KeePass

Utilisation combinée avec une YubiKey

Objectif

Vous utilisez le logiciel Keepass et vous souhaitez simplifier l'ouverture de la base de données , jusque-là réalisée avec un mot de passe fort et peut être un peu long à taper.
Keepass se charge de mémoriser tous vos mots de passe, nous allons voir comme échapper au dernier mot passe restant : celui qui ouvre la base de données.

La configuration qui est présentée ici est prévue pour un système windows, elle a également été testé avec succès sur linux (ubuntu 18.04)

Prérequis

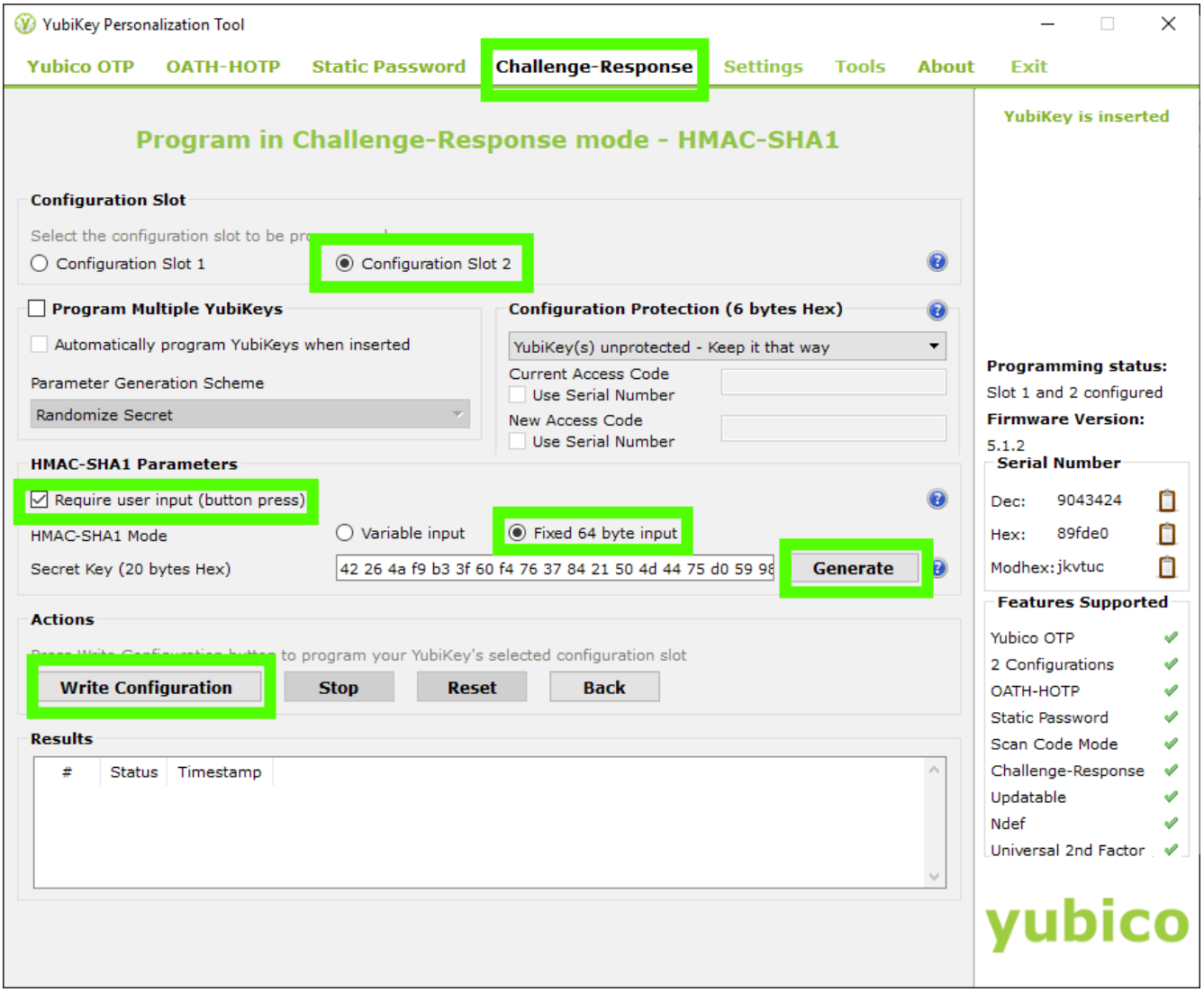
Pour cela vous devez disposer d'une yubikey.
https://www.yubico.com/

Différents modèles existent, entre 20 et 50€. Cette documentation a été testée avec une Yubikey 5 NFC.

Configuration de la Yubikey

Pour configurer votre Yubikey vous avez besoin du logiciel YubiKeyManager.
https://www.yubico.com/products/services-software/download/yubikey-manager/
Procédez à l'installation.

Allez dans le menu « Challange-Response » et paramétrez votre clé comme ceci :



- Choisir le Solt 2 qui est par défaut non-utilisé sur la yubikey et qui est compatible avec le plugin keepass qui sera installé par la suite
- (conseillé mais facultatif) cocher « button press ». Cela oblige l'utilisateur à appuyer sur la yubikey pour ouvrir keepass. Pour un utilisateur qui laisse sa clé dans le lecteur, cela évite qu'un malware n'utilise la yubikey, il ne pourra pas appuyer sur le bouton.
- Taille fixe
- générer un secret qui sera partagé avec KeePass
- écrire la configuration

Sauvegarde

Il est important à cette étape d'imprimer le **« Secret Key (20 bytes Hex) »** (42 26 4a f9 … sur l'image précédente) et de conserver ce papier à un endroit sûr. Il vous permettra d'accéder à Keepass en cas de perte de la yubikey.

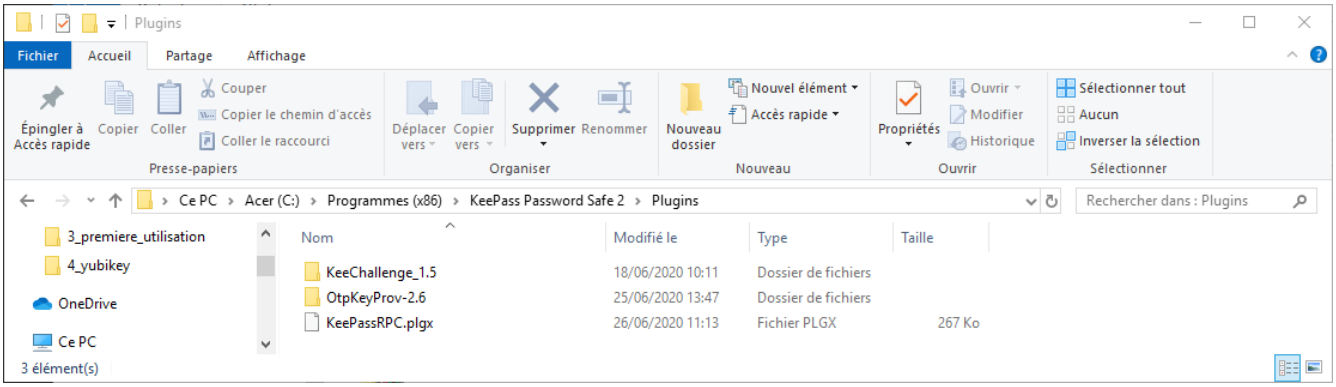
Installation du plugin Keepass

Le plugin a utilisé est « KeeChallange ». Il est disponible à cette adresse :

http://richardbenjaminrush.com/keechallenge/

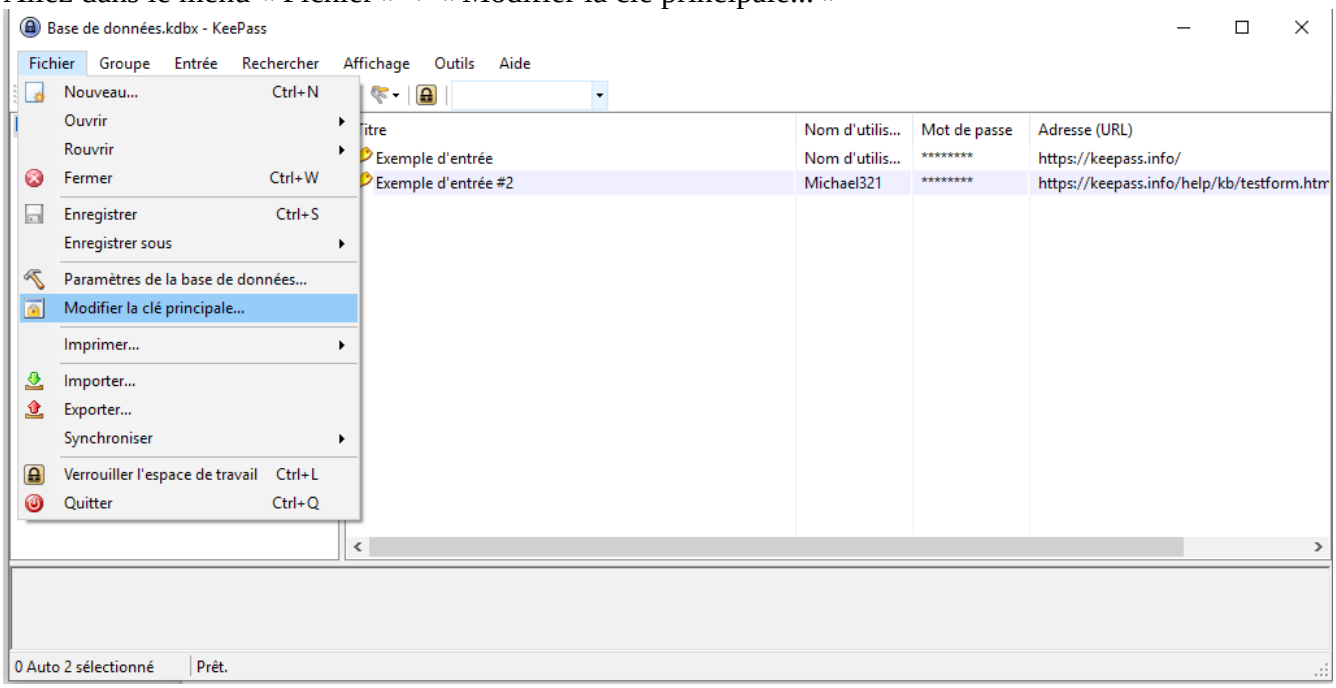
Pour l'installer il vous suffit de le télécharger, de le déziper et de placer le contenu dézipé de cette archive dans le répertoire Plugins du dossier d'installation de KeePass. Par exemple :

C:\Program Files (x86)\KeePass Password Safe 2\Plugins



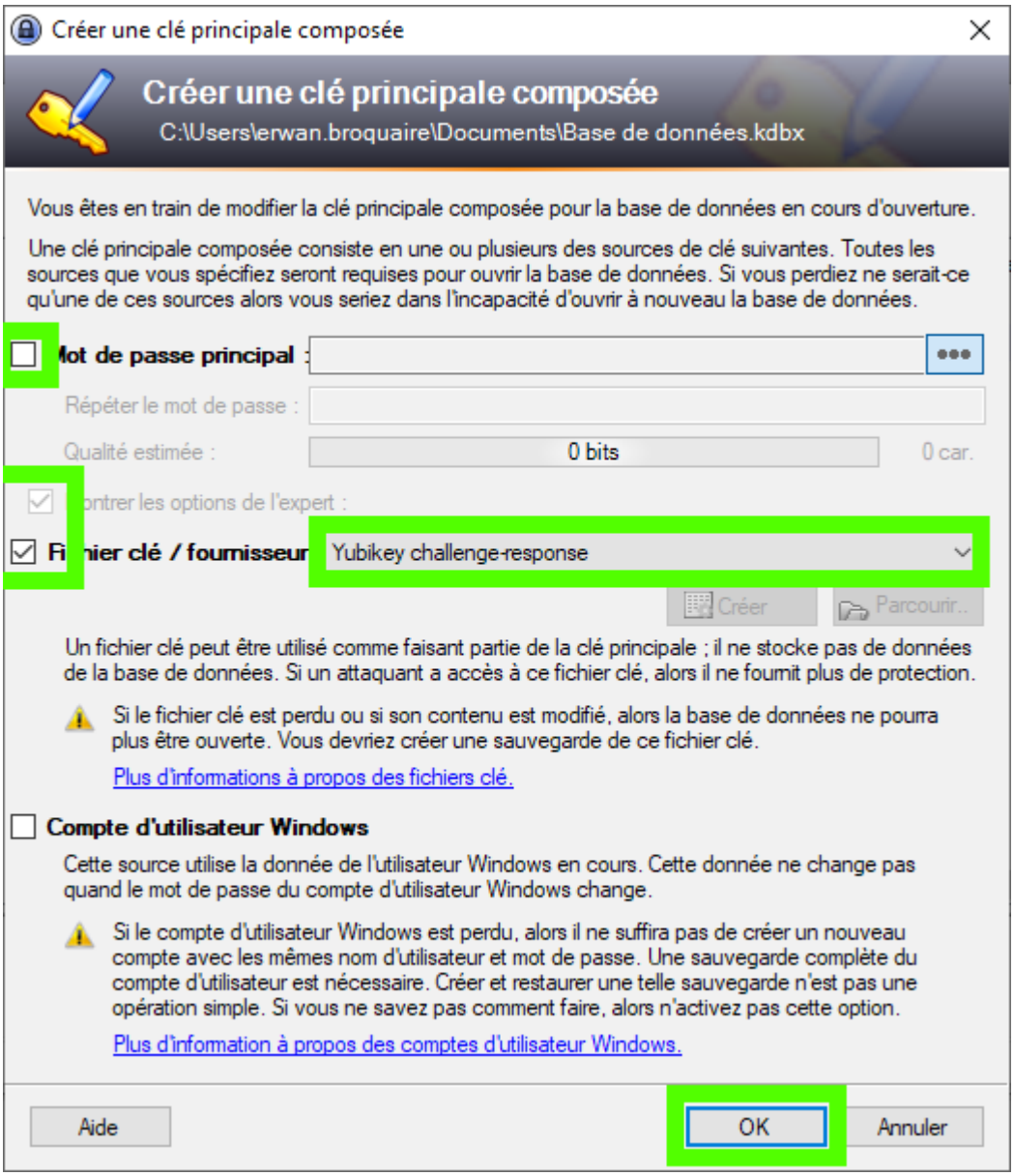
Configuration de Keepass

Ouvrez la base de données que vous voulez configurer avec votre yubikey.
Allez dans le menu « Fichier » → « Modifier la clé principale... »

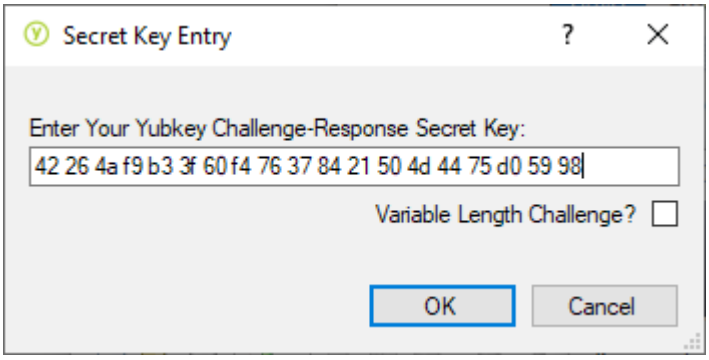


Décochez la case « Mot de passe principale »
Cochez les cases « montrer les options de l'expert » et « fournisseur »
Selectionnez « Yubikey challange-response » dans le menu déroulant
Cliquez sur ok.

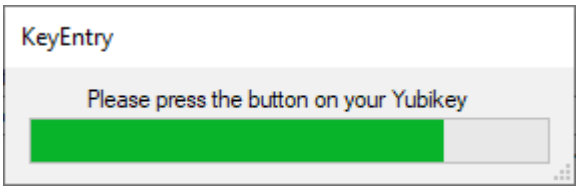
Remarque : si « Yubikey challange-response » n'apparait pas dans le menu déroulant, c'est qu'il y a eu un problème lors de l'installation du plugin.



Renseignez la clé secrète générée par votre Yubikey.



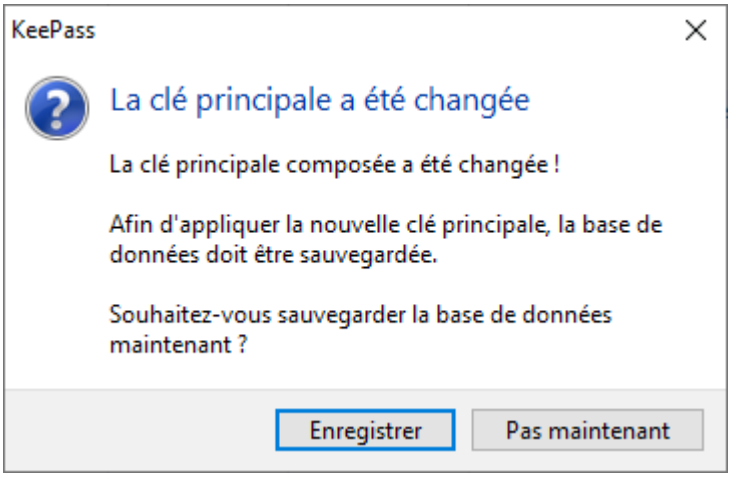
Keepass vous invite alors à toucher le bouton de votre yubikey



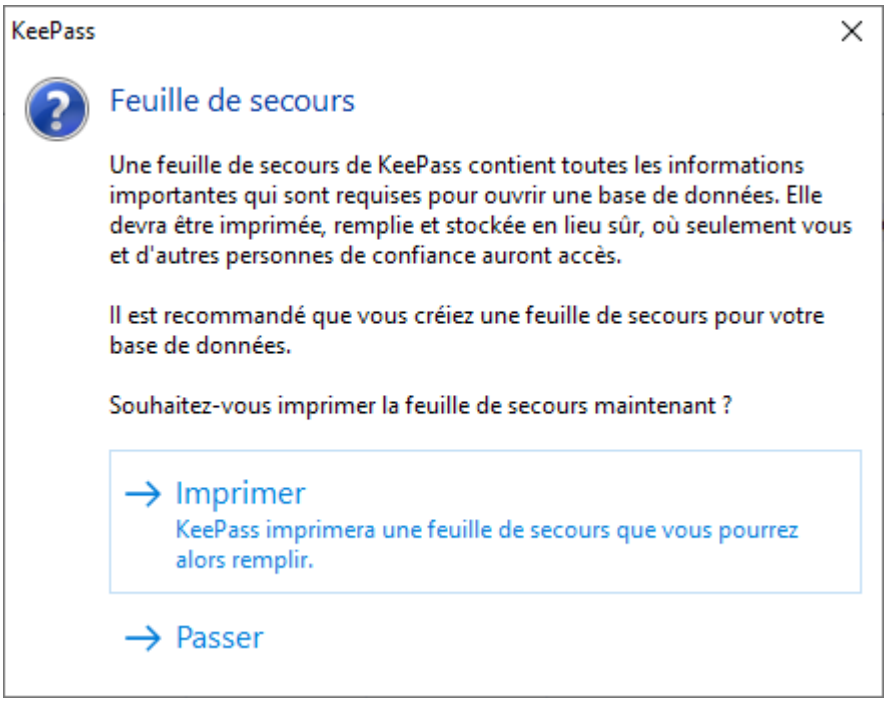
Faites-le.

Si le secret a été correctement renseigné[1], vous obtenez un message de confirmation :

1 Si vous êtes sûr que la clé a été correctement renseigné, mais que le problème persiste, reportez-vous au chapitre « problème possible avec la yubikey »



Vous êtes invité à enregistrer votre base de données et à imprimer une page de secours, elle contient le secret partagé. Imprimez là si vous ne l'avez pas déjà fait lors de la configuration de la Yubikey.

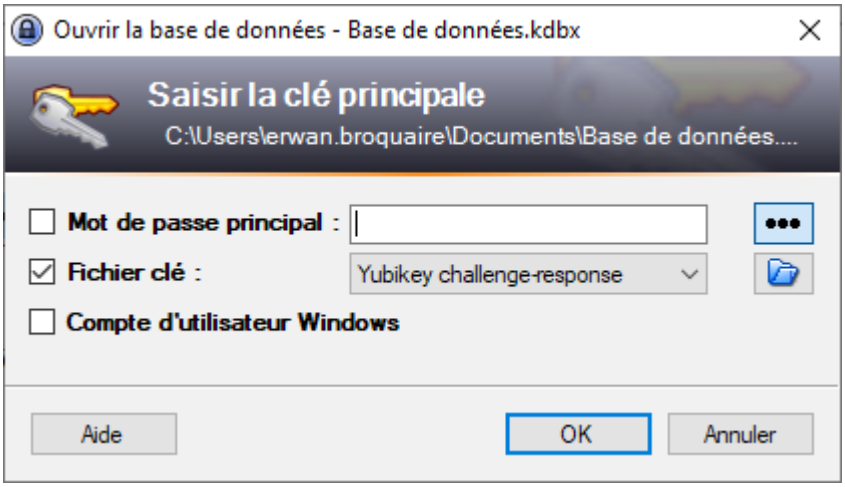


Félicitation, votre base de données Keepass est configurée pour s'ouvrir avec une simple pression sur votre Yubikey !

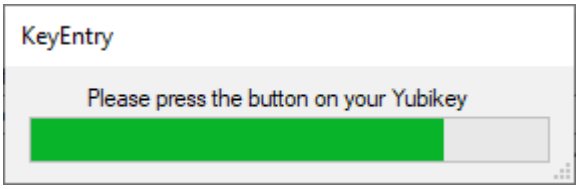
Ouverture de Keepass

À l'ouverture de Keepass, « mot de passe principal » doit être décoché.

Il faut cocher à la place « Fichier de clé » et sélectionner « Yubikey challange-response »



Keepass vous invite alors à toucher le bouton de votre yubikey



Faites-le.

Félicitation, votre base de données s’ouvre maintenant sans avoir à taper de mot de passe !

Fichier XML

Vous avez maintenant deux fichiers :

- Base de données.kdbx

- Base de données.xml

Ces deux fichiers sont liés, ils doivent tous deux être présents dans le même dossier pour ouvrir la base de données.

Pensez à sauvegarder les deux et à emporter les deux avec vous lors de vos déplacements.

Problème possible avec Yubikey

La yubikey est reconnue par votre ordinateur comme un clavier. Elle fonctionne en envoyant au système des codes qui correspondent à des touches qui seraient frappées au clavier. Il est donc possible que vous ayaez des problèmes avec l'interprétation de ces codes, comme c'est le cas entre un clavier AZERTY et un clavier QWERTY.

Pour que votre yubikey soit reconnu comme un clavier AZERTY et donc naturellement compatible avec votre système, il faut utiliser l'outil yubikey-personalization en ligne de commande.

Cet outil est disponible à cette adresse :

https://www.yubico.com/products/services-software/download/yubikey-personalization-tools/

Téléchargez et dézippez l'outil en ligne de commande.

Ouvrez un terminal.

Placez-vous dans le dossier dézippé contenant l'outil en ligne de commande.

Tapez la commande suivante :

ykpersonalize.exe -S06050708090a0b0c0d0e0f1115171819868587888 98a8b8c8d8e8f9195979899a79e9fa0a1a2a3a4a5a6382b28

Remarque 1 : L'explication détaillée de cette manipulation est décrite dans « option3 » du lien suivant :

https://www.yubico.com/blog/yubikey-keyboard-layouts/

Remarque 2 : Pour une installation sous linux, le paquet suivant sera également nécessaire :

sudo apt-get install libtool