Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

SÉCURITÉ INFORMATIQUE

BIEN GÉRER SES MOTS DE PASSE & SÉPARATION DES USAGES PRO/PERSO

Le mot de passe est aujourd'hui la principale mesure de sécurité pour accéder à de nombreux services. Mais son emploi est si abondant que les utilisateurs ont tendance à les choisir faciles à mémoriser. Pour les pirates, ils sont donc également simples à deviner.

Par ailleurs, la dématérialisation des services et le développement des usages en mobilité permettent d'accéder depuis presque n'importe où à ses informations personnelles ainsi qu'aux infrastructures informatiques professionnelles. Ce guide vise aussi à rappeler les bonnes pratiques afin de conserver l'étanchéité numérique de nos vies professionnelles et personnelles.

Ce guide détaille les règles déjà définies dans la charte informatique du ministère*.

** Charte ministérielle d'utilisation des outils numériques.*

SOMMAIRE

JE NE COMMUNIQUE JAMAIS MES MOTS DE PASSE PERSONNELS

Hormis les mots de passe destinés à protéger certains documents partagés, **tous vos mots de passe sont personnels, ils doivent rester votre secret.**

Aucune organisation sérieuse ne vous demandera de lui communiquer votre mot de passe, notamment pour une assistance informatique. Vous pouvez considérer toute demande de mot de passe comme une opération frauduleuse.

Si quelqu'un connait votre mot de passe pour accéder à votre poste de travail, toutes les actions qu'il pourrait commettre se feront en votre nom et vous seront imputées.

En cas d'oubli ou de perte d'un mot de passe, j'avertis immédiatement les services techniques.

PERSONNE N'A BESOIN DE VOTRE MOT DE PASSE POUR INTERVENIR SUR VOTRE POSTE. SI ON VOUS LE DEMANDE PAR TÉLÉPHONE, SIGNALEZ-LE !

J'EMPLOIE DES MOTS DE PASSE LONGS ET COMPLEXES

Une des principales attaques sur les mots de passe consiste à essayer toutes les combinaisons possibles de caractères jusqu'à trouver le bon mot de passe. Ce type d'attaque dite par force brute peut mettre en jeu de multiples ordinateurs et traiter plusieurs dizaines de milliers de combinaisons par seconde.

La première règle est de ne JAMAIS employer un mot courant, ou même un nom propre, comme mot de passe. Les pirates peuvent en effet tenter de tester l'équivalent d'un dictionnaire jusqu'à trouver le bon mot.

L'autre grande méthode d'attaque consiste pour les pirates à rechercher des informations personnelles qui pourraient constituer vos mots de passe (notamment sur les réseaux sociaux : nom de jeune fille ou prénom des enfants, date de naissance…). Aussi, vous ne devez pas utiliser ces informations dans vos mots de passe.

Un bon mot de passe comporte :

- au moins 14 caractères
- des majuscules et des minuscules
- des chiffres
- des signes de ponctuation ou/et caractères spéciaux

L'ANSSI PROPOSE DIFFÉRENTS MOYENS MNÉMOTECHNIQUES POUR CRÉER ET RETENIR FACILEMENT DES MOTS DE PASSE FORTS :

Phonétique :

Se servir des sons de chaque syllabe pour fabriquer une phrase facile à retenir. Par exemple, la phrase « Cet été je pars à la mer » deviendra « 7éTJEP@RSaL@MR ».

Premières lettres :

garder les premières lettres d'une phrase (citation, paroles d'une chanson…) en veillant à ne pas utiliser que des minuscules. Par exemple : « il ne faut pas mettre la charrue avant les bœufs » donnera : « infpmlC@Lb ».

La meilleure méthode reste la génération aléatoire des mots de passe via un outillage adapté comme un gestionnaire de mots de passe. Le mot de passe dont vous devrez absolument vous souvenir est le mot de passe d'accès au gestionnaire qui doit être à la fois fort et mémorisable : un mélange de caractères aléatoires et de mots sans lien et de différents dictionnaires est suffisant :

Par exemple : « Eté bread voiture h1d5 ! »

Un indice pour s'assurer de la complexité de vos mots de passe est qu'un mot de passe doit être difficile à énoncer sans épeler.

J'UTILISE DES MOTS DE PASSE DIFFÉRENTS POUR CHAQUE APPLICATION

Un mot de passe est demandé pour de nombreux services professionnels et abonnement sur internet. La tentation est grande de réutiliser le même mais en cas de vol ou de perte d'un de vos mots de passe, tous les services sur lesquels vous utilisez le même mot de passe compromis seront vulnérables.

Utilisez un gestionnaire de mots de passe qui permet de générer aléatoirement autant de mots de passe que nécessaire et de les conserver de manière sécurisée. L'outil Keepass est un gestionnaire de mots de passe qualifié par l'ANSSI utilisable à la fois dans le cadre professionnel et dans la sphère privée.

J'UTILISE DES MOTS DE PASSE DIFFÉRENTS POUR LES SERVICES PROFESSIONNELS ET PERSONNELS

Tous les services disponibles sur internet n'offrent pas un niveau de protection suffisant et pour certains il est inférieur à celui des services proposés par l'administration.

En cas de vol ou de perte d'un de vos mots de passe, sur une application non professionnelle, tous les services professionnels sur lesquels vous utilisez le même mot de passe compromis seraient vulnérables. Un attaquant pourrait ainsi voler ou détruire des informations.

Il ne faut donc jamais réutiliser ses mots de passe professionnels dans un contexte privé. L'inverse est également vrai : les identifiants d'ordre privé ne doivent pas être utilisés dans le cadre du travail.

UTILISEZ DES TROUSSEAUX DE MOTS DE PASSE DIFFÉRENTS POUR TOUS LES SERVICES PROFESSIONNELS ET PERSONNELS AUXQUELS VOUS ACCÉDEZ.

JE NE RENVOIE PAS MES COURRIELS PROFESSIONNELS VERS MA MESSAGERIE PERSONNELLE

Plusieurs scénarios peuvent conduire à une fuite d'information lors de l'utilisation d'une messagerie personnelle :

- Une mauvaise manipulation dans votre messagerie personnelle, le choix de mauvais destinataires par exemple pourrait voir des informations de l'administration vous échapper.
- Généralement les services de messagerie personnelle sont d'une part plus exposés notamment parce que les utilisateurs n'y sont pas maitrisés et d'autre part moins sécurisé que votre messagerie professionnelle. Un piratage de votre messagerie personnelle exposerait des messages professionnels pouvant être sensibles que vous auriez gardés dans votre messagerie personnelle.
- Les opérateurs de messageries personnelles ont parfois des pratiques douteuses, notamment certains analysent vos courriels afin de partager avec les annonceurs publicitaires vos centres d'intérêt.

Pour les mêmes raisons, il ne faut pas brancher sur un réseau privé du ministère un matériel (portable, un ordiphone ou clé USB personnels) qui ne soit pas administré par le ministère.

LES COURRIELS PROFESSIONNELS SONT TRAITÉS UNIQUEMENT DEPUIS LE SERVICE DE MESSAGERIE PROFESSIONNEL.

GUIDE GESTIONNAIRE DE MOTS DE PASSE KEEPASS

QU'EST-CE QUE KEEPASS ?

Keepass est un coffre-fort électronique permettant de gérer et stocker vos mots de passe en remplaçant avantageusement les aide-mémoires papier. Des applications mobiles compatibles existent par exemple « Keepass2Android Offline » et permettent de maitriser à tout moment ses mots de passe.

La protection de cet outil est assurée par un mot de passe d'accès qu'il conviendra de construire en respectant les règles de sécurité élémentaires (décrites dans la suite du document).

Pour éviter les pertes de données, il est vivement conseillé de l'intégrer dans un processus de sauvegarde automatisée des données.

Attention, en cas d'oubli du mot de passe d'accès il sera impossible de récupérer les informations stockées.

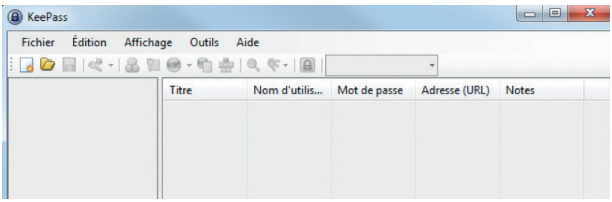
LANCEMENT

Double-cliquez sur l'icône pour lancer l'exécution ou dans le menu « Démarrer », saisissez Keepass et cliquez sur le programme Keepass 2.

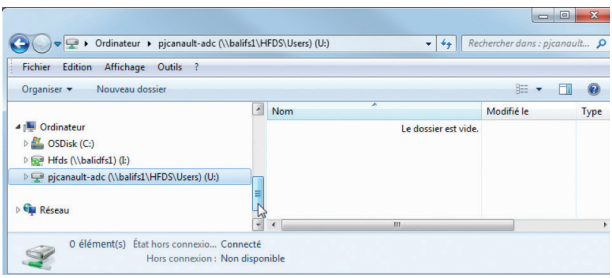
Si le programme est absent, veuillez contacter votre assistance informatique pour son installation.

CRÉATION
D'UNE BASE DE MOTS DE PASSE

Lors de la 1re utilisation, il est nécessaire de créer une Base de Mots de passe. Pour cela, il suffit de cliquer sur l'icône en haut à gauche :

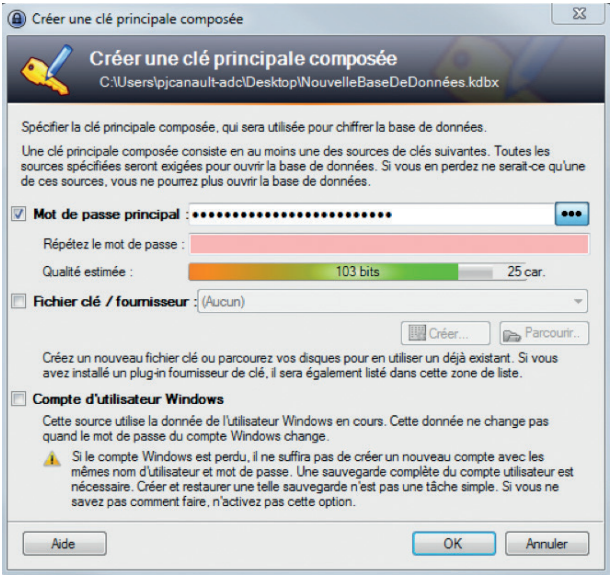


La fenêtre suivante s'ouvre pour enregistrer la base.



Afin que la base soit prise en compte dans le processus de sauvegarde du ministère, il est préconisé de l'enregistrer dans son espace de stockage personnel (lecteur u:\).

Une fenêtre s'ouvre, et demande de saisir un mot de passe principal, qui protègera la base :



L'indicateur de complexité du mot de passe permet d'évaluer le risque de sécurité de cette clé. Plus l'indicateur tend vers le vert, plus la clé est robuste.

Rappel : un mot de passe satisfaisant doit faire minimum 14 caractères, mélangeant chiffres, alphanumériques, majuscules, minuscules et caractères spéciaux.

Une fois le mot de passe principal ressaisit pour confirmation, cliquez sur OK à deux reprise.

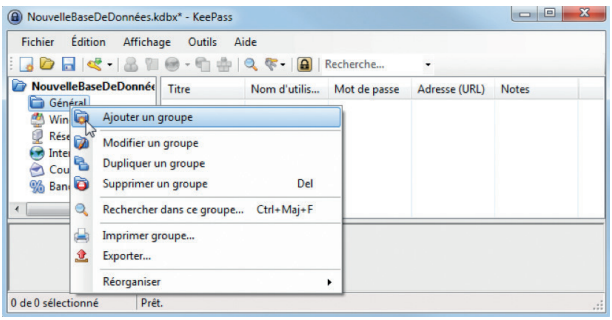
UTILISATION DE KEEPASS

AJOUTER UN GROUPE

L'outil permet d'organiser le stockage des mots de passe par catégorie et des groupes sont créés par défaut (ex : WINDOWS, RESEAU, INTERNET, COURRIEL, BANQUE EN LIGNE).

Une nouvelle fenêtre s'ouvre avec dans la partie gauche, une liste de groupes «par défaut» de mots de passe.

Ces groupes sont personnalisables en faisant un clic droit sur la catégorie :



Vous pouvez ajouter un groupe, un sous-groupe, modifier son nom, ou l'effacer.

AJOUTER UN MOT DE PASSE

Pour ajouter une nouvelle entrée de mot de passe, il suffit de cliquer sur le groupe désiré, puis sur le bouton .

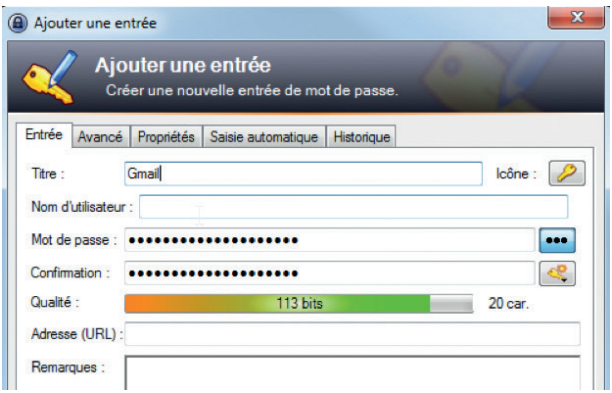
La fenêtre qui s'ouvre permet de saisir les différentes informations relatives au mot de passe qui sera stocké :

- **Titre :** permet d'identifier le mot de passe
- **Nom d'utilisateur :** permet de rappeler l'utilisateur concerné par cette clé
- **Mot de passe/Confirmation :** tapez le mot de passe à stocker et le confirmer. Par défaut, les

cellules sont pré-remplies, avec un mot de passe aléatoire qu'il peut être intéressant de conserver. La complexité des mots de passe générés est paramétrable dans l'onglet « Outils », « Générer un mot de passe… »

- **Qualité :** permet de mesurer la complexité du mot de passe tapé précédemment
- **URL :** permet de donner le lien vers le site pour lequel le mot de passe sera nécessaire
- **Notes :** permet d'ajouter des commentaires
- **Expire le :** permet d'indiquer une date d'expiration du mot passe, si celui-ci est périodique.

Quand les informations sont saisies, cliquer sur OK.



Dans la partie droite de la fenêtre principale de Keepass, l'entrée qui vient d'être saisie apparaît.

Avant de quitter l'outil, il ne faut pas oublier d'enregistrer la base, afin que les modifications effectuées ne soient pas perdues.

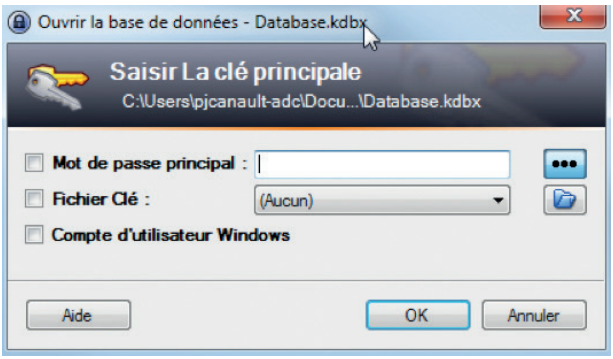
Pour cela, il suffit de cliquer sur l'icône 

Chaque modification ou suppression est automatiquement sauvegardée dans le dossier « Sauvegarde » ou « Backup ». Cela permet par exemple de retrouver d'anciens mots de passe.

Il est possible de définir une date de validité, ceci facilite la gestion des mots de passe arrivant à expiration.

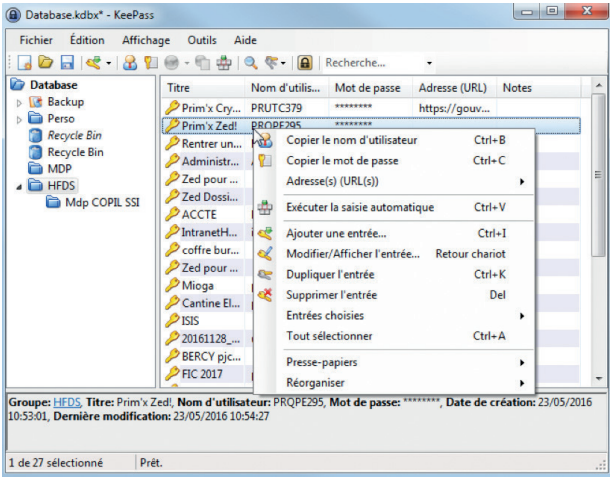
ACCÈS AUX MOTS DE PASSE

Lors du lancement de Keepass, le mot de passe de protection de la base est demandé :



Après l'avoir saisi puis validé par OK, la base est à nouveau accessible.

Pour copier rapidement le mot de passe, un clic droit sur l'entrée permet d'obtenir l'option désirée :

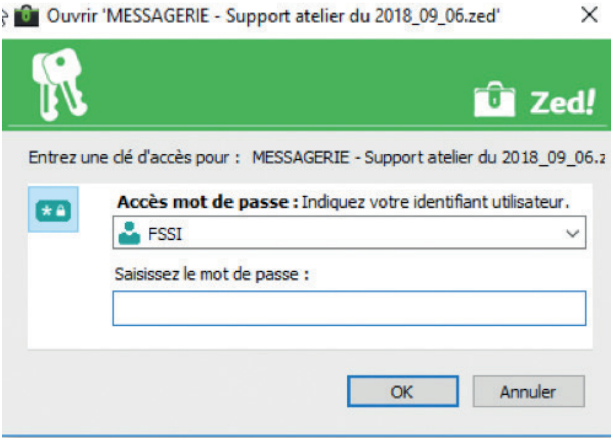


Il sera ensuite possible de coller la valeur lorsque ce mot de passe sera demandé.

SAISIE AUTOMATIQUE DES MOTS DE PASSE

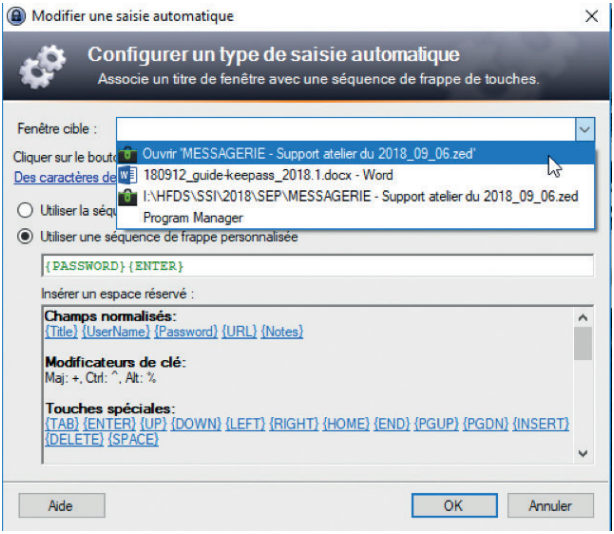
Keepass permet de paramétrer la saisie automatique d'un mot de passe dans une fenêtre de connexion, ce qui est particulièrement intéressant lorsque la fonction copier/coller ne fonctionne pas comme pour l'outil «ZED!».

Il faut d'abord ouvrir la fenêtre de login de l'application cible, ici un conteneur ZED :



Dans Keepass, faites un clic droit sur l'entrée correspondante dans la base et choisissez «Modifiez/Affichez l'entrée...». Allez dans l'onglet «Saisie automatique» et cliquez sur le bouton «Ajouter». Sélectionnez dans le champ «Fenêtre cible» la fenêtre de login précédemment ouverte, ici «Ouvrir `Messagerie – Support atelier du 2018_09_06.zed'».

Sélectionnez «Utiliser une séquence de frappe personnalisée» et saisissez dans le champ en dessous {PASSWORD}{ENTER}.



Cliquez sur le bouton OK 2 fois et enregistrez la base (Ctrl +S).

Pour l'utilisation, ouvrez la fenêtre de login. Faites un clic droit sur l'entrée correspondante dans Keepass et choisissez «Exécuter la saisie automatique».

LES PARAMÈTRES

Dans le menu Outils, Options, il est possible de paramétrer le délai d'inactivité au-delà de laquelle le coffre-fort se verrouille, de préciser le temps au-delà duquel le presse papier est effacé … Nous vous conseillons de laisser les valeurs par défaut.

QUELQUES PRÉCAUTIONS

Le coffre-fort est sensible. Le mot de passe le protégeant doit être «fort»: longueur minimale, mélange de majuscules, minuscules, nombres et caractères spéciaux. Il ne doit pas contenir de manière explicite un mot d'un dictionnaire ou trop facilement devinable tel que le nom de sa direction, «minefi», votre nom ou prénoms, une date, année, «password», «azerty», «1234»…

L'utilisation d'un fichier clé (stocké par exemple sur une clé USB) permet d'augmenter la longueur de la clé de chiffrement sans avoir à saisir un mot de passe trop long.

Il faut absolument éviter d'exporter la base de comptes au format html, ce format laissant les mots de passe en clair et donc sans protection.

Pour en savoir plus :
Mail de la DSSI :
dssi.shfds@finances.gouv.fr

LES RÈGLES D'OR DES MOTS DE PASSE

JE NE RÉVÈLE JAMAIS UN MOT DE PASSE PERSONNEL, PAS MÊME À UN ASSISTANT INFORMATIQUE OU UN COLLÈGUE

J'EMPLOIE DES MOTS DE PASSE LONGS ET COMPLEXES

JE N'UTILISE JAMAIS LE MÊME MOT DE PASSE POUR PLUSIEURS APPLICATIONS

J'UTILISE UN GESTIONNAIRE DE MOTS DE PASSE

Plus d'informations dans le guide «Bien choisir ses mots de passe» !

SG
Secrétariat général

HFDS Bercy

Secrétariat Général
139-145 rue de Bercy, PARIS
Janvier 2019