Fiches Informatique & Numérique - Fonctions avancées

*André Laurens - **Café'in Numérique** - v2 - février 2024*

Gestion des mots de passe

L'utilisation d'applications web ou mobile - qu'il s'agisse de communiquer, d'effectuer des démarches administratives ou des achats en ligne, d'accéder à des contenus divers ou à des services associatifs - s'accompagne de plus en plus systématiquement de l'ouverture d'un compte utilisateur ou client, et d'une procédure d'authentification avec identificateur et mot de passe pour accéder au service.

Tant qu'il y en avait peu, on pouvait espérer les retenir. Au-delà de la dizaine, c'est mission impossible pour la plupart des gens, même en employant des martingales ou autres moyens mnémotechniques. Il faut donc les noter quelque part.

Le propos de cette fiche est de faire un point sur la question.

Règles de base et principe de la solution

Dans le contexte actuel ou le piratage et la captation d'information personnelles sont monnaie courantes, disons tout de suite ce qu'il ne faut pas faire en la matière :

- utiliser le même mot de passe partout, ou des mots de passe trop simples,
- noter les mots de passe sur un *post-it*, une feuille de papier, un carnet, tous supports que l'on peut perdre, se faire voler, et qu'on n'a pas forcément sous la main tout le temps.

> *Pour de bons mots de passe, voir ci-après :*
>
> - *les conseils de la CNIL : https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe*
> - *ceux du gouvernement : https://www.economie.gouv.fr/particuliers/creer-mot-passe-securise*

Pour pouvoir gérer de nombreux comptes, il existe depuis assez longtemps des logiciels de stockage des identificateurs et mots de passe, plutôt orientés ordinateur. Leur principe, rappelé plus bas, est de stocker les informations dans une base de données cryptée, stockée sur l'ordinateur.

Avec le développement des terminaux mobiles, il faut adapter ces solutions à un usage nomade, pour avoir accès à ses mots de passe n'importe où.

La solution la plus rapide à mettre en œuvre, et de ce fait très tentante, est d'utiliser le service qui vient avec l'*operating system*, et donc confier ces données personnelles à Google ou Apple. Autant dire que l'on fait entrer le loup dans la bergerie.

C'est pourquoi, la présente fiche se concentre sur les logiciels libres et décrit :

- comment faire une gestion "nomade" des mots de passe,
- i.e. y accéder depuis toutes plateformes : ordinateur (Win, MacOS, Linux) et mobiles (Android, iOS),
- sans offrir sur un plateau toute sa vie privée aux GAFAM.

Offre en logiciels libres

Les KeePass*

Nom	OS	Commentaires	Test	Fiche
KeePass	GNU/Linux, BSD, Mac OS	Logiciel Windows à l'origine,	utilisé sous Windows : OK	https://fra

Nom	OS	Commentaires	Test	Fiche
	X, Windows, Android	multiplateforme aujourd'hui		malibre.org/content/keepass
KeePassX	GNU/Linux, Mac OS X, Windows, Android	A l'origine, portage Linux de KeePass, logiciel Windows ; les deux sont multiplateforme aujourd'hui	utilisé sous Linux : OK	https://framalibre.org/content/keepassx
KeePassXC	GNU/Linux, Mac OS X, Windows	Fork communautaire de KeePassX pour pallier au développement très lent de KeePassX	testé sous Linux et Windows : OK	https://framalibre.org/content/keepassxc
KeePassDX	Android	Gestionnaire de fichiers KeePass multiformats, compatible avec la majorité des programmes alternatifs (KeePass, KeePassX, KeePassXC...)	testé sur mobile Android : OK (avec quelques limitations indiquées plus bas)	https://framalibre.org/content/keepassdx
KeePassDroid	Android	Portage sous Android du logiciel KeePass	testé sur mobile Android : OK (mêmes limitations que KeePassDX)	https://framalibre.org/content/keepassdroid

Les autres

Nom	OS	Commentaires	Test	Fiche
KeeWeb	GNU/Linux, Mac OS X, Windows, Android + app web	cf. description détaillée plus bas	testé l'appli desktop sous Linux, l'appli web sous Linux et sur mobile Android	https://framalibre.org/content/keeweb ; site officiel : https://keeweb.info/
LessPass	GNU/Linux, Mac OS X, Windows, Android, FirefoxOS	ne stocke pas les mots de passe mais permet de générer des mots de passe uniques pour chaque service, et de les régénérer à l'identique à la prochaine visite, à partir d'un mot de passe principal	non testé, a paru plus orienté *geek* qu'utilisateur lambda	https://framalibre.org/content/lesspass
Passbolt	GNU/Linux, BSD, Mac OS X, Windows	Gestionnaire de mots de passe libre conçu pour la coopération, permet aux membres d'une équipe de stocker et partager leurs mots de passe de manière sécurisée, et d'être intégré à un écosystème existant par l'intermédiaire de son API et de son client console	non testé, a paru peu adapté à un usage personnel	https://framalibre.org/content/passbolt
Password Safe	GNU/Linux	Gestionnaire de mot de passe basé sur le format Keepass v.4 et intégré à l'environnement de bureau GNOME	non testé, car trop limité par son implémentation uniquement pour Linux/GNOME	https://framalibre.org/content/password-safe

Évaluations

N.B. : faute de disposer de matériel Apple, les tests ont été effectués sur un ordinateur Linux, un ordinateur Windows 10, un smartphone et une tablette Android.

Fonctionnement des KeePass*

L'application permet de constituer des bases de mots de passe dans des fichiers cryptés (formats ***.kdb** ou ***.kdbx**, devenus une sorte de standard du fait de la popularité de l'application), protégés par un mot de passe (c'est le seul dont il faille se souvenir !) ou avec un fichier clé de cryptage.

Le principe est de créer dans la base autant d'entrées que de sites ou services web utilisés. Un entrée est décrite par un nom, l'URL du site, l'identificateur de l'utilisateur (*username*), le mot de passe (*password*), et d'autres champs optionnels (dont une possibilité de provoquer l'expiration du mot de passe).
Les entrées peuvent être organisées en onglets, et une gestion de "corbeille" est intégrée à l'outil. Bien sûr on peut créer autant de bases de mots de passe que l'on veut, chacune étant protégée par un mot de passe.
Toute modification effectuée sous l'éditeur doit être enregistrée dans la base pour être conservée.

L'accès au site (ouverture de l'URL dans le navigateur, remplissage des champs identificateur et mot de passe) est automatisé avec des raccourcis.

Principe de la "nomadisation"

La plupart des logiciels cités plus haut (et les **KeePass** en particulier) stockent les mots de passe dans une base de données locale (les fichiers ***.kdb** ou ***.kdbx**) ; l'idée de la gestion nomade est alors de placer ladite base de données sur un espace partagé sur le cloud. Ici on fait le test avec un cloud **Nextcloud** accédé :

- sur PC Linux et sur PC Windows : via un répertoire synchronisé,
- sur mobile Android : via un volume monté par WebDAV dans le gestionnaire de fichiers.

KeePassX : test du partage cloud

Sur PC Linux :

- déplacement de la base de données des mots de passe dans le répertoire synchronisé avec l'espace cloud
- lancement de **KeePassX** et ouverture de la base de données sur l'espace cloud : on retrouve tous les mots de passe, fonctionnement identique.

Sur PC Windows :

- lancement de **KeePass** et ouverture de la base de données sur l'espace cloud : on retrouve tous les mots de passe, fonctionnement identique
- installation et lancement de **KeePassXC**, puis ouverture de la base de données sur l'espace cloud : on retrouve tous les mots de passe, fonctionnement identique à sa version Linux, décrite ci-après.

KeePassXC

Sur PC Linux :

- installation et lancement de **KeePassXC**, puis ouverture de la base de données sur l'espace cloud : on retrouve tous les mots de passe, fonctionnement analogue :
    - le look est légèrement différent,
    - les raccourcis pour ouvrir un URL, saisir automatiquement les *username* et *password*, ne sont pas exactement les mêmes

KeePassDX

Sur smartphone et tablette Android :

- installation depuis **F-Droid** (magasin libre d'applications Android libres, gratuites, sans pub et respectueuses de la vie privée)
- le fonctionnement de **KeePassDX** est analogue aux équivalents PC à ceci près :
    - le look est différent des versions PC et très complet (y compris bulles d'aide),
    - il y a un raccourci pour ouvrir un URL, pas pour saisir automatiquement les *username* et *password*, il faut les copier/coller l'un après l'autre en basculant entre l'appli et le navigateur.

Fonctionnement avec des fichiers locaux : RAS

Ouverture de la base de données sur l'espace cloud : on retrouve tous les mots de passe, mais les accès à un fichier sur le cloud peuvent être capricieux :

- messages d'erreur intempestifs ("*accès au fichier révoqué…*") apparemment sans incidence sur le fonctionnement,
- les modifications effectuées depuis le mobile ne peuvent pas être synchronisées sur le cloud (message d'erreur : "*impossible d'enregistrer la base de données*").

Ce comportement, que l'on n'observe pas sur ordinateur, pourrait provenir de la différence entre les modes d'accès, avec le cloud utilisé, entre ordinateur et mobile :

- sur ordinateur, on a installé un logiciel qui synchronise à tout instant l'espace cloud avec une copie locale ;

- sur mobile, un tel logiciel n'existe pas, et le *remote access* par WebDAV semble travailler sur une copie locale temporaire du fichier distant qu'il n'y a pas moyen de resynchroniser avec la source.

L'application reste parfaitement utilisable pour accéder aux mots de passe en lecture, en s'astreignant à ne faire les modifications de la base que sur ordinateur.

L'application installée depuis le Google Play Store a le même comportement.

KeePassDroid

Sur smartphone Android :

- l'installation depuis F-Droid n'aboutit pas, depuis le Google Play Store si.
- ouverture de la base de données sur l'espace cloud : on retrouve tous les mots de passe, fonctionnement analogue mais :
    - le look est très basique,
    - il y a un raccourci pour ouvrir un URL, pas pour saisir automatiquement les *username* et *password*, il faut les copier/coller l'un après l'autre en basculant entre l'appli et le navigateur

Le même problème d'enregistrement des modifications effectuées depuis le mobile éprouvé avec KeePassDX se produit avec KeePassDroid, de façon tout aussi explicite (message d'erreur : "*failed to store database*").

KeeWeb

Cette application (assez riche en fonctionnalités donc un peu complexe) permet la gestion de mots de passe dans des fichiers au format KeePass :

- stockés en local, ou bien
- sur Dropbox, Google Drive, OneDrive, Microsoft Teams, ou tout cloud implémentant WebDAV.

L'utilisation de fichiers locaux n'est bien sûr pas la solution pour un usage nomade, d'autant que l'on verra que les mécanismes de sauvegarde / synchronisation sont dépendants des choix de configuration de l'outil.

A noter que la base au format KeePass étant cryptée, la stocker sur un Google Drive ou un OneDrive, est moins risqué que confier directement la gestion des mots de passe à Google…

KeeWeb est diffusée sour la forme d'une application desktop pour les cibles courantes (GNU/Linux, Mac OS X, Windows) qui fonctionne peu ou prou comme les **KeePass*** mais la saisie automatique n'est pas aussi immédiate :

- cliquer sur l'URL permet de l'ouvrir dans le navigateur, mais pas de raccourci pour saisir automatiquement les *username* et *password*, il faut les copier/coller (ou bien utiliser la fonction auto-type) l'un après l'autre en basculant entre l'appli et le navigateur,
- ou alors il faut installer une extension (disponible pour les navigateurs courants).

Apparemment, pas d'application pour mobile Android ou iOS.

A la place, une application web pour usage nomade depuis tout ordinateur ou mobile via un navigateur.
Cette application fonctionne à première vue comme l'application desktop, mais de notables différences existent, que l'on verra dans les paragraphes suivants.

Application desktop

L'application permet d'ouvrir des fichiers locaux, et il faudra explicitement sauvegarder le fichier pour conserver les modifications effectuées.
Les fichiers "nomades" sur le cloud comme mis en place pour le test des KeePass* ci-dessus sont vus comme des fichiers locaux (donc attention à sauvegarder) mais semblent pouvoir être aussi synchronisés comme les espaces distants ci-après.

L'application permet d'accéder à des espaces cloud (cf. liste plus haut) en passant par une connexion explicite au serveur via une boîte d'authentification (dont le contenu diffère selon le serveur et le protocole) : testé OK avec WebDAV (le cloud Nextcloud utilisé plus haut) et avec Google Drive.
L'application mémorise les derniers fichiers ouverts et les paramètres de connexion au serveur (le niveau de mémorisation se règle dans les paramètres).

La synchronisation des modifications peut se faire de plusieurs façons :

- à la demande (comme l'on enregistrerait un fichier local),
- automatiquement selon les paramètres de configuration : inhibé, à chaque modification ou périodiquement (période réglable).

Une dernière façon d'avoir un usage nomade est de mettre les fichiers de mots de passe sur une clé USB que l'on pourra accéder comme un fichier local.

Application web

On l'active via l'URL https://app.keeweb.info/ et on retrouve la même interface qu'avec l'application desktop, mais :

- l'ouverture de fichiers locaux (ou vus comme tels - cf. le cloud Nextcloud synchronisé avec un répertoire local) fait l'objet d'un avertissement : le fichier est chargé dans l'espace de travail temporaire de l'appli web et ne sera pas sauvegardé automatiquement ;

- l'application mémorise les derniers fichiers ouverts (seulement l'emplacement pour le dernier fichier local ouvert), et les paramètres de connexion au serveur pour les fichiers sur le cloud, mais tout cela est mémorisé dans les cookies et l'historique du navigateur, donc perdu quand on le nettoie et il faudra alors se ré-authentifier ;
- il semble qu'il y ait un problème spécifique à l'appli web pour l'authentification WebDAV ("*network error*" et connexion impossible) alors que ça marche très bien avec l'application *desktop* ; par contre la connexion Google Drive fonctionne ;
- l'utilisation de périphériques USB n'est pas possible avec l'appli web (de toute façon, la connexion d'une clé USB sur un mobile n'est pas toujours facile).

Les modalités de synchronisation sont les mêmes que pour l'application *desktop* et fonctionnent de la même manière.

Extension navigateur

Pour bénéficier de la saisie automatique des *username* et *password*, il faut installer une extension au navigateur. En fait, il y en a deux :

- **KeeWeb Connect** : extension "officielle" de KeeWeb, elle est facile à installer via les paramètres de configuration ;
- **KeePassXC-Browser** : développée pour KeePassXC, elle est censée être plus avancée que la précédente mais peut présenter des problèmes d'intégration, et son installation est volontairement rendue difficile ; autant dire qu'on a choisi l'autre…

Cette extension semble ne pas être disponible sur mobile Android (pas trouvée pour Firefox, ni pour Chrome), aussi l'a-t-on testée uniquement pour Firefox sur ordinateur Linux.

Une fois installée, elle apparaît sous la forme d'un icône dans la barre de menu, qui permettra de l'activer et d'en configurer le fonctionnement, en particulier le mode de connexion :

- soit connexion à l'application desktop, auquel cas il faudra avoir au préalable lancé l'application et avoir ouvert la base de mots de passe,
- soit connexion à l'application web, auquel cas il faudra avoir au préalable lancé l'application dans un autre onglet du navigateur et avoir ouvert la base de mots de passe.

Quand on a besoin de s'authentifier sur un site web, il suffit de cliquer sur l'icône, la base est présentée, et un clic sur l'entrée voulue effectue la saisie automatique des *username* et *password*.

Application Nextcloud

Il existe une application KeeWeb spécifique pour Nextcloud, qui permet d'ouvrir des bases de mots de passe au format KeePass dans Nextcloud avec Keeweb juste en cliquant sur un fichier **.kdbx* dans l'explorateur de fichiers de Nextcloud.
Le service semblant d'un intérêt limité et la procédure d'installation un peu complexe, cette application n'a pas été testée.

Conclusion

On trouve une offre assez riche dans le domaine des logiciels libres pour réaliser une gestion nomade des mots de passe. Néanmoins, certains logiciels sont perfectibles, bien que "faisant le job", au prix de quelques limitations.

Le choix reste entre les 2 grandes familles - les KeePass* et KeeWeb - et pourrait se résumer ainsi :

- **les KeePass*** : fonctionnement simple, non prévu pour être nomade à l'origine, mais peut être "trompé" et rendu nomade en stockant les bases de mots de passe sur le cloud ; si les applications *desktop* sont sans conteste opérationnelles, les applications mobile sont plus inégales, et l'accès cloud sur ces dernières devrait être limité à un usage en lecture ;
- **KeeWeb** : une application très riche et complète, mais probablement trop complexe pour un utilisateur peu à l'aise avec l'outil informatique ; l'appli web permet de pallier l'absence d'appli mobile, mais présente quelques limitations par rapport à l'appli *desktop*.
