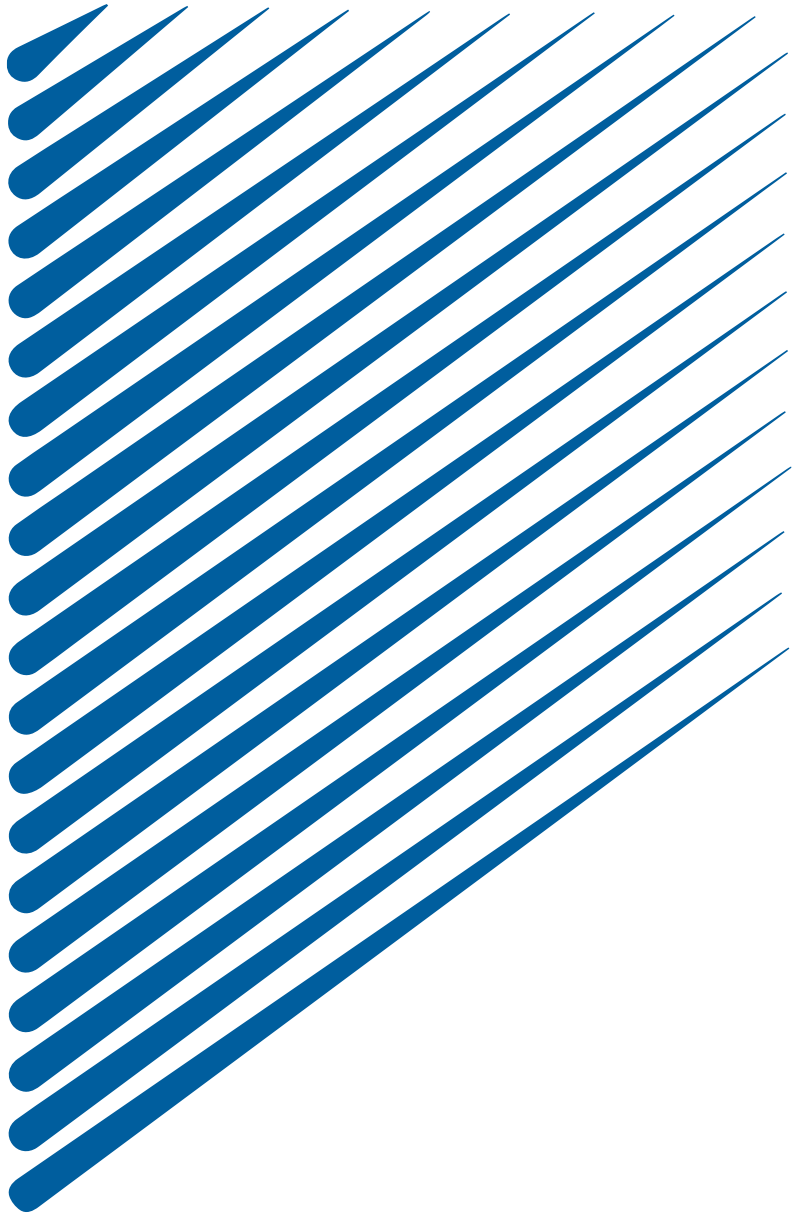


MINES PARIS | PSL

WORKSHOP SSI

Gestion des mots de passe

23 février 2023

SOMMAIRE

- UN BON MOT DE PASSE ?
- BONNES PRATIQUES
- GESTIONNAIRE DE MOT DE PASSE - KEEPASS
- DEMONSTRATION

- QUESTIONS

QU'EST CE QU'UN MOT DE PASSE ROBUSTE OU UN BON MOT DE PASSE ?

Pour protéger vos informations, il doit être difficile à retrouver à l'aide d'outils automatisés et à deviner par une tierce personne.

Un bon mot de passe contient au moins 12 caractères avec des majuscules, des minuscules, au moins un chiffre et au moins un caractère non alpha numérique. Plus la longueur est élevée, plus le mot de passe est difficile à forcer.

Recommandé : 16 caractères avec des majuscules, minuscules, caractères spéciaux et chiffres.

Exemple : Afet@Zy6o45tf6'.

choisir un mot de passe qui n'a pas de lien avec vous (mot de passe composé d'un nom, d'une date de naissance, prénom de vos enfants, animaux de compagnie, …)

Votre mot de passe doit être difficile à trouver et stocké dans un endroit sécurisé si vous ne pouvez pas le retenir

TEMPS REQUIS DE DECHIFFREMENT D'UN MOT DE PASSE

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	instant	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Etude réalisée en mars 2022 par HiveSystem sur des mots de passe en chiffré par attaque par force brute.

La puissance de calcul augmentant fortement au fil des années, les préconisations évoluent également...

COMMENT FABRIQUER UN MOT DE PASSE LONG ET FACILE À RETENIR ?

Voici deux exemples de méthodes mnémotechniques pour fabriquer et retenir facilement de tels mots de passe :

-la méthode phonétique : « J'ai acheté huit cd pour cent euros cet après-midi » deviendra : **ght8CD%E7am**

-la méthode des premières lettres : la citation « un tiens vaut mieux que deux tu l'auras » donnera **1tvmQ2tl'A**

-la méthode des préfixes/suffixes: on prend le mot de passe à retenir que l'on suffixe pour le service ciblé:

- Exemple: ght8CD%E7am devient

  Fr-ght8CD%E7am pour le compte internet Free

  Sg-ght8CD%E7am pour la banque Société Générale etc..

BONNES PRATIQUES

- Ne l'inscrivez nulle part. En particulier, **ne le stockez pas dans un fichier électronique non-protégé.**
- N'activez pas l'option permettant d'enregistrer votre mot de passe sans protéger votre navigateur, **il est nécessaire de définir un mot de passe principal dans celui-ci.**

- **L'utilisation d'un même mot de passe entre sa messagerie professionnelle, sa messagerie personnelle et les réseaux sociaux est impérativement à proscrire.**

- **Utiliser un mot de passe unique pour chaque service ou application**

- Ne pas divulguer vos mots de passe à un collègue, à vos étudiants, conformément au règlement intérieur.

- Ne pas envoyer vos mots de passe par messagerie, chat ou autre système de communication non chiffré.

- Renouveler vos mots de passe régulièrement, l'ANSSI recommande un changement minimum tous les 3 ans.

- Ne pas utiliser de gestionnaire de mot de passe en ligne (Lastpass, Dashlane, ils sont potentiellement vulnérables.

Exemple: LastPass a été victime de violation de données en août puis en décembre 2022 (mots de passe compromis)

RÈGLES DE BASE

- Je n'écris pas mon mot de passe sur un post-it sous le clavier ou sur l'écran

- Je ne communique jamais mes mots de passe / identifiants personnels (la DSI ne vous les demandera jamais !)
- Pensez aussi à ne jamais l'enregistrer dans le navigateur d’un ordinateur partagé.
- Personne n'a besoin de votre mot de passe pour intervenir sur votre poste informatique
  Si on vous le demande par téléphone , signalez-le.

KEEPASS

https://www.keepass.info

Gestion des mots de passe et informations de connexion

Logiciel Opensource et gratuit
Recommandé par l'ANSSI et certifié CSPN
Le BSI allemand, Swiss Federal Office of Information Technology...
Code audité par la commission Européenne

Chiffrement AES 256

Générateur de mot de passe intégré

Nombreux plugins disponibles

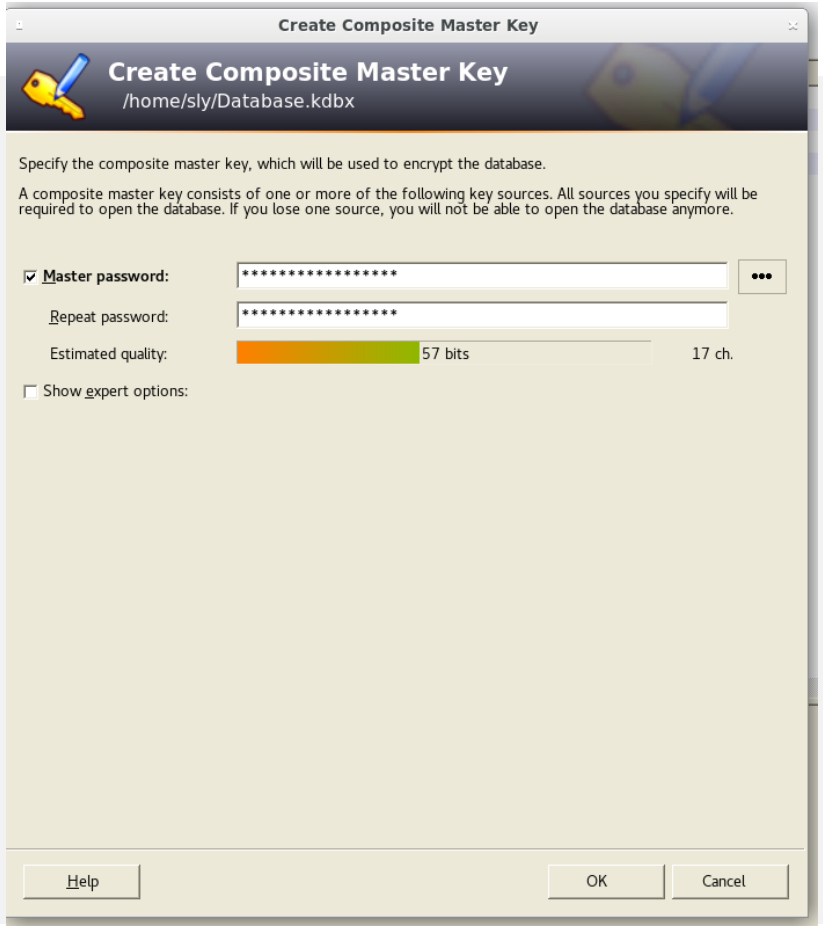
Multifichiers

Travail hors ligne possible

Le logiciel est déployé sur les postes installés par la DSI

Attention aux sites frauduleux comme https://www.keepass.fr

KEEPASS



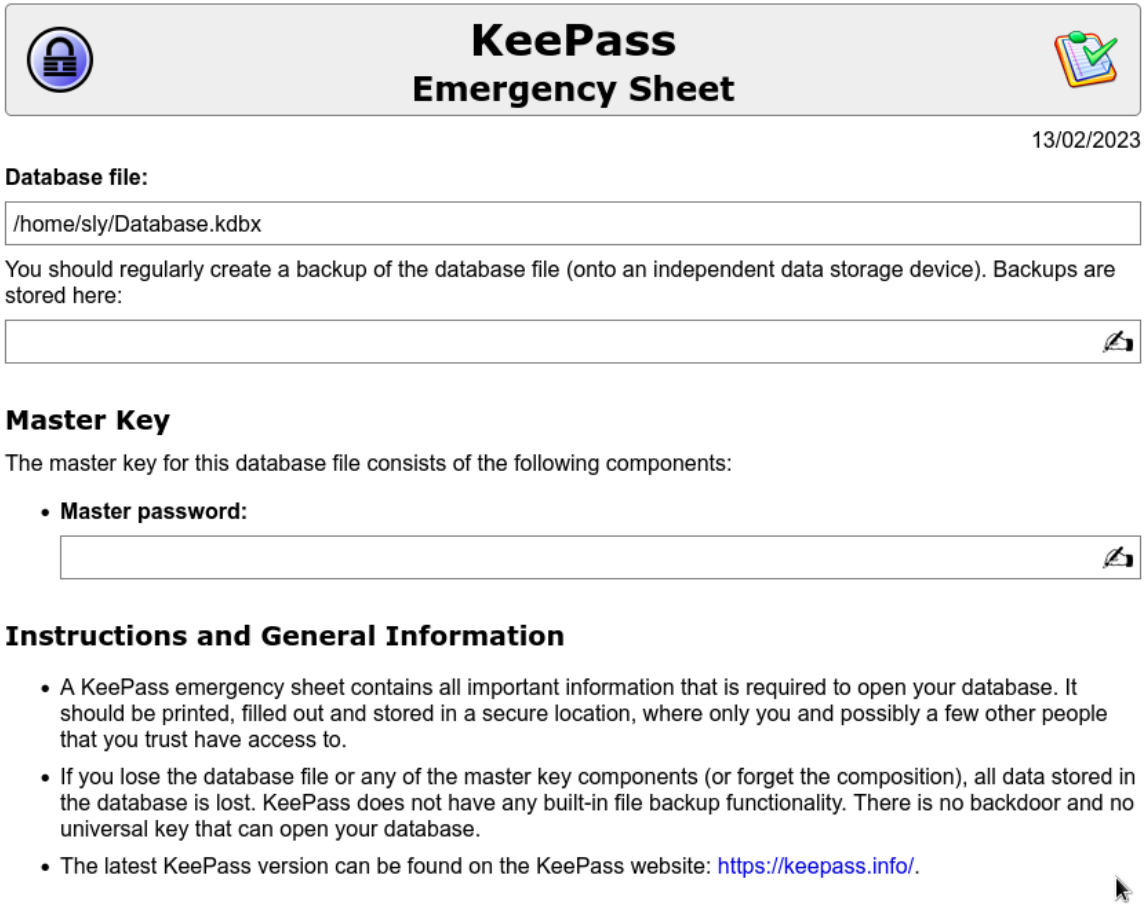
Création d'une base Keepass

Définition du mot de passe principal : Mot de passe robuste et différent de votre mot de passe habituel

Attention : l'oubli ou la perte de ce mot de passe empêchera toute récupération des données de la base

-> éventuellement imprimer la page de récupération et la stocker en lieu sûr

KEEPASS



KeePass
Emergency Sheet

13/02/2023

Database file:

/home/sly/Database.kdbx

You should regularly create a backup of the database file (onto an independent data storage device). Backups are stored here:

Master Key

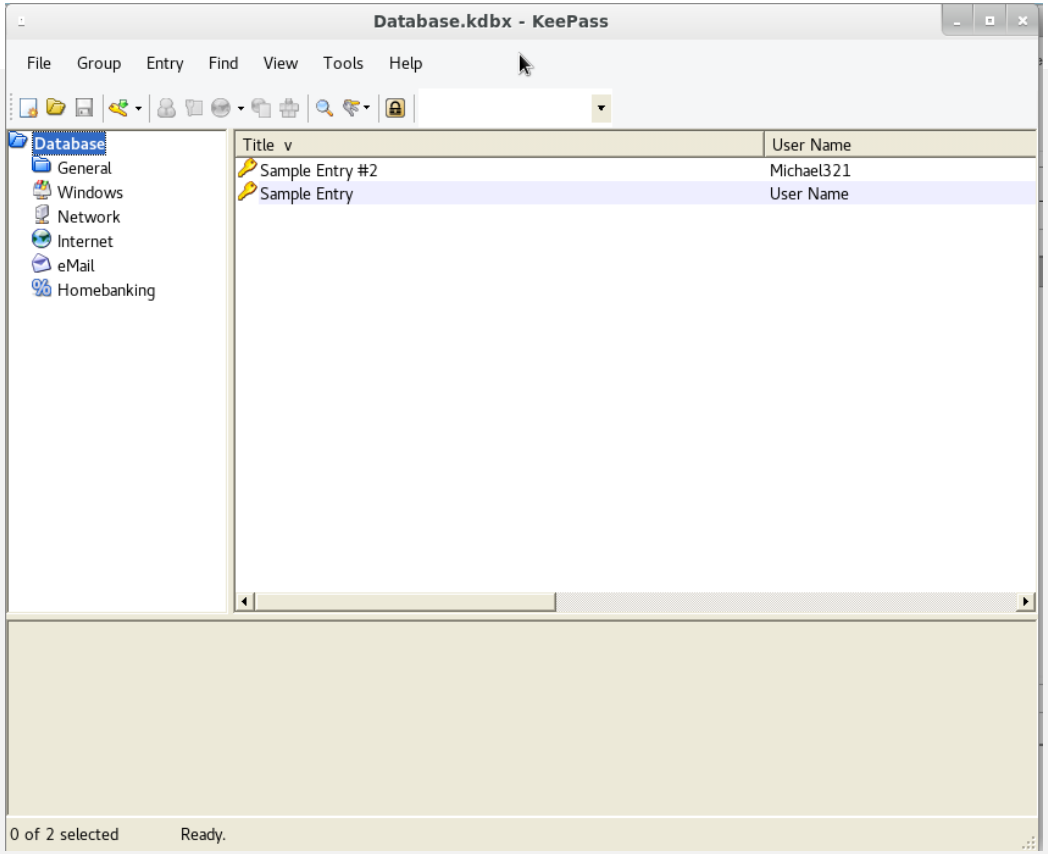
The master key for this database file consists of the following components:

- **Master password:**

Instructions and General Information

- A KeePass emergency sheet contains all important information that is required to open your database. It should be printed, filled out and stored in a secure location, where only you and possibly a few other people that you trust have access to.
- If you lose the database file or any of the master key components (or forget the composition), all data stored in the database is lost. KeePass does not have any built-in file backup functionality. There is no backdoor and no universal key that can open your database.
- The latest KeePass version can be found on the KeePass website: https://keepass.info/.

KEEPASS

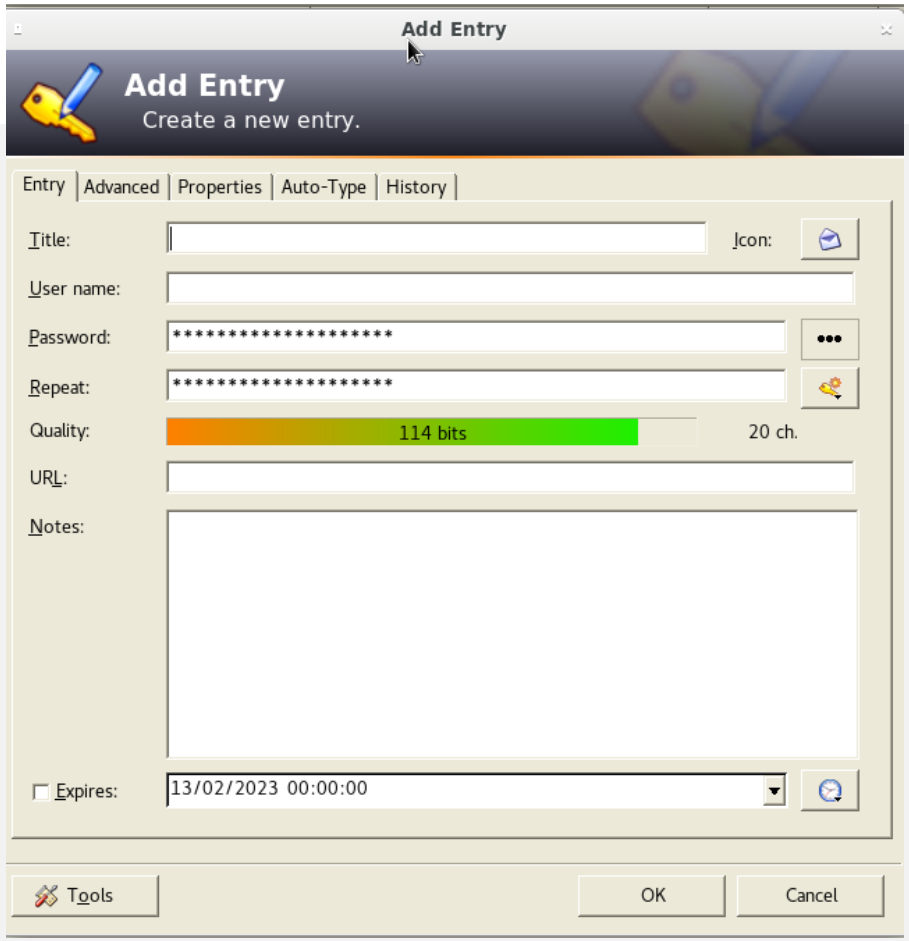


Le contenu d'une base

Structure en arborescence, modifiable

Fonction de recherche

KEEPASS



Ajout d'une entrée

Saisi du mot de passe ou utilisation du generateur de mot de passe

Possibilité d'inclure des fichiers dans des entrées

DÉMONSTRATION

Prise en main de la solution Keepass

QUESTIONS

REFERENCES

Guides et recommandations de l'ANSSI

https://www.ssi.gouv.fr/guide/mot-de-passe/

https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/

Keepass - Certification CSPN

https://www.ssi.gouv.fr/entreprise/certification_cspn/keepass-version-2-10-portable/

Guide de sécurité informatique – Ministère de l'économie

https://www.economie.gouv.fr/files/bro-guide-secu-info-print_0.pdf

Recommandations de la CNIL

https://www.cnil.fr/pourquoi-securiser-au-maximum-le-mot-de-passe-de-votre-boite-email
https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires