KeePass-1.43

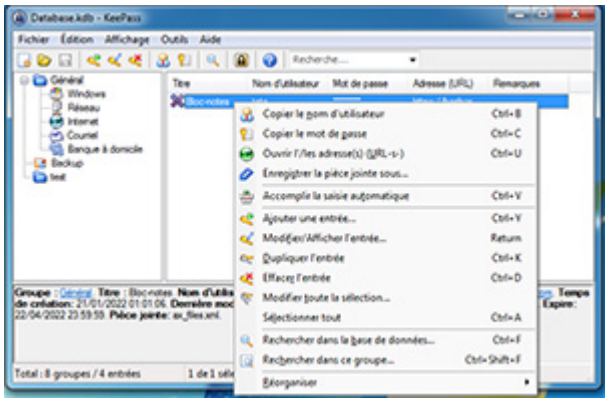
Table des matières

KeePass

Introduction

KeePass Password Safe

Introduction



Aujourd'hui, vous avez besoin de mémoriser beaucoup de mots de passe. Vous avez besoin d'un mot de passe pour de nombreux sites, votre compte de messagerie électronique, votre serveur Web, l'ouverture d'une session Windows, le compte FTP de votre site, les logins (ouvertures de session) réseau, etc. La liste est sans fin. Vous devez également utiliser un mot de passe différent pour chaque compte. Parce que si vous utilisez le même mot de passe partout et que quelqu'un l'obtienne, alors là vous auriez un problème : le voleur aurait accès à *tous* vos comptes.

KeePass est un gestionnaire de mots de passe libre/gratuit, au code source disponible (open source), qui vous aide à gérer vos mots de passe d'une façon sécurisée.

Vous pouvez stocker tous vos mots de passe dans une seule base de données, qui est verrouillée par une clé principale. Donc, vous avez simplement à vous souvenir que d'une clé principale pour déverrouiller toute la base de données. Les fichiers de bases de données sont chiffrés en utilisant les algorithmes de chiffrement les meilleurs et les plus sécurisés actuellement connus (AES256, ChaCha20 et Twofish).

La base de données se compose d'un seul fichier, elle peut donc être transférée facilement d'un ordinateur à un autre. Les données peuvent également être importées/exportées depuis/vers différents autres formats (importées depuis plus de 40 formats différents d'autres gestionnaires de mots de passe, etc.). Bien sûr, l'impression des entrées est également prise en charge.

KeePass prend en charge des groupes, qui vous permettent de convenablement organiser vos entrées. Pour localiser rapidement des entrées spécifiques, il y a des fonctions de recherche.

Il y a plusieurs méthodes pour transférer les données des entrées (comme les noms d'utilisateurs et les mots de passe) de KeePass vers d'autres applications (presse-papiers, glisser-déposer, etc.). La puissante fonction de saisie automatique peut simuler des pressions de touches.

KeePass possède un générateur de mots de passe aléatoires forts (vous pouvez définir les caractères autorisés, la longueur, les règles de génération, etc.).

Le logiciel fonctionne sur une architecture de greffon (plug-in). Des greffons peuvent ajouter des fonctionnalités dans de nombreux domaines (intégration, transfert, sauvegarde, fonctionnalité réseau, et même encore davantage de formats d'importation/exportation, et bien plus encore).

Comme KeePass est open source, vous pouvez consulter entièrement son code source et vérifier que les fonctions de sécurité sont correctement implémentées.

Cette documentation s'applique à KeePass 1.x.

Le tutoriel des premiers pas

Le tutoriel des premiers pas

Un court tutoriel vous montrant l'utilisation de base de KeePass.

Ce court tutoriel vous montre comment utiliser KeePass. Il décrit uniquement l'utilisation de base, les fonctionnalités avancées sont couvertes sur des pages séparées.

Création d'une nouvelle base de données

La toute première étape consiste à créer une nouvelle base de données de mots de passe. KeePass stockera tous vos mots de passe dans une telle base de données. Pour en créer une, cliquez sur 'Fichier' → 'Nouveau...' dans le menu principal ou cliquer sur le bouton le plus à gauche de la barre d'outils. Une fenêtre apparaîtra, vous invitant à saisir un mot de passe maître et/ou un fichier clé. La base de données sera chiffrée avec le mot de passe que vous entrez ici. Le mot de passe que vous entrez ici sera le seul mot de passe dont vous aurez à vous souvenir à partir de maintenant. Il doit être long et constitué de caractères mixtes. N'oubliez pas que lorsque quelqu'un récupère votre fichier de base de données et devine le mot de passe, il peut accéder à tous les mots de passe que vous avez stockés dans la base de données.

Pour ce didacticiel, nous n'utilisons qu'un seul mot de passe, c'est-à-dire sans fichier clé. Cliquez dans le champ d'édition du mot de passe et saisissez un mot de passe de votre choix. Le contrôle d'édition de mot de passe n'est pas limité en longueur, alors n'hésitez pas à saisir une phrase entière (gardez simplement à l'esprit que vous devrez vous en souvenir).

Après avoir cliqué sur [OK], une deuxième boîte de dialogue apparaît, dans laquelle vous devez répéter le mot de passe maître que vous venez de saisir dans la boîte de dialogue précédente. Ceci afin d'éviter toute erreur de saisie accidentelle.

Vous voyez maintenant la fenêtre principale. Sur la gauche, vous voyez les groupes d'entrées. Sur la droite, vous voyez les entrées de mot de passe réelles. Les entrées de mot de passe sont regroupées ensemble dans des groupes de mots de passe que vous voyez à gauche. Ainsi, selon le groupe que vous avez sélectionné à gauche, il vous montrera les entrées de ce groupe dans la vue de droite. KeePass a créé quelques groupes par défaut pour vous, mais vous êtes libres de les supprimer et de créer les propres vôtres.

Ajout d'une entrée

Il est temps d'enregistrer votre tout premier mot de passe dans la base de données de KeePass ! Cliquez avec le bouton droit de la souris sur la liste d'entrées et choisissez "Ajouter une entrée...". Une fenêtre va s'ouvrir. Dans cette fenêtre, vous pouvez maintenant modifier votre entrée : saisissez-lui un titre, un nom d'utilisateur, le mot de passe, une adresse (URL), etc. Si vous n'avez pas besoin de certains champs, simplement les laisser vides. Lorsque vous avez terminé, cliquez sur [OK].

Utilisation des entrées

Votre nouvelle entrée s'affiche maintenant dans la liste des entrées principales. Il existe plusieurs façons sur son utilisation.

Par exemple : vous pouvez copier le nom d'utilisateur de l'entrée dans le presse-papiers. Afin d'invoquer la commande 'Copier nom d'utilisateur', double-cliquez sur la cellule du nom d'utilisateur dans la liste des entrées principales. Alternativement, la commande peut être invoqué via le menu principal, le menu contextuel, le bouton de la barre d'outils, ou en appuyant sur Ctrl+B. Quand le nom d'utilisateur est dans le presse-papiers, vous pouvez le copier dans la fenêtre cible.

La copie de mots de passe et les autres champs fonctionne de manière similaire.

Alternativement, vous pouvez glisser&déposer des champs dans d'autres fenêtres. Pour les détails, voir Glisser&Déposer.

Sauvegarde de la base de données

Il est temps de sauvegarder notre base de données. Cliquez sur le bouton "Enregistrer" de la barre d'outils

(qui est une icône de disquette).

Davantage

Ça y est ! C'est tout ! Vous avez fait les premiers pas dans l'utilisation de KeePass ! Vous pouvez maintenant consulter les fonctionnalités les plus avancées de KeePass.

Mots de passe et fichiers clé : dans le didacticiel ci-dessus, nous avons chiffré la base de données à l'aide d'un mot de passe. Cependant, KeePass prend également en charge les fichiers clé, c'est-à-dire que vous pouvez verrouiller votre base de données à l'aide d'un fichier (que vous pouvez, par exemple, transporter sur votre clé USB). Il prend même en charge la combinaison de ces deux méthodes pour une sécurité maximale.

Les entrées de NAT (Numéro d'Authentification de Transaction ; en anglais TAN Transaction Authentication Number) : les entrées de NAT sont des mots de passe à usage unique. De nombreuses banques utilisent les NAT pour une meilleure sécurité. KeePass prend en charge les entrées de NAT, en les faisant expirer automatiquement lors de leur utilisation.

La saisie automatique : la fonctionnalité de saisie automatique est une fonctionnalité très puissante. Dans le tutoriel ci-dessus, vous avez copié le nom d'utilisateur et le mot de passe d'une entrée dans le presse-papiers. Ne serait-il pas agréable que KeePass saisisse simplement ces chaînes pour vous dans d'autres fenêtres ? Ne seriez-vous pas intéressés de définir des séquences entières de touches que KeePass taperait pour vous ? C'est exactement ce que fait la fonction de saisie automatique : elle envoie des simulations de touche pressées pour vous vers d'autres fenêtres !

Le champ d'adresse (URL) : le champ d'adresse prend bien sûr en charge les URL. Dans le didacticiel, vous avez appris que vous pouvez entrer dans ce champ des adresses simples et que KeePass ouvrira la fenêtre du navigateur à votre place. Cependant, le champ adresse peut en faire plus ! Il prend réellement en charge de nombreux protocoles différents (pas seulement `http`) et prend en charge l'exécution de lignes de commande Windows via le protocole virtuel `cmd://`. Le champ comporte également un puissant moteur de substitution, remplaçant les codes par d'autres champs (nom d'utilisateur, mot de passe, etc.) de cette entrée.

Les paramètres de la ligne de commande : vous pouvez ouvrir des fichiers .kdb(x) en les transmettant au fichier exécutable de KeePass. Cependant, saviez-vous que vous pouvez également envoyer le mot de passe pour la base de données et l'emplacement du fichier clé via une ligne de commande ? Vous pouvez également utiliser la ligne de commande pour présélectionner un fichier clé pour vous.

Les greffons : KeePass dispose d'une puissante architecture de greffons. S'il vous manque certaines fonctionnalités, alors consultez la page des greffons pour voir si d'autres personnes ont déjà écrit des greffons pour cela. De nombreux greffons existent pour importer/exporter des données depuis/vers d'autres formats de fichiers.

Remerciements

Remerciements/Crédits

Merci à diverses personnes pour leurs contributions et/ou leur travail.

À cet endroit, je tiens à remercier beaucoup de gens pour leur aide, leur code source, leurs suggestions et leurs autres contributions (sans ordre particulier).

- Remerciements aux donateurs
- Remerciements du code source
- Remerciements pour les icônes
- Remerciements pour les traductions
- Remerciements pour les greffons
- Remerciements pour les outils
- Remerciements pour l'hébergement/la distribution
- Remerciements pour les suggestions et le support du forum
- Remerciements spécifiques

- Les licences des composants/ressources/etc. :
  - le thème des icônes Nuvola
  - Boost
  - L'implémentation Twofish
  - L'implémentation SHA-2
  - CSendKeys
  - Les classes de ligne de commande
  - L'implémentation Argon2

Remerciements aux donateurs

Le développement d'applications de haute qualité prend beaucoup de temps et de ressources. Les dons permettent de maintenir le standard de développement actuel. Par conséquent, beaucoup de remerciements à tous ceux qui ont fait un don au projet.

Vous trouverez plus d'informations sur les dons et une liste des personnes qui ont fait un don ici : dons KeePass.

Remerciements du code source

KeePass utilise des classes et des bibliothèques écrites par différentes personnes et distribuées gratuitement. Ici, je tiens à les remercier d'avoir écrit ces classes et bibliothèques.

Auteur	Classes/Bibliothèques
Szymon Stefanek	L'implémentation en C++ de l'algorithme de chiffrement AES/Rijndael.
Niels Ferguson	L'implémentation en langage C de l'algorithme de chiffrement Twofish.
Brian Gladman	L'implémentation en langage C de l'algorithme de hachage SHA-2 (256/384/512).
Alvaro Mendez	La classe MFC pour la validation des contrôles d'édition (CAMSEdit).
Brent Corkum	La classe MFC pour le menu de style XP (BCMenu).
Davide Calabro	La classe MFC pour des boutons avec des icônes (CButtonST).
Zorglab, Chris Maunder, Alexander Bischofberger, James White, Descartes Systems Sciences Inc.	La classe MFC pour les sélecteurs de couleur (CColourPickerXP).
Peter Mares	La classe MFC pour les bannières côté fenêtre (CKCSideBannerWnd).
Chris Maunder	La classe MFC pour les icônes de la zone de notification du système (CSystemTray).
Hans Dietrich, Chris Maunder	La classe MFC pour les hyperliens dans les boîtes de dialogue (XHyperLink).
Lallous	La classe pour envoyer des frappes de touche simulées à d'autres applications (CSendKeys).
PJ Naughter	Les classes MFC pour la vérification de l'instance unique (CSingleInstance) et des informations de version (CVersionInfo).
Bill Rubin	Les classes en C++ de la ligne de commande.
Les développeurs de Boost	Les bibliothèques en C++ de Boost

Daniel Dinu, Dmitry Khovratovich, Jean-Philippe Aumasson, Samuel Neves, Thomas Pornin	L'implémentation en langage C de la fonction de hachage de mot de passe Argon2.

Auteur	Ressource
Mark Burnett	La liste des 10000 meilleurs mots de passe, que KeePass utilise dans son algorithme d'estimation de qualité d'un mot de passe.

Remerciements pour les icônes

Plusieurs remerciements à **Christopher Bolin** d'avoir créé l'icône principale de KeePass (voir en haut à gauche sur cette page) et ses variantes. Merci beaucoup à **Victor Andreyenkov** d'avoir affiné les icônes de l'application.

Merci beaucoup à **David Vignoni** pour la création du joli thème d'icônes *'Nuvola'*. La plupart des icônes utilisées dans KeePass et sur son site sont des icônes issues de ce thème. Vous pouvez trouver les images d'origine sur le site de l'auteur, et la licence ci-dessous.

De plus, merci aux auteurs des icônes suivantes que KeePass utilise :

- Tux le pingouin par **Mairin**.
- Les plumes par **Dear_Theophilus**.
- La pomme par **James Birkett**.
- Le certificat en couleur par **Olo**.
- La touche moderne de téléphone portable par **Shokunin**.
- La police en gras, la police en italique, la police soulignée et la police barrée par **Sixsixfive**.
- L'icône FreeBSD (sur Archive.org) par **FatCow**.
- Le symbole de la main par **Bobek Ltd**.

Remerciements pour les traductions

Plusieurs remerciements à tous ceux qui ont créé des traductions pour KeePass.

Remerciements pour les greffons

Un grand merci à toutes les personnes qui ont écrit des greffons pour KeePass. Sans vous, KeePass serait bien moins puissant et utile !

Remerciements pour les outils

Merci à **Jordan Russell** pour la création de l'installation Inno. Cet outil est utilisé pour créer le programme d'installation de KeePass.

Merci à **Dimitri van Heesch** pour l'utilitaire Doxygen, qui est utilisé pour compiler la documentation du code source.

Remerciements pour l'hébergement/la distribution

Merci à **SourceForge** pour héberger gratuitement les téléchargements de KeePass/les traductions/les greffons et pour fournir la plateforme de prise en charge du projet (forum, requêtes de fonctionnalités/les pisteurs des bogues, etc.).

Merci à **domain FACTORY** pour héberger le site de KeePass.

Merci à **datensysteme-lenk** pour avoir hébergé par le passé la prise en charge du forum d'assistance en allemand de KeePass.

Remerciements pour les suggestions et le support du forum

Merci à tous ceux qui répondent aux questions des autres sur le forum de KeePass ! Un produit est à la hauteur de son support, et je ne pourrais jamais seul fournir une aussi excellente plateforme d'aide individuelle.

Quelques personnes devraient être mentionnées ici, en raison d'une quantité extraordinaire de suggestions (fonctionnalités, rapports de bogue, etc.) et d'aider les autres dans les forums : **Paul Tannard**, **Wellread1** et **Michael Scheer**.

Remerciements spécifiques

Merci à **Daniel Turini** pour avoir suggéré *"KeePass"* comme nom du projet.

Un *grand* merci à **Bill Rubin**. Non seulement il a contribué à beaucoup de code source dans KeePass, mais il a également eu vraiment beaucoup de suggestions de fonctionnalités et d'améliorations, a aidé des gens dans les forums de KeePass, et écrit un greffon de KeePass pour sauvegarder la base de données. C'est à lui qu'on doit des sections d'aide de KeePass très précises, utiles, claires et faciles à comprendre. Au cours de nos innombrables conversations IM de longue durée, nous avons non seulement beaucoup discuté du propos de la conception de KeePass, mais Bill m'a également beaucoup parlé du C++ et d'autres choses. Merci !

Les licences des composants/ressources/etc.

Le thème des icônes Nuvola

L'utilisation des icônes est autorisée selon les termes de la licence LGPL (que vous pouvez trouver ici : GNU Lesser General Public License), plus un addendum.

```
TITLE:  NUVOLA ICON THEME for KDE 3.x
AUTHOR: David Vignoni | ICON KING
SITE:   http://www.icon-king.com
MAILING LIST: http://mail.icon-king.com/mailman/listinfo/nuvola_icon-king.com

Copyright (c)  2003-2004  David Vignoni.

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public
License as published by the Free Software Foundation,
version 2.1 of the License.
This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the GNU
Lesser General Public License for more details.
You should have received a copy of the GNU Lesser General Public
License along with this library (see the the license.txt file); if not, write
to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston,
MA  02111-1307  USA
#######**** NOTE THIS ADD-ON ****#######
The GNU Lesser General Public License or LGPL is written for software libraries
in the first place. The LGPL has to be considered valid for this artwork
library too.
Nuvola icon theme for KDE 3.x is a special kind of software library, it is an
artwork library, it's elements can be used in a Graphical User Interface, or
GUI.
Source code, for this library means:
 - raster png image* .
The LGPL in some sections obliges you to make the files carry
notices. With images this is in some cases impossible or hardly usefull.
With this library a notice is placed at a prominent place in the directory
containing the elements. You may follow this practice.
The exception in section 6 of the GNU Lesser General Public License covers
the use of elements of this art library in a GUI.
dave [at] icon-king.com

Date:       15 october 2004
```

```
Version:    1.0

DESCRIPTION:

Icon theme for KDE 3.x.
Icons where designed using Adobe Illustrator, and then exported to PNG format.
Icons shadows and minor corrections were done using Adobe Photoshop.
Kiconedit was used to correct some 16x16 and 22x22 icons.

LICENSE

Released under GNU Lesser General Public License (LGPL)
Look at the license.txt file.

CONTACT

David Vignoni
e-mail :        david [at] icon-king.com
ICQ :           117761009
http:           http://www.icon-king.com
```

Boost

```
Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization
obtaining a copy of the software and accompanying documentation covered by
this license (the "Software") to use, reproduce, display, distribute,
execute, and transmit the Software, and to prepare derivative works of the
Software, and to permit third-parties to whom the Software is furnished to
do so, all subject to the following:

The copyright notices in the Software and this entire statement, including
the above license grant, this restriction and the following disclaimer,
must be included in all copies of the Software, in whole or in part, and
all derivative works of the Software, unless such copies or derivative
works are solely in the form of machine-executable object code generated by
a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT
SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE
FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE,
ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER
DEALINGS IN THE SOFTWARE.
```

L'implémentation Twofish

```
Fast, portable, and easy-to-use Twofish implementation,
Version 0.3.
Copyright (c) 2002 by Niels Ferguson.

The author hereby grants a perpetual license to everybody to
use this code for any purpose as long as the copyright message is included
in the source code of this or any derived work.
```

L'implémentation SHA-2

```
Copyright (c) 2003, Dr Brian Gladman, Worcester, UK.   All rights reserved.
```

```
LICENSE TERMS

The free distribution and use of this software in both source and binary
form is allowed (with or without changes) provided that:

  1. distributions of this source code include the above copyright
     notice, this list of conditions and the following disclaimer;

  2. distributions in binary form include the above copyright
     notice, this list of conditions and the following disclaimer
     in the documentation and/or other associated materials;

  3. the copyright holder's name is not used to endorse products
     built using this software without specific written permission.

ALTERNATIVELY, provided that this notice is retained in full, this product
may be distributed under the terms of the GNU General Public License (GPL),
in which case the provisions of the GPL apply INSTEAD OF those given above.

DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties
in respect of its properties, including, but not limited to, correctness
and/or fitness for purpose.
---------------------------------------------------------------------------
Issue 01/08/2005
```

CSendKeys

```
Copyright (c) 2004 lallous <lallousx86@yahoo.com>
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

---------------------------------------

The Original SendKeys copyright info

SendKeys (sndkeys32.pas) routine for 32-bit Delphi.
Written by Ken Henderson
Copyright (c) 1995 Ken Henderson <khen@compuserve.com>
```

Les classes de la ligne de commande

L'implementation Argon2

Statement of Purpose

The laws of most jurisdictions throughout the world automatically confer exclusive Copyright and Related Rights (defined below) upon the creator and subsequent owner(s) (each and all, an "owner") of an original work of authorship and/or a database (each, a "Work").

Certain owners wish to permanently relinquish those rights to a Work for the purpose of contributing to a commons of creative, cultural and scientific works ("Commons") that the public can reliably and without fear of later claims of infringement build upon, modify, incorporate in other works, reuse and redistribute as freely as possible in any form whatsoever and for any purposes, including without limitation commercial purposes. These owners may contribute to the Commons to promote the ideal of a free culture and the further production of creative, cultural and scientific works, or to gain reputation or greater distribution for their Work in part through the use and efforts of others.

For these and/or other purposes and motivations, and without any expectation of additional consideration or compensation, the person associating CC0 with a Work (the "Affirmer"), to the extent that he or she is an owner of Copyright and Related Rights in the Work, voluntarily elects to apply CC0 to the Work and publicly distribute the Work under its terms, with knowledge of his or her Copyright and Related Rights in the Work and the meaning and intended legal effect of CC0 on those rights.

1. Copyright and Related Rights. A Work made available under CC0 may be protected by copyright and related or neighboring rights ("Copyright and Related Rights"). Copyright and Related Rights include, but are not limited to, the following:

  i. the right to reproduce, adapt, distribute, perform, display, communicate, and translate a Work;
 ii. moral rights retained by the original author(s) and/or performer(s);
iii. publicity and privacy rights pertaining to a person's image or likeness depicted in a Work;
 iv. rights protecting against unfair competition in regards to a Work, subject to the limitations in paragraph 4(a), below;
  v. rights protecting the extraction, dissemination, use and reuse of data in a Work;
 vi. database rights (such as those arising under Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, and under any national implementation thereof, including any amended or successor version of such directive); and
vii. other similar, equivalent or corresponding rights throughout the world based on applicable law or treaty, and any national implementations thereof.

2. Waiver. To the greatest extent permitted by, but not in contravention of, applicable law, Affirmer hereby overtly, fully, permanently, irrevocably and unconditionally waives, abandons, and surrenders all of Affirmer's Copyright and Related Rights and associated claims and causes of action, whether now known or unknown (including existing as well as future claims and causes of action), in the Work (i) in all territories worldwide, (ii) for the maximum duration provided by applicable law or treaty (including future time extensions), (iii) in any current or future medium and for any number of copies, and (iv) for any purpose whatsoever, including without limitation commercial, advertising or promotional purposes (the "Waiver"). Affirmer makes the Waiver for the benefit of each member of the public at large and to the detriment of Affirmer's heirs and successors, fully intending that such Waiver shall not be subject to revocation, rescission, cancellation, termination, or any other legal or equitable action to disrupt the quiet enjoyment of the Work by the public as contemplated by Affirmer's express Statement of Purpose.

3. Public License Fallback. Should any part of the Waiver for any reason be judged legally invalid or ineffective under applicable law, then the Waiver shall be preserved to the maximum extent permitted taking into account Affirmer's express Statement of Purpose. In addition, to the extent the Waiver is so judged Affirmer hereby grants to each affected person a royalty-free, non transferable, non sublicensable, non exclusive, irrevocable and unconditional license to exercise Affirmer's Copyright and Related Rights in the Work (i) in all territories worldwide, (ii) for the maximum duration provided by applicable law or treaty (including future time extensions), (iii) in any current or future medium and for any number of copies, and (iv) for any purpose whatsoever, including without limitation commercial, advertising or promotional purposes (the "License"). The License shall be deemed effective as of the date CC0 was applied by Affirmer to the Work. Should any part of the License for any reason be judged legally invalid or ineffective under applicable law, such partial invalidity or ineffectiveness shall not invalidate the remainder of the License, and in such case Affirmer hereby affirms that he or she will not (i) exercise any of his or her remaining Copyright and Related Rights in the Work or (ii) assert any associated claims and causes of action with respect to the Work, in either case contrary to Affirmer's express Statement of Purpose.

4. Limitations and Disclaimers.

 a. No trademark or patent rights held by Affirmer are waived, abandoned, surrendered, licensed or otherwise affected by this document.
 b. Affirmer offers the Work as-is and makes no representations or warranties of any kind concerning the Work, express, implied, statutory or otherwise, including without limitation warranties of title, merchantability, fitness for a particular purpose, non infringement, or the absence of latent or other defects, accuracy, or the present or absence of errors, whether or not discoverable, all to the greatest extent permissible under applicable law.
 c. Affirmer disclaims responsibility for clearing rights of other persons that may apply to the Work or any use thereof, including without limitation any person's Copyright and Related Rights in the Work. Further, Affirmer disclaims responsibility for obtaining any necessary consents, permissions or other rights required for any use of the Work.
 d. Affirmer understands and acknowledges that Creative Commons is not a party to this document and has no duty or obligation with respect to this CC0 or use of the Work.

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or

otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct

or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

   You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the

```
   appropriateness of using or redistributing the Work and assume any
   risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
   whether in tort (including negligence), contract, or otherwise,
   unless required by applicable law (such as deliberate and grossly
   negligent acts) or agreed to in writing, shall any Contributor be
   liable to You for damages, including any direct, indirect, special,
   incidental, or consequential damages of any character arising as a
   result of this License or out of the use or inability to use the
   Work (including but not limited to damages for loss of goodwill,
   work stoppage, computer failure or malfunction, or any and all
   other commercial damages or losses), even if such Contributor
   has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
   the Work or Derivative Works thereof, You may choose to offer,
   and charge a fee for, acceptance of support, warranty, indemnity,
   or other liability obligations and/or rights consistent with this
   License. However, in accepting such obligations, You may act only
   on Your own behalf and on Your sole responsibility, not on behalf
   of any other Contributor, and only if You agree to indemnify,
   defend, and hold each Contributor harmless for any liability
   incurred by, or claims asserted against, such Contributor by reason
   of your accepting any such warranty or additional liability.
```

Licence

Ce logiciel est distribué sous les termes de la licence publique générale GNU (ou en anglais GNU General Public License) version 2 ou ultérieure.

Pour les remerciements et les licences des composants/ressources/etc., voir la page des remerciements.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

```
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA  02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
```

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this

service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

> **a)** You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
> **b)** You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
> **c)** If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not

derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

> **a)** Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
> **b)** Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
> **c)** Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
one line to give the program's name and an idea of what it does.
```

```
Copyright (C) yyyy  name of author

This program is free software; you can redistribute it and/or
modify it under the terms of the GNU General Public License
as published by the Free Software Foundation; either version 2
of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA  02110-1301, USA.
```

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details
type `show w'.  This is free software, and you are welcome
to redistribute it under certain conditions; type `show c'
for details.
```

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright
interest in the program `Gnomovision'
(which makes passes at compilers) written
by James Hacker.

signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

End GNU General Public License

Le guide de l'utilisateur

Installation/Portabilité

Installation/Portabilité

Installation, désinstallation, portabilité et mises à jour de KeePass 1.x.

- Informations générales
- Le programme d'installation (fichier KeePass-1.xx-Setup.exe)
- La version portable (fichier KeePass-1.xx.zip)

Informations Générales

Lors du téléchargement de KeePass, vous avez le choix entre trois paquets différents :

- **KeePass-*1.xx*-Setup.exe :** le programme d'installation pour Windows.
- **KeePass-*1.xx*.zip :** le paquet KeePass au format ZIP (version portable).
- **KeePass-*1.xx*-Src.zip :** le code source.

Le programme d'installation et la version portable sont décrits en détail ci-dessous.

Le paquet de code source contient tout ce dont vous avez besoin pour compiler KeePass. Il comprend le code source C++ et les fichiers d'en-têtes, les fichiers de ressources, les sources de construction du programme d'installation, etc.

Contrairement à de nombreuses autres applications, KeePass ne *requiert* aucune fonction du dernier système d'exploitation Windows, comme la thématisation sur XP ou comme une application .NET qui nécessite le Framework .NET. Par exemple, KeePass prend en charge les thèmes, mais c'est facultatif. KeePass fonctionne parfaitement sur les systèmes plus anciens sans aucune limitation de fonctionnalités.

Mise à jour de KeePass :
Quand une nouvelle version de KeePass sort, vous pouvez alors mettre à jour votre installation existante de KeePass, sans perdre aucun paramètre de configuration. Les étapes dépendent du paquet que vous utilisez (installateur ou portable), cf. ci-dessous.

Les traductions doivent également être mises à jour lorsque vous installez une nouvelle version de KeePass. Vous pouvez trouver les derniers fichiers de traduction ici : traductions de KeePass.

Le programme d'installation (fichier KeePass-1.xx-Setup.exe)

L'équipe de développement de KeePass fournit un programme d'installation qui copie KeePass sur votre disque dur, crée des raccourcis dans le menu Démarrer et associe les fichiers KDB à KeePass, si vous le souhaitez.

De plus, KeePass est automatiquement configuré pour enregistrer ses paramètres dans le répertoire de données de l'application de l'utilisateur courant. De cette façon plusieurs utilisateurs peuvent utiliser une installation de KeePass sans écraser les paramètres de chacun (chaque utilisateur possède son propre fichier de configuration). Le programme d'installation doit être exécuté avec les droits d'un compte administrateur, cependant KeePass s'exécute bien sans les droits d'un compte administrateur une fois qu'il est installé.

Installation :
Pour installer KeePass, exécutez le fichier `KeePass-1.xx-Setup.exe` et suivez l'assistant.

Mise à jour :
Exécutez le fichier `KeePass-1.xx-Setup.exe`. Vous n'avez *pas* à désinstaller auparavant l'ancienne version. Vos options de configuration ne seront pas perdues.

Désinstallation :
Pour désinstaller KeePass, exécutez le programme de désinstallation, accessible par un raccourci dans le dossier du menu Démarrer de KeePass ou dans la section programme du panneau de configuration du système. Si vous souhaitez également supprimer vos paramètres de configuration, alors vous aurez besoin de supprimer le fichier de configuration dans le répertoire de données de l'application de votre profil utilisateur (cf. configuration).

Installation silencieuse :
Le programme d'installation de KeePass, `KeePass-1.xx-Setup.exe`, prend en charge des paramètres de ligne de commande pour une installation silencieuse, c'est-à-dire que le programme s'installe sans demander à l'utilisateur le répertoire cible ou les options d'association. Les paramètres par défaut du programme d'installation sont utilisés.

Le paramètre de ligne de commande `/SILENT` effectue une installation en mode silencieux et affiche une boîte de dialogue d'état pendant le processus d'installation. Aucune question ne sera cependant posée.

Le paramètre de ligne de commande `/VERYSILENT` effectue une installation en mode silencieux et n'affiche *pas* de boîte de dialogue d'état lors du processus d'installation.

Chemin de destination :
Le programme d'installation permet de choisir le chemin de destination sur lequel KeePass est installé. Toutefois, lorsque le programme d'installation détecte une installation existante de KeePass, il suppose que

l'utilisateur souhaite effectuer une mise à niveau et n'affiche donc pas la page de sélection du chemin de destination ; l'ancienne version sera remplacée par la nouvelle version. Si vous souhaitez déplacer une installation existante de KeePass vers un autre chemin, alors commencez par désinstaller l'ancienne version ; l'installateur de la nouvelle version affichera à nouveau la page de sélection du chemin de destination.

La version portable (fichier KeePass-1.xx.zip)

La version portable peut être transportée sur des appareils portables (comme des clés USB) et fonctionne sur n'importe quel ordinateur directement à partir de l'appareil, sans aucune installation. Il ne stocke rien sur votre système (contrairement au paquet d'installation, cf. ci-dessus). KeePass ne crée aucune nouvelle clé de registre et ne crée aucun fichier de configuration dans votre répertoire de données Windows ou d'application de votre profil utilisateur.

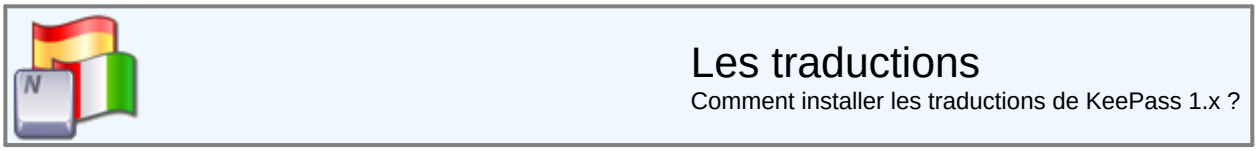
Assurez-vous que KeePass dispose d'un accès en écriture à son répertoire d'application. Sinon, le cas échéant, il essaiera d'enregistrer les options de configuration (rien de pertinent pour la sécurité) dans le répertoire de données d'application de l'utilisateur actuellement connecté (pour plus d'informations à ce sujet, cf. : configuration).

Installation :
KeePass n'a pas besoin d'être installé. Il suffit de télécharger le paquet ZIP, de le décompresser avec votre programme ZIP préféré et KeePass est prêt à être utilisé. Copiez-le à l'emplacement de votre choix (par exemple : sur votre clé USB) ; aucune configuration ou installation supplémentaire n'est nécessaire.

Mise à jour :
Téléchargez le dernier paquet portable de KeePass, décompressez-le et copiez tous les nouveaux fichiers par-dessus les anciens. Vos paramètres de configuration ne seront pas perdus (les paramètres sont stockés dans le fichier *KeePass.ini*, qui ne sera pas écrasé, car les paquets ZIP de KeePass n'incluent pas de fichier *KeePass.ini*).

Désinstallation :
Supprimer simplement le répertoire où se trouve KeePass.

Les traductions



- Installation des traductions de l'interface utilisateur
- Contenu localisé supplémentaire

Installation des traductions de l'interface utilisateur

Pour installer une traduction d'interface utilisateur, procédez comme suit :

1. Téléchargez le fichier ZIP de traduction à partir de la page des traductions et décompressez-le (dans le répertoire courant).
2. Dans KeePass, cliquez sur 'View' → 'Change Language...' → bouton 'Open Folder' ; KeePass ouvre maintenant un répertoire appelé 'Languages'. Déplacez-le/les fichier(s) décompressé(s) dans le répertoire 'Languages'.
3. Basculez sur KeePass, cliquez sur 'View' → 'Change Language...' →, sélectionnez votre langue. Redémarrez KeePass.

Remarque : pour déplacer le ou les fichiers décompressés (à l'étape 2), il est recommandé d'utiliser l'Explorateur Windows. D'autres gestionnaires de fichiers peuvent avoir des problèmes avec les droits d'accès.

Contenu localisé supplémentaire

Pour certaines langues (pas pour toutes), il existe un contenu localisé supplémentaire disponible, tel que des fichiers d'aide traduits, des didacticiels, etc. Tout ce contenu est disponible à partir de la même page où les traductions de l'interface utilisateur sont téléchargeables : page destraductions.

Si vous souhaitez créer vous-même du contenu traduit, veuillez tout d'abord demander à l'équipe de

KeePass si ce que vous envisagez de créer ne fonctionne pas déjà chez quelqu'un d'autre. Sinon, vous ferez plaisir à beaucoup de gens en créant du contenu traduit !

Les greffons

Les greffons (1.x)

Installation, désinstallation et sécurité des greffons de KeePass 1.x.

Introduction

KeePass dispose d'un framework de greffon. Les greffons peuvent fournir des fonctionnalités supplémentaires telles que la prise en charge de davantage de formats de fichiers pour l'importation/exportation, les fonctionnalités réseau, les fonctionnalités de sauvegarde, etc.

Les ressources en ligne

Les greffons se trouvent sur la page des greffons.

Installation et désinstallation

S'il n'y a pas d'instruction explicite pour savoir comment installer un greffon, alors procédez comme suit :

1. Téléchargez le greffon à partir de la page ci-dessus et décompressez le fichier ZIP dans un nouveau répertoire.
2. Dans KeePass, cliquez sur 'Outils' → 'Greffons (plug-in)...' → bouton 'Ouvrir dossier' ; KeePass ouvre maintenant un répertoire appelé 'Plugins'. Déplacez le nouveau répertoire (contenant les fichiers du greffon) dans le répertoire 'Plugins'. Quand on utilise plusieurs greffons, on les enregistre dans des répertoires séparés car c'est avantageux (aucune collision de nom de fichier, une mise à jour plus facile, etc.).
3. Redémarrez KeePass afin de charger le nouveau greffon.

Pour désinstaller un greffon, supprimez les fichiers du greffon.

La sécurité

Les greffons doivent être stockés dans le dossier 'Plugins' du répertoire de l'application KeePass. Un attaquant qui peut copier un greffon malveillant dans ce dossier pourrait également typiquement remplacer le fichier 'KeePass.exe' par un malware. Comme protection contre de telles attaques, uneliste de contrôle d'accès (ACL) au système de fichier approprié devra être utilisée (pour le répertoire de l'application KeePass en intégralité, incorporant le dossier 'Plugins') ; les privilèges de l'administrateur devront être nécéssaire pour les accès en écriture.

- L'installateur KeePass et le package MSI installe KeePass dans le répertoire Program Files par défaut. Ce répertoire a typiquement une ACL appropriée, et le répertoire de l'application KeePass hérite de cette ACL. Donc, vous n'avez pas besoin de spécifer une ACL manuellement.
- Si vous installez KeePass dans un répertoire différent ou si vous utlisez le package portable, alors il est recommandé que vous spécifiez manuellement une ACL appropriée.

Qu'en est-il de la sécurité des greffons ? Les greffons malveillants ne peuvent-ils pas s'injecter dans KeePass ?

Si les greffons peuvent s'enregistrer eux-mêmes (c'est-à-dire avoir un accès en écriture au dossier KeePass), ils pourraient également simplement remplacer le fichier « KeePass.exe » dans son intégralité. C'est un problème de droits d'accès aux fichiers, pas du système des greffons.

Si cela vous inquiète, alors installez KeePass en tant qu'administrateur dans le répertoire des fichiers programme (qui est par défaut, généralement dans un dossier 'C:\Program Files (x86)'). Ensuite, lancez

KeePass et les autres applications uniquement en tant qu'utilisateur normal (c'est-à-dire sans les privilèges du compte administrateur).

Cela résout le problème ci-dessus. Comme le répertoire KeePass est protégé en écriture pour les utilisateurs normaux, aucun autre programme ne peut y copier de fichiers. KeePass exige que les greffons soient dans le répertoire de l'application. Par conséquent, les greffons ne peuvent plus s'introduire.

Si vous utilisez le paquet portable de KeePass ou si vous l'avez installé dans un autre répertoire, alors vous devrez régler vous-même les autorisations relatives à ce répertoire.

La compatibilité

La compatibilité

La compatibilité entre les différentes versions de KeePass, utilisation côte à côte (SxS).

Cette page liste la compatibilité de **KeePass 1.43** avec les autres versions de KeePass.

Remarquez que la dernière version peut charger tous les fichiers de base de données créés par n'importe quelle ancienne version de KeePass version sans aucune perte de données.

Si vous cherchiez des instructions sur comment mettre à jour vers la dernière version, alors veuillez lire les instructions de mise à jour.

La compatibilité de fichier de base de données (fichiers KDB) :

Type de compatibilité	Versions
Côte à côte complet	1.42, 1.41, 1.40.1, 1.40, 1.39, 1.38, 1.37, 1.36, 1.35, 1.34, 1.33, 1.32, 1.31, 1.30, 1.29, 1.28, 1.27, 1.26, 1.25, 1.24, 1.23, 1.22, 1.21, 1.20, 1.19b, 1.19, 1.18, 1.17, 1.16, 1.15, 1.14, 1.13, 1.12, 1.11, 1.10, 1.09, 1.08, 1.07, 1.06, 1.05, 1.04, 1.03, 1.02
Côte à côte base de données	1.01, 1.00, 0.99c, 0.99b, 0.99a, 0.98b, 0.98a
Côte à côte avec perte	0.97c, 0.97b, 0.97a, 0.96b, 0.96a, 0.95b, 0.95a
Pas de côte à côte	0.94a, 0.93b, 0.93a, 0.92a, 0.91, 0.90a, 0.89, 0.88a, 0.87, 0.86, 0.85, 0.84, 0.83b, 0.83, 0.82, 0.81, 0.80
Retour complet	1,42, 1.41, 1.40.1, 1.40, 1.39, 1.38, 1.37, 1.36, 1.35, 1.34, 1.33, 1.32, 1.31, 1.30, 1.29, 1.28, 1.27, 1.26, 1.25, 1.24, 1.23, 1.22, 1.21, 1.20, 1.19b, 1.19, 1.18, 1.17, 1.16, 1.15, 1.14, 1.13, 1.12, 1.11, 1.10, 1.09, 1.08, 1.07, 1.06, 1.05, 1.04, 1.03, 1.02, 1.01, 1.00, 0.99c, 0.99b, 0.99a, 0.98b, 0.98a, 0.97c, 0.97b, 0.97a, 0.96b, 0.96a, 0.95b, 0.95a, 0.94a, 0.93b, 0.93a, 0.92a, 0.91, 0.90a, 0.89, 0.88a, 0.87, 0.86, 0.85, 0.84, 0.83b, 0.83, 0.82, 0.81, 0.80

Côte à côte complet : ce type de compatibilité signifie que vous pouvez utiliser la dernière version avec celles répertoriées côte à côte sans aucune perte de données. Ces versions utilisent exactement le même format de base de données et sont 100% compatibles.

Côte à côte base de données : ce type signifie que vous pouvez exécuter ces versions de KeePass côte à côte, les fichiers de base de données sont compatibles. Mais il y a quelques incompatibilités visuelles mineures. Par exemple : de KeePass 1.01 à 1.02, les icônes d'entrée ont changé. Bien que cela n'affecte pas le format de fichier de la base de données, la création d'une base de données avec la version 1.01

entraînera l'affichage d'icônes différentes dans la version 1.02.

Côte à côte avec perte : ce type signifie qu'il est possible d'utiliser les versions répertoriées avec la dernière côte à côte (le format de base de données est compatible), mais certaines données de la version la plus récente peuvent être perdues ou affichées de manière incorrecte dans les anciennes versions. Par exemple : les anciennes versions ne connaissent pas encore les méta-entrées et les affichent comme des entrées normales. Bien qu'aucune donnée ne soit perdue, les utilisateurs peuvent être confus lorsque KeePass affiche de telles méta-entrées.
Les versions répertoriées peuvent ouvrir les bases de données de la dernière, mais il n'est généralement pas recommandé de les utiliser côte à côte.

Pas de côte à côte : cela signifie que le format de la base de données de la dernière version est incompatible avec les versions KeePass répertoriées. Ceux répertoriés ne sont pas en mesure de charger les fichiers de base de données créés par la dernière version. Notez que la dernière version peut charger *toutes* les versions de la base de données (rétrocompatibilité complète).

Retour complet : la dernière version de KeePass peut charger tous les fichiers de base de données créés par une version plus ancienne. KeePass a été conçu pour être 100 % rétrocompatible. Aucune donnée n'est perdue.

Les codes d'erreur

Code d'erreur	Nom	Utilisateur	Description
0x00000000	Inconnue	✗	Une erreur inconnue s'est produite. KeePass utilise ce code d'erreur en interne et l'utilisateur ne devrait jamais voir cette erreur.
0x00000001	Succès	✓	Aucune erreur n'est survenue. Tout a parfaitement fonctionné.
0x00000002	Paramètre invalide	✗	Une fonction dans KeePass a reçu un paramètre invalide. Cela ne devrait jamais arriver.
0x00000003	Manque de mémoire	✓	Le système d'exploitation n'a pas accordé suffisamment de mémoire à KeePass. L'opération en cours a été annulée. La base de données est peut-être dans un état cassé et ne doit pas être enregistrée.
0x00000004	Clé invalide	✓	La clé principale fournie par l'utilisateur (mot de passe principal/fichier de clé) pour la base de données était incorrecte ou la base de données

			est corrompue. Assurez-vous que le mot de passe principal et/ou le fichier clé sont corrects. Si vous êtes absolument sûr que le mot de passe principal/fichier de clé est correct, alors le fichier est probablement corrompu (vous avez peut-être accidentellement retiré la clé USB de l'ordinateur sans la démonter). Dans ce cas, essayez la fonctionnalité de réparation de la base de données de KeePass.
0x00000005	Erreur d'Accès Fichier : Lire Fichier	✔	Le système d'exploitation (Windows) n'a pas accordé à KeePass l'accès en lecture au fichier de base de données spécifié. Notez que cela ne signifie pas que la base de données est corrompue ou quelque chose comme ça ; KeePass ne peut tout simplement pas obtenir un accès en lecture au fichier. Assurez-vous que vous pouvez lire le fichier.
0x00000006	Erreur d'Accès Fichier : Écrire Fichier	✔	Le système d'exploitation (Windows) n'a pas accordé à KeePass l'accès en écriture au fichier de base de données spécifié. Essayez d'enregistrer la base de données à un emplacement différent, auquel les administrateurs de votre réseau vous ont accordé un accès en écriture.
0x00000007	Erreur Fichier : Lire	✔	Une erreur s'est produite lors de la lecture de la base de

			données ou du fichier clé. Cela peut arriver si, par exemple, vous ouvrez une grande base de données à partir d'une clé USB et retirez la clé pendant que KeePass lit le fichier. Assurez-vous que KeePass peut accéder au fichier complet et ne retirez pas l'appareil avant que KeePass ne l'ait lu complètement.
0x00000008	Erreur Fichier : Écrire	✔	Une erreur s'est produite lors de l'écriture de la base de données ou du fichier clé. Cela peut arriver si, par exemple, vous enregistrez une grande base de données sur une clé USB et retirez la clé pendant que KeePass écrit le fichier. Assurez-vous qu'il reste suffisamment d'espace libre sur l'appareil cible et n'enlevez pas l'appareil avant que KeePass n'ait complètement écrit le fichier. Assurez-vous d'avoir correctement démonté l'appareil (clé USB).
0x00000009	Source d'aléas invalide	✘	Il s'agit d'une erreur cryptographique interne. La source aléatoire, utilisée pour générer des nombres aléatoires, n'est pas valide. Cela signifie qu'il produit des valeurs non aléatoires et que la sécurité (secret) de votre base de données ne peut donc pas être garantie ; donc, l'opération a été abandonnée. Cette erreur ne devrait jamais se produire. Si vous voyez ce code d'erreur, alors veuillez soumettre un rapport de bogue (voir ci-dessous).
0x0000000A	Structure de fichier	✔	La structure du fichier

	invalide		de base de données actuel n'est pas valide. Cela peut se produire si la clé principale fournie par l'utilisateur (mot de passe principal/fichier de clé) n'est pas valide ou si le fichier est corrompu. Si vous êtes sûr que la clé est correcte, alors essayez la fonctionnalité de réparation de la base de données.
0x0000000B	Erreur cryptographique	✗	Une erreur cryptographique interne s'est produite. L'un des composants cryptographiques ne peut pas être initialisé, testé et/ou a renvoyé une erreur.
0x0000000C	Taille de fichier invalide	✓	La taille du fichier n'est pas valide. Cela signifie que le fichier est corrompu.
0x0000000D	Signature de fichier invalide	✓	La signature du fichier n'est pas valide. Cela signifie que le fichier est corrompu et/ou n'est pas un fichier que KeePass peut lire.
0x0000000E	Entête de fichier invalide	✓	L'en-tête du fichier n'est pas valide. Le fichier peut être corrompu, avoir été créé par une version plus récente de KeePass ou ne pas être du tout un fichier KeePass.
0x0000000F	Erreur d'accès fichier : Lire clé	✓	Le système d'exploitation (Windows) n'a pas accordé à KeePass l'accès en lecture au fichier clé spécifié ou il n'existe pas. Notez que cela ne signifie pas que le fichier clé est corrompu, KeePass ne peut tout simplement pas obtenir un accès en lecture au fichier. Assurez-vous que le média contenant le

			fichier clé est inséré et que KeePass a le droit d'y accéder (vérifiez les droits d'accès au fichier, assurez-vous qu'aucune autre application ne bloque le fichier, ...). Si vous sélectionnez le lecteur du fichier clé (c'est-à-dire que vous ne le spécifiez pas manuellement), alors recherchez le fichier *"pwsafe.key"*. Consultez la documentation de la clé principale pour plus d'informations sur l'utilisation des fichiers de clé.
0x00000010	Fournisseur : clé invalide	✔	Le greffon du fournisseur de clé n'a pas fourni de clé valide.
0x00000011	Erreur de fichier : Vérifier	✔	Les données qui ont été envoyées au disque/lecteur ne correspondent pas aux données qui sont maintenant stockées sur le disque/lecteur, c'est-à-dire que le fichier a été corrompu par quelque chose. Voir l'erreur 0x00000008.
0x00000012	Fichier KDBX	✔	Le fichier que vous avez essayé d'ouvrir est au format KDBX. Les fichiers KDBX ne sont pris en charge que par KeePass 2.x. Soit vous utilisez KeePass 2.x soit vous utilisez la fonction "Exporter" de KeePass 2.x pour migrer le fichier vers un fichier KDB KeePass 1.x.
0x00000013	Erreur système	✔	Une erreur au niveau de l'utilisateur s'est produite et le système a fourni la description détaillée affichée dans la boîte de message d'erreur.
0x00000014	Base de données vide	✔	La base de données est vide. KeePass refuse de charger/sauvegarder des bases de données

			vides.

Utilisateur :

✔ : cette erreur n'est pas un bogue. KeePass n'a pas réussi à effectuer certaines opérations et vous pouvez corriger cette "erreur" vous-même. Par exemple : lorsque vous avez entré une clé invalide pour votre base de données, ne pas ouvrir la base de données n'est pas un bogue.

✘ : cette erreur est un bogue. Vous ne devriez jamais voir cette erreur. Veuillez soumettre un rapport de bogue.

Les fonctionnalités

Accessibilité

Accessibilité

Les informations sur les fonctionnalités pour les personnes handicapées.

- Les informations
- Les documents

Information

KeePass est développé dans un souci d'accessibilité. Nous nous efforçons d'assurer une bonne convivialité pour les personnes handicapées.

Exemples :

- **Le clavier** :
  - Toutes les entrées peuvent être effectuées à l'aide d'un clavier (sans souris ou autre dispositif d'entrée).
  - La fenêtre principale prend en charge de nombreux raccourcis clavier.
  - Les commandes de menu et les commandes de dialogue ont des clés d'accès (indiqué par un caractère souligné lorsque vous appuyez sur la touche Alt.
  - Les touches normalisées et les combinaisons de touches sont prises en charge (Entrée/Échap pour la fermeture d'une boîte de dialogue, Ctrl+C pour la copie de données dans le presse-papiers, Ctrl+F pour la recherche de données, etc.).
  - Les fenêtres/boîtes de dialogue ont un ordre d'onglet raisonnable.
- **La couleur** :
  - KeePass utilise le thème (le schéma de couleur, les polices, etc.) du système d'exploitation. Tous les thèmes (comprenant les thèmes sombres et ceux avec un haut contraste) sont pris en charge.
    Voir également : 'Est-ce que l'interface graphique de l'utilisateur prend en charge les thèmes sombres ?' .
  - Différents style de menu et de barres d'outils sont pris en charge(sélectionnable dans la boîte de dialogues des options de KeePass 2.x ; menu principal 'Outil' → 'Options...' → onglet 'Interface (IHM)').
    Voir également : 'Menu/Toolbar Style Survey'.
  - Differents styles de bannières des boîtes de dialogue sont pris en charge (choisissable dans la boîte de dialogue des options de KeePass 2.x).
  - La couleur d'arrière-plan de l'élément en alternance peut être personnalisée (dans la boîte de dialogue Options de Keepass).
- **La police** :
  - KeePass utilise le thème (le schéma de couleur, les polices, etc.) du système d'exploitation. Tous les principaux systèmes d'exploitation prennent en charge la modification de la police d'interface utilisateur par défaut.

    Voir également : 'Comment modifier (la taille de) la police de l'interface graphique de l'utilisateur ?'.

  - La police utilisée dans les contrôles de liste peut être personnalisée (dans la boîte de dialogue des options de Keepass). Par défaut, la police par défaut du cadriciel(framework)/système est utilisée.
  - La police utilisée dans les commandes d'édition de mot de passe peut être personnalisée (dans la boîte de dialogue des options de Keepass). Par défaut, la police monospace par défaut du cadriciel (framework)/système est utilisée.
- **Échelle (DPI élevé)** :
  - La mise à l'échelle de l'interface utilisateur via le paramètre DPI du système d'exploitation est pris en charge.
  - Lorsqu'une boîte de dialogue ou un menu ne s'adapte pas à l'écran actuel (par exemple en raison d'une valeur de DPI élevée ou une grande police), alors Keepass 2.x fournit des barres de défilement ou des boutons pour défiler à l'écran.
- **La technologie d'assistance** :
  - Keepass peut être commandé via des applications de technologie d'assistance. Les API d'accessibilité standard sont prises en charge.
  - La plupart des commandes de Keepass sont des commandes standard fournies par le cadriciel(framework)/système.
  - Keepass 2.x propose une option 'Optimiser pour le narrateur' (dans le menu principal 'Outils' → 'Options... → Tab 'Avancé'). Si cette option est activée ou si Keepass détecte automatiquement le narrateur (via '`SystemParametersInfo`' avec '`SPI_GETSCREENREADER`'), diverses optimisations pour les narrateurs sont effectuées, y compris, mais sans s'y limiter :
    - l'affectation d'un nom accessible pour plus de commandes. Amélioration de certains noms accessibles.
    - Affectation d'un rôle accessible pour certaines commandes.
    - Arbre de commande amélioré (par exemple : pour les applications de technologie d'assistance basées sur l'automatisation de l'interface utilisateur).
  - L'option est désactivée par défaut et ne doit être activée que par les utilisateurs qui utilisent le narrateur, car il diminue les performances de l'application et n'offre aucun avantage pour les utilisateurs sans narrateur.
- **La documentation et le site Web** :
  - Chaque page a un titre significatif.
  - Les balises HTML sémantiques ('`nav`', '`footer`', '`h1`', '`ul`', etc.) sont utilisées.
  - Les images qui transmettent des informations ont un texte alternatif (attribut '`alt`'). Les images décoratives ont un texte alternatif vide.

Les documents

Nous apprécions l'accessibilité. Cependant, nous ne fournissons aucun document (certifications, rapports, questionnaires complétés, déclarations de conformité, etc., sauf cette page d'aide) lié à l'accessibilité, car il y a généralement des incertitudes/ambiguïtés légales et conceptuelles avec de tels documents.

La saisie automatique

La saisie automatique

Fonction puissante qui envoie des pressions de touches simulées aux autres applications.

- Informations de base sur la saisie automatique
- Exigences et limitations
- Appel de la saisie automatique
  - Depuis le menu contextuel : commande '*Accomplir la saisie automatique*'
  - Raccourci clavier global de la saisie automatique
- Spécification des séquences de touches pressées et des fenêtres cibles
  - Les séquences de touches pressées de saisie automatique
  - Les filtres de fenêtre cible
  - Modifier la séquence de saisie automatique par défaut

- Exemple d'utilisation

Les informations de base sur la saisie automatique

KeePass dispose d'une fonctionnalité de "saisie automatique". Cette fonctionnalité permet de définir une séquence de touches pressées, que KeePass peut automatiquement accomplir pour vous. Les touches pressées simulées peuvent être envoyées à n'importe quelle autre fenêtre actuellement ouverte de votre choix (navigateur, boîtes de dialogue de login, etc.).

Par défaut, la séquence de touches pressées envoyée est `{USERNAME}{TAB}{PASSWORD}{ENTER}`, c'est-à-dire qu'elle tape d'abord le nom d'utilisateur de l'entrée sélectionnée, puis appuie sur la touche Tabulation, saisit le mot de passe de l'entrée et appuie finalement sur la toucheEntrée.

Pour les entrées de NAT (TAN), la séquence par défaut est `{PASSWORD}`, c'est-à-dire qu'elle saisit juste le NAT dans la fenêtre cible, sans appuyer sur Entrée.

Vous pouvez librement définir votre propre séquence de saisie automatique : écrivez simplement la séquence dans le **champ remarques** de l'entrée, préfixé par "`saisie automatique :`". Vos remarques pourraient ressembler à ceci :

```
Vous pouvez écrire des notes ici.
Mon adresse de courriel que j'utilise pour m'inscrire : moi@exemple.com

Auto-Type: {USERNAME}{TAB}{TAB}Une certaine chaîne de caractères fixée{TAB}{PASSWORD}{ENT

Ici vous pouvez continuer avec vos remarques si vous le souhaitez...
```

Comme vous pouvez le voir, la seule chose importante est que la séquence de saisie automatique soit préfixée en utilisant "`Auto-Type:`" et est une seule ligne. Une séquence de saisie automatique ne peut pas être définie à l'aide de deux lignes ou plus.

Si vous définissez deux ou plusieurs séquences de saisie automatique, alors la première est utilisée.
De plus, vous pouvez créer des associations fenêtre/séquence personnalisées, qui remplacent la séquence par défaut. Vous pouvez spécifier différentes séquences de touches pressées pour différentes fenêtres pour chaque entrée. Par exemple : imaginez une page HTML, sur laquelle vous souhaitez vous connecter, qui a plusieurs pages dont une permet la connexion. Ces pages pourraient toutes sembler un peu différentes (sur une vous pourriez de plus avoir besoin de vérifier des cases à cocher – comme on en voit souvent sur les forums). Ici la création d'associations fenêtre/séquence personnalisées résout les problèmes : il vous suffit de spécifier simplement différentes séquences de saisie automatique pour chaque fenêtre (identifiée par leur titre).

Appel de la saisie automatique :
Il y a trois méthodes différentes pour appeler la saisie automatique :

- Appel de la saisie automatique pour une entrée en utilisant la commande du menu contextuel *Accomplir la saisie automatique* tout en ayant au préalable sélectionnée l'entrée.
- Sélectionnez l'entrée et appuyez sur Ctrl+V (c'est le raccourci de la commande du menu contextuel ci-dessus).
- En utilisant les raccourcis clavier globaux de saisie automatique. KeePass recherchera dans toutes les entrées de la base de données actuellement ouverte des séquences de correspondance.

Toutes les méthodes sont expliquées en détail ci-dessous.

Focus d'entrée :
Remarquez que la saisie automatique démarre en tapant dans le contrôle de la fenêtre cible qui a le focus d'entrée. Donc, par exemple pour la séquence par défaut vous devez vous assurer que le focus d'entrée est positionné sur le contrôle d'utilisateur de la fenêtre cible avant l'appel de la saisie automatique en utilisant les méthodes ci-dessus.

Les exigences et les limitations

Les droits :
Pour que la saisie automatique fonctionne, KeePass doit s'exécuter avec les mêmes droits ou droits plus élevés que l'application cible. Notamment, si l'application cible s'exécute avec les droits d'administration, KeePass doit également s'exécuter avec les droits d'administration. Pour les détails, cf.conception du mécanisme d'intégrité de Windows. Un exemple : certaines instances de VMware Workstation s'exécutent sur un niveau d'intégrité supérieur.

Les bureaux à distance et les machines virtuelles :
KeePass ne connaît pas la disposition du clavier qui a été sélectionné sur un bureau distant ou une fenêtre de machine virtuelle. Si vous souhaitez saisir automatiquement dans une telle fenêtre, alors vous devez vous assurer que le système local et le système distant/virtuel utilise la même disposition de clavier.

Au moment d'accomplir la saisie automatique à l'intérieur d'un bureau distant ou une fenêtre de machine virtuelle, les caractères suivants peuvent être problématiques (selon les circonstances exactes) et doivent donc être évités, si possible : " (U+0022), ' (U+0027), ^ (U+005E), ` (U+0060), ~ (U+007E), ¨ (U+00A8), ¯ (U+00AF), ° (U+00B0), ´ (U+00B4), ¸ (U+00B8), les lettres qui modifient l'espacement (U+02B0 to U+02FF), et les caractères qui ne peuvent pas être réalisés en une combinaison de touches directe.

Wayland :
Sur des système Unix-like avec un compositeur Wayland, il peut y avoir d'autres limitations ; cf. la page Auto-Type on Wayland.

Menu contextuel : la commande 'Accomplir la saisie automatique'

Cette méthode est celle qui nécessite le moindre effort et est la plus simple, mais elle a l'inconvénient que vous devez sélectionner dans KeePass l'entrée dont vous souhaitez la saisie automatique.

La méthode est simple : clic droit sur l'entrée de votre base de données actuellement ouverte et cliquez '*Accomplir la saisie automatique*' (ou appuyez alternativement le raccourci Ctrl+V pour cette commande). La fenêtre qui précédemment avait le focus (c'est-à-dire celle dans laquelle vous travailliez avant de permuter vers KeePass) sera appelée au premier plan et KeePass saisit automatiquement vers cette fenêtre.

La séquence qui est saisie automatiquement dépend du titre de la fenêtre. Si vous ne spécifiez aucune association fenêtre/séquence personnalisée la séquence par défaut est envoyée. Si vous avez créé des associations, KeePass utilise la séquence de la première association qui correspond. Si aucune des associations ne correspond, alors la séquence par défaut est utilisée.

Le raccourci clavier de la saisie automatique globale

C'est la méthode la plus puissante, mais elle nécessite également un peu plus de travail/connaissance, avant de pouvoir être utilisée.

Exemple d'une simple saisie automatique globale :

1. Créer dans KeePass une entrée qui s'intitule *Bloc-notes* avec les valeurs pour le nom d'utilisateur et le mot de passe.
2. Démarrer le Bloc-notes (depuis 'Programmes' → 'Accessoires').
3. Appuyer sur Ctrl+Alt+A depuis le Bloc-notes. Le nom d'utilisateur et le mot de passe seront saisis dans le Bloc-notes.

Le titre *Bloc-notes* de l'entrée de KeePass correspond avec le titre de la fenêtre du Bloc-notes et la séquence par défaut de saisie automatique est tapée.

Comment ça fonctionne ? - Détails :

KeePass enregistre un raccourci clavier global pour la saisie automatique. L'avantage de ce raccourci clavier est que vous n'avez pas à permuter vers la fenêtre KeePass et sélectionner l'entrée. Vous appuyez simplement sur le raccourci tout en ayant la fenêtre cible ouverte (c'est-à-dire la fenêtre qui recevra la pression des touches simulées).

Par défaut, le raccourci clavier global est Ctrl+Alt+A (c'est-à-dire maintenez les touches Ctrl et Alt, appuyez sur A et relâchez toutes les touches). Vous pouvez modifier ce raccourci clavier dans la boîte de dialogue des options (menu principal → 'Outils' → 'Options...', onglet 'Avancé') : ici, cliquez dans la fenêtre de saisie de texte du raccourci de saisie automatique global et saisissez le raccourci que vous souhaitez utiliser. Si le raccourci clavier est utilisable, il apparaîtra dans la zone de texte.

Quand vous appuyez le raccourci clavier, KeePass examine le titre de la fenêtre actuellement ouverte et recherche les entrées utilisables dans la base de données actuellement ouverte. Si KeePass trouve plusieurs entrées qui peuvent être utilisées, alors il affiche une boîte de dialogue de sélection. Une entrée est considérée comme utilisable pour le titre de la fenêtre courante quand au moins une des conditions suivantes est remplie :

- Le titre de l'entrée est une sous-chaîne du titre de la fenêtre actuellement active.

- L'entrée a une association fenêtre/séquence, dont le spécifiant de fenêtre correspond au titre de la fenêtre actuellement active.

La seconde condition a déjà été mentionnée, mais la première est nouvelle. En utilisant les titres d'entrée comme filtres pour les titres des fenêtres, le coût de la configuration pour la saisie automatique est presque nul : vous n'avez besoin que de vous assurer que le titre de l'entrée est contenu dans le titre de la fenêtre dans laquelle vous souhaitez que l'entrée soit saisie automatiquement. Bien sûr, ceci n'est pas toujours possible (par exemple : si une page HTML a un titre très générique comme *"Bienvenue"*), alors ici vous devez utiliser des associations fenêtre/séquence personnalisées.

Des associations fenêtre/séquence personnalisées peuvent être spécifiées sur l'onglet *'Saisie automatique'* de chaque entrée.

Des association fenêtre/séquence personnalisées peuvent être spécifiées en utilisant le champ Remarques de l'entrée.

```
Mon adresse de courriel que j'utilise pour m'inscrire : moi@exemple.com

Auto-Type: {USERNAME}{TAB}{TAB}Une certaine chaîne de caractères fixée{TAB}{PASSWORD}{ENT
Auto-Type-Window: Un site Web - Bienvenue*

Ici, vous pouvez continuer avec vos remarques si vous le souhaitez...
```

Si vous avez maintenant une fenêtre ouverte qui commence par "Un site Web - Bienvenue" et appuyez sur la combinaison de touches de raccourci globale de saisie automatique, alors KeePass exécute la séquence de type automatique ci-dessus.

Certains sites, notamment les banques, utilisent des schémas de connexion multi-pages. Vous pouvez utiliser des chaînes `Auto-Type-Window` pour automatiser ces sites. Vous pouvez également utiliser les chaînes `Auto-Type-Window` pour normaliser votre connexion LAN dans une entrée KeePass.

Vous pouvez définir autant de chaînes `Auto-Type-Window` par entrée que vous le souhaitez.

De plus, une séquence peut être utilisée pour plusieurs fenêtres. Pour cela, définissez d'abord une paire de fenêtre/séquence comme d'habitude, puis continuez en ajoutant '-' et un nombre, en commençant par 1. Exemple :

```
Auto-Type: {USERNAME}{TAB}{PASSWORD}{ENTER}
Auto-Type-Window: Une certaine boîte de dialogue - *
Auto-Type-1: {USERNAME}{ENTER}
Auto-Type-Window-1: * - Editor
Auto-Type-Window-1: * - Notepad
Auto-Type-Window-1: * - WordPad
Auto-Type-2: {PASSWORD}{ENTER}
Auto-Type-Window-2: Une certaine page Web - *
```

Ici, la séquence `Auto-Type-1` sera utilisée pour toutes les fenêtres `Auto-Type-Window-1`.

Les associations de fenêtres personnalisées remplacent le titre de l'entrée KeePass. Si des associations de fenêtres personnalisées sont spécifiées, alors elles seront les seuls éléments utilisés pour déterminer une correspondance et le titre d'entrée KeePass sera ignoré.
Les définitions de fenêtre de saisie automatique, des titres d'entrée et adresses (URLs) sont compilées par Spr, c'est-à-dire que des paramètres substituables (placeholders), variables d'environment, références de champ, etc. peuvent être utilisés.

Les séquences de touches pressées de la saisie automatique

Une séquence de touches pressées de saisie automatique est une chaîne d'une ligne qui peut contenir des paramètres substituables et des codes de touche spéciale.

Une liste complète de tous les paramètres substituables pris en charge peut être trouvée sur la page paramètres substituables. Les codes de touche spéciale peuvent être trouvés ci-dessous.

Au-dessus vous avez déjà vu que la saisie automatique par défaut est `{USERNAME}{TAB}{PASSWORD}{ENTER}`. Ici, `{USERNAME}` et `{PASSWORD}` sont des paramètres substituables : lorsque la saisie automatique est accomplie, ceux-ci sont remplacés par les valeurs de champ appropriées de l'entrée. `{TAB}` et `{ENTER}` sont des codes de touche spéciale : ils sont remplacés par les touches appropriées. Les codes de touche spéciale sont la seule façon de spécifier des touches spéciales comme Flèche vers le

bas, Maj, Échap, etc.

Bien sûr, les séquences de touches peuvent également contenir des caractères simples à envoyer. Par exemple : la chaîne suivante est parfaitement valide en tant que chaîne de séquence de touches : `{USERNAME}{TAB}Du texte pour envoi ! {ENTER}`.

Les codes de touche spéciale sont sensibles à la casse.
Les touches spéciales :
Les codes suivants pour les touches spéciales sont pris en charge :

Touche spéciale	Code
Tabulation	{TAB}
Entrée	{ENTER} ou ~
Flèche vers le haut	{UP}
Flèche vers le bas	{DOWN}
Flèche gauche	{LEFT}
Flèche droite	{RIGHT}
Insertion	{INSERT} ou {INS}
Supprimer	{DELETE} ou {DEL}
Début	{HOME}
Fin	{END}
Page précédente	{PGUP}
Page suivante	{PGDN}
Espace	{SPACE}
Retour arrière	{BACKSPACE}, {BS} ou {BKSP}
Pause	{BREAK}
Verrouillage des majuscules	{CAPSLOCK}
Échap	{ESC}
Touche Windows	{WIN} (équ. à {LWIN})
Touche Windows : gauche, droite	{LWIN}, {RWIN}
Applications/Menu	{APPS}
À l'aide	{HELP}
Pavé numérique verrouillé	{NUMLOCK}
Imprime écran	{PRTSC}
Arrêt défilement	{SCROLLLOCK}
F1 - F16	{F1} - {F16}
Pavé numérique +	{ADD}
Pavé numérique -	{SUBTRACT}
Pavé numérique *	{MULTIPLY}
Pavé numérique /	{DIVIDE}
Pavé numérique 0 à 9	{NUMPAD0} à {NUMPAD9}
Maj	+
Ctrl	^

Alt	%

Touche spéciale	Code
+	{PLUS}
%	{PERCENT}
^	{CARET}
~	{TILDE}
(,)	{LEFTPAREN}, {RIGHTPARENT}
{, }	{LEFTBRACE}, {RIGHTBRACE}

De plus, certaines commandes spéciales sont prises en charge :

Syntaxe de commande	Action
{DELAY *X*}	Retarde *X* millisecondes.
{DELAY=*X*}	Définit le retard par défaut à *X* millisecondes pour toutes les pressions de touches suivantes.
{CLEARFIELD}	Efface le contenu du contrôle d'édition qui a actuellement le focus (seulement les contrôles d'édition sur une seule ligne).
{VKEY *X*}	Envoi la touche virtuelle de valeur *X*.
{APPACTIVATE *TitreFenêtre*}	Active la fenêtre "*TitreFenêtre*".
{BEEP *X Y*}	Émet un son avec une fréquence de *X* Hertz et une durée de *Y* millisecondes.

Exemples :

{TITLE}{TAB}{USERNAME}{TAB}{PASSWORD}{ENTER}
Saisit le titre de l'entrée, une Tabulation, le nom d'utilisateur, une Tabulation, le mot de passe de l'entrée actuellement sélectionnée, et appuie sur Entrée.

{TAB}{PASSWORD}{ENTER}
Appuie sur la touche Tabulation, saisit le mot de passe de l'entrée et appuie sur Entrée.

{USERNAME}{TAB}^v{ENTER}
Saisit le nom d'utilisateur, appuie sur Tabulation, appuie sur Ctrl+V (qui copie les données depuis le presse-papiers de Windows dans la plupart des applications), et appuie surEntrée.

Basculer les cases à cocher :
Une case à cocher (par exemple : "Rester connecté sur cet ordinateur") peut habituellement être basculé en envoyant un caractère espace (' '). Exemple :
{USERNAME}{TAB}{PASSWORD}{TAB} {TAB}{ENTER}
S'il y a un formulaire avec un champ de nom d'utilisateur, un champ de mot de passe et une case à cocher, cette séquence entrera le nom d'utilisateur, le mot de passe et activera la case à cocher qui suit le contrôle du mot de passe.

Appuyer sur les boutons autres que ceux par défaut :
En appuyant sur les boutons autres que ceux par défaut, cela revient à basculer les cases à cocher : envoie un espace (' '). Remarquez que cela doit être utilisé que pour les boutons autres que ceux par défaut ; pour les boutons par défaut, {ENTER} doit être envoyé à la place.

Les plus hauts caractères ANSI :
La fonction de saisie automatique prend en charge l'envoi des plus hauts caractères ANSI dans l'intervalle 126-255. Ce qui signifie que vous pouvez envoyer un caractère spécial comme ©, @, etc. sans aucun

problème ; vous pouvez les écrire directement dans la définition de la séquence de touches pressées.

Les filtres de la fenêtre cible

Quand on crée une association fenêtre/séquence personnalisée, vous devez indiquer à KeePass à quoi ressemblent les titres de fenêtre correspondants. Ici, KeePass prend en charge les caractères génériques simples :

Chaîne avec des caractères génériques	Signification
STRING	Correspond à tous les titres de fenêtre nommés exactement "STRING".
STRING*	Correspond à tous les titres de fenêtre commençant par "STRING".
*STRING	Correspond à tous les titres de fenêtre se terminant par "STRING".
STRING	Correspond à tous les titres de fenêtre contenant "STRING" quelque part dans le titre de la fenêtre. Cela inclut la chaîne se trouvant directement au début ou à la fin du titre de la fenêtre.

Les autres caractères génériques ne sont pas pris en charge. Le caractère générique `*` ne doit pas être dans au milieu d'une chaîne de caractères.

Par exemple : `*Windows*Explorer*` ne correspondra pas à `l'Explorateur Windows`, il ne correspondra qu'à `Windows*Explorer`, c'est-à-dire que le caractère `*` du milieu est traité comme un caractère de texte '*' au lieu d'un caractère générique.
En utilisant des caractères génériques, vous pouvez faire des associations de saisie automatique indépendamment du navigateur. cf. les exemples d'utilisation pour plus d'informations.

Modifier la séquence de saisie automatique par défaut

La séquence de saisie automatique par défaut (c'est-à-dire celle qui est utilisée quand vous n'en spécifiez pas une personnalisée) est `{USERNAME}{TAB}{PASSWORD}{ENTER}`. KeePass vous permet de modifier cette séquence par défaut. Normalement vous n'avez pas besoin de la modifier (utiliser plutôt les définitions de fenêtre/séquence personnalisées à la place !), mais c'est quand même utile quand d'autres applications interfèrent avec KeePass (par exemple un logiciel de sécurité qui vous demande toujours la permission avant d'autoriser KeePass à effectuer une saisie automatique).

La séquence de saisie automatique par défaut peut être modifiée dans la configuration de la boîte de dialogue de la saisie automatique. Cette boîte de dialogue se trouve dans *'Outils'* → *'Options...'* → *'Avancé'* → *'Saisie automatique'*.

Exemple d'utilisation

Maintenant, jetons un œil sur un exemple concret : la connexion à un site. Dans cet exemple, nous utiliserons le raccourci clavier de saisie automatique globale pour remplir la page de connexion. Tout d'abord, ouvrez la page de test, et créez ensuite une nouvelle entrée dans KeePass avec le titre *Test Form* et un nom d'utilisateur et un mot de passe de votre choix.

Supposons que le raccourci clavier de saisie automatique globale soit défini sur Ctrl+Alt+A (valeur par défaut). KeePass s'exécute en arrière-plan, vous avez ouvert votre base de données et l'espace de travail est déverrouillé.

Lorsque vous naviguez maintenant sur la page de test et que vous êtes invités à saisir votre nom d'utilisateur et mot de passe, cliquez alors simplement dans le champ du nom d'utilisateur et appuyer sur Ctrl+Alt+A. KeePass entre le nom d'utilisateur et le mot de passe pour vous !

Pourquoi cela a-t-il fonctionné ? Le titre de la fenêtre de votre navigateur était*"Test Form - KeePass - Internet Explorer"* ou *"Test Form - KeePass - Mozilla Firefox"*, selon le navigateur que vous utilisez. Parce que nous avons donné à l'entrée dans KeePass le titre *Test Form*, le titre de l'entrée est contenu dans le titre de la fenêtre, donc KeePass utilise cette entrée.

Ici vous voyez les énormes avantages de la saisie automatique : non seulement elle ne nécessite pas d'un logiciel de navigation supplémentaire (le navigateur ne sait rien de KeePass – il n'y a pas besoin de greffons d'aide de navigateur), mais elle est également indépendante du navigateur : la seule entrée que vous avez créée dans KeePass fonctionne pour Internet Explorer *et* Mozilla Firefox (et autres navigateurs) sans nécessiter une modification ou définition.

Lorsque vous utiliserez des associations fenêtre/séquence (au lieu de la correspondance du titre de l'entrée), vous pourrez obtenir le même résultat indépendamment du navigateur en utilisant des caractères génériques : vous auriez pu par exemple utiliser `Test Form - KeePass - *` comme filtre de fenêtre. Ce filtre correspond à la fois à la fenêtre Internet Explorer et à la fenêtre Firefox.

Les options de la ligne de commande

Les options de la ligne de commande

Les options de la ligne de commande pour automatiser les tâches de KeePass.

Général

Vous pouvez passer un chemin de fichier dans la ligne de commande pour dire à KeePass d'ouvrir immédiatement ce fichier après un démarrage.

Les paramètres peuvent être soit préfixés en utilisant un tiret (`-`) soit deux tirets (`--`). Sous Windows, une barre oblique (`/`) est une alternative. Les préfixes sont équivalents ; qu'importe celui que vous utilisez.

Le fichier de la base de données. L'emplacement du fichier de la base de données est passé comme argument. Seulement un fichier de base de données est permis. Si le chemin contient un espace, alors il doit être entouré entre doubles quotes (").

Le mot de passe. Le mot de passe peut être passé en utilisant l'option `-pw:`. Afin de passer 'abc' comme mot de passe, vous ajouteriez l'argument suivant à la ligne de commande : `-pw:abc`. Remarquez qu'il ne doit pas y avoir d'espace entre le '`:`' et le mot de passe. Si votre mot de passe contient un espace, alors vous devez l'entourer entre des doubles quotes. Par exemple : `-pw:"Mon mot de passe secret"`.

L'utilisation de l'option `-pw:` n'est pas recommandée pour des raisons de sécurité (le système d'exploitation permet la lecture des options de la ligne de commande d'autres applications).

Le paramètre `-pw-enc:` est similaire à `-pw:`, mais il nécessite que le mot de passe soit chiffré. Les mots de passe chiffrés peuvent être générés en utilisant le paramètre substituable `{PASSWORD_ENC}`.

En passant l'option `-pw-stdin`, KeePass lit le mot de passe depuis le flux d'entrée standard (StdIn). Cette option est censée passer en programmation le mot de passe à KeePass. Pour saisir un mot de passe à la main, il est recommandé d'utiliser plutôt la boîte de dialogue normale de la clé principale (parce que dans cette boîte de dialogue, le mot de passe est caché par des puces/astérisques et il est chiffré par la protection de la mémoire du processus).

Fichier clé/fournisseur. Pour fournir le chemin du fichier clé ou le nom du greffon fournisseur de clé, le paramètre `-keyfile:` existe. Les mêmes règles que ci-dessus s'appliquent, mais vous devez spécifier le fichier clé/fournisseur, par exemple : `-keyfile:D:\pwsafe.key`. Vous devez également mettre la valeur entre quotes, si elle contient un espace, une tabulation ou d'autres caractères d'espacement.

Présélection. Afin de juste présélectionner un fichier clé/fournisseur, utilisez l'option `-preselect:`. Par exemple : si vous verrouillez votre base de données avec un mot de passe *et* un fichier clé, mais que vous

souhaitez simplement saisir votre mot de passe (donc, sans sélectionner manuellement le fichier clé), votre ligne de commande pourrait ressembler à ceci :

```
KeePass.exe "C:\My Documents\BaseDeDonnees.kdbx" -preselect:C:\pwsafe.key
```

KeePass montrera alors une invite pour la clé principale de la base de données, dans laquelle le fichier clé/fournisseur liste le fichier `C:\pwsafe.key` qui est déjà sélectionné. Quand on utilise le paramètre `-preselect:`, KeePass par défaut active l'option du paramètre de fichier clé/fournisseur et positionne le focus sur la fenêtre d'édition du mot de passe.

Remarquez la différence ! Le paramètre `-preselect:` présélectionne juste le fichier clé/fournisseur pour vous dans la boîte de dialogue de la clé principale. En revanche, le paramètre `-keyfile:` ne vous invite pas à saisir le mot de passe (peut-être manquant).

Autre. L'argument `-minimize` de la ligne de commande fait que KeePass démarre réduit. Cette option peut ne pas fonctionner quand KeePass s'exécute avec Mono (dû à un bug dans Mono).

L'argument `-auto-type` de la ligne de commande n'engendre que les autres instances de KeePass déjà ouvertes accomplissent une saisie automatique globale.

Si le commutateur `-readonly` est présent dans la ligne de commande, alors KeePass ouvrira la base de données en mode lecture seule.

Le commutateur `-lock` force KeePass à s'ouvrir en mode verrouillé (c'est-à-dire qu'on ne vous demandera pas immédiatement la clé principale quand on passe également le chemin de la base de données). L'ordre des arguments est arbitraire.

Exemples d'utilisation

Ouvrez le fichier de la base de données *'C:\My Documents\BaseDeDonnees.kdbx'* (KeePass vous demandera de lui fournir le mot de passe et/ou le chemin de l'emplacement du fichier clé) :

```
KeePass.exe "C:\My Documents\BaseDeDonnees.kdbx"
```

Si vous avez une base de données verrouillée avec le mot de passe 'abc', alors vous pouvez l'ouvrir comme ceci :

```
KeePass.exe "C:\My Documents\BaseDeDonnees.kdbx" -pw:abc
```

Si votre clé USB se monte toujours sur le lecteur F: et que vous ayez verrouillé votre base de données avec un fichier clé sur la clé USB, alors vous pouvez ouvrir la base de données comme ceci :

```
KeePass.exe "C:\My Documents\BaseDeDonneesAvecFichier.kdbx" -keyfile:F:\pwsafe.key
```

Si vous avez verrouillé votre base de données en utilisant un mot de passe *et* un fichier clé, alors vous pouvez combiner les deux paramètres et ouvrir votre base de données comme suit :

```
KeePass.exe "C:\My Documents\BaseDeDonneesAvecDeux.kdbx" -pw:abc -keyfile:F:\pwsafe.key
```

Vous avez verrouillé votre base de données en utilisant un mot de passe *et* un fichier clé, mais vous souhaitez uniquement que le fichier clé soit présélectionné (c'est-à-dire que vous souhaitez obtenir l'invite pour le mot de passe), votre ligne de commande ressemblerait à ceci :

```
KeePass.exe "C:\My Documents\BaseDeDonneesAvecDeux.kdbx" -preselect:F:\pwsafe.key
```

Démarrer KeePass en utilisant un fichier batch

Les fichiers batch peuvent être utilisés pour démarrer KeePass. Généralement vous souhaitez spécifier certains des paramètres répertoriés ci-dessus. Vous pouvez théoriquement simplement mettre la ligne de commande (c'est-à-dire le chemin de l'application et les paramètres) à l'intérieur d'un fichier batch, mais ceci n'est pas recommandé, car la fenêtre de commande restera ouverte jusqu'à ce que KeePass soit fermé. La méthode suivante est recommandée à la place :

```
START "" KeePass.exe ..\Basededonnées.kdbx -pw:MonMDPSecret
```

Cette commande `START` exécutera KeePass (qui ouvre le fichier `..\Basededonnées.kdbx` en utilisant le mot de passe `MonMDPSecret`). KeePass est censé être dans le même répertoire (répertoire de travail) que le fichier batch, sinon vous devez spécifier un chemin différent.

`START` exécute la ligne de commande donnée et se ferme aussitôt, c'est-à-dire qu'elle n'attend pas jusqu'à ce que l'application soit terminée. Par conséquent, la fenêtre de commande disparaîtra après que KeePass a été démarré.

Veuillez remarquer les deux doubles quotes (`""`) après la commande `START`. Ces doubles quotes sont nécessaires si le chemin de l'application contient des doubles quotes (dans l'exemple ci-dessus, les doubles quotes peuvent également être supprimées). Si vous souhaitez en apprendre davantage à propos

de la syntaxe de la commande START, alors saisissez START /? dans la fenêtre de commande.

Fermeture/Verrouillage de KeePass en utilisant un fichier batch

Pour fermer toutes les instances en cours d'exécution, appelez KeePass.exe avec le paramètre '--exit-all' :

```
KeePass.exe --exit-all
```

Toutes les fenêtres de KeePass essaieront de se fermer. Si une base de données a été modifiée, alors KeePass vous demandera si vous souhaitez l'enregistrer ou non. Si dans tous les cas vous souhaitez l'enregistrer (c'est-à-dire forcer la sortie sans confirmation d'une boîte de dialogue), alors activez l'option *'Enregistrer automatiquement quand on ferme/verrouille la base de données'* dans *'Outils'* → *'Options...'* → *onglet 'Avancé'*.

L'instance de KeePass qui a été créée par la commande ci-dessus n'est pas visible (c'est-à-dire qu'elle n'affiche pas de fenêtre principale) et se terminera aussitôt après l'envoi de la requête de fermeture aux autres instances.

Les options de ligne de commande --lock-all et --unlock-all verrouillent/déverrouillent les espaces de travail de toutes les autres instances de KeePass.

L'édition des remplacements d'adresse (URL) (2.x)

KeePass 2.x prend en charge les options de ligne de commande suivantes pour l'édition des remplacements d'adresse (URL) :

- -add-urloverride:
  Ajoute un remplacement d'adresse pour un protocole spécifique. Spécifier le protocole en utilisant le paramètre de ligne de commande '-scheme:' et le remplacement en utilisant le paramètre de commande '-value:'. Si le remplacement d'adresse doit être activé, alors passer en outre l'option de ligne de commande '-activate'.
- -remove-urloverride:
  Supprime un remplacement d'adresse pour un protocole spécifique. Spécifier le protocole en utilisant le paramètre de ligne de commande '-scheme:' et le remplacement en utilisant le paramètre de ligne de commande '-value:'.
- -set-urloverride:
  La valeur de ce paramètre de ligne de commande (non pas le paramètre de ligne de commande '-value:') est enregistré comme remplacement de toutes les adresses de l'entrée.
- -get-urloverride:
  Enregistre le remplacement courant pour toutes les adresses de l'entrée vers le fichier %TEMP%\KeePass_UrlOverride.tmp' (au format INI).
- -clear-urloverride:
  Supprime le remplacement pour toutes les adresses de l'entrée.

Les remplacements d'adresse sont stockés dans le fichier de configuration imposée. Pour chacune des options de la ligne de commande ci-dessus excepté '-get-urloverride', une boîte de dialogue du contrôle du compte utilisateur (User Account Control) est affiché, si nécéssaire.

La configuration

Général

KeePass prend en charge plusieurs emplacements pour enregistrer les informations de configuration : le fichier de configuration *globale* dans le répertoire de l'application KeePass, un fichier *local* dépendant de l'utilisateur dans le dossier de configuration privé de l'utilisateur, et un fichier de configuration *imposée* dans le répertoire de l'application KeePass. Le premier se nomme *global*, parce que tout le monde utilisant cette installation de KeePass écrira vers le même fichier de configuration (et pourra éventuellement écraser les paramètres des autres utilisateurs). Le second se nomme *local*, parce que les changements effectués dans ce fichier de configuration n'affectent que l'utilisateur courant.

Les fichiers de configuration sont enregistrés au format INI.

Configuration	Emplacement	Chemin de fichier typique
Global	Répertoire de l'application	C:\Program Files (x86)\KeePass Password Safe\KeePass.ini
Global (Virtualisé)	Windows Virtual Store	C:\Users*Nom d'utilisateur*\AppData\Local\VirtualStore\Program Files (x86)\KeePass Password Safe\KeePass.ini
Local	Données de l'application de l'utilisateur	C:\Users*Nom d'utilisateur*\AppData\Roaming\KeePass\KeePass.ini
Forcée	Répertoire de l'application	C:\Program Files (x86)\KeePass Password Safe\KeePass.config.enforced.ini

Sur les systèmes Linux, le fichier de configuration locale est typiquement enregistré dans '$XDG_CONFIG_HOME/KeePass' (qui est souvent '~/.config/KeePass', où '~' est le répertoire racine de l'utilisateur).

Installation par l'administrateur, utilisation par l'utilisateur

Si vous utilisez le programme d'installation de KeePass et installez le programme avec les droits de l'administrateur, alors le répertoire du programme sera protégé en écriture quand on travaillera comme un utilisateur normal/limité. KeePass utilisera les fichiers locaux de configuration, c'est-à-dire enregistrera et chargera la configuration depuis un fichier dans votre répertoire d'utilisateur.

Plusieurs utilisateurs peuvent utiliser KeePass installé localement. Les paramètres de configuration ne seront pas partagés et peuvent être configurés individuellement pour chaque utilisateur.

La version portable

Si vous téléchargez la version portable de KeePass (paquet ZIP), alors KeePass essaiera de sauvegarder sa configuration dans le répertoire de l'application. Aucun paramètre de configuration sera enregistré dans le répertoire de l'utilisateur (si le fichier de configuration global est accessible en écriture).

Créer une version portable du KeePass installé

Si vous utilisez actuellement une version de KeePass installée localement (installée par le programme d'installation de KeePass) et que vous souhaitez en créer une version portable, alors premièrement copiez tous les fichiers de KeePass vers l'appareil portable. Récupérez ensuite le fichier de configuration depuis le répertoire de l'utilisateur (application data, cf. ci-dessus) et copiez-le par-dessus le fichier de configuration sur l'appareil portable.

Pour les administrateurs réseau : imposez la configuration

Les paramètres dans le *fichier de configuration imposée* préemptent sur les paramètres globaux et locaux des fichiers de configuration.

Cette fonctionnalité est principalement destinée aux administrateurs réseau qui souhaitent forcer certains paramètres aux utilisateurs d'une installation de KeePass partagée.

Pour des détails, cf. la page d'aide configuration imposée.

Activer à nouveau les éléments nécessitant l'imposition (2.x)

Certains éléments de fonctionnalité sont enregistrés dans le fichier de configuration imposée. Dans certaines circonstances, il peut y avoir de tels éléments dans le fichier de configuration régulière (par exemple : lorsque vous copiez le fichier de configuration régulière sur un nouveau PC, mais pas celui imposé). Si vous souhaitez continuer à utiliser les éléments, alors vous devez les activer à nouveau. Cela peut nécessiter l'autorisation de l'administrateur ; Keepass affiche une boîte de dialogue de contrôle du compte utilisateur (User Account Control), si nécessaire.

Si vous utilisez une version installée de KeePass (Configuration EXE ou MSI) et une ou plusieurs des fonctionnalités suivantes, alors veuillez noter :

- Les déclencheurs (Triggers):
  Si vos déclencheurs ne sont pas stockés dans le fichier de configuration imposé, alors Keepass désactive le système de déclenchement. Si vous souhaitez continuer à utiliser vos déclencheurs, alors ouvrez la boîte de dialogue 'Déclencheurs' (via l'élément de menu principal 'Outils' → 'Déclencheurs (triggers)'), activez l'option 'Activer le système de déclencheur', vérifiez tous les déclencheurs (en ce qui concerne la sécurité, la confidentialité, la fonctionnalité, la compatibilité, etc.) et cliquez sur le bouton 'OK'.
- Les remplacement d'adresse (URL) globaux:
  Si vos remplacements d'adresse globaux ne sont pas stockés dans le fichier de configuration imposée, alors KeePass les désactive (individuellement ; donc, il est recommandé que vous vous souveniez des remplacements qui ont été activés, par exemple en prendant une capture d'écran). Si vous souhaitez continuer à utiliser les remplacements, alors ouvrir la boîte dedialogue 'Les remplacement d'adresse (URL)...' (via l'élément du menu principal 'Outils' → 'Options...' → onglet 'Intégration' → bouton 'Les remplacements d'adresse (URL)...'), vérifiez tous les remplacement d'adresses souhaités (En ce qui concerne la sécurité, la confidentialité, la fonctionnalité, la compatibilité, etc.), les activer et cliquer sur le bouton 'OK'.
- Les profils du générateur de mot de passe :
  Si les profils du générateur de mot de passe ne sont pas stockés dans le fichier de configuration imposée , alors KeePass les désactive. Si vous souhaitez continuer à utliser vos profils, alors ouvrez la boîte de dialogue du 'Générateur de mot de passe' (via l'élément du menu principal 'Outils' → 'Générer un mot de passe'), clique le bouton bouclier (en haut à droite) et cliquer tous les profils (En ce qui concerne la sécurité, la confidentialité, la fonctionnalité, la compatibilité, etc.).

Si vous utilisez le package Zip portable, alors Keepass essaie de migrer les déclencheurs, les remplacements d'adresse et les profils du générateur de mots de passe automatiquement.

Les détails techniques

Cette section explique en détail le fonctionnement du chargement et de l'enregistrement de la configuration.

Quand KeePass démarre et trouve à la fois des fichiers de configuration globale et locale, il doit décider l'ordre dans lequel KeePass tente d'obtenir les éléments de configuration. Ceci est géré par l'indicateur (Kee)`PreferUserConfiguration` du fichier de configuration globale. S'il n'est pas présent, alors il est mis par défaut à *false* (faux).

L'indicateur (le flag) est positionné à *true* (vrai) dans le fichier de configuration globale du paquet de l'installateur de KeePass. Le paquet ZIP portable ne contient pas de fichier de configuration, par conséquent l'indicateur par défaut est à *false*.

Chargement :

- Essaye d'obtenir l'élément de configuration à partir du fichier de configuration imposé. Si trouvé, alors utiliser celui-ci.
- Si l'élément n'est ni présent dans le fichier de configuration global et ni présent dans le fichier local : alors utiliser la valeur par défaut.
- Si l'élément est présent dans le fichier de configuration global, mais pas dans le fichier local : alors utiliser l'élément de la configuration globale.
- Si l'élément est présent dans le fichier de configuration local, mais pas dans le fichier global : alors utiliser l'élément de la configuration locale.
- Si l'élément est présent dans le fichier de configuration global et local :

- Si l'indicateur `KeePreferUserConfiguration` est *True*, alors utiliser l'élément depuis le fichier de configuration local, sinon utilisez l'élément du fichier global.

Enregistrement :

- Si l'indicateur `KeePreferUserConfiguration` est à *True*, alors essayer de stocker l'élément de configuration dans le fichier de configuration local. Si cela échoue, alors essayer de stocker l'élément dans le fichier de configuration global. Si cela échoue, alors signalez l'erreur.
- Si l'indicateur `KeePreferUserConfiguration` est à *False*, essayez de stocker l'élément dans le fichier de configuration globale. Si cela échoue, alors essayer de stocker l'élément dans le fichier de configuration local. Si cela échoue, alors signalez l'erreur.

Le chemin du fichier de configuration local peut être modifié en utilisant la variable d'environnement 'KP1_CFG_LOCAL'.

Les références de champ

Les références de champ

Comment mettre des références à des données dans les champs d'autres entrées ?

Introduction

KeePass peut insérer des données enregistrées dans différentes entrées dans les champs d'une entrée. Ce qui signifie que plusieurs entrées peuvent partager un champ commun (nom d'utilisateur, mot de passe, etc.), et en changeant les données de l'entrée réelle, toutes les autres entrées utiliseront également la nouvelle valeur.

Pour créer une référence de champ, vous pouvez soit utiliser l'assistant pratique des références de champ (dans la fenêtre d'édition des entrées, cliquez le bouton 'Outils' au bas à gauche et sélectionnez 'Insérer une référence à un champ'), soit insérer manuellement le paramètre substituable (cf. syntaxe ci-dessous).

Remarquer que les références de champs sont destinées à référencer des données enregistrées dans *différentes* entrées. Si vous souhaitez insérer des données de la *même entrée/entrée en cours*, alors vous devrez utiliser des paramètres substituables locaux, comme `{TITLE}` et `{S:NomDeChamp}`; cf. paramètres substituables.

Syntaxe du paramètre substituable (placeholder)

La syntaxe du paramètre substituable pour les références de champ est la suivante :

`{REF:<ChampSouhaité>@<RechercherDans>:<Texte>}`

Les parties *<ChampSouhaité>* et *<RechercherDans>* doivent être remplacées par des codes d'une lettre identifiants le champ :

Code	Champ
T	Titre
U	Nom d'utilisateur
P	Mot de passe
A	Adresse (URL)
N	Remarques
I	UUID
O	Les autres chaînes personnalisées *(seulement KeePass 2.x)*

La partie *Texte* est la chaîne recherchée qui décrit le ou les texte(s) qui doivent apparaître dans le

champ spécifié qui correspond à une entrée.

Si plusieurs entrées correspondent au critère de recherche spécifié, alors la première entrée sera utilisée. Pour éviter toute ambiguïté, une entrée peut être identifiée par son UUID, qui est unique. Exemple : `{REF:P@I:46C9B1FFBD4ABC4BBB260C6190BAD20C}` insérerait le mot de passe de l'entrée ayant comme UUID.

Exemple

Supposons que vous avez deux entrées : une avec le titre "Exemple de site Web" et une avec "Exemple de forum", et que vous souhaiteriez insérer le nom d'utilisateur du compte du site Web dans l'adresse (URL) de l'entrée du forum. À l'intérieur de l'adresse (URL) de l'entrée du forum, vous devrez référencer le nom d'utilisateur comme suit :
`https://forum.exemple.com/?user={REF:U@T:Exemple de site Web}`

Importer/Exporter

KeePass 1.x prend en charge l'importation de données depuis **des fichiers CSV** (formulaire spécial), **CodeWallet**, **Password Safe** et **Personal Vault**.

KeePass 2.x prend en charge l'importation de données depuis **des fichiers CSV** (tout), **KeePass 1.x (KDB, XML et CSV)**, **KeePass 2.x XML**, **1Password**, **1Password Pro**, **1PW**, **Alle meine Passworte**, **Any Password**, **Bitwarden**, **CodeWallet**, **Dashlane**, **DataVault**, **DesktopKnox**, **Enpass**, **FlexWallet**, **Google Chrome**, **Handy Safe**, **Handy Safe Pro**, **Kaspersky Password Manager**, **KeePassX**, **Keeper**, **Key Folder**, **LastPass**, **Mozilla Bookmarks**, **mSecure**, **Network Password Manager**, **Norton Identity Safe**, **nPassword**, **PassKeeper**, **Passphrase Keeper**, **Password Agent**, **Password Depot**, **Password Exporter**, **Password Keeper**, **Password Memory**, **Password Prompter**, **Password Safe**, **Password Saver**, **Passwords Plus**, **Passwort.Tresor**, **Personal Vault**, **PINs**, **Revelation**, **RoboForm**, **SafeWallet**, **Security TXT**, **SplashID**, **Steganos Password Manager**, **Sticky Password**, **True Key**, **TurboPasswords**, **VisKeeper**, **Whisper 32** et **ZDNet's Password Pro**.

Pour les deux KeePass 1.x et 2.x, il existe des greffons qui ajoutent davantage de possibilités d'importation/exportation.

- Pour KeePass 1.x :
  - Format de fichier : CSV
  - Format de fichier : XML
- Pour KeePass 2.x :
  - Importateur de CSV générique
  - Les formats qui nécessitent des options/étapes personnalisées pour être importés :
    - Comment importer CodeWallet TXT ?
    - Comment importer des PIN TXT ?
    - Comment importer des données depuis RoboForm ?
    - Comment importer des données depuis Steganos Password Manager 2007 ?
    - Comment importer des données depuis PassKeeper 1.2 ?
    - Comment importer 1PW et 1Password Pro CSV ?
  - Exporter : Option 'Exporter en plus les groupes parents'

Malheureusement, le format des bases de données de mots de passe n'est pas normalisé. Tous les gestionnaires de mots de passe utilisent le leur. Qu'importe, presque tous prennent en charge l'exportation vers des fichiers CSV ou XML. De prime abord ceci semble a priori correct, mais les fichiers CSV et XML ne sont pas spécialisés aux formats des bases de données de mots de passe, ils spécifient seulement une disposition de bas niveau des données enregistrées (pour CSV : les champs de données sont séparés par des virgules ; pour XML : une forme hiérarchique utilisant des balises). Ces formats ne spécifient pas le haut niveau d'agencement des données (pour CSV : l'ordre/signification des champs ; pour XML : des

noms de balises et une structure). Pour cette raison, de nombreux utilisateurs sont confus quand l'application #1 exporte les données vers CSV/XML et que l'application #2 ne peut pas lire les fichiers CSV/XML, bien qu'elle clame pouvoir lire ces fichiers.

Cette page d'aide détaille les formats de fichiers CSV et XML attendus. En connaissant les formats que KeePass attend, vous pouvez reformater les fichiers CSV et XML exportés par d'autres gestionnaires de mots de passe pour les faire correspondre aux formats de KeePass. Les fichiers CSV peuvent être reformatés en utilisant par exemple : *LibreOffice Calc* (cf. ci-dessous). Les fichiers XML peuvent être reformatés en utilisant un éditeur XML.

KeePass peut importer directement plusieurs formats de bases de données de mots de passe (cf. en haut de cette page). De plus, il existe des greffons spécialisés disponibles dans KeePass pour importer davantage de formats (comme AnyPassword CSV, fichiers Oubliette, PINs TXT, fichiers ZSafe, et bien d'autres encore, etc.). En utilisant ces greffons, vous n'avez pas besoin de reformater manuellement la sortie de ces autres gestionnaires de mots de passe ; vous pouvez directement importer les fichiers exportés.

Si aucun greffon d'importation n'existe pour l'importation des données de votre précédent gestionnaire de mots de passe, alors soyez certain de poser une requête pour ceci dans KeePass Feature Requests Tracker ou dans le forum de discussion ouverte.

Format de fichier : CSV (KeePass 1.x)

KeePass importe et exporte les données depuis/vers des fichiers CSV au format suivant :

```
"Account","Login Name","Password","Web Site","Comments"
```

le champ 'Account' dans un fichier CSV correspond au champ du titre d'une entrée de KeePass, 'Login Name' correspond au nom d'utilisateur, 'Web Site' correspond à l'adresse (URL), et 'Comments' correspond à Remarques. Les noms de champ CSV field sont différents depuis les noms de champ d'entrée afin d'assurer une compatibilité avec certaines autres appplications.

Pour un exemple détaillé, téléchargez ce fichier : FileSample_CSV.zip. Ce fichier est zippé seulement afin d'assurer un encodage correct (s'il n'était pas zippé, les navigateurs ou les gestionnaires de téléchargement pourraient automatiquement le convertir vers un encodage différent). Quand on importe un fichier CSV, il *ne* doit *pas* être zippé !

Des remarques importantes à propos du format :

- Le fichier doit être encodé en utilisant UTF-8 (Unicode). Les autres encodages ne sont pas pris en charge.
- Les fichiers CSV prennent en charge les champs suivants : titre, nom d'utilisateur, mot de passe, adresse (URL) et remarques. Les autres champs comme le temps de la dernière modification, la date d'expiration, l'icône, les pièces jointes de l'entrée, etc. *ne* sont *pas* pris en charge. Si vous souhaitez transférer de telles informations, alors vous devez utiliser un format différent (comme XML).
- Tous les champs doivent être entourés entre deux doubles quotes ("). Ces doubles quotes sont nécessaires, les champs non quottés ne sont pas autorisés.
- Les doubles quotes (") dans les chaînes sont encodées en tant que `\"` (deux caractères). Les barres obliques inversées (\) sont codées en tant que `\\`.
- Plusieurs lignes Comments sont réalisées à travers des sauts de nouvelles lignes. Le codage des sauts de ligne par `\n` n'est pas pris en charge.

Par défaut Excel de Microsoft n'entoure pas les champs entre doubles quotes ("). Il est recommandé d'utiliser LibreOffice Calc pour créer un fichier CSV correct (cf. ci-dessous), ou utilisez l'Importateur de CSV générique de KeePass 2.x (importez votre fichier CSV dans KeePass 2.x, puis exportez les données vers un fichier KDB de KeePass 1.x), ou corrigez manuellement le fichier CSV en ajoutant des doubles quotes en utilisant un éditeur de texte.

Si vous souhaitez transférer des données entre des bases de données de KeePass 1.x, alors vous ne devez pas modifier les options d'exportation par défaut de KeePass. N'exportez pas des champs supplémentaires ou ne décochez aucune option, sinon KeePass ne pourra plus réimporter le fichier CSV, parce qu'il n'est plus conforme aux spécifications ci-dessus.

L'utilisation de *LibreOffice Calc* pour créer un fichier CSV :
LibreOffice Calc peut être utilisé pour créer des fichiers CSV qui peuvent être correctement importés

dans KeePass. Suivez ces étapes :

- Assurez-vous d'avoir 5 colonnes comme décrites ci-dessus.
- Sélectionnez tout, clic droit et sélectionnez *'Format des cellules'*. Dans la boîte de dialogue, choisissez *Texte* comme catégorie. Cliquez sur [OK].
- Allez dans *'Fichier'* → *'Enregistrer sous...'*, choisir un emplacement et le type de fichier 'Text CSV', et assurez-vous que la case *'Édition paramètres de filtre'* est bien cochée. Cliquez sur le bouton *'Enregistrer'*.
- Choisissez *'Unicode (UTF-8)'* comme jeu de caractères. Le séparateur de champ doit être défini sur une virgule. Le séparateur de texte doit être ". Assurez-vous que l'option *'Quotter toutes les cellules de texte'* est cochée, et que l'option *'Taille de colonne fixe'* n'est pas cochée. Cliquez sur [OK].

Format de fichier : XML (KeePass 1.x)

Cette section décrit le format XML de KeePass 1.x. Remarquez que ce format est différent du format XML utilisé par KeePass 2.x (qu'importe, KeePass 2.x peut importer des fichiers XML de KeePass 1.x).

Vous pouvez télécharger un exemple de fichier XML détaillé ici : FileSample_XML.zip. Ce fichier est zippé uniquement afin d'assurer un encodage correct (s'il n'était pas zippé, les navigateurs ou les gestionnaires de téléchargement pourraient automatiquement convertir le fichier vers un encodage différent). Quand on importe un fichier XML, il*ne* doit bien sûr *pas* être zippé !

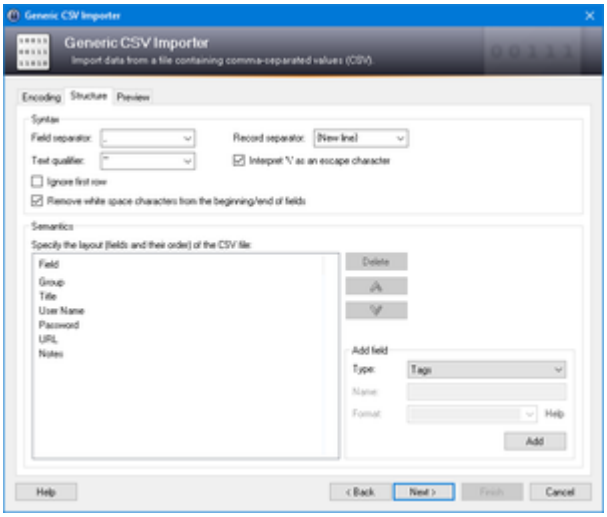
Remarques importantes à propos du format :

- Les fichiers doivent être encodés en UTF-8 (Unicode). Les autres encodages ne sont pas pris en charge.
- Les cinq entités suivantes doivent être codées : `< > & " '`. Elles sont codées par `< > & " '`.
- l'UUID est un chaîne de 16 octets au format hexadécimal (c'est-à-dire une chaîne de 32 caractères hexadécimaux ANSI dans les fichiers XML). Il est unique (également sur plusieurs bases de données) et peut être utilisé pour identifier les entrées.
- Les dates/heure sont encodés au format XML de date/heure standard (YYYY-MM-DDTHH:mm:ss): premièrement la date sous la forme YYYY-MM-DD, un caractère 'T', et l'heure sous la forme HH:mm:ss.

L'importateur de CSV générique

KeePass 2.x dispose d'un importateur de CSV générique. Cet outil peut importer presque tous les formats CSV. Les fichiers CSV sont chargés et vous pouvez spécifier manuellement l'encodage/jeu de caractères, affecter des colonnes aux champs de données, et spécifier à quoi ressemble la structure de bas niveau (l'utilisation de doubles quotes, etc.).

Pour démarrer l'importateur de fichier CSV générique, cliquez sur *'Fichier'* → *'Importer...'* et choisir *'Importateur de CSV générique'*.



Des détails à propos de l'importateur de CSV générique (avec des descriptions des options, des exemples, etc.) peuvent être trouvés sur la page d'aide Generic CSV Importer.

Comment importer CodeWallet TXT ?

CodeWallet est un gestionnaire de mots de passe qui prend en charge différents types de carte (champs). KeePass ne peut pas savoir à quel champ de CodeWallet correspond le champ standard de KeePass (titre, nom d'utilisateur, etc.), parce qu'ils n'ont pas des noms fixes (dépendant de la langue, personnalisable par l'utilisateur, etc.). Donc tous les champs depuis le fichier CodeWallet sont importés dans des champs de chaîne personnalisés d'entrées de KeePass. Après l'importation du fichier, vous pouvez déplacer des chaînes vers leurs champs standards corrects (en cliquant le bouton *'Déplacer'* sur la page du second onglet da la boîte de dialogue des entrées).

Comment importer des PIN TXT ?

Pour réussir à importer un fichier de PIN TXT, vous devez effectuer les opérations suivantes :

- Basculez la langue des PIN sur 'anglais'.
- Dans la boîte de dialogue d'exportation des PIN : activez*tous* les champs.
- Dans la boîte de dialogue d'exportation des PIN : définissez *'tabulation'* comme séparateur.
- Dans la boîte de dialogue d'exportation des PIN : activez*'Quotter les textes'*.

Après l'exportation d'un fichier TXT en utilisant les paramètres ci-dessus, importez-le en utilisant *'Fichier → Importer...'* dans KeePass 2.x.

Comment importer des données depuis RoboForm ?

1. Dans RoboForm, ouvrir l'*'RoboForm Editor'* (dans les anciennes version de RoboForm, il était appelé *'Passcard Editor'* ou *'Edit Passcards'*). Clicquer le bouton *'RoboForm'* en haut à gauche(dans les anciennes versions de RoboForm, cliquer l'élément du menu principal *'Passcard'*) → *'Print List'* → *'Logins'*. Dans la boîte de dialogue qui s'ouvre, cliquer le bouton *'Save'*, spécifier un emplacement et cliquer le bouton *'Save'*.
2. Dans KeePass, ouvrir votre fichier de base de données KeePass 2. et cliquer*'Fichier'* → *'Importer...'*. Choisir *'RoboForm HTML'* comme format, sélectionner le fichier HTML que vous venez d'enregistrer et cliquer sur le bouton *'OK'*.

Comment importer des données depuis Steganos Password Manager 2007 ?

Attention ! Il est possible que le transfert échoue et que KeePass écrase accidentellement vos mots de passe existants dans Steganos Password Manager. Donc sauvegardez votre fichier SEF avant de commencer l'importation ! Dans tous les cas vous devrez restaurer vos mots de passe en restaurant la sauvegarde que vous venez juste de créer après le processus d'importation ! Même si vous pensez que KeePass n'a rien changé, restaurer la sauvegarde !

Malheureusement Steganos Password Manager (SPM) n'a aucune forme de fonctionnalité pour exporter. Comme le format de fichier SEF (dans lequel sont sauvegardées les données) est propriétaire et qu'aucune spécification n'est disponible, KeePass doit essayer d'extraire toutes les données des fenêtres de SPM.

Le processus d'import fonctionne comme suit. Premièrement démarrer SPM et ouvrez votre base de données de mot de passe. La fenêtre principale de gestion des mots de passe devrait s'ouvrir (c'est-à-dire celui qui répertorie vos éléments au milieu de l'écran, et contient les boutons de la pseudo barre d'outils en haut). Assurez-vous que *tous* vos éléments sont affichés dans la liste (sélectionnez le filtre correct dans la combobox au-dessus de la liste des éléments).

Maintenant basculer sur KeePass 2.x et ouvrez votre base de données KeePass. Cliquer *Fichier → Importer...* et choisissez *'Steganos Password Manager 2007'*. Cliquez sur [OK]. Maintenant lisez le reste avant de continuer.

Après la pression du bouton [Oui] dans la boîte de dialogue de confirmation d'importation de KeePass, vous avez 10 secondes pour basculer sur la fenêtre de SPM. Sélectionnez la toute première entrée à l'intérieur de la fenêtre SPM (mais ne l'ouvrez pas, sélectionnez-la simplement). C'est important ! La première entrée doit avoir le focus du clavier et doit être sélectionnée.

Une fois les 10 secondes écoulées, KeePass démarrera l'importation. Vous verrez comment KeePass ouvre les éléments de SPM, copie les données, ferme la fenêtre de l'élément, sélectionne le prochain élément, etc. Tout est maintenant automatisé et vous pouvez simplement vous asseoir en arrière et

regarder. Parfois Windows joue un son *ding*, ceci est normal.

Remarquer que cela peut prendre quand même du temps pour importer vos éléments. **Ne** faites **rien** tant que KeePass importe ! Un seul clic de souris ou une touche pressée peut ruiner en entier le processus d'importation.

Le dernier élément sera scanné deux fois. Quand ce sera terminé, KeePass affichera un message "The import process has finished!" (le processus d'importation est terminé !).

Il est possible que KeePass ne réussisse pas à importer des éléments (principalement causé par d'imprévisibles temps de réponse lents de SPM). Il est fortement recommandé que vous compariez chaque entrée.

Comment importer des données depuis PassKeeper 1.2 ?

Le processus d'importation fonctionne visuellement, exactement comme la méthode d'importation des données de Steganos Password Manager 2007. Veuillez lire toutes les instructions dans comment importer des données depuis Steganos Password Manager 2007.

Comment importer 1PW et 1Password Pro CSV ?

KeePass peut importer les fichiers CSV exportés par 1PW et 1Password Pro. Quand on exporte les données, assurez-vous :

- De choisir la tabulation (Tab) comme séparateur de champ.
- Que l'option pour entourer les champs entre double quotes est activée.
- Que tous les champs doivent être exportés, dans l'ordre d'origine.

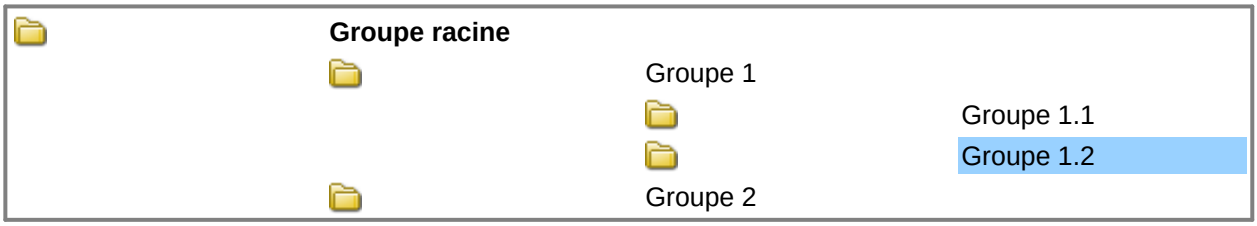
Exporter : Option 'Exporter en plus les groupes parents'

Dans KeePass 2.x, il y a une option 'Exporter en plus les groupes parents' dans la boîte de dialogue Exporter. Si cette option est activée, alors les groupes parents des groupes/entrées sélectionnés sont exportés, également (jusqu'au groupe racine de la base de données). Les groupes/entrées non sélectionnés dans les groupes parents ne sont pas exportés.

Si le format de fichier sélectionné ne prend pas en charge les groupes, alors l'option n'a pas d'effet. Quand on exporte la base de données entière (via 'Fichier' → 'Exporter') ou le groupe racine, l'option est désactivée, parce que le groupe racine n'a pas de parent.

Les propriétées des groupes parent (icônes, remarques, paramètres de saisie automatique, etc.) sont exportées, si le format de ficheir les prend en charge. Quand on importe un fichier, les propriétés des groupes de la base de données en cours peuvent être écrasées par les propriétés des groupes dans le fichier (cela dépend du mode d'importation et des derniers temps de modification).

Exemple : supposons que l'utilisateur sélectionne l'entrée 'Entrée B' qui est enregistrée dans les groupes 'Groupe 1' → 'Groupe 1.2' de la base de données.



Titre		Nom d'utilisateur	Mot de passe	Adresse (URL)	Remarques
	Entrée A	Michael42	********	https://exemple.net/	Aucune.
	Entrée B	Michael42	********	https://exemple.com/	Aucune.
	Entrée C	Michael42	********	https://exemple.org/	Aucune.

En exportant l'entrée sélectionnée (via 'Entrée' → 'Échange de données' → 'Exporter l'entrée') vers un

fichier de base de données KDBX sans activer l'option donnera :

	Groupe racine

Titre		Nom d'utilisateur	Mot de passe	Adresse (URL)	Remarques
	Entrée B	Michael42	********	https://exemple.com/	Aucune.

En revanche, en exportant l'entrée sélectionnée vers un fichier de base de données KDBX avec l'option activée donnera :

	Groupe racine	
	Groupe 1	
		Groupe 1.2

Titre		Nom d'utilisateur	Mot de passe	Adresse (URL)	Remarques
	Entrée B	Michael42	********	https://exemple.com/	Aucune.

L'intégration

L'intégration

Comment KeePass s'intègre dans votre environnement de système d'exploitation ?

- Le raccourci clavier global pour restaurer la fenêtre de KeePass
- L'option limiter à une seule instance

Le raccourci clavier global pour restaurer la fenêtre de KeePass

Pour revenir rapidement d'une application à KeePass, vous pouvez utiliser le raccourci clavier global qui restaure la fenêtre principale de KeePass.

Si vous avez plusieurs instances de KeePass en cours d'exécution, alors appuyer sur le raccourci clavier global pour restaurer la première instance qui a été démarrée.

Le raccourci clavier global est `Ctrl`+`Alt`+`K`.

La touche de raccourci ne peut pas être modifiée, mais elle peut être désactivée dans le menu des options avancées.

L'option limiter à une seule instance

Si vous activez l'option *'Limiter l'application à une seule instance'*, alors au plus une instance de KeePass peut être exécutée à la fois. Si vous essayez de démarrer une seconde instance de KeePass, alors elle est immédiatement terminée, et la première instance est mise au premier plan.

Si la seconde instance a été démarrée à l'aide d'une ligne de commande spécifiant une base de données à ouvrir, et la première instance n'a pas de boîte de sous-dialogue ouverte, alors la première instance tente de fermer la base de données en cours. Si cette tentative réussit (ou si aucune base de données n'était ouverte en premier lieu), alors la première instance ouvre la base de données spécifiée par la ligne de commande de la seconde instance, en utilisant n'importe quelles options `-pw`, `-pw-stdin` et `-keyfile` spécifiées par la seconde instance. Toutes les autres options de ligne de commande de la seconde instance sont ignorées.

La clé principale

La clé principale

Les détails à propos des composants d'une clé principale.

- Le mot de passe maître
- Le fichier clé
- Le compte utilisateur Windows
- Pour les administrateurs : spécifications des propriétés minimales des clés principales

---

Votre fichier de base de données de KeePass est chiffré en utilisant une clé principale. Cette clé principale peut être constituée de plusieurs composants : un mot de passe maître, un fichier clé et/ou une clé qui est protégée en utilisant le compte utilisateur courant de Windows.

Pour ouvrir un fichier de base de données, alors *tous* les composants de la clé principale sont nécessaires.

Si vous oubliez/perdez un composant de la clé principale (ou oubliez la composition), alors toutes les données enregistrées dans la base de données sont perdues. Il n'y a pas de porte dérobée et ni de clé universelle qui puisse ouvrir votre base de données.

Le mot de passe maître

Si vous utilisez un mot de passe maître, vous n'avez qu'à seulement vous souvenir d'un mot de passe ou d'une phrase de passe (ce qui devrait être bon) pour ouvrir votre base de données.

KeePass propose une fonctionnalité de protection contre les attaques par force-brute ou par dictionnaire sur la clé principale, lire la page d'informations sur la sécurité pour plus de détails.

Le fichier clé

Un fichier clé est un fichier qui contient une clé (et éventuellement d'autres données comme, par exemple un hachage qui permet de vérifier l'intégrité d'une clé). L'extension du fichier est typiquement 'keyx' ou 'key'.

Un fichier clé ne peut pas être modifié, sinon vous ne pourrez plus du tout ouvrir votre base de données. Si vous souhaitez utiliser un fichier clé différent, alors ouvrez la boîte de dialogue pour changer la clé principale (via 'Fichier' → 'Modifier la clé principale...') et créer/sélectionner le nouveau fichier clé.

La protection à deux facteurs : un fichier clé est quelque chose que vous devez *posséder* afin d'être capable d'ouvrir la base de données (contrairement à un mot de passe maître, que vous devez *connaître*). Si vous utilisez à la fois un fichier clé et un mot de passe maître, alors vous avez une protection à deux facteurs : possession et connaissance.

Emplacement : comme mentionné ci-dessus, l'idée c'est que vous *possédez* quelque chose, si un attaquant s'accapare à la fois de votre base de données et de votre fichier clé, alors le fichier clé n'offre plus de protection. Donc, les deux fichiers doivent être stocké à deux endroits différents. Par exemple, vous pourriez enregistrer le fichier clé sur une clé USB à part.

En cachant la localisation : le *contenu* du fichier clé doit être tenu secret, pas sa localisation (chemin/nom du fichier). En essayant de cacher le fichier clé (par exemple : en le sauvegardant parmi des milliers d'autres fichiers, dans l'espoir qu'un attaquant ne saura pas quel fichier est celui qui est bon) n'augmentera pas typiquement la sécurité, parce qu'il est facile de trouver le bon fichier (par exemple : en inspectant le dernier temps d'accès des fichiers, les listes des fichiers récemment utilisés du système d'exploitation, l'audit des logs du système de fichiers, les logs du logiciel anti-virus, etc.).

KeePass posséde une option pour se souvenir des chemins des fichiers clé, qui est activée par défaut ; le désactiver diminue seulement l'utilisation sans augmenter la sécurité. Cette option n'affecte que KeePass lui-même (c'est-à-dire la désactiver n'empêche pas le système d'exploitation ou d'autres logiciels de mémoriser les chemins). Si vous souhaitez uniquement empêcher un fichier clé d'apparaître dans la liste des fichiers récemment utilisés de Windows (ce qui n'affecte pas vraiment la sécurité) après l'avoir sélectionné dans KeePass, alors pensez à activer l'option de saisie de la clé principale sur un bureau sécurisé (KeePass affichera alors une boîte de dialogue de sélection de fichier clé plus simple qui n'ajoute pas le fichier à la liste des fichiers récemment utilisés de Windows).

Sauvegarde : vous devriez créer une sauvegarde de votre fichier clé (sur un équipement de stockage de

données indépendant). Si votre fichier clé est un fichier XML (ce qui est le cas par défaut), alors vous pouvez également créer une sauvegarde au papier (KeePass 2.x fournit une commande pour imprimer une sauvegarde d'un fichier clé dans le menu 'Fichier' → 'Imprimer'). Dans tous les cas, la sauvegarde devrait être stockées à un endroit sécurisé, où seulement vous et éventuellement d'autres personnes en qui vous aurez confiance auront accès. Plus de détails à propos de la sauvegarde d'un fichier clé peuvent être trouvés dans la FAQ ABP.

KeePass prend en charge les formats de fichier clé suivants :

- **XML (recommandé, par défaut) :** il existe un format XML pour les fichiers clé. KeePass 2.x utilise ce format par défaut, c'est-à-dire que lorsqu'on crée un fichier clé dans la boîte de dialogue de la clé principale, un fichier clé XML est créé. La syntaxe et la sémantique du format XML permettent de détecter certaine corruptions (notamment celles causées par des erreurs matérielles ou des problèmes de transfert), et un hachage (en fichier clé XML version 2.0 ou supérieure) permet de vérifier l'intégrité de la clé. Ce format résiste à la plupart des changements d'encodages et de caractère nouvelle ligne (ce qui est utile par exemple quand l'utilisateur ouvre et enregistre le fichier clé ou quand on le transfert depuis/vers un serveur). Un tel fichier clé peut être imprimé (en guise de sauvegarde sur papier), et des commentaires peuvent être ajoutés au fichier (avec la syntaxe XML usuelle : `<!-- ... -->`). C'est le format le plus flexible ; de nouvelles fonctionnalités pourront être facilement ajoutées dans le futur.
- **32 octets :** Si le fichier clé contient exactement 32 octets, alors ceux-ci sont utilisés comme une clé cryptographique de 256 bits. Ce format nécessite le moins d'espace disque.
- **Hexadécimal :** si le fichier clé contient exactement 64 caractères hexadécimaux (0-9 et A-F, en encodage ASCII/UTF-8, une ligne, aucun espace), ceux-ci sont décodés vers une clé cryptographique de 256 bits.
- **Haché :** si un fichier clé ne correspond pas à un des formats ci-dessus, alors son contenu est haché en utilisant une fonction de hachage cryptographique afin de fabriquer une clé (typiquement une clé de 256 bits avec SHA-256). Ceci permet d'utiliser des fichiers arbitraires en guise de fichier clé.

Réutilisation : Vous pouvez utiliser un fichier clé pour plusieurs bases de données. Ceci peut être intéressant, mais gardez à l'esprit que lorsqu'un attaquant obtient votre fichier clé, vous devez modifier les clés principales de tous les fichiers de base de données protégés avec ce fichier clé.

Pour réutiliser un fichier clé existant, cliquez sur le bouton avec l'icône 'Enregistrer' dans la boîte de dialogue de création de la clé principale et sélectionnez le fichier existant. Après avoir accepté la boîte de dialogue, KeePass vous demandera si vous souhaitez écraser ou réutiliser le fichier (voir capture d'écran).

Le compte utilisateur Windows

KeePass 1.x ne prend pas en charge le chiffrement des bases de données à l'aide de l'accréditation d'un compte d'utilisateur Windows. Seuls KeePass 2.x et supérieur le prennent en charge.

Pour les administrateurs : spécifications des propriétés minimales des clés principales

Des administrateurs peuvent spécifier une longueur minimale et/ou la qualité estimée minimale qu'un mot de passe maître doit avoir afin d'être accepté. Vous pouvez signaler à KeePass de vérifier ces deux exigences minimales en ajoutant/éditant les définitions appropriées dans le fichier de configuration INI/XML.

La valeur de la clé `KeeMasterPasswordMinLength` peut contenir la longueur minimale du mot de passe principal en caractères. Par exemple, en spécifiant `KeeMasterPasswordMinLength=10`, KeePass n'acceptera que des mots de passe principaux comportant au moins 10 caractères.

La valeur de la clé `KeeMasterPasswordMinQuality` peut contenir la qualité minimale estimée en bits que les mots de passe maîtres doivent avoir. Par exemple, en spécifiant `KeeMasterPasswordMinQuality=64`, uniquement les mots de passe principaux avec une qualité estimée d'au moins 64 bits seront acceptés.

Utilisateurs mutiple

Utilisateurs multiples

Détails à propos de la fonctionnalité multi-utilisateurs de KeePass.

- **Modification de la base de données partagée :**
  - Les informations générales à propos des bases de données partagées
  - KeePass 1.x : verrouillage style Office
  - KeePass 2.x : synchroniser ou écraser

Les informations générales à propos des bases de données partagées

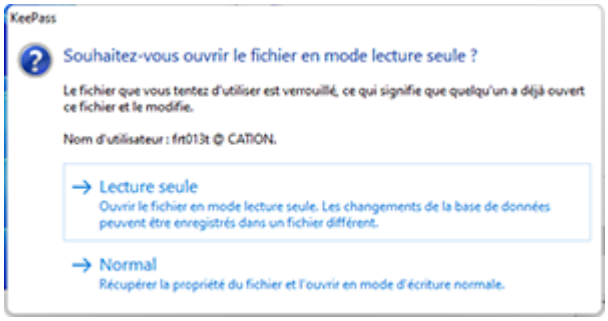
Les deux versions KeePass 1.x et 2.x permettent à plusieurs utilisateurs de travailler avec une seule base de données, qui est généralement enregistrée sur un lecteur réseau partagé ou un serveur de fichiers.

Tous les utilisateurs utilisent le même mot de passe maître et/ou même fichier clé pour ouvrir la base de données. Il n'y a pas de liste de contrôle d'accès (ACL) par groupe ou par entrée.

Afin de restreindre l'accès en écriture sur le fichier de la base de données (c'est-à-dire qu'un seul ensemble sélectionné d'utilisateurs peut modifier les données enregistrées), on utilise les droits d'accès du système de fichiers.

KeePass 1.x : verrouillage style Office

Avec KeePass 1.x, une base de données peut être enregistrée sur le lecteur réseau partagé et utilisé par plusieurs utilisateurs. Quand un utilisateur essaie d'ouvrir une base de données qui est déjà ouverte par quelqu'un d'autre, une invite lui demande s'il souhaite ouvrir la base de données en lecture seule ou en mode normal (cf. image sur le droit).



En ouvrant une base de données en mode normal, l'utilisateur courant prend possession du fichier (c'est-à-dire que les subséquents essais d'ouverture montreront l'utilisateur courant comme propriétaire).

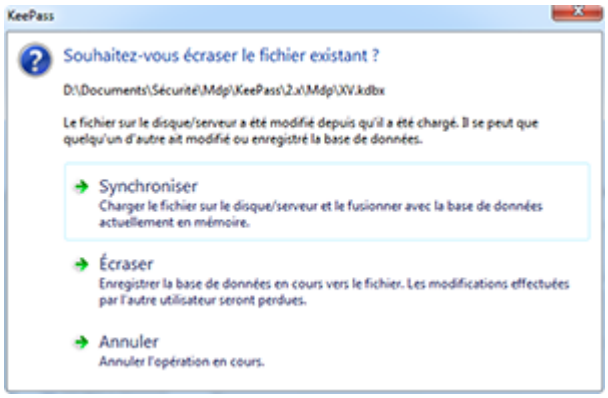
KeePass 1.x ne fournit pas de synchronisation, c'est-à-dire qu'en enregistrant la base de données vous enregistrez les données courantes sur le disque. Si un autre utilisateur a entre-temps modifié une entrée (c'est-à-dire depuis que vous avez chargé la base de données), ses changements sont écrasés.

Si vous souhaitez utiliser KeePass 1.x avec une base de données sur un lecteur réseau partagé, alors il est recommandé de laisser l'administrateur écrire sur la base de données et de laisser les utilisateurs seulement la lire (cela assure l'utilisation des droits d'accès du système de fichier). En utilisant le paramètre -readonly de la ligne de commande, KeePass ouvrira automatiquement une base de données en mode lecture seule (c'est-à-dire n'affichera pas l'invite de mode). Les utilisateurs ouvriraient la base de données en utilisant un raccourci qui contient ce paramètre de ligne de commande.

S'il n'y a pas d'administrateur central gérant la base de données, alors les utilisateurs ont besoin de faire attention à ne pas écraser les modifications de chacun.

KeePass 2.x : synchroniser ou écraser

Avec KeePass 2.x, une base de données peut être enregistrée sur un lecteur réseau partagé et utilisée par plusieurs utilisateurs. Quand on essaie d'enregistrer, KeePass vérifie d'abord si le fichier sur le disque a été modifié depuis qu'il a été chargé. Si oui, alors KeePass demande si on doit synchroniser ou écraser le fichier (cf. image sur le droit).



En synchronisant, les modifications apportées par d'autres utilisateurs (fichier sur le disque) et modifications faites par l'utilisateur courant sont fusionnées. Après que le processus de synchronisation est terminé, l'utilisateur courant voit également les modifications effectuées par les autres (c'est-à-dire que les données de l'instance KeePass en cours sont à jour).

S'il y a un conflit (c'est-à-dire que si plusieurs utilisateurs ont modifié la même entrée), alors KeePass utilise la dernière version basée sur le temps de dernière modification.

Remarque : l'invite de synchronisation est seulement déclenchée par la commande 'Enregistrer', *non* par la commande 'Enregistrer sous'. Quand on exécute la commande 'Enregistrer sous' et qu'on sélectionne manuellement un fichier, ce fichier sera toujours écrasé.

Le génénerateur de mot de passe

Le générateur de mots de passe

Les détails à propos du générateur de mots de passe intégré dans KeePass.

- La génération basée sur des jeux de caractères
- La génération basée sur des motifs
- La génération des mots de passe conforme à des règles
- Les options réduisant la sécurité
- La création et l'utilisation des profils du générateur de mots de passe
- La configuration des paramètres de mots de passe générés automatiquement pour les nouvelles entrées

La génération basée sur des jeux de caractères

Cette méthode de génération de mot de passe est la voie recommandée pour générer des mots de passe aléatoires. Les autres méthodes (génération basée sur un motif, etc.) ne devraient seulement être utilisées que si les mots de passe doivent suivre des règles spéciales ou remplir certaines conditions.

La génération basée sur un jeu de caractères est très simple. Vous laissez simplement KeePass connaître quels caractères peuvent être utilisés (par exemple : des lettres en majuscules, des chiffres, etc.) et KeePass sélectionnera au hasard des caractères du jeu.

Définir un jeu de caractères :
Le jeu de caractères peut être défini dans la fenêtre du générateur de mot de passe. Par commodité, KeePass propose d'ajouter des plages de caractères communément utilisés dans le jeu. Pour cela, cochez la case appropriée. En plus de ces plages de caractères prédéfinies, vous pouvez spécifier des caractères manuellement : tous les caractères que vous saisissez dans la zone de texte *'Inclure également les caractères suivants'* seront directement ajoutés au jeu de caractères.

Les caractères que vous saisissez dans la zone de texte *'Inclure également les caractères suivants'* sont incorporés au jeu de caractères à partir duquel le générateur de mot de passe choisit aléatoirement des caractères. Cela signifie que les caractères ajoutés sont *autorisés* à apparaître dans les mots de passe générés, mais ils ne sont pas *imposés*. Si vous souhaitez imposer que certains caractères apparaissent

dans les mots de passe générés, alors vous devez utiliser une génération basée sur un motif.

Les jeux de caractères sont des ensembles :
En terme mathématique, les jeux de caractères sont des ensembles, pas des vecteurs. Ceci signifie que les caractères ne peuvent pas être ajoutés deux fois au jeu. Soit un caractère est dans le jeu soit il n'y est pas.

Par exemple : si vous saisissez *'AAAAB'* dans la case des caractères supplémentaires, alors c'est exactement le même jeu que *'AB'*. *'A' n'*y sera *pas* 4 fois plus probable mais autant que *'B'* ! Si vous avez besoin de suivre des règles comme *'le caractère 'A' est plus probable que B'*, alors vous devez utiliser la génération basée sur un motif + la permutation des caractères de mot de passe.

KeePass 'optimisera' votre jeu de caractères en enlevant tous les caractères dupliqués. Si vous saisissiez le jeu de caractères *'AAAAB'* dans la case de caractères supplémentaire, alors fermez et rouvrez le générateur de mot passe, il affichera le plus petit jeu de caractères *'AB'*. De même, si vous cochez la case *'Chiffres'* et entrez *'3'* dans la case supplémentaire, le *'3'* sera ignoré car il est déjà inclus dans la plage de caractères *'Chiffres'*.

Les caractères pris en charge :
Tous les caractères Unicode dans les plages [U+0001, U+D7FF] et [U+E000, U+FFFF] exceptés { U+0009 / '\t', U+000A / '\n', U+000D / '\r' } sont pris en charge. Les caractères dans la plage [U+010000, U+10FFFF] (qui doivent être codés en UTF-16 en utilisant des paires de substitution depuis [0xD800, 0xDFFF]) ne sont pas pris en charge. Le traitement ultérieur des mots de passe peut avoir d'autres limitations (par exemple : le caractère U+FFFF est interdit dans les fichiers XML/KDBX et sera remplacé ou supprimé).

La génération basée sur des motifs

Le générateur de mot de passe peut créer des mots de passe en utilisant des motifs. Un motif est une chaîne définissant la disposition du nouveau mot de passe. Les paramètres substituables (placeholders) suivants sont pris en charge :

Paramètre substituable	Type	Jeu de caractères
a	Minuscules alphanumériques	abcdefghijklmnopqrstuvwxyz 0123456789
A	Alphanumériques à casse mixte	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789
U	Majuscules alphanumériques	ABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789
d	Chiffres	0123456789
h	Minuscules en caractères hexadécimaux	0123456789 abcdef
H	Majuscules en caractères hexadécimaux	0123456789 ABCDEF
l	Lettres en minuscule	abcdefghijklmnopqrstuvwxyz
L	Lettres à casse mixte	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz
u	Lettres en majuscule	ABCDEFGHIJKLMNOPQRSTUVWXYZ
v	Voyelles en minuscule	aeiou
V	Voyelles à casse mixte	AEIOU aeiou
Z	Voyelles en majuscule	AEIOU
c	Consonnes en minuscule	bcdfghjklmnpqrstvwxyz

c	Consonnes à casse mixte	BCDFGHJKLMNPQRSTVWXYZ bcdfghjklmnpqrstvwxyz
z	Consonnes en majuscule	BCDFGHJKLMNPQRSTVWXYZ
p	Ponctuation	,.;:
b	Crochets (parenthèses)	()[]{}<>
s	Caractères spéciaux 7 bits imprimables	!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
S	ASCII 7 bits imprimables	A-Z, a-z, 0-9, !"#$%&'()*+,-./ :;<=>?@[\]^_`{|}~
x	Supplément Latin-1	Plage [U+00A1, U+00FF] excepté U+00AD: ¡¢£¤¥¦§¨©ª«¬®¯ °±²³ ´µ¶·¸¹º»¼½¾¿ ÀÁÂÃÄÅÆÇÈÉÊËÌÍÎÏ ÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞß àáâãäåæçèéêëìíîï ðñòóôõö÷øùúûüýþÿ
\	Échappement (caractère fixé)	Utiliser le caractère suivant tel quel.
{*n*}	Échappement (Répétition)	Répétez le paramètre substituable précédent *n* fois.
[...]	Jeu de caractères personnalisés	Définissez un jeu de caractères personnalisés.

Le paramètre substituable **** est spécial : c'est un caractère d'échappement. Le prochain caractère qui suit le **** est écrit directement dans le mot de passe généré. Si vous souhaitez un \ dans votre mot de passe à une place spécifique, alors vous devez écrire `\\`.

En utilisant le code **{*n*}** vous pouvez définir combien de fois le paramètre substituable précédent devrait arriver. L'opérateur **{ }** duplique les paramètres substituables, et non pas les caractères générés. Exemples :
» `d{4}` est équivalent à `dddd`,
» `dH{4}a` est équivalent à `dHHHHa` et
» `Hda{1}dH` est équivalent à `HdadH`.

La notation **[...]** peut être utilisée pour définir un jeu de caractères personnalisés, depuis lequel le générateur de mot de passe choisira aléatoirement un caractère. Tous les caractères entre les crochets **[**' et '**]**' suivent les mêmes règles que les paramètres substituables ci-dessus. Le caractère **^**' supprime les paramètres substituables suivants du jeu de caractères. Exemples :
» `[dp]` génère exactement 1 caractère aléatoire parmi les jeux chiffres + ponctuation,
» `[d\m\@^\3]{5}` génère 5 caractères parmi le jeu "012456789m@",
» `[u\_][u\_]` génère 2 caractères parmi le jeu majuscules + '_'.

Davantage d'exemples :

`ddddd`
Génère par exemple : 41922, 12733, 43960, 07660, 12390, 74680, etc.

`\H\e\x\:\ HHHHHH`
Génère par exemple : 'Hex: 13567A', 'Hex: A6B99D', 'Hex: 02243C', etc.

Les motifs de mots de passe communs :

Nom	Motif
Touche hexadécimale - 40-Bit	`H{10}`
Touche hexadécimale - 128-Bit	`H{32}`
Touche hexadécimale - 256-Bit	`H{64}`

Adresse MAC	`H\2\-HH\-HH\-HH\-HH\-HH`

Chacun de ces motifs génère exactement une clé hexadécimale, pas plusieurs clés hexadécimales. Par conséquent, on utilise la forme singulière.

La génération des mots de passe conforme à des règles

Voici ci-dessous quelques exemples d'utilisation de fonction de génération de motif pour générer des mots de passe qui suivent certaines règles.

Important ! Pour tous les exemples suivants, vous devez activer l'option 'Permuter aléatoirement des caractères du mot de passe' !

Règle	**Motif**
Doit contenir 2 lettres majuscules, 2 lettres minuscules et 2 chiffres.	`uulldd`
Doit contenir 9 chiffres et 1 lettre.	`d{9}L`
Doit contenir 10 caractères alphanumériques, où au moins 1 est une lettre et au moins 1 est un chiffre.	`LdA{8}`
Doit contenir 10 caractères alphanumériques, où au moins 2 sont des lettres majuscules et au moins 2 sont des lettres minuscules.	`uullA{6}`
Doit contenir 9 caractères du jeu "ABCDEF" et un symbole '@'.	`\@[\A\B\C\D\E\F]{9}`

Les options réduisant la sécurité

Le générateur de mot de passe prend en charge plusieurs options comme *'Chaque caractère doit apparaître au plus une fois'*, *'Exclure les caractères similaires'* (`O0`, `Il1|`) et un champ pour spécifier explicitement les caractères qui ne devraient pas apparaître dans les mots de passe générés.

Ces options réduisent la sécurité des mots de passe générés. Vous ne devriez les activer que si seulement vous êtes obligés de suivre de telles règles par le site/application, pour lequel/laquelle vous êtes en train de générer le mot de passe.

Les options peuvent être trouvées dans la boîte de dialogue de l'onglet *'Avancé'*.

Si vous activez une option réduisant la sécurité, alors le bouton *'Avancé'* dans la fenêtre du générateur de mot de passe est affiché en rouge.

La création et l'utilisation des profils du générateur de mots de passe

Les options du générateur de mots de passe (jeu de caractères, longueur, motif, etc.) peuvent être enregistrées en tant que profils du générateur de mots de passe.

Création/modification d'un profil :

1. Ouvrez la fenêtre du *générateur de mot de passe*.
2. Spécifiez toutes les options du nouveau profil.
3. Cliquez sur le bouton '*Enregistrer les paramètres actuels dans un profil.* '.
4. Entrez le nom du nouveau profil, ou sélectionnez un nom de profil existant depuis la liste déroulante pour l'écraser. Fermez la boîte de dialogue avec *OK*.
5. Si vous souhaitez immédiatement créer un mot de passe en utilisant le nouveau profil, alors cliquez sur *OK/Accepter*. Sinon cliquez sur *Annuler/Fermer* (le profil n'est pas perdu ; la gestion des profils est indépendante de la génération du mot de passe).

Utilisation d'un profil :
Pour utiliser un profil, sélectionnez-le simplement depuis la liste déroulante des profils de la fenêtre du générateur de mots de passe. Tous les paramètres de ce profil seront restaurés tels quels.

Un méta profil 'Dérivé du mot de passe précédent' :
Quand ce méta profil est sélectionné, un mot de passe est généré sur la base d'un jeu de caractères

dérivé du mot de passe précédent. Le nouveau mot de passe a la même longueur que l'ancien, et chaque caractère de l'ancien mot de passe active le sous-ensemble de caractères qui contient ce caractère. Par exemple, si l'ancien mot de passe contient la lettre 'R', alors le jeu de caractères utilisé pour la génération du nouveau caractère contient la plage 'A' à 'Z'.
Attention ! Ce méta profil ne devrait pas être utilisé aveuglément (c'est-à-dire sans revoir le jeu de caractères utilisé). Le nouveau mot de passe ne doit pas nécessairement contenir au moins un caractère de chaque sous-ensemble de caractères (cf. 'La génération basée sur des jeux de caractères'), ainsi la génération aveugle de nouveaux mots de passe avec ce méta-profil peut entraîner une dégradation de la qualité du profil effectivement utilisé.

La configuration des paramètres de mots de passe générés automatiquement pour les nouvelles entrées

Quand vous créez une nouvelle entrée, KeePass génère automatiquement un mot de passe aléatoire pour celle-ci. Les propriétés de ces mots de passe générés peuvent être configurées dans la boîte de dialogue du générateur de mot de passe.

Pour configurer, spécifiez les options de votre choix et écrasez le profil*'(Mots de passe générés automatiquement pour les nouvelles entrées)'* (cf. la section ci-dessus).

Désactivation des mots de passe générés automatiquement :
Pour désactiver les mots de passe générés automatiquement pour les nouvelles entrées, sélectionnez *'Générer en utilisant un jeu de caractères'* et spécifiez *0* comme longueur de mot de passe. Écrasez le profil approprié (cf. ci-dessus).

Les paramètres substituables

Les paramètres substituables (placeholders)

KeePass prend en charge divers paramètres substituables.

À de nombreux endroits dans KeePass (la saisie automatique, le champ d'adresse (URL), les déclencheurs, etc.), des paramètres substituables peuvent être utilisés.

- Les paramètres substituables de champ d'entrée
- Les références de champ de l'entrée
- Les paramètres substituables des chemins et date/heure
- Les variables d'environnement
- Les transformations de texte
- Les autres paramètres substituables

Les paramètres substituables sont sensibles à la casse.
KeePass utilise l'abréviation "Spr" pour "String placeholder replacement" ("le remplacement du paramètre substituable par une chaîne"). Un champ compilé par *Spr* est un champ où les paramètres substituables sont remplacés quand on effectue une action avec ce champ (par exemple : comme la copie vers le presse-papiers, l'envoyer en utilisant la saisie automatique, etc.).

Les références dans un champ vers (les parties du) le champ lui-même ne sont pas prises en charge. Par exemple : le paramètre substituable `{URL:HOST}` ne peut pas être utilisé dans le champ d'adresse (URL) (mais il peut être utilisé dans le champ 'Remplacer l'adresse (URL - par exemple : pour utiliser un navigateur spécifique) :'.

Les paramètres substituables sont similaires aux variables d'environnement, mais ils ne fonctionnent seulement que dans KeePass (par exemple : il y a un paramètre substituable {APPDIR}, qui est remplacé par le chemin du répertoire de l'application.

Les paramètres substituables de champ d'entrée

Paramètre substituable	Valeur
`{TITLE}`	Titre de l'entrée

{USERNAME}	Nom d'utilisateur de l'entrée
{URL}	Adresse (URL) de l'entrée
{PASSWORD}	Mot de passe de l'entrée
{NOTES}	Remarques de l'entrée

Les références de champ de l'entrée

Les champs d'*autres* entrées peuvent être insérés en utilisant des références de champ.

Les paramètres substituables des chemins et date/heure

Le paramètre substituable	Valeur
{EDGE}	Le chemin vers Microsoft Edge, s'il est installé.
{FIREFOX}	Le chemin vers Mozilla Firefox, s'il est installé.
{GOOGLECHROME}	Le chemin vers Google Chrome (ou Chromium sur les systèmes Unix-like), s'il est installé.
{INTERNETEXPLORER}	Le chemin vers Internet Explorer, s'il est installé.
{OPERA}	Le chemin vers Opera, s'il est installé.
{SAFARI}	Le chemin vers Safari, s'il est installé.

Le paramètre substituable	Valeur
{APPDIR}	Le chemin du répertoire de l'application KeePass.

Le paramètre substituable	Valeur
{DT_SIMPLE}	La date/heure locale actuelle sous la forme d'une chaîne simple et qui peut être triée. Par exemple : pour 2028-07-25 17:05:34 la valeur est 20280725170534.
{DT_YEAR}	La composante année de la date/heure locale actuelle.
{DT_MONTH}	Le composant mois de la date/heure locale actuelle.
{DT_DAY}	Le composant jour de la date/heure locale actuelle.
{DT_HOUR}	La composante heure de la date/heure locale actuelle.
{DT_MINUTE}	La composante minute de la date/heure locale actuelle.
{DT_SECOND}	La composante seconde de la date/heure locale actuelle.
{DT_UTC_SIMPLE}	La composante date/heure UTC

	actuelle sous la forme d'une chaîne simple et qui peut être triée.
{DT_UTC_YEAR}	La composante année de la date/heure UTC actuelle.
{DT_UTC_MONTH}	Le composant mois de la date/heure UTC actuelle.
{DT_UTC_DAY}	Le composant jour de la date/heure UTC actuelle.
{DT_UTC_HOUR}	La composante heure de la date/heure UTC actuelle.
{DT_UTC_MINUTE}	La composante minute de la date/heure UTC actuelle.
{DT_UTC_SECOND}	La composante seconde de la date/heure UTC actuelle.

Les variables d'environnement

Les variables d'environnement système sont prises en charge. Le nom de la variable doit être entouré par le caractère '%'. Par exemple : %TEMP% est remplacé par le chemin temporaire de l'utilisateur.

Les transformations de texte

Les autres paramètres substituables

Les paramètres substituables	Valeur
{PASSWORD_ENC}	Le mot de passe dans sa forme chiffrée. cf. ci-dessous.

{PASSWORD_ENC} – Chiffrement des mots de passe :
Le paramètre substituable {PASSWORD_ENC} est remplacé par le mot de passe de l'entrée en cours sous forme chiffrée. Le mot de passe est chiffré à l'aide de l'accréditation de l'utilisateur Windows en cours. Le mot de passe chiffré ne doit pas être stocké et ne fonctionne que pour l'utilisateur actuel.

Il est destiné à être utilisé en conjonction avec le paramètre deligne de commande -pw-enc (voir la page Le champ adresse (URL) pour un exemple de définition d'une URL pour ouvrir une base de données KeePass supplémentaire). Le paramètre substituable ne peut pas être utilisé pour transférer des mots de passe vers d'autres applications (à l'exception de KeePass), car les applications cibles ne savent pas comment déchiffrer les mots de passe chiffrés générés par {PASSWORD_ENC}.

Réparer les bases de données

La réparation des bases de données

KeePass peut réparer des bases de données corrompues dans certains cas.

KeePass possède de nombreuses fonctionnalités pour éviter la corruption des fichiers de base de données (écriture de base de données transactionnelle, vidage de la mémoire-tampon du périphérique, etc.). Cependant, la corruption des données peut toujours être causée par d'autres programmes, le système ou

des périphériques de stockage cassés (remarquez que KeePass par défaut vérifie l'intégrité des fichiers de base de données immédiatement après les avoir écrits, c'est-à-dire qu'à ce stade, KeePass garantit l'intégrité des fichiers ; cependant, KeePass ne peut bien sûr rien faire lorsque les données deviennent corrompues/illisibles à un moment ultérieur).

Dans ces cas, la fonctionnalité de réparation de la base de données peut vous aider. Ici, KeePass essaie de lire autant de données que possibles à partir du fichier corrompu.

⚠ En mode réparation, l'intégrité des données n'est pas vérifiée (afin de récupérer autant de données que possible). Lorsque aucune vérification d'intégrité n'est effectuée, des données corrompues/malveillantes peuvent être incorporées dans la base de données. Ainsi, la fonctionnalité de réparation ne doit être utilisée que lorsqu'il n'y a vraiment aucune autre solution. Si vous l'utilisez, vous devez ensuite vérifier soigneusement toute votre base de données pour les données corrompues/malveillantes.

Dans KeePass 1.x, la fonctionnalité de réparation se trouve dans *'Outils'* → *'Réparer le fichier de base de données de KeePass...'*.
Quoi qu'il en soit, si vous avez perdu la clé principale de la base de données, la fonctionnalité de réparation ne peut pas vous aider. De plus, si l'en-tête de la base de données (les premiers octets) est corrompu, alors vous n'avez également pas de chance : la fonctionnalité de réparation ne pourra pas restaurer les entrées (car l'en-tête contient les informations nécessaires pour déchiffrer la base de données).

La fonctionnalité de réparation doit être considérée comme le dernier espoir. Faire des sauvegardes régulières de vos bases de données est bien mieux et doit être préféré. Les sauvegardes*n*'ont *aucune* incidence sur la sécurité cryptographique. Il existe des greffons qui automatisent le processus de sauvegarde, cf. la page des greffons de KeePass.

En-tête/signature de fichier

Si votre fichier de base de données a été supprimé et que vous souhaitiez essayer de le récupérer à l'aide d'un outil qui prend en charge une détection d'en-tête/signature de fichier : alors vous trouverez ci-dessous les premiers octets (en notation hexadécimale) par lesquels tous les fichiers de base de données commencent.

- Fichier KDB de KeePass 1.x :
  `03 D9 A2 9A 65 FB 4B B5`
- Fichier KDBX de KeePass 2.x :
  `03 D9 A2 9A 67 FB 4B B5`

L'en-tête du fichier ne contient pas de champ qui spécifie la longueur du fichier. Si la longueur ne peut pas être déterminée à partir du système de fichiers, alors essayez de récupérer suffisamment de données (c'est-à-dire les données du fichier de base de données et peut-être des données ultérieures inutiles) et utilisez la fonctionnalité de réparation ci-dessus, qui ignorera simplement toutes les données suivantes.

Rechercher

Rechercher

Les détails à propos des fonctions de recherche de KeePass.

- Le mode de recherche 'Expression simple'
  - Exemple : termes multiples
  - Exemple : terme avec espaces
  - Exemple : Exclusions (2.x)
- Le mode de recherche 'Expression régulière'
  - Exemple : terme exact
  - Exemple : mots de passe courts
  - Exemple : balises multiple (OR, exact)
- Le mode de recherche 'Expression XPath' (2.x)
  - Exemple : icône
  - Exemple : expiré spécifié en années
  - Exemple : champ chaîne de caractères personnalisé
  - Exemple : fichiers PDF joints

    - Exemple : couleur d'arrière-plan
    - Exemple : balises multiple (AND, exact)
    - Exemple : le compteur d'entrée de l'historique
    - Exemple : les remarques de groupe
- Le profils de recherche (2.x)
- Boîte de recherche rapide

🔍 *Le mode recherche 'Expression simple'*

Dans ce mode, KeePass recherche les termes spécifiés dans les champs sélectionnés. Pour qu'une entrée corresponde, alors *tous* les termes doivent correspondre.

- **Termes multiples :**
  Afin de rechercher pour des termes multiples, séparer les termes en utilisant des espaces. Si vous souhaitez recherche un terme contenant des espaces, alors imbriquer le terme entre doubles quotes (`"..."`).
- **Exclusions (2.x) :**
  Afin de chercher des entrées qui *ne* contiennent *pas* un certain terme, alors précéder le terme d'un signe moins.

Une entrée correspond si les termes spécifiés peuvent être trouvés en tant que sous-chaînes. Si vous souhaitez trouver plutôt des correspondances exactes, alors utiliser une expression régulière (voir l'exemple 'Terme exact').

Exemples :

Termes multiple	
Que chercher :	`Michael Home`
Options :	☐ Titre
Cherche chaque entrée dont le titre contient à la fois le terme 'Michael' et le terme 'Home' (dans n'importe quel ordre).	

Termes avec des espaces	
Que chercher :	`Michael "Serveur Web"`
Options :	☐ Titre
Cherche chaque entrée dont le titre contient à la fois le terme 'Michael' et le terme 'Serveur Web'.	

Exclusions (2.x)	
Que chercher :	`Michael -Home`
Options :	☐ Titre
Cherche chaque entrée dont le titre contient le terme 'Michael', mais pas le terme 'Home'.	

🔍 *Le mode de recherche 'Expression régulière'*

Dans ce mode, KeePass recherche les correspondances d'une expression régulière dans les champs sélectionnés.

Des informations à propos des expressions régulières et des outils peuvent être trouvés ici :

- Microsoft: Regular Expression Language - Quick Reference
- Wikipedia: Regular expression
- Regex101: Build, test and debug regex

Exemples :

Terme exact

Que chercher :	`^Michael$`
Options :	☐Nom d'utilisateur
Cherche chaque entrée dont le nom d'utilisateur est 'Michael' (c'est-à-dire que 'Michael' n'est pas seulement exactement une sous-chaîne du nom d'utilisateur de l'entrée).	

Mots de passe courts	
Que chercher :	`^.{1,10}$`
Options :	☐Mot de passe
Cherche chaque entrée dont le mot de passe à une longueur entre 1 et 10 (inclusif).	
Si vous souhaitez plutôt chercher des mots de passe faibles, alors utiliser la commande de 'Qualité du mot de passe' dans le menu 'Rechercher'.	

Balises multiple (OR, exact)	
Que chercher :	`^(Home|Privé)$`
Options :	☐ Balises
Cherche chaque entrée qui possède la balise 'Home' ou la balise 'Privé' (ou bien les deux à la fois).	

Le mode de recherche 'Expression XPath' (2.x)

Dans ce mode, un DOM XML KeePass 2.x de la base de données en cours est créé en mémoire et l'expression XPath spécifiée est utilisée pour trouver les entrées.

Des informations à propos des expressions XPath peuvent être trouvées ici :

- W3C: XML Path Language (XPath) 2.0
- Microsoft: XPath Reference
- Microsoft: XPath Examples
- Wikipedia: XPath

Si vous souhaitez trouver et *remplacer* des données en utilisant des expressions XPath et régulières, alors voir la fonctionnalité Remplacement XML.

Exemples :

Icône	
Que chercher :	`//Entry[(IconID = '3') and not(CustomIconUUID)]`
Trouve chaque entrée qui possède une icône .	

Expiré spécifié en année	
Que chercher :	`//Entry/Times[(Expires = 'True') and starts-with(ExpiryTime, '2022-')]/..`
Trouve chaque entrée qui a expiré en 2022.	

Champ chaîne de caractères personnalisé	
Que chercher :	`//Entry/String[(Key = 'Telephone') and contains(Value, '12345')]/..`
Options :	☐Autres chaînes
Trouve chaque entrée qui a un champ de chaîne de caractères personnalisé nommé 'Telephone' dont la	

valeur contient '12345'.

Fichiers PDF joints	
Que chercher :	`//Entry/Binary/Key[(string-length(.) >= 4) and (substring(., string-length(.) - 3) = '.pdf')]/../..`
Trouve chaque entrée qui possède un fichier joint dont le nom de termine par '.pdf'.	
Si au contraire vous souhaitez trouver des entrées volumineuses, alors utiliser la commande 'Entrées volumineuses' dans le menu 'Rechercher'.	

Couleur d'arrière-plan	
Que chercher :	`//Entry[BackgroundColor = '#CCFFCC']`
Trouve chaque entrée qui possède une lumière verte en couleur d'arrière-plan.	
Les couleurs d'arrière-plan normalisées sont lumière rouge (`#FFCCCC`), lumière verte (`#CCFFCC`), lumière bleue (`#99CCFF`) et lumière jaune (`#FFFF99`).	

Balises multiple (AND, exact)	
Que chercher :	`//Entry[contains(concat(';', Tags, ';'), ';Home;') and contains(concat(';', Tags, ';'), ';Privé;')]`
Options :	☐ Balises (tags)
Trouve chaque entrée qui possède à la fois la balise 'Home' et la balise 'Privé'.	
Contrairement à ceci, en recherchant avec l'expression simple '`Home Privé`' cela trouve également les entrées qui ont 'Home' et 'Privé' en tant que sous-chaînes dans les balises.	

Le compteur d'entrée de l'historique	
Que chercher :	`//Entry[count(History/Entry) >= 4]`
Options :	☐ Historique
Trouve chaque entrée qui possède au moins quatre entrées d'historique.	

Les remarques de groupe	
Que chercher :	`//Group[contains(Notes, 'Privé')]/Entry`
Trouve chaque entrée dont le groupe parent (direct) contient le mot 'Privé' dans les remarques (du groupe, et non de l'entrée). S'il existe plusieurs de tels groupes, alors les entrées de tous ces groupes sont trouvées.	

Les profils de recherche (2.x)

KeePass peut sauvegarder les paramètres de recherche en tant que profil de recherche. Ceci peut être utile quand vous accomplissez régulièrement des recherches similaires.

La création d'un profil :
Afin de sauvegarder les paramètres de la recherche en cours spécifiés dans la boîte de dialogue 'Rechercher', clique sur le bouton création de profil. KeePass affichera alors une boîte de dialogue où vous pourrez saisir un nom pour le nouveau profil.

Écraser un profil :

L'écrasement d'un profil existant fonctionne de la même manière que la création d'un profil, excepté que vous sélectionnez un nom de profil existant dans le nom de la boîte de dialogue.

L'utilisation d'un profil :
Il existe deux façons de charger un profil et d'accomplir une recherche avec lui :

- Ouvrir la boîte de dialogue 'Rechercher' (via le menu 'Rechercher' ou Ctrl+F), cliquer sur la case 'Profil' et sélectionner le profil souhaité ; cela implique que KeePass charge le profil. Si nécessaire, alors ajuster les paramètres de recherche. Finalement, cliquer sur le bouton 'Rechercher'.
- Dans le menu de la fenêtre principale, cliquer sur 'Rechercher' → 'Rechercher des profils'. Dans ce menu, tous les profils sont listés. Pour chaque profil, il existe des commandes pour accomplir directement une recherche avec le profil (les commandes 'Rechercher...') et des commandes pour afficher les profils dans la boîte de dialogue 'Rechercher' (les commandes 'Ouvrir...').

La suppression d'un profil :
Afin de supprimer un profil, sélectionner le dans la boîte de dialogue 'Rechercher' et cliquer sur le bouton de suppression de profil.

Boîte de recherche rapide

La boîte de recherche rapide dans la barre d'outils de la fenêtre principale prend en charge des recherches par expression simple et expression régulière.

Afin d'indiquer que la chaîne de recherche est une expression régulière, enfermer la avec des '//'. Par exemple : '//A{6}//' trouve toutes les entrées contenant la chaîne de caractères 'AAAAAA'. Noter que cette syntaxe spéciale ne fonctionne pas dans la boîte de dialogue 'Rechercher'. Dans cette boîte de dialogue, vous devez sélectionner le mode de l'expression régulière tel quel, c'est-à-dire sans l'enfermer avec des '//'.

Options :
La boîte de dialogue 'Rechercher' et la boîte de recherche rapide sont indépendantes. Les options/paramètres dans la boîte de dialogue 'Rechercher' n'affectent pas les recherches rapides. Des options pour des recherches rapides peuvent être trouvées dans les options de la boîte de dialogue (menu 'Outils' → 'Options...' → onglet 'Interface').

Les contrôles d'édition sécurisée

Les contrôles d'édition sécurisés

KeePass prend en charge les contrôles d'édition sécurisés évolués.

KeePass a été l'un des premiers gestionnaires de mots de passe à proposer des contrôles d'édition sécurisés. Les contrôles d'édition utilisés dans KeePass sont résistants aux révélateurs de mot de passe et aux espions de contrôle de mot de passe. De plus, les mots de passe saisis sont protégés contre les attaques de vidage de la mémoire : les mots de passe ne sont même pas visibles dans la mémoire du processus de KeePass !

KeePass utilise des contrôles d'édition sécurisés uniquement lorsque l'option masquage par des astérisques est activée . Si vous affichez les mots de passe en texte clair, ils ne sont pas protégés (les contrôles d'édition sécurisés sont alors simplement désactivés, remplacés par des contrôles d'édition Windows standard).

Sélection :
Une limitation de ces contrôles d'édition sécurisés est que vous ne pouvez pas sélectionner une plage de caractères. Vous ne pouvez par exemple pas sélectionner 3 caractères et les remplacer par le contenu actuel du presse-papiers à l'aide de la commande coller.

Si vous souhaitez supprimer tout le contenu d'un contrôle d'édition sécurisé, alors appuyez sur Maj+Origine ou Maj+Fin. Cela supprimera tous les caractères saisis.

La sécurité

Le chiffrement de la base de données

Les fichiers de base de données de KeePass sont chiffrés. KeePass chiffre toute la base de données, c'est-à-dire non seulement vos mots de passe, mais également vos noms d'utilisateurs, adresses (URL), remarques, etc.

Les algorithmes de chiffrement suivants sont pris en charge :

KeePass 1.x :

Algorithme	Taille de la clé	Norme/Réf.
Advanced Encryption Standard (AES/Rijndael)	256 bits	NIST FIPS 197
Twofish	256 bits	Info

KeePass 2.x :

Algorithme	Taille de la clé	Norme/Réf.
Advanced Encryption Standard (AES/Rijndael)	256 bits	NIST FIPS 197
ChaCha20	256 bits	RFC 8439
Il existe différents greffons prenant en charge des algorithmes de chiffrement supplémentaires, y compris, mais sans s'y limiter, Twofish, Serpent et GOST.		

Ces algorithmes bien connus et analysés en profondeur sont considérés comme très sécurisés. AES (Rijndael) est devenue une norme du gouvernement fédéral américain et est approuvée par la National Security Agency (NSA) pour les informations les plus secrètes (top secret). Twofish était l'un des quatre autres finalistes de l'AES. ChaCha20 est le successeur de l'algorithme Salsa20 (qui est inclus dans le portefeuille eSTREAM).

Les chiffrements par blocs sont utilisés dans le mode de chiffrement par blocs CBC (Cipher Block Chaining). En mode CBC, les modèles de texte en clair sont masqués.

Un vecteur d'initialisation (IV) est généré de manière aléatoire chaque fois qu'une base de données est enregistrée. Ainsi, plusieurs bases de données chiffrées avec la même clé principale (par exemple : des sauvegardes) ne posent aucun problème.

L'authenticité et l'intégrité des données :

L'authenticité et l'intégrité des données sont assurées par un hachage SHA-256 du texte en clair.
voir aussi :

- Spécification du format de fichier KDBX.
- Prise en charge du mode FIPS.

Le hachage de clé et la dérivation de clé

SHA-256 est utilisé pour compresser les composants de la clé principale (consistant en un mot de passe maître, un fichier clé, une clé de compte utilisateur Windows et/ou une clé fournie par un greffon) en une clé *K* de 256 bits.

SHA-256 est une fonction de hachage cryptographique considérée comme très sécurisée. Elle a été normalisée par le NIST FIPS 180-4. L'attaque contre SHA-1 découverte en 2005 n'affecte pas la sécurité de SHA-256.

Afin de générer la clé de l'algorithme de chiffrement,*K* est transformée à l'aide d'une fonction de dérivation de clé (avec un sel aléatoire). Cela évite le précalcul des clés et rend plus difficiles les attaques par dictionnaire et par devinettes. Pour plus de détails, cf. la section la protection contre les attaques par dictionnaire'.

La protection contre les attaques par dictionnaire

KeePass offre une protection contre les attaques par dictionnaire et devinettes.

De telles attaques ne peuvent pas être évitées, mais elles peuvent être rendues plus difficiles. Pour cela, la clé *K* dérivée de la clé principale de l'utilisateur (cf. ci-dessus) est transformée à l'aide d'une fonction de dérivation de clé avec un sel aléatoire. Cela évite un précalcul des clés et ajoute un facteur de travail que l'utilisateur peut rendre aussi grand que souhaité pour augmenter l'effort de calcul d'une attaque par dictionnaire ou devinette.

Des fonctions de dérivation de clé multiple sont prises en charge. Dans la boîte de dialogue des paramètres de la base de données, vous pouvez en sélectionner une et spécifier certains paramètres pour elle.

En cliquant sur le bouton 'Délai d'une seconde' dans les paramètres de la boîte de dialogue de la base de données, KeePass calcule le nombre d'itérations qui résulte en un délai d'une seconde quand on charge/enregistre une base de données. De plus, KeePass 2.x possède un bouton 'Test' qui accomplit une transformation de clé avec les paramètres spécifiés (ce qui peut être annulé) et rend le temps requis.

La clé de transformation peut nécessiter plus ou moins de temps sur d'autres appareils. Si vous utilisez KeePass ou un de ses portages sur d'autres appareils, alors assurez-vous que tous les appareils sont assez rapides (et ont suffisamment de mémoire) pour charger la base de données avec vos paramètres en un temps acceptable.

Les fonctions de dérivation de clé prises en charge :

- **AES-KDF** (KeePass 1.x et 2.x) :
  Cette fonction de dérivation de clé est basée sur l'itération d'AES.
  Dans la boîte de dialogue des paramètres de la base de données, vous pouvez modifier le nombre d'itérations. Plus il y a d'itérations, et plus les attaques par dictionnaire et devinettes sont difficiles, mais le chargement/la sauvegarde de la base de données prend également plus de temps (linéairement). Sur Windows Vista et les versions ultérieures, KeePass peut utiliser l'API CNG/BCrypt de Windows pour la transformation de clé, ce qui est approximativement 50 % plus rapides que le code de transformation de clé intégré dans KeePass.
- **Argon2** (uniquement KeePass 2.x) :
  Argon2 est le gagnant du concours de hachage de mots de passe. Le principal avantage

d'Argon2 par rapport à AES-KDF est qu'il offre une meilleure résistance contre les attaques par GPU/ASIC (en raison de sa fonction mémoire en dure). Le nombre d'itérations varie linéairement avec le temps requis.
La spécification officielle de l'algorithme Argon2 définit trois variantes : Argon2d, Argon2id et Argon2i. Argon2i est la variante la moins adaptée dans notre cas (fichier de base de données KeePass) ; par conséquent, KeePass ne propose que Argon2d et Argon2id.

Argon2d offre la meilleure résistance aux attaques GPU/ASIC. La résistance d'Argon2id contre les attaques GPU/ASIC est un peu plus faible, mais Argon2id rend en outre certaines attaques par canaux latéraux légèrement plus difficiles.

Les attaques par canaux latéraux tentent d'obtenir des informations d'un système en observant son comportement (par exemple : la durée et la consommation d'énergie de certaines opérations). Sur les serveurs, les attaques par canaux latéraux sont une réelle menace. Sur les appareils clients (PC), les attaques par canal latéral sont plus difficiles (plus de bruit, etc.) ; il y a des idées sur la façon dont certains pourraient fonctionner en théorie, mais nous ne sommes au courant d'aucune attaque réelle dans la pratique. Par exemple : l'attaque décrite dans l'article 'The Spy in the Sandbox / Side-Channel Attacks in Web Browsers' était intéressante (le code JavaScript était capable de détecter certaines interactions de l'utilisateur), mais pas une menace réelle (pas d'extraction de données sensibles, comme mentionné explicitement dans l'article). Cela peut ou peut ne pas changer à l'avenir. Notez que cela n'a rien à voir avec le stockage en nuage ; KeePass chiffre/déchiffre un fichier de base de données sur un appareil client, et donc peu importe où le fichier de base de données est stocké (pour les attaques par canal latéral). De plus, il existe des attaques par canal latéral contre lesquelles ni Argon2d ni Argon2id (ni Argon2i, ni aucune autre fonction de dérivation de clé) ne protègent (par exemple : les attaques par canal latéral Spectre/Meltdown, qui permettent aux logiciels espions de lire toute la mémoire).

Dans le cas de KeePass, nous recommandons actuellement Argon2d au lieu d'Argon2id, car nous pensons qu'une meilleure protection contre une menace réellement existante (le casse de mots de passe à l'aide de GPU/ASIC est l'état de l'art) est plus importante qu'une protection contre certaines attaques par canal latéral qui peuvent ou non devenir un problème sur les appareils clients à l'avenir. Si vous vous inquiétez des attaques par canaux latéraux (et êtes prêt à sacrifier une certaine résistance GPU/ASIC) ou si vous développez un logiciel où les attaques par canaux latéraux pourraient poser problème (par exemple : un service de serveur qui fonctionne avec les fichiers de base de données KeePass), utilisez Argon2id.

Remarque : la norme Internet IRTF CFRG Argon2 recommande Argon2id par défaut. Pour les applications serveur, Argon2id est en général en effet plus adapté qu'Argon2d, mais notre situation (appareil client) est différente, comme mentionné ci-dessus.

Le nombre d'itérations évolue linéairement avec le temps requis. En augmentant le paramètre de mémoire, les attaques GPU/ASIC deviennent plus difficiles (et le temps requis augmente). Le paramètre parallélisme spécifie le nombre de threads à utiliser.

Nous recommandons la procédure suivante pour déterminer les paramètres Argon2 :

1. Définissez le nombre d'itérations sur 2 :
2. Découvrez la taille de la mémoire vive de chacun de vos appareils sur lesquels vous souhaitez ouvrir votre fichier de base de données. Soit *M* le minimum de ces tailles. Réglez le paramètre de mémoire sur min(*M*/2, 1 Go) (c'est-à-dire utilisez la moitié de *M*, si elle est inférieure à 1 Go, sinon utilisez 1 Go).
   - Exemple 1 : si vous avez un PC avec 32 Go de RAM et un téléphone mobile avec 1 Go de RAM (sur lequel vous souhaitez ouvrir votre fichier de base de données), réglez le paramètre de mémoire sur 500 Mo.
   - Exemple 2 : si vous avez un PC avec 32 Go de RAM et un PC avec 8 Go de RAM, réglez le paramètre de mémoire sur 1 Go.

   Sur Windows 10 et versions ultérieures, la taille de la RAM peut être trouvée dans les paramètres système → 'Système' → 'À propos'.
3. Découvrez le nombre de processeurs logiques de chacun de vos appareils. Réglez le paramètre de parallélisme au minimum de ces nombres. Sur Windows 10 et versions ultérieures, le nombre de processeurs logiques peut être trouvé dans le Gestionnaire des tâches (clic droit sur la barre des tâches → 'Gestionnaire des tâches') sur la page de l'onglet 'Performances'.
4. Cliquez sur le bouton 'Test'.
   - Si la transformation de clé prend trop de temps (plus longtemps que vous n'êtes prêt

à attendre lors de l'ouverture/enregistrement du fichier de base de données, par exemple : plus d'une seconde), alors annulez-la, diminuez le paramètre de mémoire et cliquez à nouveau sur le bouton 'Test'. Répétez cette opération jusqu'à ce que le temps requis soit acceptable.

- Si la transformation de clé prend trop peu de temps (dans le cas d'une mémoire de 1 Go), alors augmentez le nombre d'itérations et cliquez à nouveau sur le bouton 'Test'. Répétez cette opération jusqu'à ce que vous aimiez le temps requis.

5. Enregistrez le fichier de base de données et essayez de l'ouvrir sur chacun de vos autres appareils. Si cela prend trop de temps sur l'un des appareils, alors diminuez le nombre d'itérations (recommandation : pas moins de 2) et/ou diminuez le paramètre de mémoire, et réessayez.

Lorsque vous cliquez sur le bouton 'Délai d'une seconde', KeePass utilise une stratégie différente pour déterminer les paramètres (des valeurs relativement faibles pour les paramètres de mémoire et de parallélisme, un nombre d'itérations relativement élevé), car KeePass ne connaît pas les détails de la RAM et du processeur de vos autres appareils (les valeurs par défaut doivent être compatibles avec la plupart des appareils). Si vous connaissez ces détails, alors il est recommandé de plutôt suivre la procédure ci-dessus.

Argon2 sur iOS : si vous utilisez une application compatible KeePass sur iOS, alors veuillez noter la limitation suivante d'iOS. Si l'application utilise beaucoup de RAM (par exemple, en raison de l'utilisation d'Argon2 avec un paramètre de mémoire important), alors le remplissage automatique peut ne pas fonctionner. Dans ce cas, nous recommandons d'utiliser une valeur relativement faible pour le paramètre de mémoire Argon2 (64 Mo ou moins, selon l'application et la taille de la base de données) et un nombre d'itérations relativement élevé.

KeePassX : contrairement à KeePass, le portage Linux KeePassX ne prend en charge que partiellement la protection contre les attaques par dictionnaires et devinette.

La génération de nombres aléatoires

KeePass commence par créer un pool d'entropie à l'aide de différentes sources d'entropie (y compris des nombres aléatoires générés par le fournisseur cryptographique du système, la date/heure courante et la disponibilité, la position du curseur, la version du système d'exploitation, le nombre de processeurs, les variables d'environnement, les statistiques de processus et de mémoire, la culture actuelle, un nouveau GUID aléatoire, etc.). Les informations de culture comportent par exemple le nom de la langue, le type de calendrier, le format des nombres et la disposition du clavier.

Les bits aléatoires pour les méthodes de génération de haut niveau sont générés à l'aide d'un générateur de nombres pseudo-aléatoires sécurisé de façon cryptographique (basé sur SHA-256/SHA-512 et ChaCha20) qui est initialisé à l'aide du pool d'entropie.

La protection de la mémoire du processus

Pendant l'exécution de KeePass, les données sensibles sont stockées de manières chiffrées dans la mémoire du processus. Cela signifie que même si vous vidiez la mémoire du processus KeePass sur le disque, vous ne pourriez trouver aucune donnée sensible. Pour des raisons de performance, la protection de la mémoire du processus s'applique uniquement aux données sensibles ; les données sensibles incluent ici, par exemple, la clé principale et les mots de passe des entrées, mais pas les noms d'utilisateur, les remarques et les pièces jointes. Remarquez que cela n'a rien à voir avec le chiffrement des fichiers de base de données ; dans les fichiers de base de données, toutes les données (y compris les noms d'utilisateur, etc.) sont chiffrées.

De plus, KeePass efface toute la mémoire critique pour la sécurité (si possible) quand elle n'est plus nécessaire, c'est-à-dire qu'il écrase ces zones de mémoire avant de les libérer.

KeePass utilise Windows DPAPI pour chiffrer des données sensibles en mémoire (via ProtectedMemory). Avec DPAPI, la clé pour le chiffrement de la mémoire est stockée dans une zone de mémoire sécurisée, non permutable gérée par Windows. DPAPI est disponible sur Windows 2000 et supérieur. KeePass 2.x utilise toujours DPAPI s'il est disponible ; dans KeePass 1.x, il peut être désactivé (dans les options avancées ; l'utilisation de DPAPI est activé par défaut). Si DAPI n'est pas disponible ou est désactivé, alors KeePass se contente de chiffrer le processus mémoire en utilisant ChaCha20 avec une clé aléatoire ; remarquez que c'est moins sécurisé que DPAPI, car la clé est également stockée dans la mémoire du processus échangeable. Sur les systèmes Unix-like, KeePass 2.x utilise ChaCha20, car Mono ne fournit aucune méthode efficace de protection de la mémoire.

Pour certaines opérations, KeePass doit mettre les données sensibles à disposition de manières déchiffrées dans la mémoire du processus. Par exemple, pour afficher un mot de passe dans le contrôle d'affichage de liste standard fourni par Windows, KeePass doit fournir le contenu de la cellule (le mot de passe) sous forme de chaîne non chiffrée (sauf si le masquage à l'aide d'astérisques est activé). Les opérations qui aboutissent à des données déchiffrées dans la mémoire de processus incluent, sans toutefois s'y limiter : l'affichage de données (pas d'astérisque) dans les contrôles standards, quand on transfert les données vers/depuis les autres applications (via le presse-papiers, glisser&déposer, StdIn/StdOut, etc.), quand on remplace les paramètres substituables (par exemple : durant la saisie automatique), quand on recherche les données (par exemple les commandes dans le menu 'Rechercher' qui implique des données sensibles), quand on importe/exporte des fichiers (excepté KDBX) et quand on charge/enregistre des fichiers déchiffrés. Windows et .NET peuvent créer des copies des données (dans la mémoire du processus) qui ne peuvent pas être effacées par KeePass.

La saisie de la clé principale sur un bureau sécurisé (protection contre les enregistreurs de frappe)

KeePass 2.x possède une option (dans 'Outils' → 'Options...' → onglet 'Sécurité') pour afficher des boîtes de dialogue de clé principale sur un bureau différent/sécurisé (pris en charge sous Windows 2000 et supérieur), similaire au contrôle de compte utilisateur de Windows (UAC). Presque aucun enregistreur de frappe ne fonctionne sur un bureau sécurisé.

L'option est désactivée par défaut pour des raisons de compatibilité.

Vous trouverez plus d'informations sur la page d'aide du bureau sécurisé.

Remarque : KeePass a été l'un des premiers gestionnaires de mots de passe permettant d'entrer la clé principale sur un bureau différent/sécurisé !

Le verrouillage de l'espace de travail

Lors du verrouillage de l'espace de travail, KeePass ferme le fichier de la base de données et ne mémorise que son chemin et certains paramètres d'affichage.

Cela offre une sécurité maximale : déverrouiller l'espace de travail est aussi difficile que l'ouverture normale du fichier de la base de données. En outre, cela évite la perte de données (l'ordinateur peut se bloquer lorsque KeePass est verrouillé, sans endommager la base de données).

Lorsqu'une sous-boîte de dialogue est ouverte, l'espace de travail peut ne pas être verrouillé ; pour plus de détails, cf. la FAQ.

Affichage/Édition de pièces jointes

KeePass 2.x possède un afficheur/éditeur interne pour les pièces jointes. Pour plus d'informations sur son utilisation pour travailler avec des textes, reportez-vous à la section 'Comment stocker et travailler avec de grandes quantités de texte (formaté) ? '.

L'afficheur/éditeur interne travaille avec les données dans la mémoire principale. Il n'extrait/ne stocke pas les données sur le disque.

Lorsque vous essayez d'ouvrir une pièce jointe que l'afficheur/éditeur interne ne peut pas manipuler (par exemple : un fichier PDF), KeePass extrait la pièce jointe dans un fichier temporaire (chiffré en EFS) et l'ouvre à l'aide de l'application par défaut associée à ce type de fichier. Une fois l'afficheur/édition terminé, l'utilisateur peut choisir d'importer ou annuler toute modification apportée au fichier temporaire. Dans tous les cas, KeePass efface ensuite en toute sécurité le fichier temporaire (y compris l'écrase).

Les greffons (plug-in)

Une page distincte existe sur : la sécurité des greffons.

Les autotests

À chaque fois que vous démarrez KeePass, le programme effectue un rapide autotest pour vérifier si les algorithmes de chiffrement et de hachage fonctionnent correctement et passent leurs vecteurs de test. Si l'un des algorithmes ne réussit pas ses vecteurs de test, alors KeePass affiche une boîte de dialogue d'exception de sécurité.

Les logiciels espions spécialisés

Cette section donne des réponses aux questions suivantes :

- Est-ce que le chiffrement du fichier de configuration renforcerait la sécurité en empêchant des modifications par un programme malveillant ?
- Est-ce que le chiffrement de l'application (fichier exécutable, éventuellement associé au fichier de configuration) renforcerait la sécurité en empêchant toute modification par un programme malveillant ?
- Est-ce qu'une option permettant d'empêcher le chargement de greffons renforcerait la sécurité ?
- Est-ce que l'enregistrement des options de sécurité dans la base de données (pour remplacer les paramètres de l'instance KeePass) renforcerait la sécurité ?
- Est-ce que verrouiller la fenêtre principale de sorte que seule la saisie automatique soit autorisée renforcerait la sécurité ?

La réponse à toutes ces questions est : non. L'ajout de l'une de ces fonctionnalités ne renforcerait pas la sécurité.

Toutes les fonctionnalités de sécurité de KeePass protègent contre les menaces *génériques* comme les enregistreurs de frappe, les moniteurs de presse-papiers, les moniteurs de contrôle de mot de passe, etc. (et contre les attaques hors exécution sur la base de données, analyseurs de dump mémoire, etc.). Cependant, dans toutes les questions ci-dessus, nous supposons qu'un programme espion malveillant est en cours d'exécution sur le système et qu'il est spécialisé dans l'attaque de KeePass.

Dans cette situation, les meilleures fonctionnalités de sécurité échoueront. Il s'agit de la loi n° 1 des dix lois immuables de la sécurité (article de Microsoft TechNet ; cf. l'article de Microsoft TechNet revoir les 10 lois immuables de la sécurité, première partie) :
"Si un méchant type peut vous persuader de lancer son programme sur votre ordinateur, ce n'est plus votre ordinateur".

Par exemple, considérons le logiciel espion très simple suivant, spécialisé pour KeePass : une application qui attend le démarrage de KeePass, puis masque l'application démarrée et imite KeePass lui-même. Toutes les interactions (telles que la saisie d'un mot de passe pour déchiffrer la configuration, etc.) peuvent être simulées. La seule façon de découvrir ce logiciel espion consiste à utiliser un programme qu'il ignore ou ne peut pas manipuler (bureau sécurisé) ; dans tous les cas, il ne peut s'agir de KeePass.

Pour protéger votre PC, nous vous recommandons d'utiliser un logiciel antivirus. D'utiliser un pare-feu approprié, exécutez le logiciel uniquement à partir de sources fiables, n'ouvrez pas les pièces jointes inconnues, etc.

Les données malveillantes

L'utilisateur devrait vérifier toutes les données qu'il saisit et/ou exécute.

Si vous saisissez/exécutez des données sans d'abord les vérifier, cela peut amener à de sérieux problèmes de sécurité (comme la divulgation de données sensibles ou une exécution de code malveillant). Il s'agit d'un principe général ; il s'applique à la plupart des applications, pas seulement à KeePass.

Exemples :

- Le champ Adresse (URL) d'une entrée prend en charge l'exécution d'une ligne de commande. Donc, si vous (saisissez et) exécutez une adresse (URL) sans d'abord la vérifier, alors vous pourriez exécuter un programme/code malveillant.
- En exécutant une adresse (URL), une malveillante adresse (URL) remplacée (globale ou spécifique à l'entrée) peut être exécutée à la place, si vous ne la vérifiez pas.
- KeePass prend en charge les paramètres substituables (placeholders). Tous les paramètres substituables réguliers sont sous la forme '`{...}`', et les variables d'environnement sont sous la forme '`%...%`'. Toutes les données devraient être vérifiées pour des paramètres substituables et des variables d'environnement malveillant.
  - Les références de champ peuvent insérer les données d'autres entrées dans la donnée courante. Par exemple : si vous avez un compte Facebook, saisir et exécuter l'adresse (URL) suivante, pourrait envoyer votre nom d'utilisateur et mot de passe Facebook au serveur 'exemple.com' :
    `https://exemple.com/?u={REF:U@T:Facebook}&p={REF:P@T:Facebook}`
  - Le paramètre substituable `{CMD:...}` exécute une ligne de commande. Par exemple,

l'adresse (URL) suivante, ouvre 'https://exemple.com/' et exécute 'Calc.exe' :
`https://exemple.com/{CMD:/Calc.exe/W=0/}`

Les paramètres substituables de transformation de texte peuvent être utilisés pour obfusquer des parties des données.

- La séquence de saisie automatique suivante accomplit une connexion à un login (ouverture de session) et exécute en outre 'Calc.exe' :
`{USERNAME}{TAB}{PASSWORD}{ENTER}{VKEY 91}{T-CONV:/%43%61%6C%63%2E%65%78%65/Uri-Dec/}{VKEY 13}`
Cette séquence ne fonctionne typiquement que sur un système Windows, mais des séquences similaires peuvent être construites pour d'autres systèmes d'exploitation (comme Linux et MacOS).
- Si vous spécifiez des paramètres de transformation de clé faibles suggérés par un attaquant, cela pourrait être plus facile pour l'attaquant de déchiffrer/ouvrir votre base de données.
- Si vous saisissez/utilisez un profil du générateur de mot de passe (suggéré par un attaquant) qui autorise seulement des mots de passe faibles, alors les comptes utilisant de tels mots de passe peuvent ne pas être bien protégés.
- En utilisant la fonctionnalité de remplacement XML avec des paramètres malveillants peut induire à une modification malveillante des données de votre base de données.
- Copier/saisir des déclencheurs malveillants dans la boîte de dialogue sans vérifier qu'ils peuvent induire des problèmes de sécurité.

Si l'utilisateur vérifie que les données qu'il entre/exécute, aucune des "attaques" ci-dessus ne fonctionne. Saisir des données est une opération manuelle (c'est-à-dire qu'un attaquant ne peut pas le faire lui-même), et seulement l'utilisateur peut décider si les effets produits sont prévus ou non. Afficher des boîtes de dialogue d'avertissement/confirmation tout le temps ne serait pas raisonnable.

Quand on ouvre une base de données qui a été créée/modifiée par quelqu'un d'autre, vous devriez vérifier avec attention toutes les données que vous souhaitez utiliser. Si vous ne faites pas entièrement confiance au créateur de la base de données, alors n'ouvrez pas une pièce jointe d'une entrée.

Les options pour les experts

La plupart des options de sécurité peuvent être configurées dans la boîte de dialogue des options de KeePass (menu 'Outils' → 'Options...') et dans la boîte de dialogue des paramètres de la base de données (menu 'Fichier' → 'Paramètres de la base de données...').

Cependant, dans KeePass 2.x, il existe en outre quelques options de sécurité pour les experts qui ne peuvent pas être configurées dans l'interface utilisateur. Par exemple, KeePass peut protéger son processus avec une liste de contrôle d'accès discrétionnaire (DACL).

⚠ L'activation de ces options pour les experts peut entraîner des problèmes de compatibilité et rendre KeePass inutilisable. Par conséquent, ces options ne peuvent être activées qu'en éditant le fichier de configuration manuellement (à l'aide d'un éditeur XML ou de texte). Cela garantit que les utilisateurs savent comment ils peuvent désactiver les options problématiques (en éditant à nouveau le fichier de configuration) afin de rendre KeePass utilisable à nouveau.

Si vous savez comment fonctionne le système de configuration de KeePass, alors consultez la page d'aide personnalisation, sur laquelle ces options sont documentées.

Les options pour les administrateurs

Les administrateurs peuvent imposer certains paramètres, interdire certaines fonctions, spécifier des exigences pour les mots de passe maîtres, et bien plus encore. Vous trouverez des détails sur les pages d'aide suivantes :

- Configuration.
- Configuration imposée.
- Personnalisation (KeePass 2.x), Personnalisation (KeePass 1.x).
- La stratégie de l'application (KeePass 2.x).

Les problèmes de sécurité

Pour obtenir une liste des problèmes de sécurité, leur statut et leurs clarifications, veuillez vous reporter à la page problèmes de sécurité.

La prise en charge des NAT

La prise en charge des NAT (TANs)
KeePass prend en charge les Numéros d'Autorisation de Transaction (NAT).

- Utilisation de *l'assistant de NAT* pour ajouter des NAT
- L'utilisation des NAT

KeePass supporte les NAT, c'est-à-dire des mots de passe qui peuvent être utilisés qu'une seule fois. Ces mots de passe spéciaux sont utilisés par certaines banques : vous devez confirmer les transactions à l'utilisation de ces TAN. Cela offre une sécurité supplémentaire, car un espion ne peut pas effectuer de transaction, même s'il connaît le mot de passe de votre compte bancaire.

Utilisation de l'assistant de NAT pour ajouter des NAT

Vous pouvez utiliser **l'assistant de NAT** de KeePass pour ajouter plusieurs NAT à la fois à votre base de données. Ouvrez simplement la boîte de dialogue de l'assistant NAT (menu *Outils - Assistant NAT (TAN)...*) et entrez tous vos NAT. Le formatage n'a pas vraiment d'importance, KeePass utilise simplement toutes les chaînes alphanumériques, c'est-à-dire que les caractères comme les sauts de ligne, les tabulations, les espaces, les points, etc. sont interprétés comme des séparateurs.

L'assistant générera ensuite plusieurs entrées de NAT à partir des données que vous avez saisies dans la boîte de dialogue. Chaque NAT est une entrée standard de KeePass. Le titre d'une entrée de NAT est toujours défini sur "<TAN>". Cela indique à KeePass que l'entrée est une entrée de NAT. Vous ne pouvez pas modifier le titre, le nom d'utilisateur et l'URL d'un NAT. Mais vous pouvez librement ajouter des remarques à une entrée de NAT, si vous le souhaitez.

L'utilisation des NAT

Lorsque vous utilisez le NAT (par exemple : exécutez la commande "Copier le mot de passe" dessus), sa date d'expiration sera définie sur l'heure actuelle, ce qui expire l'entrée. Il obtiendra un **X** rouge comme icône. Si vous voulez savoir plus tard quand vous avez utilisé un NAT spécifique, vous pouvez simplement jeter un œil à sa date d'expiration.

Lors de la copie d'un NAT dans le presse-papiers, la base de données est marquée comme modifiée. Vous devez enregistrer le fichier afin de vous souvenir de l'utilisation d'un NAT.

Si vous avez accidentellement utilisé un NAT sans en avoir besoin, vous pouvez le réinitialiser (c'est-à-dire supprimer le **X** rouge et l'afficher à nouveau comme un NAT valide). Pour ce faire, ouvrez l'entrée de NAT (cliquez dessus avec le bouton droit et choisissez *'Modifier l'entrée...'*). Ici, décochez la case *'Expire le :'*. Cliquez sur [OK] pour fermer la boîte de dialogue.

Le champ d'adresse (URL)

Le champ d'adresse (URL)
Le champ d'adresse prend en charge divers protocoles spéciaux et paramètres substituables.

- Les capacités standardes
- L'exécution de lignes de commande
- Les paramètres substituables
- La modification du gestionnaire d'adresse (les remplacements d'adresse)

Conseils et astuces d'utilisation :

- Démarrage de sessions RDP/TS (Remote Desktop/Terminal Server Connection - Connexion de bureau à distance/Connexion serveur de terminal)
- L'exécution de commandes Shell intégrées

Les capacités standardes

Le champ d'adresse peut exécuter n'importe quelle URL valide pour laquelle un gestionnaire de protocole est défini. Sur la plupart des systèmes, au moins les protocoles `http://`, `https://`, `ftp://` et `mailto:` sont définis. KeePass prend en charge tous les protocoles pris en charge par Windows.

Par exemple, si vous enregistrez globalement (c'est-à-dire en utilisant l'explorateur Windows) PuTTY pour les URL `ssh://`, alors KeePass utilisera également automatiquement PuTTY pour les URL `ssh://`.

L'exécution de lignes de commande

Au lieu d'une URL, vous pouvez également exécuter des lignes de commande en utilisant le champ d'adresse. Pour indiquer à KeePass que la ligne que vous avez saisie est une ligne de commande, préfixez-la en utilisant `cmd://`. Par exemple : si vous souhaitez exécuter le Bloc-notes, votre URL pourrait ressembler à ceci :

```
cmd://C:\Windows\Notepad.exe C:\Test\MonFichierDeTest.txt
```

Le protocole `cmd://` virtuel prend également en charge les paramètres des fichiers exécutables, contrairement au protocole `file://`. C'est la principale raison pour laquelle `cmd://` a été introduit ; avec `file://` vous ne pouvez pas passer de paramètres aux applications démarrées. Utilisez plutôt le protocole `cmd://`.

Les chemins du protocole `cmd://` n'ont pas besoin d'être codés. Par exemple : vous n'avez pas besoin de remplacer les espaces par `%20`, comme il est normalement requis pour les autres URL. KeePass élimine simplement le préfixe de protocole virtuel `cmd://` et transmet la ligne de commande restante au système.

Si le chemin du fichier contient des espaces, alors vous devez le mettre entre doubles quotes (").

Les variables d'environnement :
Les variables d'environnement système sont prises en charge. Le nom de la variable doit être entouré de caractères '%'. Par exemple : `%TEMP%` est remplacé par le chemin temporaire de l'utilisateur.

Les chemins UNC :
Les chemins UNC de style Windows (commençant par `\\`) sont directement pris en charge, c'est-à-dire qu'ils n'ont pas besoin d'être préfixés par `cmd://`.

Les doubles quotes (") et les barres obliques inverses (\) :
il existe plusieurs ensembles de règles pour l'analyse des lignes de commande (structure `SHELLEXECUTEINFOW`, fonction `CommandLineToArgvW`, fonction `main` et arguments de ligne de commande, etc.). Ces ensembles de règles sont contradictoires ; les lignes de commande sont interprétées différemment. Par exemple : dans la documentation de la structure`SHELLEXECUTEINFOW`, les barres obliques inverses n'ont pas de signification particulière, tandis que la fonction `CommandLineToArgvW` interprète parfois une barre oblique inverse comme un caractère d'échappement. Autre exemple : `A"""B C"""D` est interprété comme *un* argument (à savoir `A"B C"D`) par le code de démarrage Microsoft C/C++ (fonction `main`), alors que la fonction `CommandLineVersArgvW` renvoie *deux* arguments (à savoir `A"B` et `C"D`). KeePass ne peut pas savoir comment l'application exécutée interprétera sa ligne de commande, et il n'y a pas d'encodage de ligne de commande qui soit interprété comme prévu par toutes les applications. Par conséquent, nous recommandons :

- d'utiliser des doubles quotes(") uniquement pour indiquer le début et la fin du chemin du fichier ou d'un argument. N'utilisez pas de double quote dans les données qui nécessitent un codage. Par exemple : si votre ligne de commande contient un paramètre substituable `{PASSWORD}`, alors le mot de passe ne doit pas contenir de double quote.
- d'utiliser une barre oblique inverse uniquement lorsque le caractère suivant n'est pas une double quote, c'est-à-dire évitez `\"`. En particulier, évitez les données se terminant par une barre oblique inverse si une double quote suit sur la ligne de commande. Par exemple, si la ligne de commande contient un argument comme `-pw"{PASSWORD}"`, le mot de passe ne doit pas se terminer par une barre oblique inverse, car sinon le remplacement du paramètre substituable entraîne la séquence `\"` problématique.

Systèmes de type Unix :
sur les systèmes de type Unix, KeePass suppose que les doubles quotes (") et les barres obliques inverses (\) doivent être encodées. De plus, KeePass suppose que les simples quotes (') n'apparaissent que dans des contextes où elles ne doivent pas être encodées (par exemple : à l'intérieur de doubles quotes). Ainsi, si l'un de vos arguments peut contenir une simple quote, alors vous devez vous assurer qu'elle se trouve dans un tel contexte. Sous Windows, cela n'a pas d'importance, car les simples quotes

n'ont pas de signification particulière ici.

Les paramètres substituables

Dans le champ adresse (URL), vous pouvez utiliser plusieurs paramètres substituables qui seront automatiquement remplacés lors de l'exécution de l'URL. Par exemple :

```
https://www.exemple.com/par_defaut.php?user={USERNAME}&pass={PASSWORD}
```

Pour cette entrée, KeePass remplacera {USERNAME} par les données du champ de Nom d'utilisateur et {PASSWORD} par les données du champ de Mot de passe lorsque vous exécutez le lien.

Pour une liste complète des paramètres substituables réservés pris en charge, alors consulter la page Les paramètres substituables.

Notez également que les paramètres substituables spéciaux sont également pris en charge. Par exemple : le paramètre substituable `{APPDIR}` est remplacé par le chemin du répertoire de l'application de l'instance KeePass en cours d'exécution. C'est le chemin absolu du répertoire contenant l'exécutable KeePass, sans barre oblique inverse à la fin. Si vous souhaitez démarrer une nouvelle instance de KeePass, alors vous pouvez définir l'URL sur :

```
cmd://"{APPDIR}\KeePass.exe"
```

Pour utiliser différents navigateurs pour les entrées, vous pouvez utiliser des URL telles que les suivantes :

```
cmd://{EDGE} "https://www.exemple.com/"
cmd://{FIREFOX} "https://www.exemple.com/"
cmd://{GOOGLECHROME} "https://www.exemple.com/"
cmd://{INTERNETEXPLORER} "https://www.exemple.com/"
cmd://{OPERA} "https://www.exemple.com/"
cmd://{SAFARI} "https://www.exemple.com/"
```

Le paramètre substituable du navigateur sera remplacé par le chemin de l'exécutable du navigateur (si le navigateur est installé).

La modification du gestionnaire d'adresse (les remplacements d'adresse [URL])

Le comportement du champ d'adresse peut être remplacé individuellement pour chaque entrée à l'aide du champ *Remarques*. Cela vous permet d'exécuter une URL spécifique, tout en utilisant le champ d'adresse pour (uniquement) stocker des données.
Saisissez simplement `Url-Override:` suivi par la ligne de commande que vous souhaitez dans le champ des remarques. Lorsque vous double-cliquez sur le champ d'adresse (URL) de l'entrée dans la fenêtre principale, la ligne de commande spécifiée (dans le champ 'Remarques') sera exécutée.

En utilisant un navigateur différent :
Si votre navigateur par défaut est Firefox et que vous souhaitiez ouvrir un site spécifique avec Internet Explorer, alors ajouter les éléments suivants au champ Remarques :

```
Url-Override: cmd://{INTERNETEXPLORER} "{URL}"
```

KeePass ouvrira Internet Explorer et transmettra les données du champ d'adresse (URL) en tant que paramètre. Cela utilise un paramètre substituable pour trouver Internet Explorer.

La modification globale du comportement de l'URL :
Si vous souhaitez modifier l'action d'URL *par défaut* (c'est-à-dire pour *toutes* les URL), alors vous pouvez ajouter une ligne `KeeUrlOverride` dans le fichier `KeePass.ini`.

Le démarrage de sessions RDP/TS

Vous pouvez utiliser le champ d'adresse (URL) des entrées et le protocole virtuel `cmd://` pour démarrer des connexions de bureau à distance.

Pour cela, saisissez ce qui suit dans le champ d'adresse (URL) d'une entrée :

```
cmd://mstsc.exe
```

Maintenant, lorsque vous double-cliquez sur le champ d'adresse (URL) de l'entrée dans la fenêtre principale, une connexion de bureau à distance Windows est initiée.

MSTSC est le programme de connexion au serveur de terminaux Windows (connexion au bureau à distance). Vous pouvez transmettre un chemin d'accès à un fichier RDP existant au programme pour l'ouvrir. Par exemple : l'URL suivante ouvre le fichier RDP spécifié :

`cmd://mstsc.exe "C:\Mes fichiers\Connexion.rdp"`
MSTSC prend également en charge plusieurs options de ligne de commande :

- **/v:<Server[:Port]>**
  Définit le serveur de terminaux auquel se connecter.
- **/console**
  Se connecte à la session de terminal du serveur.
- **/f**
  Démarre le client en mode plein écran.
- **/w:<Width>**
  Définit la largeur de l'écran du bureau à distance.
- **/h:<Height>**
  Définit la hauteur de l'écran du bureau à distance.
- **/edit**
  Ouvre le fichier RDP spécifié pour édition.
- **/migrate**
  Migre les anciens fichiers de connexion vers les nouveaux fichiers RDP.

L'exécution de commandes Shell intégrées

Le champ d'adresse (URL) peut être utilisé pour démarrer des applications/documents et URL. Si vous souhaitez exécuter une commande Shell intégrée, telle que par exemple `COPY`, alors cela ne fonctionne cependant pas directement, car il n'y a pas de `COPY.EXE` (en fait dans Windows 9x il y en avait une, mais sur tous les systèmes d'exploitation Windows modernes, ces commandes sont intégrées à la fenêtre de ligne de commande).

Afin d'exécuter des commandes Shell intégrées, vous devez les transmettre à l'interpréteur de ligne de commande `cmd.exe`.

Pour la commande `COPY`, vous devez spécifier `cmd.exe` en tant que fichier exécutable et `/C COPY depuis vers` comme arguments (où 'depuis' et 'vers' sont des chemins). Le paramètre `/C` indique à `cmd.exe` d'exécuter la ligne de commande qui suit.

Dans le champ d'adresse (URL), votre URL ressemblerait à ce qui suit :
`cmd://cmd.exe /C COPY depuis vers`
Dans d'autres emplacements, comme les lignes de commande dans le système de déclencheur, vous pouvez omettre le préfixe d'URL `cmd://`.

L'utilisation des mots de passe stockés

L'utilisation des mots de passe stockés

Comment transférer des mots de passe stockés dans KeePass vers d'autres applications.

Il existe de nombreuses méthodes différentes pour transférer les mots de passe stockés dans KeePass vers d'autres applications :

- La liste d'entrée principale
- Glisser&Déposer
- La saisie automatique
- Les greffons

La liste d'entrée principale

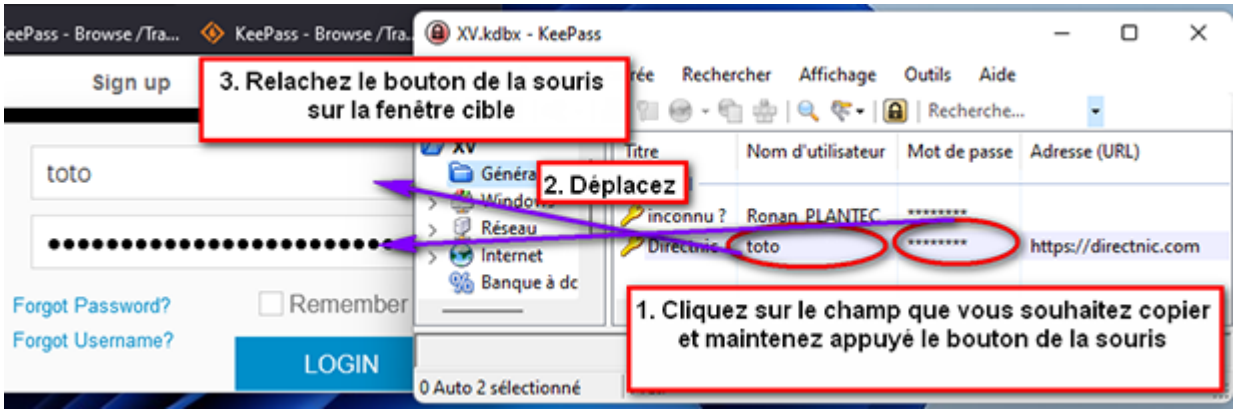
Selon le champ sur lequel vous double-cliquez dans la liste de l'entrée de la fenêtre principale, différentes actions sont effectuées :

- **Le champ Titre :** ouvre la boîte de dialogue d'édition d'entrée pour cette entrée.
  Si vous maintenez la touche `Maj` enfoncée tout en double-cliquant, alors le titre est copié dans le presse-papiers à la place.
- **Le champ Nom d'utilisateur :** copie le nom d'utilisateur dans le presse-papiers.

- **Le champ Mot de passe :** copie le mot de passe dans le presse-papiers.
- **Le champ Adresse (URL) :** ouvre une URL.
  Si vous maintenez la touche `Maj` enfoncée tout en double-cliquant, alors l'URL est copiée dans le presse-papiers à la place. Ce comportement peut être inversé en activant l'option 'Copier les adresses (URLs) dans le presse-papiers au lieu de les ouvrir'.
- **Le champ remarques :** copie les remarques dans le presse-papiers.
- **Le champ Pièces jointes :** [1.x] copie dans le presse-papiers, [2.x] s'ouvre dans l'éditeur/la visionneuse interne.
- **Les autres champs** (comme les champs du temps et l'UUID): copie les contenus de ces champs dans le presse-papiers.

Glisser&Déposer

Vous pouvez glisser&déposer tous les champs des entrées de KeePass dans d'autres fenêtres :



La saisie automatique

La saisie automatique est une fonctionnalité puissante qui envoie des pressions de touches simulées vers d'autres applications.

Vous pouvez trouver plus de détails à ce sujet ici : page de documentation de la saisie automatique.

Les greffons

Il existe de nombreux plugins disponibles qui intègrent KeePass avec d'autres applications.

Vous pouvez trouver ces greffons d'intégration sur la page des greffons.

Les FAQ

La FAQ administrative

La FAQ administrative
La Foire Aux Questions à propos du projet, la licence, etc.

- Comment puis-je vous aider ? (Soutenir le projet Keepass)
- KeePass peut-il être utilisé en entreprise ?
- Qu'en est-il d'un serveur Internet KeePass centralisé ?

Comment puis-je vous aider ?

Si vous aimez Keepass et souhaitez aider les développeurs d'une manière ou d'une autre :

- **Faire un don**
  C'est la meilleure façon d'aider, si vous n'avez pas beaucoup de temps ou d'expérience dans le

développement d'applications.

- **Faire une traduction**
  Si vous avez du temps libre, alors vous pouvez faire une traduction de KeePass (bien sûr seulement si votre langue n'est pas déjà proposée).
- **Tester les nouvelles versions et signaler des bogues**
  Keepass est constamment en développement, de nouvelles fonctionnalités sont implémentées, les bogues sont corrigés. Si vous avez du temps libre, alors vous pouvez tester scrupuleusement de nouvelles versions et signaler des bugs. Si vous êtes programmeur, alors regardez les sources pour trouver des bogues et peut-être même soumettre des correctifs.
- **Passer le mot**
  Si vous aimez Keepass, alors racontez-vous à tous vos amis à quel point Keepass est bien, publiez des articles à ce sujet, graver le sur CD/DVD, expédiez des clés USB préinstallées avec, soumettez-le aux archives de logiciels, parlez de ce sujet dans les forums, etc. !

KeePass peut-il être utilisé en entreprise ?

Oui. Keepass est un logiciel libre et vous n'avez pas à payer de frais. Vous pouvez librement utiliser KeePass selon les termes de sa licence.

Mais bien sûr, si vous aimez KeePass, alors les dons sont toujours très appréciés.

Vous pourriez être intéressé par cette page : Personnalisation (1.x).

Qu'en est-il d'un serveur Internet Keepass centralisé ?

L'idée à première vue semble simple et utile : il devrait y avoir un serveur Internet de KeePass centralisé, sur lequel tous les utilisateurs pourraient stocker leurs mots de passe. En ayant une connexion Internet, vous auriez accès à tous vos mots de passe.

Remarquez que cette idée est différente que de simplement fournir un espace Web. Keepass 2.x prend déjà en charge le stockage des bases de données sur des serveurs à l'aide de HTTP/FTP. Le point est d'avoir un serveur pour tous les utilisateurs.

Lors de la création d'un tel serveur, plusieurs difficultés se présentent :

- Un mécanisme de synchronisation et de mise en cache assez complexe sera nécessaire. Vous ne voudrez pas transférer la base de données complète, sinon le service sera inutilisable pour tous ceux qui stockent des pièces jointes, etc.

- Directement lié au point précédent : pour effectuer la synchronisation, le serveur doit être capable de lire et de comprendre les bases de données, c'est-à-dire qu'un serveur KeePass dédié devrait être écrit. Bien que la voie de transport puisse être sécurisée par HTTPS, le serveur dispose certainement des données de l'utilisateur en tant que texte brut en mémoire pendant un certain temps. Il faut être très prudent ici. Que faire si le serveur est compromis ? Les implications de sécurité seraient horribles, si un attaquant pouvait lire des données utilisateur.

- Comment éviter les compromissions de serveur ? Si un serveur Internet normal est compromis, alors les implications de sécurité sont minimes : dans le pire des cas, tous les comptes utilisateur et les données de ce site Web sont perdus. Mais avec un serveur de KeePass, des identités entières seraient perdues. Un attaquant pourrait seulement imiter quelqu'un d'impersonnel sur ce serveur particulier, mais sur l'Internet complet et le monde réel, cela dépend de ce qui est stocké dans les bases de données.

  Par conséquent, les systèmes de sécurité au niveau des banques pourraient requérir un serveur Keepass. Garder PHP/ASP/Linux/Windows (ou tout ce qui sera utilisé) à jour n'est définitivement pas assez suffisant ici.

- Fondamentalement, vous offrez à des personnes un espace Web pour leurs bases de données, le service coûtera donc évidemment quelque chose. En facturant des personnes, ils attendent une fiabilité et vous devez prendre des garanties de durée de fonctionnement. Par conséquent, au moins 2 serveurs sont requis (par des hébergeurs différents), qui doivent être synchronisés.

En résumé : un serveur Internet centralisé est actuellement hors de portée. Si quelqu'un veut créer une entreprise fournissant un tel service, n'hésitez pas à utiliser Keepass comme application de base (bien sûr,

respecter les termes de l'open source).

Mais ce qui peut et sera probablement fait plus tard, c'est un serveur de KeePass intranet local (pour les entreprises par exemple). Les employés pourraient se connecter au serveur de mots de passe de l'entreprise et l'utiliser. Mais un serveur Internet centralisé – aucune chance.

La FAQ technique

La FAQ technique
La Foire Aux Questions sur l'utilisation de KeePass.

Configuration :

- J'ai enregistré mes options, mais lorsque je rouvre KeePass, j'obtiens les anciennes options. Qu'est-ce qui ne va pas ?

Installation/Intégration :

- Pourquoi le fichier d'aide CHM ne fonctionne-t-il pas ?
- Où puis-je trouver plus d'*icônes de l'application* pour les raccourcis Windows ?
- Comment puis-je ajouter plus d'*icônes clientes* pour les entrées de mot de passe ?
- Est-ce que KeePass prend en charge un mode mini ?
- Pourquoi KeePass ne se verrouille-t-il pas après la saisie automatique ?
- Pourquoi la saisie automatique ne fonctionne-t-elle pas correctement sur les systèmes polonais ?
- Pourquoi l'impression ne fonctionne pas dans Keepass 1.x? < LI>
- Pourquoi KeePass essaie-t-il de se connecter à l'Internet ?
- Est-ce que l'interface graphique de l'utilisateur prend en charge les thèmes sombres ?
- Comment modifier (la taille de) la police de l'interface graphique de l'utilisateur ?

Sécurité :

- Est-ce que la saisie automatique est protégée contre les renifleurs de clavier ?
- Est-ce la saisie automatique peut localiser les commandes de l'enfant ?
- Pourriez-vous ajouter l'algorithme de chiffrement ... à KeePass ?
- Pourquoi KeePass ne se verrouille-t-il pas lorsqu'une sous-boîte de dialogue est ouverte ?
- L'impression crée un fichier temporaire. Sera-t-il effacé en toute sécurité ?
- Pourquoi la qualité estimée d'un mot de passe chute soudainement ?

Utilisation :

- Comment stocker et travailler avec de grandes quantités de texte (formaté) ?
- Un champ d'adresse de courriel peut-il être ajouté ?

J'ai enregistré mes options, mais lorsque je rouvre KeePass, j'obtiens les anciennes options. Qu'est-ce qui ne va pas ?

KeePass prend en charge deux emplacements différents pour stocker les informations de configuration : le fichier de configuration global dans le répertoire de KeePass et un fichier local, dépendant de l'utilisateur, dans le dossier de configuration privé de l'utilisateur. Vous n'avez probablement pas l'accès en écriture à votre fichier de configuration global.

Pour plus de détails, alors voir La configuration.

Pourquoi le fichier d'aide CHM ne fonctionne-t-il pas ?

Les symptômes : lorsque vous essayez d'ouvrir le fichier d'aide de KeePass CHM à partir d'un ordinateur distant ou d'un lecteur réseau partagé, il ne s'affiche pas correctement (navigation interrompue, etc.).

La solution : Consulter le bulletin de sécurité Microsoft MS05-026.

Où puis-je trouver plus d'icônes de l'application pour les raccourcis Windows ?

Les icônes d'application sont des icônes au format Windows ICO. Ils peuvent être utilisés dans les raccourcis Windows et/ou comme icônes d'association de fichiers. L'exécutable KeePass contient diverses icônes d'application qui peuvent être utilisées à ces fins.

Des icônes d'application supplémentaires sont disponibles dans les répertoires ""`Ext/Icons_*`"" du package de code source KeePass. La plupart d'entre eux, illustrés à droite, sont de légères variations de l'icône principale de KeePass.

De plus, les icônes contribuées (par les utilisateurs) peuvent être trouvées sur la page des greffons.

Si vous avez plusieurs bases de données KeePass, alors vous pouvez utiliser des icônes d'application KeePass de couleurs différentes afin de les distinguer.

Ces icônes ne sont pas incluses dans la distribution binaire car cela rendrait le fichier d'application trop volumineux.

Comment puis-je ajouter plus d'icônes clientes pour les entrées de mot de passe ?

Les icônes client sont les icônes utilisées pour les entrées de mot de passe et les groupes dans KeePass. Chaque entrée peut se voir attribuer sa propre icône.

Ces icônes sont intégrées (built-in). Vous ne pouvez pas ajouter/importer vos propres icônes.

Est-ce que KeePass prend en charge un mode mini ?

Oui, voir KeePass 1.x Mini Mode.

Pourquoi KeePass ne se verrouille-t-il pas après la saisie automatique ?

J'ai activé les options "Utiliser la méthode alternative de saisie automatique (fenêtre minimisée)" " et "Verrouiller l'espace de travail lors de la réduction de la fenêtre principale". Pourquoi KeePass ne verrouille pas après une saisie automatique?

Dans ce cas très spécial, seulement la minimisation de la fenêtre est un moyen de perdre le focus, c'est-à-dire que la fenêtre en-dessous arrive au premier plan. La minimisation n'est pas initiée par l'utilisateur (ce n'est qu'un effet secondaire de saisie automatique), ni une conséquence d'une commande de minimisation externe, donc Ce n'est pas (et ne devrait pas être) affecté par le gestionnaire de verrouillage automatique de l'espace de travail.

Si vous vous inquiétez d'avoir KeePass minimisé et déverrouillé, alors activez l'option *"Verrouiller l'espace de travail après un délai d'inactivité (en secondes)"* et spécifiez un nombre raisonnable.

Pourquoi la saisie automatique ne fonctionne-t-elle pas correctement sur les systèmes polonais ?

Sur les systèmes polonais, la touche de raccourci de saisie automatique globale par défaut Ctrl+Alt+A entre en conflit avec une commande système et est fréquemment utilisée lors de la saisie. Par conséquent, la saisie automatique est souvent exécutée accidentellement.

La touche de raccourci globale de saisie automatique peut être remplacée par une combinaison de touches différente dans les options KeePass (voir la saisie automatique pour plus de détails).

Pourquoi KeePass essaie-t-il de se connecter à l'Internet ?

KeePass a une option pour vérifier automatiquement les mises à jour à chaque démarrage du programme. Afin de vérifier les mises à jour, KeePass télécharge un petit fichier d'informations sur la version et compare la version disponible avec la version installée. Aucune information personnelle n'est envoyée au serveur Web de KeePass.

Les vérifications automatiques des mises à jour sont effectuées de manière non intrusive en arrière-plan. Une notification s'affiche uniquement lorsqu'une mise à jour est disponible. Les mises à jour ne sont pas téléchargées ou installées automatiquement.

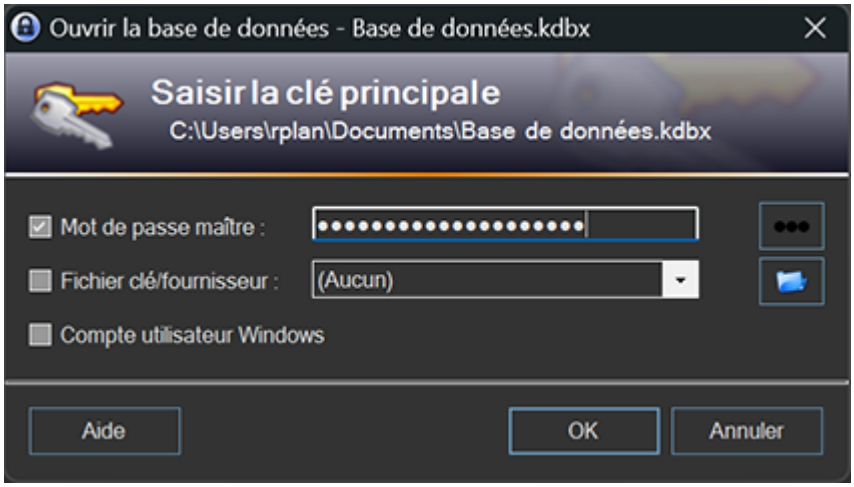
Quand on démarre KeePass pour la première fois, il demande si les vérifications de mise à jour automatique doivent être activées (recommandé). Elle peuvent être activées/désactivées à tout moment en utilisant l'option dans 'Outils' → 'Options...' → onglet 'Avancé'.

Est-ce que l'interface graphique de l'utilisateur prend en charge les thèmes sombres ?

Oui. KeePass prend en charge tous les thèmes systèmes, incluant ceux qui sont sombres.

- Sur Windows 11, un thème (sombre) peut être sélectionné dans les paramètres Windows→ 'Accessibilité' → 'Thèmes contrastés'.
- Sur Windows 10, un thème (sombre) peut être sélectionné dans les paramètres Windows → 'Options d'ergonomie' → 'Contraste élevé'.
- Sur Windows 7, 8 et 8.1, un thème (sombre) peut être sélectionne dans le panneau de configuration Windows → 'Apparance et personnalisation' → 'Personalisation'.

Exemple (Windows 11, thème 'Crépuscule') :



Option 'Choisissez votre mode (application par défaut) ' → 'Sombre'.
Windows 11 possède une option 'Choisissez votre mode' (sur Windows 10, c'est nommé 'Choisissez votre mode application par défault'), qui peut être positionné à 'Sombre'. Remarquez que cela ne s'applique que seulement aux applications UWP, et pas aux application Windows régulières. Windows permet l'option UWP pour contredire le thème système (par exemple : un thème système clair peut être activé même quand l'option UWP est positionnée à 'Sombre'). KeePass est une application Windows régulière, et non pas une application UWP, donc il suis le thème du système, et non l'option UWP. C'est le comportement attendu ; KeePass n'a rien à voir avec les options UWP.

Apparance personnalisée.
Si vous souhaitez modifier l'apparence de KeePass indépendamment du thème système actif, alors vous pourriez être intéressé par le greffon KeeTheme.

Comment changer (la taille de) la police de l'interface graphique de l'utilisateur ?

KeePass utilise la police de l'interface graphique de l'utilisateur par défaut qui a été spécifiée dans les paramètres du système d'exploitation. Par conséquent, si vous changez la police (notamment la taille de la police) que KeePass utilise, alors changez-là globalement.

- Sur Windows 11, la taille de la police peut être changée dans les paramètres Windows → 'Système' → 'Écran' → 'Mise à l'échelle' → option 'Taille du texte'. Redémarrer Windows après la modification de cette option.
  ⚠ *Ne pas* utiliser l'option 'Taille du texte' (dans les paramètres Windows → 'Accessibilité' →

'Vision'), parce que cette option ne met pas correctement à l'échelle tous les textes.

- Sur Windows 10, la taille de la police peut être modifiée dans les paramètres Windows → 'Système' → 'Écran' → 'Mise à l'échelle' → option 'Changer la taille du texte, apps, et autres éléments'. Redémarrer Windows après avoir changé cette option.
  ⚠ *N*'utilisez *pas* l'option 'Agrandir le texte' (dans les paramètres Windows → 'Option d'ergonomie' → 'Écran'), parce que cette option ne mets pas tous les textes à la bonne échelle.
- Sur Windows 7, 8 et 8.1, la taille de la police peut être changée dans le panneau de configuration Windows ; 'Apparance et Personalisation' → 'Écran'.
- Sur les systèmes Linux systems avec KDE 5 ou ultérieur, la police peut être changée dans les paramètres système → 'Fonts'.
- Sur les systèmes Linux avec GNOME 3 ou ultérieur, la police peut être changée en utilisant les ajustements (Tweaks) GNOME → 'Fonts'.

De plus pour supporter ces paramètres systèmes, KeePass permet de personnaliser la police qui est utilisée dans les listes et pour les mots de passe (dans les options de la boîte de dialogue ; ces options n'affectent que seulement KeePass, aucune autre applicatiopn).

Si vous voulez modifier la police de l'interface graphique de KeePass (ce qui n'est typiquement pas une bonne idée : le greffon KeeUIExt fourni une option pour ça. Cependant, il est recommandé d'utiliser plutôt les paramètres ci-dessus.

Est-ce que la saisie automatique est protégée contre les renifleurs de clavier ?

Non. La fonction de saisie automatique a été conçue de manière à ce qu'il soit impossible pour des applications cibles de distinguer les clés réelles des touches saisies automatiquement. D'une part, ceci a l'avantage que la fonctionnalité est vraiment compatible avec *toutes* les applications en dehors. D'autre part, les touches saisies automatiquement peuvent bien sûr être enregistrées par les enregistreurs de frappe. Si vous vous inquiétez des enregistreurs de frappe, alors vous devez utiliser l'une des autres méthodes (glisser&déposer, copie dans le presse-papiers, keeform, etc.).

Est-ce la saisie automatique peut localiser les commandes de l'enfant ?

Non. La saisie automatique vérifie uniquement si le titre de la fenêtre de niveau supérieur actuellement active correspond.

Les navigateurs comme Mozilla Firefox dessinent complètement la fenêtre (tous les contrôles) eux-mêmes, sans utiliser les contrôles Windows standard. Par conséquent, il est techniquement impossible pour KeePass de vérifier si une URL correspond (des méthodes telles que la création d'une capture d'écran et l'utilisation de la reconnaissance optique des caractères ne sont pas fiables et sécurisées). De plus, il est impossible de vérifier quel contrôle enfant a actuellement le focus. Ces problèmes ne peuvent être évités qu'en utilisant des greffons d'intégration de navigateur, c'est-à-dire en n'utilisant pas du tout la saisie automatique.

L'utilisateur doit s'assurer que le focus est placé dans le bon contrôle avant de commencer la saisie automatique.

Pourriez-vous ajouter l'algorithme de cryptage ... à KeePass ?

AES (Rijndael) et Twofish sont pris en charge. Il n'est pas prévu d'ajouter plus d'algorithmes pour les raisons suivantes:

- **La compatibilité :** si de nouveaux algorithmes sont mis en œuvre et utilisés, alors les plus anciennes versions et portages ne seront pas en mesure de lire des fichiers chiffrés avec les nouveaux algorithmes.
- **La sécurité:** certaines personnes ne sont pas bien informées sur les algorithmes de cryptage et pourraient choisir un algorithme faible tel que TEA, s'il était mis en œuvre, alors cela compromettrait la sécurité des mots de passe gérés par KeePass.
- **La taille & et la fonctionnalité :** Keepass est un gestionnaire de mots de passe sécurisé, pas un couteau suisse d'algorithmes de l'armée.

Pourquoi KeePass ne se verrouille-t-il pas lorsqu'une sous-boîte de dialogue est ouverte ?

KeePass dispose de diverses options pour verrouiller automatiquement son espace de travail (après un

certain temps d'inactivité, lorsque l'ordinateur se verrouille ou que l'utilisateur change d'utilisateur, lorsque l'ordinateur est suspendu, etc.). Cependant, l'espace de travail n'est pas automatiquement verrouillé lorsqu'une sous-boîte de dialogue (telle que la boîte de dialogue "Modifier l'entrée...") est ouverte.

Pour comprendre pourquoi ce comportement est logique, il est d'abord important de savoir ce qui se passe lorsque l'espace de travail est verrouillé. Lors du verrouillage, KeePass ferme complètement la base de données et ne mémorise que quelques paramètres d'affichage, comme le dernier groupe sélectionné, la première entrée visible, les entrées sélectionnées, etc. Du point de vue de la sécurité, cela permet d'obtenir la meilleure sécurité possible : briser un espace de travail verrouillé est équivalent à casser la base de données elle-même.

Revenons maintenant à la question initiale. Supposons qu'une sous-boîte de dialogue soit ouverte et que l'un des événements se produise et qui devrait verrouiller automatiquement l'espace de travail. Alors que doit faire KeePass maintenant ? Dans cette situation, KeePass ne peut pas demander à l'utilisateur quoi faire et doit prendre une décision automatique. Il existe plusieurs possibilités :

- *Ne pas enregistrer la base de données et verrouiller.*
  Dans ce cas, toutes les données non enregistrées de la base de données seraient perdues. Cela s'applique non seulement aux données saisies dans la boîte de dialogue actuelle, mais à toutes les autres entrées et groupes qui ont été modifiés précédemment.
- *Enregistrer la base de données et verrouiller.*
  Dans ce cas, les modifications éventuellement indésirables sont enregistrées. Souvent, vous ouvrez des fichiers, essayez quelque chose, en gardant à l'esprit que vous pouvez simplement fermer le fichier sans enregistrer les modifications. KeePass a une option 'Enregistrer automatiquement quand on ferme/verrouille la base de données'. Si cette option est activée et qu'aucune sous-boîte de dialogue n'est ouverte, alors la marche à suivre est claire : essayez d'enregistrer la base de données et en cas de succès : verrouillez l'espace de travail. Mais que faire des modifications non enregistrées dans la sous-boîte de dialogue ? Doivent-elles être enregistrées automatiquement, supprimant la possibilité d'appuyer sur le bouton 'Annuler' ?
- *Enregistrer dans un fichier temporaire et verrouiller.*
  Cela semble être la meilleure alternative à première vue, mais cela pose également plusieurs problèmes. Tout d'abord, l'enregistrement dans un fichier temporaire peut échouer (par exemple : il peut y avoir trop peu d'espace disque libre ou un autre programme comme un antivirus peut le bloquer). Secundo, l'enregistrement dans un fichier temporaire n'est pas sans importance du point de vue de la sécurité. Lorsque vous devez choisir un emplacement, le répertoire temporaire de l'utilisateur sur le disque dur est généralement choisi (car il dispose probablement de suffisamment d'espace libre, des droits d'accès requis, etc.). Les bases de données KeePass pourraient y être divulguées et accumulées. Il n'est pas clair ce qui devrait se passer lorsque l'ordinateur est éteint ou tombe en panne alors qu'il est verrouillé. Lors de la prochaine ouverture de la base de données, doit-elle plutôt utiliser la base de données stockée dans le répertoire temporaire ? Que se passe-t-il si la 'vraie' base de données a été modifiée entre-temps (une situation assez réaliste si vous transportez votre base de données sur une clé USB) ?

Évidemment, aucune de ces alternatives n'est satisfaisante. Par conséquent, KeePass implémente le comportement simple et facile à comprendre suivant :

KeePass ne se verrouille pas lorsqu'une sous-boîte de dialogue est ouverte.

Ce concept simple évite les problèmes ci-dessus. L'utilisateur est responsable de l'état du programme.

Notez que l'ouverture d'une sous-boîte de dialogue n'est généralement requise que pour *éditer* quelque chose ; il n'est pas nécessaire pour *utiliser* les entrées, car la fenêtre principale propose différentes méthodes pour cela.

Le verrouillage lorsque Windows se verrouille. Sur Windows XP et versions antérieures, le service Windows *'Terminal Services'* doit être activé. Si ce service est désactivé, alors le verrouillage de KeePass lorsque Windows se verrouille peut ne pas fonctionner. Ce service n'est pas requis sur les systèmes d'exploitation plus récents.

L'impression crée un fichier temporaire. Sera-t-il effacé en toute sécurité ?

KeePass crée un fichier HTML temporaire lors de l'impression des listes de mots de passe et de l'affichage des aperçus avant impression. Ce fichier est supprimé en toute sécurité lors de la fermeture de la base de données.

Vous devez attendre que le fichier soit complètement imprimé avant de fermer KeePass (et fermer l'aperçu

avant impression avant de fermer KeePass), sinon il se peut que l'application d'impression empêche KeePass de supprimer le fichier.

Il n'existe aucun moyen de contourner le fichier temporaire dans le système d'impression actuel. Si vous souhaitez écrire un greffon qui envoie directement les données à l'imprimante, alors vous pouvez trouver un tutoriel de développement de greffon ici : Développement de greffon KeePass 2.x.

Pourquoi la qualité estimée d'un mot de passe chute soudainement ?

Pour estimer la qualité/la force d'un mot de passe, KeePass utilise non seulement des méthodes statistiques (comme vérifier quelles plages de caractères sont utilisées, répéter les caractères et les différences), il a également une liste intégrée de mots de passe communs et vérifie les modèles. Lors de la saisie d'un mot de passe commun ou d'une répétition, la qualité estimée peut chuter.

Les détails peuvent être trouvés sur la page d'aide de l'estimation de la qualité des mots de passe.

Comment stocker et travailler avec de grandes quantités de texte (formaté) ?

Il n'y a pas de prise en charge directe pour stocker et travailler avec de grands textes formatés.

Un champ d'adresse de courriel peut-il être ajouté ?

Plusieurs fois, il a été demandé qu'un champ de saisie standard pour les adresses de courriel soit ajouté (sur l'onglet de la page principale dans la boîte de dialogue d'édition des entrées). La réponse courte : un champ d'adresse e-mail ne sera pas ajouté pour des raisons de convivialité. Maintenant, la réponse longue.

Tout d'abord, supposons que la plupart des entrées stockées dans KeePass contiennent des informations permettant de se connecter à des sites Web. Lorsque vous enregistrez un compte pour un site Web, vous devez souvent spécifier un nom d'utilisateur ainsi qu'une adresse de courriel. Lorsque vous vous connectez régulièrement par la suite, il vous suffit généralement de fournir soit le nom d'utilisateur + le mot de passe associé, soit l'adresse de courriel + le mot de passe associé (mais jamais le nom d'utilisateur + adresse de courriel + le mot de passe associé). Ici, la première partie (qui est soit le nom d'utilisateur soit l'adresse de courriel) sert d'identification : vous dites au site Web qui vous êtes. La seconde partie (le mot de passe) assure l'authentification : vous prouvez au site que vous êtes bien celui que vous prétendez être.

Il existe différentes méthodes permettant à KeePass de transférer des données vers d'autres applications. Toutes ces méthodes supposent par défaut que le contenu du champ du nom d'utilisateur est utilisé pour l'identification. Par exemple, la séquence de saisie automatique par défaut d'une entrée est `{USERNAME}{TAB}{PASSWORD}{ENTER}`, la configuration par défaut de KeeForm utilise le nom d'utilisateur, etc. Maintenant, d'une part, certains sites Web nécessitent une adresse de courriel au lieu d'un nom d'utilisateur. D'autre part, nous voulons que la configuration de transfert de données par défaut fonctionne pour la plupart des sites Web (de sorte que le travail que l'utilisateur doit mettre dans la configuration soit minime et nécessaire uniquement pour les sites Web utilisant des formulaires de connexion spéciaux).

La solution est simple : au lieu d'interpréter le champ 'Nom d'utilisateur' strictement comme un champ contenant un nom d'utilisateur, les utilisateurs devraient plutôt l'interpréter comme un champ dans lequel sont stockées les données nécessaires à l'identification. Ces données peuvent consister en un nom d'utilisateur, une adresse de courriel ou autre chose (par exemple : un numéro de compte pour un site Web de banque en ligne). En le manipulant ainsi, la configuration de transfert de données par défaut fonctionnera pour la plupart des sites Web, c'est-à-dire qu'aucune quantité de travail ne doit être mise dans la configuration. Si vous deviez fournir à la fois un nom d'utilisateur et une adresse de courriel au moment de l'inscription, les autres informations (qui ne sont pas requises régulièrement) peuvent être stockées, par exemple dans le champ des remarques ou un champ personnalisé de chaîne de caractères de l'entrée KeePass.

Supposons maintenant qu'un champ d'adresse de courriel séparé est ajouté. Lorsque les utilisateurs stockent à la fois un nom d'utilisateur et une adresse de courriel, KeePass ne peut pas savoir lequel des deux est requis pour l'identification. Ainsi, afin de configurer le transfert de données pour l'entrée, les utilisateurs seraient obligés de choisir lequel des deux champs doit être utilisé.

Ainsi, l'ajout d'un champ d'adresse de courriel serait un pas en arrière dans la convivialité, car cela oblige les utilisateurs à consacrer plus de temps à la configuration du transfert de données. Le système actuel ('Nom d'utilisateur' contenant des informations d'identification, sans champ d'adresse de courriel séparé) ne l'exige pas et constitue donc la meilleure solution.

Pour les utilisateurs qui souhaitent configurer manuellement le transfert de données pour chaque entrée, il existe plusieurs façons d'obtenir un champ d'adresse de courriel distinct. Après être passé à l'onglet 'Avancé' dans la boîte de dialogue d'édition d'entrée, un champ d'adresse de courriel peut être ajouté en tant que chaîne personnalisée de caractères. Si le champ doit apparaître sur la page de l'onglet principal de la boîte de dialogue, le greffon KPEntryTemplates peut être utilisé.

Le développement

La personnalisation

La personnalisation (1.x)

KeePass 1.x propose diverses fonctionnalités permettant aux administrateurs réseau de personnaliser l'apparence et le comportement du programme.

- Les préliminaires
- Le mode mini
- Les opérations dangereuses
- Les groupes dans les bases de données nouvellement créées
- Le suffixe du titre de la fenêtre
- L'apparence de la bannière de la boîte de dialogue
- Les exigences du mot de passe maître minimum
- Davantage d'options

Les préliminaires

La plupart des options ci-dessous sont configurées en éditant directement le fichier de configuration `KeePass.ini`. Si, vous envisagez de déployer une version personnalisée de KeePass, alors vous devez bien comprendre le système de configuration de KeePass, en particulier comment imposer certains paramètres et laisser les autres aux utilisateurs.

Remarquez que KeePass propose un riche cadre de greffons. S'il n'y a pas d'élément dans le fichier INI pour configurer ce à quoi vous pensez, alors vous pourrez peut-être penser à écrire un greffon.

Le mode mini

KeePass prend en charge un mode mini. En précisant `KeeMiniMode=True` dans le fichier `KeePass.ini`, KeePass fonctionnera dans un mode de fonctionnalité minimal.

Dans ce mode, les fonctionnalités suivantes sont cachées :

- Les options de configuration et d'administration (paramètres de la base de données, les options du programme global, les greffons, etc.).
- La fonctionnalité qui n'intéresse pas les utilisateurs dans une entreprise (comme la vérification des mises à jour, etc.).
- Importer/Exporter.
- La saisie automatique.
- Les fichiers clés (seulement un mot de passe maître peut être saisi).
- Les opérations de fichier (seulement la commande *Enregistrer* est affichée).

Si la base de données spécifiée n'existe pas, alors KeePass crée et en ouvre une automatiquement. Pour spécifier le chemin de base d'une base de données nouvellement créée, utilisez l'option de configuration `KeeAutoNewDbBasePath` (ne doit pas se terminer par un '\' final ; KeePass créera l'arborescence de répertoires spécifiée, si elle n'existe pas déjà). Pour spécifier le nom de base du fichier de la base de données, utilisez l'option `KeeAutoNewDbBaseName` (sans ".kdb").

Les opérations dangereuses

Les opérations critiques pour la sécurité (telles que la modification de la clé principale, l'impression, l'exportation, l'affichage des mots de passe, etc.) peuvent être désactivés en spécifiant `KeeDisableUnsafe=True` dans le fichier INI.

Certaines opérations peuvent être réactivées en spécifiant explicitement des éléments de configuration. Notez que pour des raisons de sécurité, ces éléments additionnels ne sont chargés qu'à partir des fichiers INI imposés et globaux, pas à partir du fichier INI local de l'utilisateur. Ils remplacent les paramètres des opérations dangereuses et du mode mini. Les éléments booléens suivants sont pris en charge : `KeeForceAllowChangeMasterKey`, `KeeForceAllowPrinting`, `KeeForceAllowImport`, `KeeForceAllowExport`.

Pour interdire l'impression des mots de passe, spécifier `KeeDisallowPrintingPasswords=True`.

Les groupes dans les bases de données nouvellement créées

Utilisation des éléments `KeeRootInNewDb` et `KeeGroupInNewDb#` dans le fichier INI, vous pouvez spécifier les groupes qui sont automatiquement créés lorsqu'un utilisateur crée un nouveau fichier de base de données.

Exemple : si vous souhaitez que l'arbre initial ressemble à celui de droite, alors votre fichier INI contiendrait les lignes suivantes :


```
KeeRootInNewDb=@My Company Name@35
KeeGroupInNewDb0=@Windows@38
KeeGroupInNewDb1=@Network@3
KeeGroupInNewDb2=@Internet@1
KeeGroupInNewDb3=@eMail@19
KeeGroupInNewDb4=@Applications@32
```

Les éléments doivent être numérotés consécutivement dans l'ordre croissant à partir de 0. Le premier caractère de la valeur de l'élément spécifie un caractère séparateur. Dans l'exemple ci-dessus, '@' est utilisé comme séparateur, mais vous pouvez choisir n'importe quel autre caractère (si le nom du groupe contient un '@'). Le nom du groupe suit le caractère séparateur et se termine par le caractère séparateur. Le nombre qui suit est l'ID d'une icône client intégré dans KeePass (voir la boîte de dialogue de sélection d'icônes de KeePass pour une liste d'icônes). Créer des arborescences (c'est-à-dire des sous-groupes des groupes ci-dessus) n'est pas pris en charge.

Le suffixe du titre de la fenêtre

Un suffixe de titre de fenêtre principale peut être spécifié à l'aide d'élément `KeeWindowTitleSuffix` dans le fichier INI.

L'apparence de la bannière de la boîte de dialogue

L'apparence des bannières de la boîte de dialogue de KeePass peut être configurée à l'aide des éléments suivants dans le fichier INI :

- **KeeBannerColorStart** : spécifie la couleur de départ du gradient de l'arrière-plan. Définissez-le sur un triplet d'octet BGR (en décimal).
- **KeeBannerColorEnd** : spécifie la couleur de fin du gradient de l'arrière-plan. Définissez-le sur un triplet d'octet BGR (en décimal).
- **KeeBannerColorText** : spécifie la couleur du texte de premier plan. Définissez-le sur un triplet d'octet BGR (en décimal).
- **KeeBannerFlip** : valeur booléenne qui spécifie s'il faut permuter la direction du gradient naturel (c'est-à-dire de l'horizontale à la verticale ou de la verticale à l'horizontale). La direction naturelle dépend de la version de KeePass que vous utilisez.

Les exigences du mot de passe maître minimum

Vous pouvez spécifier plusieurs propriétés que les mots de passe principaux doivent avoir afin d'être accepté (longueur, qualité estimée, etc.). Voir la spécification des propriétés minimales d'un mot de passe maître.

Davantage d'options

Le nombre de jours en dessous duquel les entrées sont traitées comme arrivant à expiration peut être spécifié à l'aide de l'élément de configuration **KeeSoonToExpireDays**.

Les emplacements des fichiers de configuration peuvent être remplacés à l'aide des paramètres **KeeConfigFileOverrideGlobal** et **KeeConfigFileOverrideUser** (dans le fichier de configuration imposée). Des chemins de fichier complets et absolus doivent être spécifiés, et les deux remplacements *ne* doivent *pas* pointer vers le même fichier.

Les remplacements d'expressions régulières peuvent être appliqués aux remarques avant de les afficher dans la liste des entrées principales. Les éléments**KeeNotesRegex#** dans le fichier de configuration spécifient les expressions régulières et **KeeNotesFormat#** les remplacements. Par exemple : les paramètres suivants remplacent les caractères de tabulations par des points au milieu :

```
KeeNotesRegex0=(\t)
KeeNotesFormat0=\xB7
```

La création de greffons

Le développement de greffon (1.x)

Comment développer des greffons pour KeePass 1.x.

Cette documentation s'applique aux greffons de KeePass 1.x (toutes les versions ≥ 1.15). Les greffons 1.x sont fondamentalement différents des greffons 2.x. Les greffons 2.x ne peuvent pas être chargés par KeePass 1.x.

Une documentation détaillée du SDK est disponible ici : Plugin SDK Documentation.

- Les exigences
- Le tutoriel pas à pas
- Les conventions et recommandations relatives aux greffons
- Mettre à jour les greffons depuis ≤ 1.14 à ≥ 1.15
- La documentation détaillée de toutes les interfaces
- Le Framework de greffon pour le C++

Les exigences

Avant de pouvoir commencer à développer un greffon KeePass, vous avez besoin des prérequis suivants :

- Le dernier package de code source de KeePass. Vous pouvez l'obtenir auprès du site Web de KeePass.
- Un IDE/compilateur de développement C++.
- Le SDK de la plate-forme Windows.

L'API du greffon KeePass utilise certains concepts de la norme du Component Object Model (COM). Si vous n'avez pas d'expérience avec COM, alors les pages suivantes sont recommandées pour la lecture :

- Wikipedia: IUnknown.
- La section de comptage de référence sur Wikipedia: Component Object Model.
- MSDN: COM Interfaces and Interface Implementations.
- MSDN: COM Interface Pointers and Interfaces.
- MSDN: COM QueryInterface: Navigating in an Object.

Le tutoriel pas à pas

Démarrez votre IDE préféré et créez un nouveau *projet Win32* (type d'application *DLL*, projet vide). Dans ce tutoriel, l'exemple de greffon que nous développons s'appelle `TestPlugin`. Créez deux fichiers dans le nouveau projet : un fichier source C++ (*TestPlugin.cpp*) et un fichier d'en-tête (*TestPlugin.h*).

Afin d'accéder aux interfaces KeePass, vous devez inclure un fichier d'en-tête du SDK KeePass : placez une instruction `#include` dans le fichier *TestPlugin.h*, qui inclut le fichier

`KeePassLibCpp/SDK/KpSDK.h` du code source de KeePass.

Les DLL Windows peuvent éventuellement implémenter une fonction `DllMain`. Alors si vous en voulez une (non requis par KeePass cependant), alors en implémenter une par défaut maintenant dans le fichier *TestPlugin.cpp* (qui retourne toujours juste `TRUE`) :

```
BOOL WINAPI DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
{
UNREFERENCED_PARAMETER(hinstDLL);
UNREFERENCED_PARAMETER(fdwReason);
UNREFERENCED_PARAMETER(lpvReserved);

return TRUE;
}
```

L'étape suivante consiste à créer une classe de greffon, qui doit implémenter l'interface `IKpPlugin`. Alors, recherchez l'interface `IKpPlugin` (classe C++ abstraite) et concevez une classe qui implémente toutes ces méthodes. Vous trouverez des détails sur les méthodes ici Plugin SDK Documentation.

Exportez maintenant une fonction que KeePass utilisera pour créer une instance de votre classe de greffon :

```
KP_EXPORT HRESULT KP_API KP_I_CREATEINSTANCE_DECL(REFIID riid, void**
ppvObject, IKpUnknown* pAPI);
```

Dans cette fonction, vous devrez créer une instance de votre classe de greffon et stocker un pointeur d'interface du type demandé par KeePass (`riid`) dans le paramètre `ppvObject`. Le paramètre `pAPI` est un pointeur d'interface vers l'API KeePass, que vous devez stocker pour une utilisation ultérieure au cas où vous seriez en mesure de retourner une interface de greffon valide.

KeePass est actuellement proposé uniquement en tant qu'application ANSI, et non Unicode. Par conséquent, allez dans *Projet → Testez les propriétés du plugin* et choisissez *Multi Byte* comme jeu de caractères.

Il est recommandé (mais pas nécessaire) d'établir un lien statique avec la bibliothèque d'exécution (et la MFC, si vous l'utilisez). Pour ce faire, rendez-vous sur *Projet → Tester les propriétés du plugin → C/C++ → Génération de code* et choisissez une bibliothèque d'exécution ne se terminant pas par '-DLL'.

La dernière étape avant de créer votre greffon consiste à ajouter une ressource d'information de version. Alors, allez dans l'onglet 'Ressources' du projet de greffon et ajoutez une ressource de type 'Version'. Ici, définissez le nom du produit sur `KeePass Plugin`. Tous les autres champs peuvent être librement définis sur des chaînes de votre choix.

Exemple. Vous pouvez trouver une version entièrement documentée et étendue de ce simple greffon sur la page web des plugins KeePass (*"Test Plugin"*).

Les conventions et recommandations relatives aux greffons

Les conventions :

- Le fichier DLL doit avoir une ressource d'informations de version, dans laquelle le nom du produit est défini sur `KeePass Plugin`. KeePass utilise ceci pour déterminer si la DLL est un greffon KeePass ou non (c'est-à-dire si vous ne créez pas une ressource d'informations de version avec cette chaîne, alors KeePass ne chargera pas votre fichier DLL).
- Si vous souhaitez utiliser le nom "KeePass" en tant que partie du nom de votre plugin, alors préfixez/ajoutez directement un préfixe/suffixe non numérique. Par exemple : "KeePassSync" est correct, mais "KeePass Sync" ne l'est pas.
- Un greffon KeePass doit exporter la fonction suivante :
  ```
  KP_EXPORT HRESULT KP_API KP_I_CREATEINSTANCE_DECL(REFIID riid, void**
  ppvObject, IKpUnknown* pAPI);
  ```

  KeePass appellera cette fonction pour créer une instance de votre classe de greffon. Vous devez retourner une interface de type `riid` dans le paramètre `ppvObject`, si votre classe de greffon prend en charge cette interface (il retournera `S_OK`). Sinon, positionnez `ppvObject` sur `NULL` et retournez `E_NOINTERFACE`. Vous pouvez stocker le pointeur d'interface `pAPI` pour une utilisation ultérieure. KeePass garantit que le pointeur est valide tant qu'il a un pointeur vers votre instance de classe de greffon.

  Important : vérifiez explicitement pour quelle interface KeePass demande (`riid`), sinon votre

greffon ne sera pas descendant compatible et pourrait planter dans les futures versions de KeePass.

- Un greffon KeePass peut éventuellement exporter les fonctions suivantes :
```
KP_EXPORT HRESULT KP_API KP_I_INITIALIZELIB_DECL(IKpUnknown* pAPI);
KP_EXPORT HRESULT KP_API KP_I_RELEASELIB_DECL(IKpUnknown* pAPI);
```

  KeePass appellera la première fonction après le chargement de la DLL, et la seconde un peu avant le déchargement de la DLL.

  Vous ne devez pas stocker le pointeur d'interface `pAPI` pour une utilisation ultérieure. Considérez les pointeurs comme temporaires ; ils pourraient devenir invalides dès que vous retournez depuis `KP_I_INITIALIZELIB_DECL` ou `KP_I_RELEASELIB_DECL`. Les valeurs du pointeur d'interface `pAPI` transmises à `KP_I_INITIALIZELIB_DECL` et `KP_I_RELEASELIB_DECL` ne sont pas garanties comme étant les mêmes comme chacune d'entre elles, ou comme la valeur de pointeur transmise à `KP_I_CREATEINSTANCE_DECL`.
- Le protocole est `DllMain` (si présent), `KP_I_INITIALIZELIB_DECL` (si présent), `KP_I_CREATEINSTANCE_DECL`, méthodes d'interface de greffon, `KP_I_RELEASELIB_DECL` (si présent).
- KeePass utilise le jeu de caractères multi-octets. Par conséquent, assurez-vous que vous compilez également votre greffon en mode jeu de caractères multi-octets, et pas Unicode.

Les recommandations :

- Tous les fichiers de greffon doivent commencer par un préfixe commun. Par exemple : si votre greffon s'appelle *VariousImport*, alors le fichier DLL peut être nommé *VariousImport.dll* et son fichier d'aide *VariousImport.html*. Si vous n'utilisez pas de préfixe commun, alors les utilisateurs peuvent rencontrer des problèmes d'écrasement lors de l'installation de plusieurs greffons, car tous les greffons doivent être copiés dans le répertoire de l'application KeePass. Par exemple : s'il y a un greffon qui est livré avec un fichier *ReadMe.txt* et un autre greffon qui est également livré avec un tel fichier, alors ce dernier écrase le fichier readme du premier, ou l'utilisateur choisit de ne pas l'écraser et le fichier readme du deuxième greffon n'est alors pas disponible. En utilisant un préfixe commun cela évite ce problème.
- Le bloc d'informations sur la version doit au moins être disponible en langue anglaise (États-Unis).
- Il existe deux implémentations de l'interface `IKpConfig`. Une implémentation est identifiée par `CLSID_KpConfig`, l'autre par `CLSID_KpConfig_ReadOnly`. La première prend en charge à la fois la lecture et l'écriture, tandis que la seconde uniquement la lecture. Il est fortement recommandé que vous utilisiez la deuxième implémentation, si vous ne voulez lire que les éléments de la configuration.

  Essayer d'écrire en utilisant l'implémentation `CLSID_KpConfig_ReadOnly` vérifiera si KeePass est compilé en mode débogage et échouera en mode Release (et pourrait éventuellement détruire des parties de la configuration actuelle).

Mettre à jour les greffons depuis ≤ 1.14 à ≥ 1.15

Lors de la mise à jour d'un greffon depuis KeePass ≤ 1.14 à ≥ 1.15, il est fortement recommandé de créer un nouveau fichier de projet, de recommencer à zéro et copier/remplir les méthodes d'interface avec l'ancien code.

Remarques :

- Il n'y a plus de fichier `KeePass.lib`. La nouvelle architecture des greffons est basée sur des interfaces. On inclut le fichier d'en-tête `KpSDK.h` c'est tout ce que vous avez à faire.

  Ne compilez avec aucun des fichiers du code source de KeePass ou n'incluez tout autre fichier d'en-tête que `KpSDK.h`.
- Auparavant, un préfixe de ligne de commande était enregistré en définissant le membre de la structure d'informations du greffon `cmdLineArgPrefix`. Dans la nouvelle architecture, le préfixe de la ligne de commande doit être retourné par le membre de la méthode de l'interface du greffon `GetProperty` quand il est appelé par le paramètre `KPPS_COMMANDLINEARGPREFIX`.

  Votre `GetProperty` pourrait ressembler à ceci :

```
STDMETHODIMP_(LPCTSTR) CYourPluginImpl::GetProperty(LPCTSTR lpName)
{
if(lpName == NULL) retourne NULL ;

if(_tcscmp(lpName, KPPS_COMMANDLINEARGPREFIX) == 0)
return _T("mypluginprefix.");

return NULL ;
}
```

Le greffon ne doit pas accéder à la ligne de commande de KeePass après que tous les greffons ont été chargés. C'est parce qu'à ce moment KeePass ne peut bien sûr pas encore appeler la méthode `GetProperty` de votre greffon et par conséquent ne connaît pas encore le préfixe (et cela conduira à des avertissements 'option de ligne de commande inconnue'). Au lieu de cela, effectuez une ligne de commande dépendante de l'initialisation lorsque KeePass appelle votre gestionnaire de méthode `OnMessage` avec le code `KPM_DELAYED_INIT`.

La documentation détaillée de toutes les interfaces

Voir Plugin SDK Documentation.

Le Framework de greffon pour le C++

Merci à Bill Rubin, il existe un *Plugin Framework* disponible, facilitant le développement de greffons KeePass en C++. Les fonctionnalités en détail :

1. Implémentation complète de l'interface `IID_IKpUnknown`.
2. Implémentation de l'interface `IID_IKpPlugin`, excepté pour la fonction membre `OnMessage`, qui est toujours une application spécifique.
3. La possibilité d'obtenir des pointeurs intelligents vers n'importe quelle autre interface KeePass, y compris `IKpAPI`, `IKPCommandLine`, `IKpCommandLineOption`, `IKpConfig`, `IKpDatabase`, `IKpFullPathName` et `IKpUtilities`.
4. Implémentation de la fonction `KpCreateInstance`, dont le greffon doit s'exporter de ses DLL.
5. Vérification complète des erreurs de l'établissement de liaison COM pour les éléments 3 et 4. Si une erreur est détectée, alors PFK affiche une boîte de message contenant toutes les informations sur l'erreur. Sans cette fonctionnalité, un greffon échouera dans la plupart des cas à se charger de façon silencieuse. Dans les autres cas, il échouera à remplir sa fonction.
6. Utilitaires pratiques, pour afficher une boîte de message, traduire un code d'erreur Windows dans une chaîne en langage naturel et déclarez une chaîne standard indépendamment du type de caractère.
7. Vérification du temps de la compilation des invocations de constructeur pour les pointeurs COM intelligents. Sans cette fonctionnalité, il est difficile pour un développeur d'interpréter les messages d'erreur du compilateur causés en utilisant le mauvais constructeur de pointeur COM intelligent.
8. Le code PFK évite de définir des macros. Au lieu des modèles, les fonctions en ligne, typedefs et autres constructions C++ maintiennent des pratiques de conception sécurisée, sans pénalité d'exécution.

Il y a également un greffon de test disponible en utilisant le Framework de greffon.