed Jun 17 17:56:56 2020 +0200

    hobo_deploy: increase SAML keys size from 1024 to 2048 bits (#43121)
```

#9 - 17 juillet 2020 12:16 - Frédéric Péters

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

Fichiers

0001-hobo_deploy-increase-SAML-keys-size-from-1024-to-204.patch	902 octets	17 juin 2020	Thomas Noël