KeePass-2.61.1

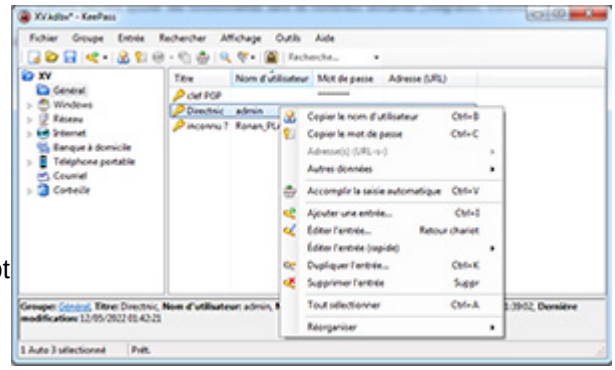
Table des matières

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 connexions (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 (au code ouvert), 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, importateur de CSV générique, 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 au code ouvert, vous pouvez consulter entièrement son code source et vérifier que les fonctions de sécurité sont correctement implémentées.

Cette documentation s'applique à KeePass 2.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'utiliserons 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 cette boîte de dialogue, vous pouvez configurer certaines propriétés de la base de données générique. Pour l'instant, simplement laisser tout tel quel et cliquer sur [OK].

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 dans 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 est maintenant affichée dans la liste d'entrées principale. Il y a différentes façons de l'utiliser.

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-cliquer sur la cellule du nom d'utilisateur dans la liste d'entrées principale. Alternativement, la commande peut être invoquée 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 des mots de passe et des autres champs fonctionne de manière analogue.

Alternativement, vous pouvez glisser&déposer les champs dans d'autres fenêtres. Pour plus de détails, alors 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 clés : 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 clés, 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 par 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, merci beaucoup 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	Utilisés dans KeePass
Szymon Stefanek	L'implémentation en C++ de l'algorithme de chiffrement AES/Rijndael.	1.x
Niels Ferguson	L'implémentation en langage C de l'algorithme de chiffrement Twofish.	1.x
Brian Gladman	Implémentation en langage C de l'algorithme de hacha ge SHA-2 (256/384/512).	1.x
Alvaro Mendez	La classe MFC pour la validation des contrôles d'édition (CAMSEdit).	1.x
Brent Corkum	La classe MFC pour le menu de style XP (BCMenu).	1.x
Davide Calabro	La classe MFC pour des boutons avec des icônes (CButtonST).	1.x
Zorglab, Chris Maunder, Alexander Bischofberger, James White, Descartes Systems Sciences Inc.	La classe MFC pour les sélecteurs de couleur (CColourPickerXP).	1.x
Peter Mares	La classe MFC pour les bannières côté fenêtre (CKCSideBannerWnd).	1.x
Chris Maunder	La classe MFC pour les icônes de la zone de notification du système (CSystemTray).	1.x
Hans Dietrich, Chris Maunder	La classe MFC pour les hyperliens dans les boîtes de dialogue (XHyperLink).	1.x
Lallous	La classe pour envoyer des frappes de touche simulées à d'autres applications (CSendKeys).	1.x
PJ Naughter	Les classes MFC pour la vérification de l'instance unique (CSingleInstance) et des informations de version	1.x

	(CVersionInfo).	
Bill Rubin	Les classes en C++ de la ligne de commande.	1.x
Les développeurs de Boost	Les bibliothèques en C++ de Boost	1.x
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.	1.x & 2.x

Auteur	Ressource	Utilisés dans KeePass
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.	1.x & 2.x

Remerciements pour les icônes

Merci beaucoup 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**.
- Icône FreeBSD (sur Archive.org) par **FatCow**.
- Le symbole de la main par **Bobek Ltd**.

Remerciements pour les traductions

Merci beaucoup 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

Copyright (c) 2006, Bill Rubin <rubin@contractor.net>
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* 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.

* Neither the name of Quality Object Software, Inc., nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS 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 COPYRIGHT OWNER 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.

L'implémentation Argon2

Argon2 reference source code package - reference C implementations

Copyright 2015
Daniel Dinu, Dmitry Khovratovich, Jean-Philippe Aumasson, and Samuel Neves

You may use this work under the terms of a Creative Commons CC0 1.0 License/Waiver or the Apache Public License 2.0, at your option. The terms of these licenses can be found at:

- CC0 1.0 Universal : http://creativecommons.org/publicdomain/zero/1.0
- Apache 2.0 : http://www.apache.org/licenses/LICENSE-2.0

The terms of the licenses are reproduced below.

Creative Commons Legal Code

CC0 1.0 Universal

CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDE LEGAL SERVICES. DISTRIBUTION OF THIS DOCUMENT DOES NOT CREATE AN

ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN "AS-IS" BASIS. CREATIVE COMMONS MAKES NO WARRANTIES REGARDING THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS PROVIDED HEREUNDER, AND DISCLAIMS LIABILITY FOR DAMAGES RESULTING FROM THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS PROVIDED HEREUNDER.

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 2.x.

Les informations générales

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

- **KeePass-*2.xx*-Setup.exe :** le programme d'installation pour Windows.
- **KeePass-*2.xx*.zip :** le paquet KeePass au format ZIP (version portable).
- **KeePass-*2.xx*-Source.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#/C++ et les fichiers d'en-têtes, les fichiers de ressources, les sources de construction du programme d'installation, etc.

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-2.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 KDBX 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-2.xx-Setup.exe` et suivez l'assistant.

Mise à jour :
Exécutez le fichier `KeePass-2.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).

Le 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.

Options/composants :
Les options/composants d'installation sont expliqué(e)s en détail ici : 'Que signifient les options/composants d'installation 2.x en détail ?'.

La version portable (fichier KeePass-2.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.config.xml*, qui ne sera pas écrasé, car les paquets ZIP de KeePass n'incluent pas de fichier *KeePass.config.xml*).

Désinstallation :
Supprimer simplement le répertoire où se trouve KeePass.

L'installation silencieuse

Le programme d'installation (`KeePass-2.x-Setup.exe`) et le package MSI (`KeePass-2.x.msi`) prennent tous deux en charge l'installation silencieuse de KeePass.

Vous trouverez des informations détaillées sur les options et composants d'installation ici : 'Que signifient en détail les options et composants d'installation de la version 2.x ?'.

- **KeePass-2.x-Setup.exe:**
  Le programme d'installation est conçu avec Inno Setup, qui prend en charge divers paramètres de ligne de commande, notamment pour une installation silencieuse (`/SILENT`, `/VERYSILENT`) et pour la sélection des composants/tâches (`/COMPONENTS="..."`, `/TASKS="..."`, `/MERGETASKS="..."`):
  Inno Setup : les paramètres de ligne de commande de configuration.
  - Les composants : `Core`, `UserDoc`, `KeePassLibN`, `XSL`, `NGen`, `PreLoad`.
  - Les tâches : `FileAssoc`, `DesktopIcon`.
  - Pour plus de détails, alors voir le fichier `Ext/KeePass.iss` dans le package de code source de KeePass.

  Par exemple, si vous souhaitez installer KeePass en mode silencieux, sans associer de fichiers KDBX à KeePass et sans créer de raccourci sur le bureau, alors vous pouvez exécuter le programme d'installation comme suit (en tant qu'administrateur) :

  ```
  KeePass-2.x-Setup.exe /VERYSILENT /MERGETASKS="!FileAssoc,DesktopIcon"
  ```

- **KeePass-2.x.msi:**
  Le package MSI peut également être utilisé pour installer KeePass en mode silencieux. Vous trouverez des informations détaillées sur les paramètres de ligne de commande de `MsiExec.exe` et ses propriétés ici :
  Microsoft: MsiExec,
  Microsoft: Windows Installer Property Reference.
  Outre les paramètres de ligne de commande et les propriétés standard, la propriété `KPS_OPTIONS` permet de personnaliser l'installation. Sa valeur peut être une liste d'options séparées par des virgules. Pour désactiver une option, ajoutez un point d'exclamation (`!`) devant son nom.

  - Options : `StartMenuIcons`, `DesktopIcon`, `NGen`, `PreLoad`.

Par exemple, si vous souhaitez installer KeePass en mode silencieux pour tous les utilisateurs sans créer de raccourci sur le bureau et sans optimiser les performances de démarrage de KeePass, vous pouvez exécuter `MsiExec.exe` comme suit (en tant qu'administrateur) :

```
MsiExec.exe /i "C:\Path\KeePass-2.x.msi" /qn ALLUSERS=1 KPS_OPTIONS="!DesktopIcon,!P
```

L'Exécution de KeePass sous Mono (Linux, MacOS, BSD, etc.)

En plus de Windows, KeePass 2.x fonctionne sous Mono, c'est-à-dire Linux, MacOS, BSD, etc.

Des liens vers tous les paquets pris en charge sont disponibles sur la page des téléchargements.

- **Linux Debian/Ubuntu :**
  Installez le paquet *keepass2*/*KeePass 2.x pour Linux Debian/Ubuntu* (par exemple : à l'aide de la commande apt). Un lien vers une page contenant plus d'informations sur ce paquet est disponible sur la page des téléchargements.

- **Linux Fedora/RHEL/Rocky/Alma :**
  Installez le paquet *keepass* (à partir du référentiel Linux Fedora/RHEL/Rocky/Alma ; lien sur la page des téléchargements).

- **Linux OpenSUSE :**
  Installez le paquet *keepass* (à partir du référentiel Mono d'OpenSUSE ; lien sur la page des téléchargements).

- **Linux Gentoo :**
  Installez le paquet *keepass* (depuis le dépôt Linux Gentoo ; lien sur la page des téléchargements).

- **Linux Arch :**
  Installer le paquet *keepass* (à partir du référentiel Linux Arch ; lien sur la page des téléchargements).

- **MacOS :**
  Installer le paquet *KeePass 2.x* pour Mac OS X (lien sur la page des téléchargements).

- **FreeBSD :**
  Installer le paquet *keepass* (à partir de l'arborescence des portages FreeBSD ou du référentiel pkg des binaires ; lien sur la page des téléchargements).

- **Les autres systèmes Unix-like :**
  Pour exécuter KeePass, procéder comme suit :
  1. Installez Mono ≥ 2.6 (les versions antérieures ne fonctionneront pas et ne sont pas prises en charge). Selon votre plateforme utilisée, les paquets à installer sont appelés `mono-stable`, `MonoFramework`, `mono-devel` ou `mono-2.0-devel` ; cf. la page du projet Mono, si vous n'êtes pas sûrs des paquets à installer.
  2. Sur certaines plateformes, l'implémentation de Windows Forms (System.Windows.Forms) est proposée dans un paquet à part. KeePass a besoin de ce paquet ; alors si vous en voyez un, installez-le également.
  3. Sur certaines plateformes, l'espace de nom Runtime (System.Runtime) est proposé sous forme de paquet à part. KeePass a besoin de ce paquet ; alors si vous en voyez un, installez-le également.
  4. Si vous souhaitez utiliser la saisie automatique sous Linux/MacOS/BSD/etc., vous avez également besoin du paquet `xdotool`.
  5. Téléchargez la version portable de KeePass (paquet ZIP) et décompressez-la à l'emplacement de votre choix.
  6. Lorsque vous vous trouvez dans le répertoire KeePass, exécuter la ligne de commande "`mono KeePass.exe`". Vous pouvez également faire un clic droit sur le fichier `KeePass.exe`, et choisir "Ouvrir avec une autre application" et tapez `mono` en tant que commande personnalisée.

  Pour la dernière étape, vous pouvez créer un raccourci ou un fichier de script shell avec cette ligne

de commande (utilisez un chemin absolu vers `KeePass.exe`, si le raccourci/fichier de script shell se trouve à un emplacement différent).

Saisie automatique globale :
Afin d'utiliser la saisie automatique globale, vous devez créer une touche de raccourci appropriée à l'échelle du système. Cela ne doit être fait qu'une fois manuellement. KeePass effectue la saisie automatique globale lorsqu'il est invoqué avec l'option `--auto-type` de la ligne de commande.

Voici quelques exemples de création d'une touche de raccourci à l'échelle du système pour la saisie automatique globale, pour différents systèmes d'exploitation :

7. **KDE.** Sur les systèmes Linux avec KDE, la touche de raccourci peut être créée dans *Computer → System Settings → Shortcuts and Gestures*: dans la boîte de dialogue, aller dans *Edit → New → Global Shortcut → Command/URL*, spécifié le raccourci sur l'onglet *Trigger* et saisissez
`mono /VotreCheminVersKeePass/KeePass.exe --auto-type`
à l'intérieur du champ *Command/URL* sur l'onglet *Action*.
8. **Linux Ubuntu ≥ 11.04 (Unity/GNOME).** Ouvrez la boîte de dialogue *Raccourcis Clavier (Keyboard Shortcuts)* dans les préférences système, cliquez sur le bouton *Ajouter (Add)*, saisissez `KeePass --auto-type` comme nom et
`mono /VotreCheminVersKeePass/KeePass.exe --auto-type`
en tant que nom de commande, puis cliquez sur [Appliquer] ([Apply]). Cliquez sur *Désactivé* (Disabled) de l'élément nouvellement créé (tel que le texte *'Nouveau raccourci...' 'New shortcut...'* s'affiche), appuyez sur Ctrl+Alt+A et fermez la boîte de dialogue.
9. **Linux Ubuntu ≤ 10.10 (GNOME).**
    1. Appuyez sur Alt+F2, saisissez `gconf-editor` et cliquez sur [OK].
    2. Naviguez vers `apps → metacity → keybinding_commands`.
    3. Double-cliquez sur l'un des éléments `command_i`, saisissez
    `mono /VotreCheminVersKeePass/KeePass.exe --auto-type`
    et cliquez sur [OK].
    4. Cliquez sur le nœud `global_keybindings` sur la gauche.
    5. Double-cliquez sur l'élément `run_command_i` approprié (par exemple : lorsque vous avez utilisé `command_5` aux étapes précédentes, double-cliquez maintenant sur `run_command_5`) et spécifiez le raccourci clavier de votre choix. Par exemple, pour utiliser Ctrl+Alt+A comme raccourci clavier, saisissez `<Control><Alt>a`.

Important : pour la saisie automatique globale, la version du paquet `xdotool` doit être 2.20100818.3004 ou supérieure ! Si votre distribution ne propose qu'une version plus ancienne, alors vous pouvez télécharger et installer manuellement la dernière version du paquet (cf. le site `xdotool`).

La saisie automatique sur Wayland:
Si vous souhaitez utiliser la saisie automatique sur un système avec un compositeur Wayland, alors cf. la page la saisie automatique sur Wayland.

AES-KDF:
Pour des transformations de clé rapides utilisant AES-KDF, assurez-vous que la librairie `libgcrypt` est installée.

Argon2:
Pour des transformations de clé rapides utilisant Argon2, assurez-vous que la librairie `libargon2` est installée.

Greffons :
Sur certains systèmes Linux, le paquet `mono-complete` peut être nécessaire au bon fonctionnement des greffons.

TLS 1.2 :
Pour la prise en charge de TLS 1.2, Mono 4.8.0 ou supérieur (ou .NET Framework 4.5 ou supérieur) est requis.

Polices :
Sur certains systèmes Linux, le paquet `ttf-mscorefonts-installer` peut être exigé.

L'exécution de KeePass sous Wine (Linux, MacOS, BSD, etc.)

Bien que vous puissiez exécuter KeePass 2.x de manière plus ou moins native sur des systèmes Unix-like en utilisant Mono (cf. ci-dessus), l'interface utilisateur n'est pas toujours jolie. Certains utilisateurs préfèrent donc exécuter KeePass 2.x sous Wine, qui fonctionne également très bien.

Pour exécuter KeePass 2.x avec Wine, procéder comme suit :

1. Assurez-vous que Wine est installé. Généralement, le paquet à installer s'appelle `wine`.
2. Assurez-vous que le Framework .NET 4.5 ou version ultérieure est installé dans Wine (cf. WineHQ AppDB: .NET Framework).
   Pour l'installation du Framework .NET 4.5 `winetricks` peut être utilisé (cf. WineHQ AppDB: .NET Framework 4.5).
3. Téléchargez le dernier paquet portable de KeePass 2.x (fichier ZIP) et décompressez-le dans le répertoire de votre choix.
4. Exécutez `wine KeePass.exe`.

Thème. Par défaut, Wine utilise le thème Windows classique. Si vous préférez un autre thème, vous pouvez l'installer dans 'Applications' → 'Wine' → 'Configurer Wine' ('Configure Wine)' → onglet 'Intégration au bureau' ('Desktop Integration'). Des liens vers des thèmes se trouvent par exemple sur Wikipédia: Windows XP visual styles.

Saisie automatique. Actuellement Wine n'implémente pas toutes les fonctions de l'API Windows requises pour la saisie automatique, c'est-à-dire que la saisie automatique ne fonctionne pas quand on exécute KeePass sous Wine.

La migration depuis KeePass 1.x vers 2.x

Afin de migrer KeePass depuis 1.x vers 2.x, suivre ces étapes :

1. Installez KeePass 2.x.
   Si vous utilisez le programme d'installation, assurez-vous que le composant 'Native Support Library' est installé (par défaut ce composant est activé).
2. Exécutez KeePass 2.x et créez un nouveau fichier de base de données (via 'Fichier' → 'Nouveau...').
3. Importez votre ancien fichier de base de données KDB dans votre nouveau fichier de base de données KDBX (via 'Fichier' → 'Importer...', format de fichier 'KeePass KDB (1.x)').

Si tout fonctionne correctement, vous pouvez effacer votre ancienne installation de KeePass 1.x. L'ancien fichier de base de données KDB n'est également plus nécessaire, mais vous pourriez souhaiter le garder comme sauvegarde.

Les traductions

- L'installation des traductions de l'interface utilisateur
- Le contenu localisé supplémentaire

L'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 de fichiers Windows. D'autres gestionnaires de fichiers peuvent avoir des problèmes avec les

droits d'accès.

Le 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 (2.x)
Installation, désinstallation et sécurité des greffons de KeePass 2.x.

- Introduction
- Les ressources en ligne
- L'installation et la désinstallation
- La sécurité
- Le cache

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.

L'installation et la 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.

Linux :
Sur certains systèmes Linux, le paquet `mono-complete` peut être nécessaire au bon fonctionnement des greffons.

Portabilité :
Les greffons PLGX sont compilés par KeePass et les fichiers générés sont stockés dans uncache de greffon, qui se trouve par défaut dans le répertoire de données d'application de l'utilisateur (par conséquent, l'exécution d'un greffon PLGX crée par défaut des fichiers en dehors du répertoire de l'application KeePass). Ces fichiers de cache de greffon n'ont donc pas besoin d'être copiés sur d'autres systèmes, car ils sont générés sur chaque système et ne contiennent aucune donnée utilisateur.

La sécurité

Les greffons doivent être stockés dans le dossier 'Plugins' du répertoire de l'application KeePass. Un

attaquant qui peux copier un greffon malicieux dans ce dossier pourrait également typiquement remplacer le fichier 'KeePass.exe' par un malware. En tant que protection contre de telles attaques, un système de fichier approprié access control list (ACL) devrait être utilisé (pour le répertoire de l'application KeePass dans sa totalité, incluant le dossier 'Plugins'); les privilèges de l'administrateur devraient être requis pour l'accès en écriture.

- L'installateur KeePass et le paquetage MSI package installent KeePass dans le dossier Programmes par défaut. Ce répertoire a typiquement une ACL appropriée, et le répertoire de l'application KeePass hérite de cette ACL. Donc, vous ne devez pas spécifier une ACL manuellement.
- Si vous installez KeePass dans un dossier différent ou si vous utilisez l'application portable, alors il est recommandé que vous spécifiez une ACL manuellement.

DLL vs. PLGX:
KeePass prend en charge deux format de fichier de greffon : DLL et PLGX. Un greffon DLL est chargé directement, tandis que KeePass doit d'abord compiler un greffon PLGX vers un greffon DLL, qui est stocké dans le cache greffon (voir la section ci-dessous).

Par défaut, l'utilisateur a le droit en écriture sur le dossier du cache des greffons PLGX (sans les privilèges de l'administrateur). Ceci n'est pas une vulnérabilité de sécurité. Supposons que l'attaquant a accès en écriture sur le dossier du cache de greffon et que le but est l'exécution de code. Le dossier du cache de greffon est typiquelement situé dans le répertoire du profil de l'utlisateur et a la même ACL, c'est-à-dire l'accès en écriture dans le dossier du profil de l'utilisateur. Avec ceci, il y a plusieurs façons d'éxécuter un malware (quelques exemples peuvent être trouvés ici : 'Accès en écriture vers le fichier de configuration'). Un malware autonome peut également être spécifié sur l'attaque de KeePass (voir 'Espion spécialisé'); il n'a pas besoin d'être un greffon pour ceci. De plus, un scanne logiciel d'anti-virus parcourt tous les fichiers contenant du code exécutable (EXE, DLL, etc.); un malware est soit détecté ou non, indépendamment du dossier du profile utilisateur où il est stocké.

Si vous vous souciez à propos de ceci alors de toute façon, considérez d'ajuster l'ACL du dossier de cache de greffon PLGX pour nécessiter les privilèges de l'administrateur pour un accès en écriture. Remarquer que bien que cela peut engendrer que les greffons ne fonctionnent plus correctement (ceux qui supposent d'avoir un accès en écriture dans le dossier du cache des greffons), et l'option de KeePass 'Supprimer les anciens fichier du cache' pourrait également ne plus fonctionner du tout.

Dans le cas d'un double package (DLL et PLGX dans le même dossier), KeePass charge le fichier DLL (et ignore le fichier PLGX), si possible.

Le cache

Les greffons PLGX (et non les greffons DLL) sont compilés et stockés dans un répertoire de cache de greffons sur le système de l'utilisateur. Ce cache améliore considérablement les performances de démarrage de KeePass. Les anciens fichiers sont normalement supprimés automatiquement du cache (ceci peut être désactivé dans la boîte de dialogue des greffons). Le cache ne contient aucune donnée utilisateur.

Par défaut, le cache de greffon est situé dans le répertoire de données d'application locale de l'utilisateur (`%LOCALAPPDATA%\KeePass\PluginCache`). Cependant, ceci peut être remplacé à l'aide du paramètre `Application/PluginCachePath` du fichier de configuration imposée (ce paramètre prend en charge les paramètres substituables et les variables d'environnement). Ainsi, si vous utilisez, par exemple, KeePass sur un périphérique portable et ne souhaitez pas que le cache se trouve sur le système, alors vous pouvez définir le chemin d'accès vers `{APPDIR}\PluginCache`.

⚠ Ne déplacez pas le cache de greffon dans le répertoire 'Plugins' du répertoire de l'application KeePass, car cela peut entraîner une grave dégradation des performances.

La compatibilité

Les fichiers KDBX (créés par KeePass 2.x) et les fichiers KDB (créés par KeePass 1.x) *ne* sont *pas* compatibles, car KeePass 2.x prend en charge plus de fonctionnalités que KeePass 1.x.

Cependant, KeePass 2.x peut importer les fichiers KDB créés par KeePass 1.x. Pour cela, vous devez d'abord créer une nouvelle base de données dans KeePass 2.x puis importer la base de données de KeePass 1.x en utilisant *'Fichier' → 'Importer...'*.

Via *'Fichier' → 'Exporter...'*, KeePass 2.x peut également exporter les données au format KDB de KeePass 1.x. Cependant, remarquez que tous les champs de KeePass 2.x ne sont pas pris en charge par KeePass 1.x (c'est-à-dire que l'exportation est avec perte).

Les fonctionnalités

Accessibilité

- Les informations
- Les documents

Les informations

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 stratégie de l'application

La stratégie de l'application

Détails à propos du système de politique de l'application au sein de KeePass.

L'aide pour les utilisateurs

La stratégie de l'application est une fonctionnalité de KeePass qui permet aux administrateurs de vous empêcher de compromettre accidentellement le système de sécurité de votre entreprise.

Des opérations telles que l'exportation d'entrées vers des fichiers non chiffrés ou l'impression, par exemple, peuvent être efficacement empêchées à l'aide de la stratégie de l'application.

Si vous utilisez KeePass à la maison, alors vous pouvez ignorer la stratégie de l'application (de toute façon tout est autorisé) ou réduire vos droits en utilisant la politique vous-même, afin d'éviter une fuite accidentelle d'informations sensibles.

Afin d'empêcher la modification de la stratégie après qu'elle a été spécifiée, il est recommandé d'utiliser un fichier de configuration imposé.

L'aide pour les administrateurs

KeePass peut être installé sur un lecteur réseau et une politique peut être imposée (par exemple : interdire aux utilisateurs d'imprimer la liste des entrées).

L'imposition de la politique de l'application est basée sur comment KeePass enregistre ses paramètres de configuration ? Vous devez d'abord comprendre cette méthode avant de pouvoir continuer la création d'une stratégie ; cf. la page d'aide configuration.

La politique imposée à l'installation de KeePass se présente comme suit : les fichiers de l'application KeePass sont enregistrés sur un lecteur réseau et tous les utilisateurs démarrent KeePass depuis ce lecteur (c'est-à-dire qu'ils ont seulement un lien vers l'exécutable sur le lecteur réseau). En utilisant le fichier de configuration imposé sur le lecteur réseau (souvenez-vous que ce fichier remplace tous les autres), une stratégie peut être imposée.

Afin de créer une telle installation, procédez comme suit :

1. Copiez KeePass sur un lecteur réseau partagé prenant en charge les droits d'accès aux fichiers (tels que NTFS).
2. Créez un fichier de configuration imposé qui applique les paramètres souhaités de la stratégie de l'application.
3. Ajustez les droits d'accès aux fichiers : autorisez uniquement les utilisateurs à lire et à exécuter tous les fichiers KeePass, sans accès en écriture.

Politique de sécurité

Rappelez-vous à quoi ressemble le mécanisme de la stratégie : KeePass et le fichier de configuration sont stockés sur le disque réseau. Si vous accordez à vos utilisateurs un accès libre à l'Internet ou leur permettez d'insérer des cédéroms/DVD/clés USB, alors rien n'empêche un utilisateur de télécharger une nouvelle copie de KeePass et de l'exécuter. Dans ce cas, la stratégie n'est pas imposée, puisque le KeePass téléchargé ne connaît rien du fichier de configuration imposé sur le lecteur réseau.

L'imposition de la stratégie n'est donc efficace que si vos utilisateurs utilisent réellement que la version de KeePass installée sur le lecteur réseau.

La saisie automatique

- Informations de base sur la saisie automatique
- Exigences et limitations
- Appel de la saisie automatique
  - Depuis le menu contextuel : commande '*Accomplir la saisie automatique*'
  - Le 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

Informations sur la saisie automatique de base

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 connexion, 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 touche Entrée.

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.

La saisie automatique peut être configurée individuellement pour chaque entrée en utilisant l'onglet de *saisie automatique* sur la boîte de dialogue de l'entrée (sélectionner une entrée → *Modifier l'entrée...*). Sur cette page, vous pouvez spécifier une séquence par défaut et personnaliser des associations fenêtre/séquence spécifiques.

Deux canaux d'obfuscation de saisie automatique sont pris en charge (ce qui rend la saisie automatique résistante aux enregistreurs de frappe).
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 sélectionné 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.

Exigences et limitations

Les droits :
Pour que la saisie automatique fonctionne, KeePass doit s'exécuter aux mêmes droits ou à un niveau de privilège d'interface utilisateur supérieur que l'application cible. Pour les détails, cf. conception du mécanisme d'intégrité de Windows.

Lorsque la saisie automatique ne semble rien envoyer (par exemple : dans certaines boîtes de dialogue 'Sécurité Windows' ou dans certaines instances de VMware Workstation), envisagez d'exécuter KeePass en tant qu'administrateur (ce qui lui octroie un niveau de privilèges d'interface utilisateur plus élevé). Pour ce faire, cliquez avec le bouton droit sur le raccourci KeePass, ou sur le fichier 'KeePass.exe' → puis sélectionnez 'Exécuter en tant qu'administrateur'. Vous pouvez également envisager d'utiliser une autre méthode de transfert de données (presse-papiers, greffon d'intégration , etc.).

KeePass ne prend pas en charge intentionnellement UIAccess, car cela constituerait une faille de sécurité : dans certaines circonstances, des attaques par élévation de privilèges seraient possibles (un logiciel malveillant exécuté avec des droits d'utilisateur standard pourrait exécuter du code avec des droits d'administrateur). L'exécution de KeePass en tant qu'administrateur empêche de telles attaques par

élévation de privilèges.

Les bureaux à distance et les machines virtuelles :
KeePass ne connait 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 utilisent 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 systèmes Unix-like avec un compositeur Wayland, il peut y avoir d'autres limitations ; cf. la page Auto-Type on Wayland.

Depuis le 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 global de la saisie automatique

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 *Notepad* avec les valeurs pour le nom d'utilisateur et le mot de passe.
2. Démarrer Notepad (depuis 'Programmes' → 'Accessoires').
3. Appuyer sur Ctrl+Alt+A depuis Notepad. Le nom d'utilisateur et le mot de passe seront saisis dans Notepad.

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

Comment ça marche ? - 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 'Intégration') : 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.

Les associations complètent le titre de l'entrée de KeePass.

Toute association spécifiée sera utilisée en plus au titre de l'entrée de KeePass pour déterminer une correspondance.
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'environement, 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**
+	{+}
%	{%}
^	{^}
~	{~}
(,)	{(}, {)}
[,]	{[}, {]}
{, }	{{}, {}}

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*}	Envoie 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.

Syntaxe de commande	Action
{VKEY *X F*}	Envoie la touche virtuelle de valeur *X* ; cf. ci-dessous.

{VKEY *X F*}:
cette commande envoie la touche virtuelle de valeur *X*. Le paramètre *F* est optionnel et pourrait être une combinaison des valeurs suivantes :

- **E**: " Envoie une touche étendue ; cf. ci-dessous.
- **N**: Envoie une touche non-étendue ; cf. ci-dessous.
- **D** : Appuyer et tenir enfoncée la touche (sans la relâcher).
- **U**: Relâcher la touche (sans la presser).

Les valeurs E et N sont exclusives mutuellement. Il est recommandé de spécifier ni E ni N, si possible ; KeePass détermine alors automatiquement si la touche virtuelle est typiquement réalisée en utilisant une touche étendue.

Les valeurs D et U sont mutuellement exclusives. Si ni D ni U est spécifié, alors KeePass envoie une touche pressée (c'est-à-dire bas et haut).

Sur les systèmes Linux, KeePass convertit automatiquement la plupart des codes de touche virtuelle Windows vers des codes de touche Linux (c'est-à-dire : la commande{VKEY ...} fonctionne sur les deux systèmes à la fois).

Exemples :

- {VKEY 13}
  Appuie et relâche la touche Entrée primaire. Ceci est équivalent à {ENTER}.
- {VKEY 13 E}
  Appuie et relâche la touche Entrée du pavé numérique.
- {VKEY 91 D}e{VKEY 91 U}
  Envoie Win+E (c'est-à-dire qu'il presse et maintient appuyer la touche Win de gauche, appuie et relâche la touche E, et relâche la touche Win), qui exécute l'explorateur de fichiers de Windows (sur Windows). Ceci n'est pas équivalent à {LWIN}e (qui d'abord appuie et relâche la touche Win de gauche puis appuie et relâche la touche E).
  Remarquer que l'explorateur de fichiers de Windows peut également être démarré en utilisant {CMD:/Explorer.exe/W=0/} (le paramètre substituable {CMD:/.../} peut arbitrairement exécuter des lignes de commande).

N'utilisez pas la commande {VKEY ...} pour changer l'état des modificateurs Maj, Ctrl et Alt. Pour ceci, utilisez +, ^ et % à la place (voir ci-dessus).
Les touches et les touches spéciales (pas les paramètres substituables ni les commandes) peuvent être répétées en ajoutant un nombre dans le code. Par exemple : {TAB 5} appuie la touche Tabulation 5 fois.
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 basculée 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 caractères génériques peuvent également apparaître au milieu des motifs. Par exemple : `*Windows*Explorer*` correspondrait à `Windows Internet Explorer`.

De plus, la correspondance utilise la prise en charge d'expressions régulières. Afin d'indiquer à KeePass que le motif est une expression régulière, on l'entoure entre `//`. Par exemple : `//B.?g Window//` correspondrait à `Big Window`, `Bug Window` et `Bg Window`.
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).

Par défaut, les entrées héritent de la séquence de saisie automatique du groupe auquel elles appartiennent. Les groupes héritent également de la séquence de saisie automatique de leurs groupes parents. Il n'y a qu'un seul groupe au top (le premier groupe contient tous les autres groupes). Par

conséquent, si vous modifiez la séquence de saisie automatique de ce tout premier groupe, alors tous les autres groupes et leurs entrées utiliseront cette séquence. En pratique, il s'agit d'une dérogation globale. Pour le changer, faites un clic droit sur le premier groupe, choisissez *'Modifier un groupe...'* et passez à l'onglet *'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 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.

L'obfuscation de la saisie automatique

L'obfuscation de la saisie automatique à deux canaux

Description de la fonction d'obfuscation de la saisie automatique à deux canaux dans KeePass 2.x.

- Informations pour les utilisateurs :
  - Introduction : qu'est-ce que l'obfuscation de la saisie automatique à deux canaux ?
  - Quand peut-on utiliser l'obfuscation de la saisie automatique à deux canaux ?
  - Comment activer/configurer l'obfuscation de la saisie automatique à deux canaux ?
- Informations techniques :
  - Aperçu technique
  - En divisant le texte intelligemment
  - En divisant les secrets

Introduction : qu'est-ce que l'obfuscation de la saisie automatique à deux canaux ?

La fonction de saisie automatique de KeePass est très puissante : elle envoie des touches pressées simulées aux autres applications. Cela fonctionne avec toutes les applications Windows et pour les applications cibles, il est impossible de faire la distinction entre des touches réellement pressées et celles simulées par la saisie automatique. C'est en même temps le principal inconvénient de la saisie automatique, car les enregistreurs de frappe peuvent écouter les touches simulées. C'est à ce moment

qu'entre en jeu l'obfuscation de la saisie automatique à deux canaux.

L'obfuscation de la saisie automatique à deux canaux rend les standards d'enregistreurs de frappe inutiles. Ils utilisent le presse-papiers de Windows pour transférer des parties de texte saisies automatiquement dans l'application cible. Les enregistreurs de frappe peuvent voir les touches Ctrl+V pressées, mais n'enregistrent pas le contenu actuellement copié depuis le presse-papiers.

L'espionnage du presse-papiers ne fonctionne plus non plus, parce que seulement les parties de l'information sensible sont transférées de cette manière.

Qu'importe, ils ne sont pas parfaitement sécurisés (et malheureusement ils ne peuvent l'être en théorie). Aucun des enregistreurs de frappe actuels ou espions de presse-papiers actuellement disponible ne peut écouter un processus de saisie automatique obfusquée, mais il est théoriquement possible d'écrire une application d'espionnage dédiée à la journalisation de la saisie automatique obfusquée.

Quand peut-on utiliser l'obfuscation de la saisie automatique à deux canaux ?

L'obfuscation de la saisie automatique à deux canaux ne peut pas être utilisée avec toutes les fenêtres. La/les fenêtre(s) cible(s) doivent prendre en charge les opérations du presse-papiers et la navigation à l'intérieur des contrôles d'édition en utilisant les touches fléchées. De plus, l'interface de l'utilisateur cible ne doit pas contenir de fonctionnalités d'automatisation comme sauter le focus lorsque la longueur maximale d'une zone de texte est atteinte (par exemple : comme cela a été vu dans les boîtes de dialogue d'enregistrement des numéros).

Les règles de base :

- **Peut être utilisée dans :**
  - Les navigateurs.
  - Les programmes Windows avec des zones de texte standardes.
- **Ne peux pas être utilisée dans :**
  - Les applications basées sur la console (terminaux interactifs, etc.).
  - Jeux.

Parce qu'elle ne fonctionne pas avec toutes les fenêtres, c'est une fonction qui adhère à chaque entrée. Vous devez l'activer explicitement sur la page de l'onglet *'Saisie automatique'* de la boîte de dialogue *'Modifier l'entrée...'*.

Comment activer/configurer l'obfuscation de la saisie automatique à deux canaux

Tout ce dont vous avez besoin c'est de cocher la case *"Obfuscation de la saisie automatique à deux canaux"* d'une entrée (onglet 'Saisie automatique' de la fenêtre d'édition d'une entrée) ; KeePass fera le reste.

Aperçu technique

Plutôt que de simplement envoyer des touches pressées simulées vers l'application cible (comme le fait normalement la saisie automatique), la saisie automatique obfusquée fait ceci :

- Elle sauvegarde le contenu actuel du presse-papiers.
- Elle divise intelligemment le texte en plusieurs parties.
- Pour chaque partie : elle vérifie si le presse-papiers peut être utilisé.
  - *Si oui :* alors elle le divise en deux sous-parties (par caractère, comme deux peignes entrelacés à plat). Copie/colle la première partie, fusionne le reste en envoyant des touches pressées.
  - *Si non :* alors, elle l'envoie normalement en utilisant des touches pressées simulées.
- Elle restaure le précédent contenu du presse-papiers.

Ces étapes sont décrites en détail ci-dessous.

En divisant le texte intelligemment

Le texte à envoyer doit tout d'abord être divisé intelligemment. Toutes les parties de la chaîne ne peuvent pas être envoyées en utilisant le presse-papiers : des codes de touche spéciale et des modifications de clé doivent être transmis inchangés à la fonction `SendInput`. Par exemple : regardez la chaîne suivante :

`mymail@myprovider.com{TAB}MyTopSecretPassword{TAB} {TAB}{ENTER}`
Ceci est un exemple de chaîne typique envoyée par KeePass vers une autre application. Premièrement, il saisit l'adresse de messagerie électronique de l'utilisateur, puis une `tabulation`, puis le mot de passe, une `tabulation`, bascule la case à cocher, une autre `tabulation` et finalement, appuie sur la touche `Entrée`.
Cette séquence peut être divisée en les parties suivantes :

```
mymail@myprovider.com
{TAB}
MyTopSecretPassword
{TAB}
' ' (space)
{TAB}
{ENTER}
```

Pour chaque ligne, il est vérifié si le presse-papiers peut être utilisé. Si la ligne contient un '{', '}', '(', ')', '+', '^', '%' ou un whitespace (espace), elle peut seulement être directement envoyée que par la fonction `SendInput`. '+' par exemple presse la touche `Maj`, il ne devrait pas être copier/coller en tant que caractère '+'. Les espaces ne peuvent pas non plus être copiés/collés, parce qu'ils sont habituellement utilisés pour cocher les cases.

Dans l'exemple ci-dessus, "mymail@myprovider.com" et "MyTopSecretPassword" peuvent être envoyés en utilisant le presse-papiers.

En divisant les secrets

Transférons "mymail@myprovider.com" à l'application cible en utilisant de l'obfuscation de la saisie automatique à deux canaux.

Premièrement, la chaîne secrète "mymail@myprovider.com" est aléatoirement divisée en caractères dans deux parties comme deux peignes qui s'entrelacent à plat :

```
 y  il m   o  d  .c
m ma  @ ypr vi er  om
```

La première chaîne "yilmod.c" est maintenant copiée vers le presse-papiers. La chaîne qui doit être envoyée par la fonction `SendInput` est maintenant assemblée comme suit :

- Elle commence par coller depuis le presse-papiers : `^v`.
- Elle appuie la touche ← *n* fois, avec *n* = *longueur de la chaîne du presse-papiers*.
- Elle envoie les caractères restants et appuie la touche → pour garder ceux qui sont déjà collés depuis le presse-papiers.

Dans notre exemple ci-dessus, la séquence de touches serait assemblée pour :

`^v{LEFT 8}m{RIGHT}ma{RIGHT}{RIGHT}@{RIGHT}ypr{RIGHT}vi{RIGHT}er{RIGHT}{RIGHT}om`
Ceci collera premièrement le contenu du presse-papiers, ira à son début et remplira les caractères restants, reconstruisant la chaîne d'origine "mymail@myprovider.com".

Le temps de rétention dans le presse-papiers pour la première partie de chaîne est minimal. Il est copié vers le presse-papiers, collé dans l'application cible et immédiatement effacé. Ce processus ne prend habituellement que quelques millisecondes au maximum.

En savoir plus sur la division de chaîne secrète :
Dans l'exemple ci-dessus, la chaîne "mymail@myprovider.com" a été divisée et envoyée. Si la chaîne était divisée différemment à chaque fois, alors une application malveillante pourrait rassembler la chaîne en capturant plusieurs saisies automatiques en les combinant. Afin d'éviter cela, KeePass initialise le générateur de nombre aléatoire pour la division basée sur un hachage de la chaîne. Ceci signifie que chaque chaîne est divisée différemment, mais les parties de la chaîne sont déterminées de manière unique. Donc, en invoquant plusieurs fois la saisie automatique, un attaquant ne peut pas rassembler la chaîne d'origine, parce qu'il capture toujours la même moitié.

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 subsituable `{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 prendre en charge le chemin du fichier clé, ou le nom du greffon fournisseur de clé, le paramètre `-keyfile:` existe. Les mêmes règles qu'au-dessus s'appliquent, spécifiez juste le fichier clé/fournisseur, exemple : `-keyfile:D:\pwsafe.key`. Vous devez également mettre entre doubles quotes la valeur, si elle contient des caractères d'espace, tabulation ou autres whitespace.

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:\Mes Documents\BaseDeDonnees.kdbx" -preselect:C:\pwsafe.key`
KeePass montrera alors une invite pour la clé principale de la base de données, dans laquelle la liste de fichiers clé/fournisseur, le fichier `C:\pwsafe.key` est déjà sélectionné. Quand on utilise le paramètre `-preselect:`, par défaut KeePass 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 dans la boîte de dialogue de la clé principale pour vous et affiche l'invite de connexion (ouverture de session). 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 bogue dans Mono).

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

De plus, le paramètre `-useraccount` est pris en charge. S'il est spécifié, l'accréditation (credentials) du compte utilisateur courant sera utilisée. L'accréditation, ce n'est pas seulement le mot de passe. Vous pouvez penser à sa clé cryptographique qui est chiffrée que l'utilisateur fourni pour son logon (mot de passe, carte à puce, etc.).

Le paramètre `-iocredfromrecent` engendre que KeePass charge le fichier des mots de passe

système (pas la clé de la base de données) depuis la plus récente liste de fichiers utilisés. Autrement, le fichier des mots de passe système peut être spécifié en utilisant les paramètres `-iousername:` et `-iopassword:`. Le paramètre optionnel `-ioiscomplete` indique à KeePass que le chemin et le fichier des mots de passe système sont complets (la boîte de dialogue 'Ouvrir adresse (URL)' ne sera alors pas affichée).

L'option `-entry-url-open` engendre que les autres instances de KeePass ouvertes cherchent une entrée et ouvre son adresse (URL). L'entrée est identifiée par son UUID, que vous pouvez passer comme paramètre `-uuid:` de ligne de commande.

L'option `-auto-type-password` est similaire à `-auto-type`, mais saisit automatiquement seulement le mot de passe de l'entrée correspondante. `-auto-type-selected` accompli la saisie automatique pour l'entrée en cours de sélection.

Dans le premier cas, KeePass recherche une entrée correspondante (basée sur le titre de la fenêtre cible) et saisit automatiquement seulement son mot de passe (indépendant de toute séquence de saisie automatique associée avec la fenêtre). Dans le second cas, l'entrée actuellement sélectionnée (dans la liste des entrées de la fenêtre principale) est utilisée, et la même logique pour la détermination de la séquence automatique est utilisée comme une saisie automatique régulière.

L'option `-cancel` implique que toutes les autres instances de KeePass annulent l'ouverture/enregistrement d'un fichier base de données.

Le chemin du fichier de la configuration locale peut être modifié en utilisant le paramètre `-cfg-local:` de la ligne de commande.

Si l'option `-debug` est spécifiée, des messages d'erreur sont plus détaillés. Veuillez remarquer que les messages d'erreur plus détaillées peuvent contenir des données sensibles (exemple : les mots de passe).

L'ordre des arguments est arbitraire.

Exemple d'utilisation

Ouvrez le fichier de la base de données *'C:\Mes 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:\Mes 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:\Mes Documents\BaseDeDonnees.kdbx" -pw:abc
```

Si votre clé USB se monte toujours sur le lecteur F: et que vous avez 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:\Mes 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:\Mes 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:\Mes 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 ..\BaseDeDonnees.kdbx -pw:MonMDPSecret
```

Cette commande `START` exécutera KeePass (qui ouvre le fichier `..\BaseDeDonnees.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 remplacement d'adresse (URL) (2.x)

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

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

Les remplacement d'URL sont stockés dans le fichier configation imposée. Pour toutes les options de la ligne de commande ci-dessus excepté '`-get-urloverride`', un contrôle de compte utilisateur est affiché, si nécessaire.

La configuration

La configuration

Les détails à propos de comment et où KeePass enregistre sa configuration ?

- Général

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 XML.

Configuration	Emplacement	Chemin de fichier typique
Global	Répertoire de l'application	C:\Program Files\KeePass Password Safe 2\KeePass.config.xml
Global (Virtualisé)	Windows Virtual Store	C:\Users*Nom d'utilisateur*\AppData\Local\VirtualStore\Program Files\KeePass Password Safe 2\KeePass.config.xml
Local	Données de l'application de l'utilisateur	C:\Users*Nom d'utilisateur*\AppData\Roaming\KeePass\KeePass.config.xml
Forcée	Répertoire de l'application	C:\Program Files\KeePass Password Safe 2\KeePass.config.enforced.xml

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 essayera de sauvegarder sa configuration dans le répertoire de l'application. Aucun paramètre de configuration ne 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 : la configuration imposée

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.

Réactivation des éléments nécessitant une imposition (2.x)

Certains éléments de fonctionnalités sont enregistrés dans le fichier de configuration imposée. Sous certaines conditions, il pourrait y avoir de tels articles seulement dans le fichier de configuration habituel (par exemple, lorsque vous copiez le fichier de configuration habituel sur un nouveau PC, mais pas celui imposé). Si vous souhaitez continuer à utiliser les éléments, vous devez les réactiver. Cela peut nécessiter l'autorisation de l'administrateur ; KeePass affiche une boîte de dialogue de contrôle du compte d'utilisateur, si nécessaire.

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

- Les déclencheurs :
  Si vos déclencheurs ne sont pas stockés dans le fichier de configuration imposée, 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 du 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 remplacements d'adresse (URL) globale :
  Si vos remplacements d'adresse globale ne sont pas stockés dans le fichier de configuration imposée, alors KeePass les désactive (individuellement ; par conséquent, il est recommandé de mémoriser les remplacements que vous avez activés, par ex. en prenant une capture d'écran). Si vous souhaitez continuer à utiliser vos remplacements, ouvrez la boîte de dialogue « Les remplacements d'adresse (URL)... » (via l'élément de menu principal 'Outils' → 'Options...' → onglet 'Intégration' → bouton « Remplacements d'adresse (URL)... »), cochez tous les remplacements souhaités (en ce qui concerne la sécurité, la confidentialité, la fonctionnalité, la compatibilité, etc.), activez-les et cliquez sur le bouton "OK".
- Les profils du générateur de mots de passe :
  Si vos profils de générateur de mots de passe ne sont pas stockés dans le fichier de configuration imposé, alors KeePass les désactive. Si vous souhaitez continuer à utiliser vos profils, alors ouvrez la boîte de dialogue « Générateur de mot de passe » (via l'élément de menu principal 'Outils' → 'Générer un mot de passe...'), cliquez sur le bouton de bouclier (en haut à droite) et vérifiez 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 de 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 du fichier de configuration imposée. S'il est trouvé, alors

on utilise celui-ci.

- Si l'indicateur `PreferUserConfiguration` est à *true*, alors on utilise l'élément depuis le fichier de configuration locale, sinon on utilise celui qui est global. Si le fichier de configuration choisi n'existe pas ou ne contient pas l'élément, alors on utilise la valeur par défaut.

Enregistrement :

- Si l'indicateur `PreferUserConfiguration` est à *true*, alors on essaye d'enregistrer tous les éléments de configuration dans le fichier de configuration locale. Si ceci échoue, alors on envoie une erreur et on essaye de les enregistrer dans le fichier de configuration globale. Si ceci échoue, alors il y a un rapport d'erreur.
- Si l'indicateur `PreferUserConfiguration` est à *false*, alors on essaye d'enregistrer toute la configuration dans le fichier de configuration globale. Si ceci échoue, alors on envoie une erreur et on essaye de les enregistrer dans le fichier de configuration locale. Si ceci échoue, alors il y a un rapport d'erreur.

Le chemin du fichier de configuration local peut être modifié en utilisant le paramètre '`-cfg-local:`' de la ligne de commande.

Les réferences 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

0	Les autres chaînes personnalisées *(seulement KeePass 2.x)*

La partie *Texte* est la chaîne recherchée, qui décrit le ou les textes qui doivent apparaître dans le champ spécifié d'une entrée pour correspondre.

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 46C9B1FFBD4ABC4BBB260C6190BAD20C comme UUID.

Le référencement des champs des autres entrées ne fonctionne qu'avec les champs standards, pas avec des chaînes utilisateur personnalisées. Si vous souhaitez référencer une chaîne utilisateur personnalisée, alors vous devez placer une redirection dans un champ standard de l'entrée avec la chaîne personnalisée, en utilisant `{S:<Nom>}`, et la référence du champ standard.

Des chaînes personnalisées peuvent être référencées localement (c'est-à-dire à l'intérieur d'une entrée) en utilisant `{S:<Nom>}`, cf. la page paramètres substituables pour les détails.

Vous pouvez utiliser le code 0 pour que KeePass recherche dans la base de données des champs de chaîne personnalisée (pour identifier l'entrée source référencée), mais 0 ne peut pas être utilisé pour récupérer des données depuis des champs personnalisés (c'est-à-dire que le code ne peut pas être utilisé comme *ChampSouhaité*).

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**, **Mozilla Firefox**, **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

Malheureusement, il n'y pas de format de base de données de mots de passe 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 sont différents depuis les noms de champ d'entrée afin d'assurer une compatibilité avec certaines autres applications.

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 quotés 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 !

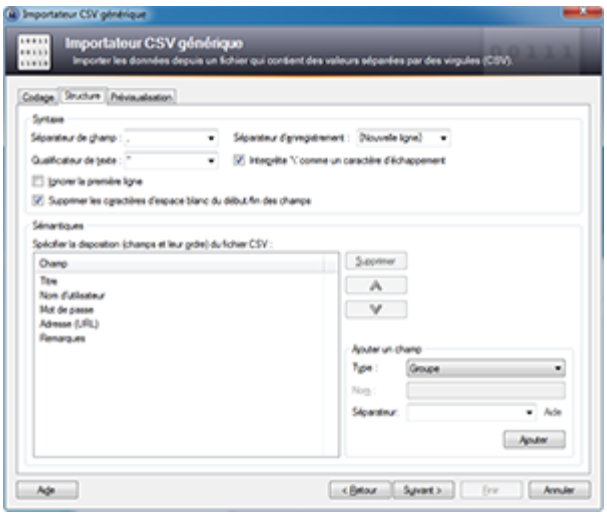
Remarques importantes à propos du format :

- 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 une 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 encodées 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 (en fonction 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 de 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 le *'RoboForm Editor'* (dans les anciennes versions de Roboform, c'était nommé *'Passcard Editor'* ou *'Edit Passcards'*). Cliquer 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'*, spécifiez un emplacement et cliquer le bouton *'Save'*.
2. Dans KeePass, ouvrir votre fichier de base de données KeePass 2.x et cliquer *'Fichier'* → *'Importer'*. Choisir *'RoboForm HTML'* comme format, sélectionner le fichier HTML que vous venez juste de sauvegarder et cliquer le bouton *'OK'*.. Pour réaliser ceci, ouvrir *l'éditeur Passcard* de RoboForm (*'Edit Passcards'* ou *'RoboForm Editor '* dans le menu Démarrer de Windows) et aller dans le menu principal de *l'éditeur allez à 'Passcard'* → *'Print List'* (dans les plus récentes versions vous devez cliquer sur le bouton *'RoboForm'* et aller dans *'Print List'* → *'Logins'*). Dans la boîte de dialogue qui s'ouvre, cliquez sur le bouton *'Save'*. Choisissez un emplacement et un nom de fichier, puis cliquez sur *'Save'*.
3. Ouvrez votre fichier de base de données dans votre KeePass 2.x et allez dans *'Fichier'* → *'Importer...'*. Choisissez *'RoboForm HTML'* comme format et sélectionnez le fichier HTML que vous venez juste d'exporter, puis cliquez sur *'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, démarrez 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, basculez sur KeePass 2.x et ouvrez votre base de données KeePass. Cliquez sur *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 propriétés des groupes parents (icônes, remarques, paramètres de saisie automatique, etc.) sont exportées, si le format de fichier 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.

- **Groupe racine**
  - Groupe 1
    - Groupe 1.1
    - Groupe 1.2
  - Groupe 2

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-t-il dans votre environnement de système d'exploitation ?

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

Le raccourci clavier global pour restaurer la fenêtre 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 appuyez sur le raccourci clavier global pour restaurer la première instance qui a été démarrée.

Le raccourci clavier global est Ctrl+Alt+K.

Le raccourci clavier global peut être librement modifié vers une combinaison de touches différentes (ou désactivé) sur l'onglet 'Intégration' de la boîte de dialogue 'Options...' du menu 'Outils' de la barre de menu principal.

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.

KeePass 2.x peut ouvrir de multiples bases de données sur une instance/fenêtre (une barre d'onglets apparaît, qui vous permet de commodément basculer entre les bases de données).

Quand plusieurs bases de données sont ouvertes dans une instance et que vous appuyez sur le raccourci clavier de saisie automatique globale, alors la saisie automatique recherche dans toutes les bases de données ouvertes pour l'entrée correspondante. Remarquer que seule une instance de KeePass peut enregistrer le raccourci clavier global ; donc quand vous désactivez l'option à une seule instance et ouvrez des bases de données dans différentes instances, alors seulement la première instance recherche pour des entrées correspondantes quand la saisie automatique globale est invoquée, pas les autres.

La clé principale

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 stockés 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 antivirus, etc.).

KeePass possède une option pour se souvenir des chemins des fichiers clés, 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 que 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, 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 stockée 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 clés. 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 certaines 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.

Afin de réutiliser un fichier clé existant, cliquez sur le bouton 'Parcourir...' dans la boîte de dialogue de création de la clé principale.

Le compte utilisateur Windows

KeePass peut rendre la base de données dépendante du compte courant de l'utilisateur Windows. Si vous activez cette option, alors vous pouvez seulement ouvrir la base de données que quand vous êtes connectés en tant que même utilisateur Windows qui a créé la base de données.

⚠ Faites très attention en utilisant cette option. Si votre compte utilisateur Windows venait à être supprimé, alors vous ne pourriez plus du tout ouvrir votre base de données KeePass. De plus, quand vous utilisez cette option chez vous et que votre ordinateur tombe en panne (par exemple : un disque dur endommagé), alors il ne suffit pas de créer simplement un nouveau compte Windows sur la nouvelle installation avec le même nom et mot de passe ; vous devez copier le compte *complet* (c'est-à-dire SID, etc.). Ce n'est pas une tâche simple, par conséquent si vous ne savez pas faire ceci, alors il est fortement recommandé que vous n'activiez pas cette option. Des instructions détaillées sur, " Comment retrouver un compte utilisateur Windows ? ", peuvent être trouvées ici : Recover Windows User Account Credentials' (un court tutoriel technique peut être trouvé dans un article TechNet de Microsoft : 'How to recover a Vault corrupted by lost DPAPI keys)'.

Vous pouvez modifier le mot de passe du compte de l'utilisateur Windows à volonté ; cela n'affecte pas la base de données de KeePass. Remarquer qu'en *changeant* le mot de passe (par exemple : un utilisateur en utilisant le panneau de configuration ou en appuyant sur Ctrl+Alt+Suppr. et en sélectionnant 'Modifier le mot de passe') et en le *réinitialisant* à un nouveau (par exemple : un administrateur utilisant la commande `NET USER <Utilisateur> <NouveauMotDePasse>`) sont deux choses différentes. Après avoir *changé* votre mot de passe, vous pouvez toujours ouvrir votre base de données KeePass. Quand on *réinitialise* le mot de passe à un nouveau, habituellement l'accès n'est plus possible (parce que les clés DPAPI de l'utilisateur sont perdues), mais il existe des exceptions (par exemple : quand l'utilisateur est dans un domaine, Windows peut retrouver les clés DPAPI de l'utilisateur depuis le contrôleur de domaine, ou un utilisateur chez soi peut utiliser un disque de réinitialisation de mot de passe précédemment créé). Des détails peuvent être trouvés dans l'article MSDN 'Windows Data Protection' et dans l'article de support 'How to troubleshoot the Data Protection API (DPAPI)'.

Si vous décidez d'utiliser cette option, alors il est fortement recommandé de ne pas compter exclusivement dessus, mais d'utiliser en plus l'une des autres deux options (mot de passe et fichier clé).

Au lieu de sauvegarder le compte utilisateur Windows, vous pouvez alternativement créer une sauvegarde non *chiffrée* de la clé en utilisant 'l'utilitaire de sauvegarde et de restauration du compte utilisateur Windows'. Une telle sauvegarde n'est pas chiffrée, elle doit être stockée dans un emplacement sécurisé.
Chaque fois que l'utilisateur tente d'ouvrir la base de données, KeePass déprotège la clé (à l'aide de DPAPI) et utilise le résultat dans le cadre de la clé principale.

La protection en utilisant des comptes utilisateur n'est pas prise en charge sous Windows 98/ME.

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 du nœud `Security/MasterPassword/MinimumLength` spécifie la longueur minimale du mot de passe maître (en caractères). Par exemple : en le positionnant à `10`, alors KeePass n'acceptera que les mots de passe maîtres qui comprennent au moins 10 caractères.

La valeur du nœud `Security/MasterPassword/MinimumQuality` spécifie la qualité minimale estimée (en bits) que les mots de passe maîtres doivent avoir. Par exemple : en le positionnant à`80`, alors seuls les mots de passe avec une qualité estimée d'au moins 80 bits seront acceptés.

Les nœuds `Security/MasterKeyExpiryRec` et `Security/MasterKeyExpiryForce` peuvent être positionnés à une date XSD ou une durée XSD (cf. XSD Date and Time Data Types). Si la clé principale n'a pas été modifiée depuis la date spécifiée ou que le temps qui s'échelonne entre maintenant et la dernière modification de la clé principale dépasse la durée spécifiée, alors KeePass recommande/force de/à la modifier. Ces paramètres s'appliquent à toutes les bases de données qui sont

ouvertes avec cette instance de KeePass ; une expiration de clé principale peut également être configurée pour chaque base de données individuellement (dans 'Fichier' → 'Paramètres de la base de données' → onglet 'Avancé').

En spécifiant `KeyCreationFlags` et/ou `KeyPromptFlags` (dans le nœud `UI`), vous pouvez forcer les états (activé, désactivé, vérifié, non vérifié) des contrôles de source de clé dans les boîtes de dialogue de création de la clé principale et d'invite. Ces valeurs peuvent être des combinaisons au niveau du bit d'un ou plusieurs des flags suivants :

Flag (Hex)	Flag (Dec)	Description
0x0	0	Ne pas forcer d'état (par défaut).
0x1	1	Activer mot de passe.
0x2	2	Activer fichier clé.
0x4	4	Activer le compte utilisateur.
0x8	8	Activer le bouton 'masquer mot de passe'.
0x100	256	Désactiver le mot de passe.
0x200	512	Désactiver le fichier clé.
0x400	1024	Désactiver le compte utilisateur.
0x800	2048	Désactiver le bouton 'masquer mot de passe'.
0x10000	65536	Vérifier le mot de passe.
0x20000	131072	Vérifier le fichier clé.
0x40000	262144	Vérifier le compte utilisateur.
0x80000	524288	Vérifier l'option/bouton 'masquer mot de passe'.
0x1000000	16777216	Ne pas vérifier le mot de passe.
0x2000000	33554432	Ne pas vérifier le fichier clé.
0x4000000	67108864	Ne pas vérifier le compte utilisateur.
0x8000000	134217728	Ne pas vérifier l'option/bouton 'cacher le mot de passe'.

Les valeurs de `KeyCreationFlags` et `KeyPromptFlags` doivent être spécifiées en notation décimale.

Par exemple : si vous forcez l'utilisation de l'option du compte utilisateur, alors vous pourriez vérifier et désactiver le contrôle (de telle sorte que l'utilisateur ne pourrait plus ne pas le vérifier) en spécifiant 263168 comme valeur (0x40000 + 0x400 = 0x40400 = 263168).

Utilisateurs multiples

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

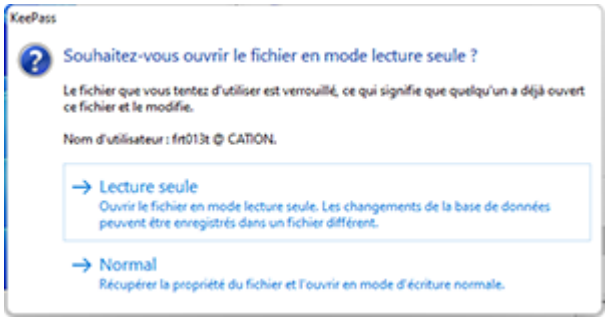
Les informations générales à propos des bases de données partagées

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).

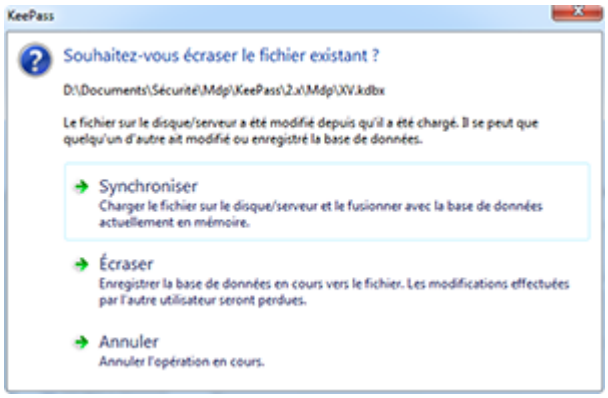
KeePass 1.x ne fournit pas de synchronisation, c'est-à-dire qu'en enregistrant la base de données vous enregistrez les données courantes sur le disque. Si un autre utilisateur a entre-temps modifié une entrée (c'est-à-dire depuis que vous avez chargé la base de données), ses changements sont écrasés.

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 générateur 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 substitutions 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 caractère hexadécimal	0123456789 abcdef
H	Majuscules en caractère hexadécimal	0123456789 ABCDEF
l	Lettres en minuscules	abcdefghijklmnopqrstuvwxyz
L	Lettres à casse mixte	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz
u	Lettres en majuscules	ABCDEFGHIJKLMNOPQRSTUVWXYZ
v	Voyelles en minuscules	aeiou
V	Voyelles à casse mixte	AEIOU aeiou
Z	Voyelles en majuscules	AEIOU
c	Consonnes en minuscules	bcdfghjklmnpqrstvwxyz

c	Consonnes à casse mixte	BCDFGHJKLMNPQRSTVWXYZ bcdfghjklmnpqrstvwxyz
z	Consonnes en majuscules	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 motifs 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}`

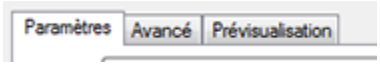
Les options réduisant la sécurité

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 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 de réduction de sécurité alors un point d'exclamation (!)
est ajouté à l'onglet *'Avancé'*.



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 de l'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 ne sont pas 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 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 de l'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

Des chaînes personnalisées peuvent être référencées en utilisant {S:*Nom*}. Par exemple : si vous avez une chaîne personnalisée nommée "Courriel", alors vous pouvez utiliser le paramètre substituable {S:Courriel}.

Le paramètre substituable	Valeur
{URL:RMVSCM}	L'adresse (URL) de l'entrée sans le nom du protocole (scheme).
{URL:SCM}	Le protocole de l'adresse (URL) de l'entrée.
{URL:HOST}	Le composant d'hôte de l'adresse (URL) de l'entrée.
{URL:PORT}	Le numéro de port de l'adresse (URL) de l'entrée.
{URL:PATH}	Le composant du chemin de l'adresse (URL) de l'entrée.
{URL:QUERY}	La recherche d'informations sur l'adresse (URL) de l'entrée.
{URL:USERINFO}	L'information de l'utilisateur de l'adresse (URL) de l'entrée.
{URL:USERNAME}	Le nom d'utilisateur de l'adresse (URL) de l'entrée.
{URL:PASSWORD}	Le mot de passe de l'adresse (URL) de l'entrée.
{UUID}	L'UUID de l'entrée (32 caractères hexadécimaux).

Un exemple pour les paramètres substituables {URL:...} se trouve ci-dessous.

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
{GROUP}	Le nom du groupe parent de l'entrée.
{GROUP_PATH}	Le chemin complet du groupe parent de l'entrée.
{GROUP_NOTES}	Les remarques du groupe parent de l'entrée.
{GROUP_SEL}	Le nom du groupe actuellement sélectionné dans la fenêtre principale.
{GROUP_SEL_PATH}	Le chemin complet du groupe actuellement sélectionné dans la fenêtre principale.
{GROUP_SEL_NOTES}	Les remarques du groupe actuellement sélectionné dans la fenêtre principale.
{DB_PATH}	Le chemin complet de la base de données actuelle.
{DB_DIR}	Le répertoire de la base de données actuelle.
{DB_NAME}	Le nom du fichier (y compris son extension) de la base de données actuelle.
{DB_BASENAME}	Le nom du fichier (sans son extension) de la base de données actuelle.
{DB_EXT}	L'extension du nom du fichier de la base de données actuelle.
{ENV_DIRSEP}	Le séparateur de répertoire ('\' sous Windows, '/' sous Unix).
{ENV_PROGRAMFILES_X86}	Il s'agit de `%ProgramFiles(x86)%`, s'il existe, sinon `%ProgramFiles%`.

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

Paramètre substituable	Valeur
{T-REPLACE-RX:*/Texte/Recherche/Remplace/*}	Recherche l'expression régulière *Recherche* dans *Texte* et remplace toutes correspondances par *Remplace*. Cf. ci-dessous.
{T-CONV:*/Texte/Type/*}	Converti *Texte* en *Type*. Cf. ci-dessous.

{T-REPLACE-RX:*/Texte/Recherche/Remplace/*} – Remplacer à l'aide d'une expression régulière :
Ce paramètre substituable recherche l'expression régulière *Recherche* dans *Texte* et remplace toutes les correspondances par *Remplace*.

Tous les paramètres sont compilés par Spr, c'est-à-dire que des paramètres substituables peuvent être utilisés en leur sein.

Le premier caractère après le premier ':' spécifie le caractère séparateur. Tout caractère excepté '}' peut être utilisé comme caractère séparateur. Il ne doit pas apparaître dans les paramètres. Par exemple : {T-REPLACE-RX:/A/B/C/} et {T-REPLACE-RX:!A!B!C!} sont équivalents. Le dernier caractère séparateur (avant le '}') est requis.

Exemple d'utilisation : laissez le champ du nom de l'utilisateur contenir l'adresse de messagerie électronique '`monnom@exemple.com`' et le champ de l'adresse (URL) '`{T-REPLACE-RX:!{USERNAME}!.*@(.*)!https://$1!}`'. Quand on exécute le champ Adresse (URL), KeePass ouvre '`https://exemple.com`'.

`{T-CONV:/`*`Texte`*`/`*`Type`*`/}` – Convertir :
Ce paramètre substituable convertit *Text* en *Type*.

Tous les paramètres sont compilés par Spr, c'est-à-dire que les paramètres substituables peuvent être utilisés en leur sein.

Les types pris en charge sont :

- **Upper** ou **U**:
  Majuscule.
- **Lower** ou **L**:
  Minuscule.
  Exemple : laissez le nom d'utilisateur d'une entrée être '`Bob`' et l'adresse (URL) '`https://exemple.com/?user={T-CONV:/{USERNAME}/L/}`'. Quand on exécute l'adresse (URL), KeePass ouvre '`https://exemple.com/?user=bob`'.
- **Base64**:
  Le codage Base64 de la représentation UTF-8 du texte.
- **Hex**:
  Le codage hexadécimal de la représentation UTF-8 du texte.
- **Uri**:
  La représentation URI-escaped du texte.
- **Uri-Dec**:
  La représentation URI-unescaped du texte.
- **Raw**:
  Spr compile *Texte* sans encoder le résultat pour le contexte actuel.
  Exemple : Laissons le nom d'utilisateur d'une entrée être '+'. La séquence de saisie automatique '`{USERNAME}a`' donne pour résultat dans le texte '+a', tandis que la séquence de saisie automatique '`{T-CONV:/{USERNAME}/Raw/}a`' donne pour résultat dans le texte 'A' (parce que ce paramètre substituable insère '+' dans la séquence de saisie automatique sans l'encoder, et que '+a' signifie appuyer sur `Maj`+`A`, qui donne pour résultat dans le texte '`A`').
  Le paramètre substituable {T-CONV:...} avec le type 'Raw' ne fonctionne habituellement qu'avec la séquence de saisie automatique, et pas avec les champs de donnée. Ceci pourrait changer dans le futur.

Les autres paramètres substituables

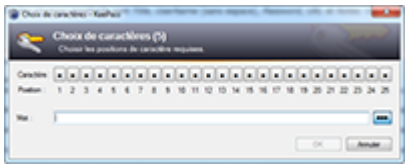
Paramètre substituable	Valeur
`{PASSWORD_ENC}`	Le mot de passe dans sa forme chiffrée. See ci-dessous.

Paramètre substituable	Valeur/Action
`{PICKCHARS}` `{PICKCHARS:`*`Fld`*`:`*`Opt`*`}`	Affiche une boîte de dialogue pour sélectionner certains caractères dans une chaîne d'entrée. Cf. ci-dessous.
`{PICKFIELD}`	Affiche une boîte de dialogue pour choisir un champ dont la valeur sera insérée.
`{NEWPASSWORD}`	Génère un nouveau mot de passe.

{NEWPASSWORD:*/Profile/.../*}	Cf. ci-desssous.
{HMACOTP}	Génère un mot de passe à usage unique basé sur HMAC. Cf. ci-dessous.
{TIMEOTP}	Génère un mot de passe à usage unique basé sur le temps. Cf. ci-dessous.
{C:*Commentaire*}	Commentaire ; est retiré.
{BASE} {BASE:RMVSCM} {BASE:SCM} {BASE:HOST} {BASE:PORT} {BASE:PATH} {BASE:QUERY} {BASE:USERINFO} {BASE:USERNAME} {BASE:PASSWORD}	À l'intérieur d'un remplacement d'adresse (URL), chacun de ces paramètres substituables est remplacé par la partie spécifiée de la chaîne qui est remplacée. Cf. ci-dessous.
{CLIPBOARD}	Obtient le contenu du presse-papiers (texte).
{CLIPBOARD-SET:*/Texte/*}	Copie *Texte* dans le presse-papiers.
{CMD:*/LigneCommande /Options/*}	Exécute une ligne de commande. Cf. ci-dessous.

{PASSWORD_ENC} – Le chiffrement des mots de passe :
Le paramètre substituable {PASSWORD_ENC} est remplacé par le mot de passe de l'entrée actuelle sous forme chiffrée. Le mot de passe est chiffré à l'aide de l'accréditation de l'utilisateur Windows actuel. 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` (cf. la page Le champ d'adresse (URL) pour un exemple de définition d'une URL pour ouvrir une base de données KeePass supplémentaire). Le paramètre substiutuable 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}.

{PICKCHARS} – Choisir des caractères :

Le paramètre substituable {PICKCHARS} affiche une boîte de dialogue, dans laquelle vous pouvez sélectionner des caractères d'une chaîne d'entrée (par exemple : le mot de passe) à certaines positions.

{PICKCHARS} sans aucun paramètre vous permet de sélectionner une quantité arbitraire de caractères depuis le mot de passe de l'entrée.
Une chaîne d'entrée différente peut être spécifiée en ajoutant ':' et le nom du champ ; c'est-à-dire {PICKCHARS:UserName}. Les noms des champs standards sont *Title*, *UserName* (sans espace), *Password*, *URL* et *Notes*. Une chaîne d'entrée personnalisée peut être référencée par son nom (sans le préfixe S:).

De plus, le paramètre substituable prend en charge diverses options (facultatives !). Les options sont ajoutées après le nom du champ, séparées par ':'. Si vous souhaitez spécifier plusieurs options, alors les séparer par une virgule ','. Les options sont des paires clé-valeur, séparées par '='. Les options suivantes sont prises en charge :

- **ID**: spécifie un ID alphanumérique pour le paramètre substituable (cf. ci-dessous).
- **C** ou **Count**: spécifie le nombre de caractères à sélectionner dans la chaîne. Quand suffisamment de caractères ont été choisis, la boîte de dialogue se ferme automatiquement (c'est-à-dire que vous n'avez plus besoin de cliquer manuellement sur [OK]).

- **Hide**: s'il est positionné à *False* (Faux), les caractères choisis dans la boîte de dialogue sont affichés par défaut en texte brut, c'est-à-dire non masqués par des astérisques. Par défaut, KeePass utilise le paramétrage de masquage des mots de passe dans la fenêtre principale.
- **Conv**: Spécifie comment convertir les caractères sélectionnés. Quand le paramètre est omis, aucune conversion n'est accomplie, c'est-à-dire que les caractères sélectionnés sont directement saisis automatiquement. L'option prend en charge les valeurs suivantes :
  - **D**: Convertit les caractères sélectionnés en touches fléchées vers le bas ; par exemple '2', 'c' et 'C' sont convertis en deux touches fléchées vers le bas.

    Un nombre fixe de touches fléchées vers le bas peut être ajouté en les spécifiant à l'aide de l'option **Conv-Offset**. Par exemple : si vous spécifiez `Conv=D, Conv-Offset=1`, alors '2', 'c' et 'C' sont convertis en 3 touches fléchées vers le bas.

    En utilisant l'option **Conv-Fmt**, vous pouvez spécifier la disposition des comboboxes. Par défaut, KeePass suppose qu'une combobox contient les valeurs de 0 à 9 *ou* de A à Z. Si la combobox contient les valeurs 0-9A-Z (c'est-à-dire tout d'abord les dix chiffres, immédiatement suivis par tous les caractères de A à Z), alors spécifiez`Conv=D, Conv-Fmt=0A`. Similairement, s'il contient les valeurs A-Z0-9, alors spécifiez `Conv=D, Conv-Fmt=A0`. Si les chiffres commencent à 1 au lieu de 0 (c'est-à-dire que le 0 apparaît après le 9), alors utilisez `1A` et `A1` au lieu de `0A` et `A0`. Si la combobox contient les valeurs 0-9A-Za-z (c'est-à-dire les caractères sensibles à la casse), alors spécifiez `0Aa`. Toutes les combinaisons de '`0`', 'A', 'a' et '?' sont prises en charge. Si 'A' et 'a' ne sont pas tous les deux spécifiés à la fois, alors les caractères sont traités comme insensibles à la casse. '?' ignore un élément de combobox.

Si vous souhaitez afficher la boîte de dialogue de sélection de caractères plusieurs fois dans une même séquence, alors attribuez des ID différents aux paramètres substituables. Si un ID est spécifié plusieurs fois (ou si aucun ID n'est spécifié et que les paramètres substituables sont les mêmes), alors KeePass affiche la boîte de dialogue de sélection des caractères une fois et réutilise les caractères sélectionnés dans tous les paramètres substituables suivants avec le même ID.

Exemples d'utilisation :

`{USERNAME}{TAB}{PICKCHARS:Password:C=5}{ENTER}`
Tout d'abord, une boîte de dialogue s'affiche dans laquelle l'utilisateur peut choisir exactement 5 caractères depuis le mot de passe d'entrée. Ensuite, KeePass saisit le nom d'utilisateur dans la fenêtre cible, appuie sur Tabulation, tape les 5 caractères choisis et appuie sur Entrée.

`{S:Memorable}{TAB}{PICKCHARS:Password:ID=1, C=1, Conv=D, Conv-Offset=1}{TAB}{PICKCHARS:Password:ID=2, C=1, Conv=D, Conv-Offset=1}{TAB}{PICKCHARS:Password:ID=3, C=1, Conv=D, Conv-Offset=1}{ENTER}`
Tout d'abord, la boîte de dialogue de sélection de caractères s'affiche trois fois et chaque fois, l'utilisateur peut sélectionner exactement un caractère depuis le mot de passe d'entrée. Ensuite, le processus de saisie automatique démarre : KeePass saisit le contenu d'une chaîne d'entrée personnalisée nommée "Memorable" dans la fenêtre cible. Le focus est basculé sur le contrôle suivant en appuyant sur la touche Tabulation, et le premier caractère précédemment sélectionné est converti en touches fléchées vers le bas (avec une touche supplémentaire ; par exemple : un '1' est converti en deux touches fléchées vers le bas). Ceci est répété deux fois de plus avec les autres caractères sélectionnés, et enfin la toucheEntrée est pressée.

Remarquez que cela ne revient pas à choisir trois caractères à la fois. Si vous utilisez `{S:Memorable}{TAB}{PICKCHARS:Password: C = 3, Conv = D, Conv-Offset = 1}`, toutes les touches fléchées vers le bas sont envoyées au même contrôle actuellement actif.

Dans certains navigateurs (par exemple : Opera), mettre le focus sur une combobox peut être lent. Si vous rencontrez des échecs de saisie automatique, envisagez de ralentir les changements de focus (par exemple : en ajoutant `{DELAY 250}` après chaque `{TAB}`, ou en ralentissant toute la séquence, par exemple en ajoutant `{DELAY = 150}`).

{NEWPASSWORD} and {NEWPASSWORD:/*Profil*/.../} – Génération de nouveaux mots de passe :
Le paramètre substituable {NEWPASSWORD} génère un nouveau mot de passe pour l'entrée actuelle, basé sur le profil de générateur 'Mots de passe générés automatiquement pour les nouvelles entrées'.

Ce paramètre substituable est évalué seulement qu'une fois dans un processus de saisie automatique, c'est-à-dire pour une boîte de dialogue typique 'Ancien mot de passe' - 'Nouveau mot de passe' - 'Répéter nouveau mot de passe', vous pouvez utiliser {PASSWORD}{TAB}{NEWPASSWORD}{TAB}{NEWPASSWORD}{ENTER} comme séquence de saisie automatique.

Pour utiliser un profil de générateur de mot de passe différent, utilisez{NEWPASSWORD:/*Profil*/}, où *Profil* est le nom du profil. Si le profil spécifié est introuvable, le profil 'Mots de passe générés automatiquement pour les nouvelles entrées' est utilisé.

- **~**: Lorsque vous spécifiez '~' comme nom du profil (c'est-à-dire lorsque vous utilisez le paramètre substituable {NEWPASSWORD:/~/}), KeePass dérive un profil du mot de passe de l'entrée actuelle. Non recommandé, car la qualité peut se dégrader.
- **#**: Quano on spécifie '#' comme nom de profil, alors vous pouvez spécifier deux paramètres en plus : un modèle de chaîne de caractères et une option.
  - **R**: Spécifie si réarranger/permuter les caractères aléatoirement du mot de passe généré. La valeur par défaut est 0.
    - **0**: Ne pas réarranger.
    - **1**: Réarranger.

  Exemples :
  - {NEWPASSWORD:/#/H\2\-HH\-HH\-HH\-HH\-HH/}
    génère une adressse MAC.
  - {NEWPASSWORD:/#/uldA{17}/R=1/}
    génère un mot de passe alphanumerique d'une longueur de 20 qui contient au moins une capitale, au moins une minuscule et au moins un chiffre (à des positions aléatoires).

Comme avec le paramètre substituable {NEWPASSWORD}, les paramètres substituables {NEWPASSWORD:/.../} sont évalués une seule fois (même quand différent profile/paramètres sont spécifiés).

Les mots de passe à usage unique (OTPs):
KeePass fournit des commandes de menu dans la fenêtre principale pour la génération de mots de passe à usage unique ('Copier OTP basé sur HMAC', 'Montrer OTP basé sur HMAC', 'Copier OTP basé sur le temps', 'Montrer OTP basé sur le temps'). De plus, des mots de passe à usage unique peuvent être générés pendant la saisie automatique en utilisant les paramètres substituables {HMACOTP} et {TIMEOTP}.
Les paramètres pour la génération d'OTP sont enregistrés dans des chaînes de caractères de l'entrée et peuvent être efficacement édités en utilisant la boîte de dialogue 'Les paramètres du générateur OTP...' (qui vérifie les valeurs saisies, affiche une prévisualisation, etc.). Alternativement, vous pouvez directement éditer les chaînes de caractères de l'entrée, tel que documenté ci-dessous.

{HMACOTP} – La génération de mots de passe à usage unique basé sur HMAC :
Le paramètre substituable {HMACOTP} génère un mot de passe (HOTP) à usage unique basé sur HMAC selon la RFC 4226.

Le secret partagé et les autres paramètres peuvent être spécifiés en utilisant les champs de chaîne d'entrée (qui peuvent être ajoutés/édités dans la boîte de dialogue de l'entrée sur la page de l'onglet 'Avancé'):

- **HmacOtp-Secret**
  HmacOtp-Secret-Hex
  HmacOtp-Secret-Base32
  HmacOtp-Secret-Base64
  Au moins un de ces champs doit être présent, et sa valeur doit être mise vers le secret partagé dans l'encodage correspondant. Dans le premier cas ('HmacOtp-Secret'), l'encodage UTF-8 de la valeur est utilisé comme secret partagé.

- **HmacOtp-Counter** (automatique)
  Ce champ stocke la valeur du compteur dans sa représentation décimale. La valeur par défaut est 0. Quand le paramètre substituable `{HMACOTP}` est remplacé (c'est-à-dire quand on génère un mot de passe à usage unique), KeePass met à jour automatiquement la valeur du compteur.

`{TIMEOTP}` – En générant des mots de passe à usage unique basés sur le Temps :
Le paramètre substituable `{TIMEOTP}` génère un mot de passe (TOTP) à usage unique selon la RFC 6238.

Le secret partagé et les autres paramètres peuvent être spécifiés en utilisant les champs de chaîne d'entrée suivants (qui peuvent être ajoutés/édités dans la boîte de dialogue sur la page de l'onglet 'Avancé') :

- **TimeOtp-Secret**
  TimeOtp-Secret-Hex
  TimeOtp-Secret-Base32 (plus commun)
  TimeOtp-Secret-Base64
  Au moins un de ces champs doit être présent, et sa valeur doit être positionnée au secret partagé dans l'encodage correspondant. Dans le premier cas ('TimeOtp-Secret'), l'encodage UTF-8 de la valeur est utilisé en tant que secret partagé. La plupart des services utilisent l'encodage Base32.
- **TimeOtp-Length** (optionnel)
  Spécifie la longueur du mot de passe à usage unique généré. La valeur par défaut est 6 ; le maximum est 8.
- **TimeOtp-Period** (optionnel)
  Spécifie l'écoulement du temps en secondes. La valeur par défaut est 30.
- **TimeOtp-Algorithm** (optionnel)
  Spécifie l'algorithme cryptographique utilisé pour la génération du mot de passe à usage unique. Les algorithmes suivant sont pris en charge :
  - HMAC-SHA-1
  - HMAC-SHA-256
  - HMAC-SHA-512

  La valeur par défaut est HMAC-SHA-1.

La date et le temps de votre système doivent être justes, sinon le service/serveur peut rejeter l'OTP généré.

Exemple d'utilisation : Créez une nouvelle entrée et modifiez sa séquence de saisie automatique par défaut à `{USERNAME}{TAB}{PASSWORD}{ENTER}{DELAY 3000}{HMACOTP}{ENTER}`. Ouvrez la boîte de dialogue 'Les paramètres du générateur OTP...', positionnez le secret partagé pour les OTP basés sur HMAC à '12345678901234567890' et sélectionnez l'encodage UTF-8. Quand on accomplit la saisie automatique, alors KeePass envoie le nom d'utilisateur, appuie sur Tab, envoie le mot de passe, appuie sur Entrée, attends 3 secondes, génère et envoie l'OTP basé sur HMAC et appuie encore finalement sur la touche Entrée. La valeur du compteur pour la génération du mot de passe à usage unique est automatiquement mise à jour. Avec le secret partagé ci-dessus et le compteur initialisé à la valeur 0, les mots de passe à usage unique suivant sont générés : 755224, 287082, 359152, 969429, 338314, etc. (d'autres OTP générés peuvent être trouvés dans l'exemple de la RFC 4226).

Les greffons : Il existe des greffons qui prennent en charge des OTP non normalisés (par exemple : Steam) et offre des fonctions supplémentaires relatives aux OTP.
`{URL:...}` et `{BASE:...}` :
Le paramètre substituable `{URL:...}` est remplacé par la partie spécifiée de l'adresse (URL) de l'entrée courante ; cela est généralement utile dans un remplacement d'adresse (URL) spécifique d'une entrée (défini dans l'onglet « Propriétés » de la boîte de dialogue d'entrée). Le paramètre substituable `{BASE:...}` est remplacé par la partie spécifiée de l'URL qui est remplacée ; ceci est généralement utile dans un remplacement d'URL global (défini dans 'Outils' → 'Options' → onglet 'Intégration' → bouton 'Les remplacements d'adresse (URL)...'), car aucun contexte d'entrée ne peut être disponible.

Exemple d'utilisation : Pour l'adresse (URL) de l'entrée `https://identifiant:motdepasse@keepass.info:80/chemin/exemple.php?q=e&s=t`, les paramètres substituables retournent les valeurs suivantes :

Paramètre	Valeur

substituable	
{URL}	https://identifiant:motdepasse@keepass.info:80/chemin/exemple.php?q=e&s=t
{URL:RMVSCM}	identifiant:motdepasse@keepass.info:80/chemin/exemple.php?q=e&s=t
{URL:SCM}	https
{URL:HOST}	keepass.info
{URL:PORT}	80
{URL:PATH}	/chemin/exemple.php
{URL:QUERY}	?q=e&s=t
{URL:USERINFO}	identifiant:motdepasse
{URL:USERNAME}	identifiant
{URL:PASSWORD}	motdepasse

{BASE} prend en charge exactement les mêmes parties que {URL}.

{CMD:/*LigneDeCommande/Options/*} – Exécution d'une ligne de commande :
Le paramètre substituable {CMD:/*LigneDeCommande/Options/*} exécute la ligne de commande spécifiée.

Une ligne de commande se compose d'un chemin d'accès à un fichier exécutable ou à un document et à des paramètres de ligne de commande. Si le chemin contient des espaces, alors il doit être placé entre double quotes (").

Le caractère après le premier ':' spécifie le caractère séparateur. Il peut être choisi librement (sauf '{' et '}'), mais il ne doit pas apparaître dans la ligne de commande ni dans aucune des options. Par exemple : {CMD:/Notepad.exe/W=0/} et {CMD:!Notepad.exe!W=0!} sont équivalents. Le séparateur à la fin (avant le '}') est obligatoire.

Une option est une paire clé-valeur, séparée par '='. Plusieurs options doivent être séparées à l'aide de virgules ','.

Options :

- **M** : spécifie la méthode d'exécution/d'ouverture de l'exécutable/document.
  La valeur par défaut est S.
  - **S** : utilisez le shell système (via ShellExecute). Avec cela, les fichiers exécutables sont exécutés et les documents sont ouverts à l'aide de leurs applications associées. Cependant, aucune entrée/sortie standarde n'est prise en charge.
  - **C**: Exécutez un fichier exécutable (EXE ou COM, via CreateProcess) ; les documents ne sont pas pris en charge. L'entrée/sortie standard est prise en charge.
- **O** : spécifie ce qu'il faut faire avec la sortie standard de l'application exécutée.
  La valeur par défaut est 1.
  - **0** : ignorer la sortie standard. Le paramètre substituable est remplacé par une chaîne vide.
  - **1** : remplacez le paramètre substituable par la sortie standard.
- **W** : spécifie s'il faut attendre la fin de l'application exécutée.
  La valeur par défaut est 1.
  - **0** : ne pas attendre.
  - **1** : Attendre.
- **WS** : spécifie le style de fenêtre. Toutes les applications ne prennent pas en charge cette option.

La valeur par défaut est `N`.
  - **`N`** : Normal.
  - **`H`** : Caché.
  - **`Min`** : Minimisé.
  - **`Max`** : Maximisé.
- **`V`** : spécifie le verbe (action à effectuer), par exemple 'Open' ('Ouvrir') ou 'Print' ('Imprimer'). Lorsque vous utilisez le verbe 'RunAs' ('Exécuter en tant que'), l'application est exécutée avec des droits administratifs (cela peut nécessiter une confirmation via la boîte de dialogue UAC).

Les caractères de nouvelle ligne à la fin de la sortie sont supprimés (de la même manière que les substitutions de commandes shell '`$(...)`' et '`` `...` ``').

Exemples d'utilisation :

- `{CMD:/Notepad.exe/W=0/}`
  Exécute le Bloc-notes et continue immédiatement.
- `{CMD:/PowerShell.exe -Command "(Get-FileHash '%SYSTEMROOT%\Win.ini' -Algorithm SHA256).Hash"/M=C,WS=H/}`
  Le paramètre substituable est remplacé par le hachage SHA-256 du fichier Win.ini de Windows.

Réparer les bases de données

La réparation des bases de données

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

KeePass possède des 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 possible à partir du fichier corrompu.

⚠ En mode réparation, l'intégrité des données n'est pas vérifiée (afin de récupérer autant de données que possible). Lorsqu'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.

Afin d'utiliser la fonctionnalité de réparation dans KeePass 2.x, créez d'abord un nouveau fichier de base de données. Ensuite, allez dans *'Fichier' → 'Importer...'* et importez le fichier de base de données corrompu, en utilisant *'KeePass KDBX (2.x) (mode de réparation)'* comme format.

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'

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 rechercher un terme contenant des espaces, alors imbriquer le terme entre double 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 multiples	
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 trouvées 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 utilisez la commande de 'Qualité du mot de passe' dans le menu 'Rechercher'.	

Balises multiples (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.

Afin de voir votre base de données dans le format XML de KeePass 2.x, vous pouvez l'exporter (via 'Fichier' → 'Exporter') vers un fichier 'KeePass XML (2.x)'.

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 personnalisée	
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 utilisez 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 multiples (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 ajustez 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, sélectionnez le dans la boîte de dialogue 'Rechercher' et cliquez sur le bouton de suppression de profil.

La boîte de recherche rapide

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

Afin d'indiquer que la chaîne de recherche est une expression régulière, enfermez 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 boite 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 sécurisés

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 pas visibles dans l'espace 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:
Il n'y a aucune limitation de sélection. Les contrôles d'édition sécurisés se comportent exactement comme les contrôles d'édition Windows standard.

La protection de la mémoire du processus :
Sur les systèmes Windows, tous les caractères sont protégés. Sur les systèmes Unix-like (Linux, MacOS, etc.), les caractères au-dessus de U+D7FF (voir Basic Multilingual Plane) ne sont pas protégés.

La sécurité

La sécurité

Informations détaillées sur la sécurité de KeePass.

- Le chiffrement de la base de données
- Le hachage de clé et la dérivation de clé
- La protection contre les attaques par dictionnaire
- La génération de nombres aléatoires
- La protection de la mémoire du processus
- La saisie de la clé principale sur un bureau sécurisé (protection contre les enregistreurs de frappe)
- Le verrouillage de l'espace de travail
- Affichage/Édition de pièces jointes
- Les greffons (plug-in)
- Les autotests
- Les logiciels espions spécialisés
- Les données malveillantes
- Les options pour les experts
- Les options pour les administrateurs
- Les problèmes de 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 garanties à l'aide d'un hachage HMAC-SHA-256 du texte chiffré (schéma Encrypt-then-MAC).
Voir également :

- La spécification du format de fichier KDBX.
- La 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 rapide 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 mentionnée 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 mentionnée 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 CryptProtectMemory / 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 DPAPI n'est pas disponible ou est désactivé, alors KeePass se contente de chiffrer le processus mémoire en utilisant ChaCha20 avec une clé aléatoire ; notez que c'est moins sécurisé que DPAPI, car la clé est également stockée dans la mémoire de 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, le transfert de données vers/depuis d'autres applications (via le presse-papiers, glisser&déposer, Entrée standard/Sortie standard, etc.), le remplacement des paramètres substituables (c'est-à-dire lors de la saisie automatique, la recherche de données (c'est-à-dire les commandes dans le menu 'Rechercher' qui implique des données sensibles, l'importation/exportation de fichiers (sauf KDBX) et le chargement/enregistrement de fichiers non chiffrés. 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.

Remarquez que la saisie automatique peut également être sécurisée contre les enregistreurs de frappe à l'aide de l'obfuscation à deux canaux.
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-il 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-il la sécurité en empêchant toute modification par un programme malveillant ?
- Est-ce qu'une option permettant d'empêcher le chargement de greffons renforcerait-elle 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-il la sécurité ?
- Est-ce que verrouiller la fenêtre principale de sorte que seule la saisie automatique soit autorisée renforcerait-il 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 (telle 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 malveillants.
  - 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 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 synchronisation

- Introduction et exigences
- Appel d'une synchronisation
- Les détails techniques
- Les protocoles de synchronisation avancés

Introduction et exigences

KeePass 2.x dispose d'un puissant mécanisme de synchronisation intégré. Les modifications apportées à plusieurs copies d'un fichier de base de données peuvent être fusionnées en toute sécurité.

Après avoir synchronisé deux fichiers A et B, A et B sont à jour (c'est-à-dire que KeePass enregistre les données fusionnées aux deux emplacements lors de l'exécution d'une synchronisation).

Exigences :

- Si les fichiers à synchroniser sont accessibles via un protocole supporté par défaut par KeePass (par exemple : des fichiers sur un disque dur local ou un partage réseau, FTP, HTTP, HTTPS, WebDAV, etc., voir la page 'Charger/Enregistrer depuis/vers une adresse (URL)' pour des détails), alors aucun greffon/extension n'est requis.
- Si l'un des fichiers à synchroniser doit être accessible via SCP, SFTP ou FTPS, alors vous avez besoin du greffon IOProtocolExt, qui ajoute la prise en charge de ces protocoles à KeePass.
- Si l'un des fichiers à synchroniser est stocké dans un stockage en nuage : pour la plupart des

stockages en nuage, il existe une intégration avec le système de fichiers local de disponible (c'est-à-dire que vous pouvez accéder à vos fichiers stockés à l'aide de l'Explorateur de fichiers Windows). Par exemple : Dropbox, Microsoft OneDrive et Google Drive fournissent une telle intégration. Si une telle intégration est disponible, alors il est recommandé d'accéder à votre fichier de base de données de cette façon ; cela fonctionne souvent mieux que d'y accéder via un protocole comme FTP ou WebDAV. Si aucune intégration de ce type n'est disponible et que votre stockage en nuage n'est pas non plus accessible via un protocole standard, alors un greffon spécifique de KeePass pour ce stockage en nuage pourrait être disponible.

Appel d'une synchronisation

Il existe plusieurs manières d'invoquer une synchronisation :

- **Manuellement :** une synchronisation peut être démarrée manuellement en naviguant vers *'Fichier' → 'Synchroniser'* et en cliquant sur *'Synchroniser avec le fichier...'* ou *'Synchroniser avec l'adresse (URL)...'* (selon que le fichier à synchroniser est stocké sur un lecteur local/partage réseau ou sur un serveur accessible via une URL). Si vous avez déjà ouvert ou synchronisé avec le fichier cible, alors vous pouvez aussi simplement pointer sur 'Fichiers récents' (dans le menu *'Synchroniser'*) et sélectionner le fichier. La synchronisation manuelle n'est possible que lorsque la base de données actuellement ouverte est un fichier local (les fichiers sur un partage réseau sont ici considérés comme des fichiers locaux) ; lorsque vous avez ouvert un fichier depuis un serveur à l'aide d'une URL, le menu *'Synchroniser'* est désactivé.
- **La commande 'Enregistrer' :** lors de l'appel de la commande 'Enregistrer', KeePass vérifie si le fichier sur le disque/serveur a été modifié pendant que vous l'éditiez. S'il a été modifié, alors KeePass vous demande si vous souhaitez écraser ou synchroniser avec le fichier. Remarquez que cela s'applique uniquement à la commande 'Enregistrer', pas à la commande 'Enregistrer sous'. Voir la page Utilisateur multiple pour plus de détails (section 'KeePass 2.x : Synchroniser ou écraser').
- **Déclencheurs :** Dans des situations plus complexes, vous pouvez utiliser l'action de déclenchement de synchronisation. Voir la page 'Déclencheurs' pour plus de détails.
- **Script :** Afin d'effectuer une synchronisation sans ouvrir KeePass, la commande de synchronisation de KPScript peut être utilisée. Consultez la page d'aide de KPScript Opérations à commande unique' pour plus de détails.

Les détails techniques

L'algorithme de synchronisation est assez complexe et il faudrait de nombreuses pages pour décrire en détail son fonctionnement. Les développeurs intéressés par cela peuvent consulter le code source de KeePass. Voici les propriétés les plus importantes de l'algorithme de synchronisation :

- Afin de décider quelle copie d'un objet est la plus récente, KeePass utilise principalement l'heure de la dernière modification de l'objet (que KeePass met automatiquement à jour à chaque fois que l'objet est modifié).
- La synchronisation est effectuée au niveau de l'entrée. Ceci par exemple signifie qu'une combinaison nom d'utilisateur/mot de passe est toujours cohérente (la synchronisation au niveau du champ ne sera pas mise en œuvre, car les combinaisons pourraient devenir incohérentes avec cela).
- En cas de mises à jour et de collisions parallèles, KeePass essaie de stocker toutes les informations dans un endroit approprié. Par exemple : lorsque vous avez une entrée E dans une base de données A, faites une copie B de A, modifiez E dans B, modifiez E dans A et synchronisez A et B, alors E dans A est traité comme courant et les modifications apportées à E dans B sont stockés comme une entrée d'historique de E (voir l'onglet 'Historique' dans la boîte de dialogue de l'entrée), c'est-à-dire que les modifications apportées dans B ne sont pas perdues.
- Les entrées d'historique sont fusionnées sans accomplir de suppression. Cependant, la maintenance automatique de l'historique peut supprimer des entrées (en fonction du nombre d'entrées ou de leur taille, configurables dans « Fichier » → « Paramètres de la base de données... » onglet → « Avancé »).

Les protocoles de synchronisation avancés

- Synchronisation locale↔Maître :
  Un protocole de synchronisation qui empêche la perte de données lorsque les fichiers de base de

données sont écrasés par d'autres applications (par exemple : un logiciel de service de stockage en nuage), à l'aide d'un déclencheur.

- Greffons.
  Il existe des greffons pour des protocoles de synchronisation plus sophistiqués. Par exemple : pour synchroniser seulement un sous-ensemble d'entrées.

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 NAT. 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.

Les déclencheurs

Les déclencheurs

Automatisez les flux de travail à l'aide du système de déclenchement.

- Introduction au système de déclenchement
- Les événements
- Les conditions
- Les actions
- Exemples

Introduction au système de déclenchement

KeePass dispose d'un puissant système de déclenchement événement-condition-action. Avec ce système, les flux de travail peuvent être automatisés. Par exemple, vous pouvez définir un déclencheur qui télécharge automatiquement votre base de données sur un serveur de sauvegarde après avoir enregistré le fichier localement.

Un déclencheur commence à s'exécuter lorsque l'*un* des événements spécifiés correspond. Lorsque cela se produit, les conditions sont vérifiées. Si *toutes* les conditions sont remplies, les actions du déclencheur sont exécutées. Les actions sont exécutées consécutivement ; si une action échoue, l'exécution de l'événement est généralement interrompue (c'est-à-dire que toutes les actions suivantes ne sont pas exécutées).

Un déclencheur doit être à la fois *activé* et *amorcé* pour être exécuté. L'état *activé* est défini par l'utilisateur ; un déclencheur désactivé n'a aucune fonction. L'état *amorcé* dépend de l'état du programme. En activant l'option *'Initialement amorcé'*, un déclencheur est *amorcé* par défaut. Si vous activez l'option *'Désamorcé après l'exécution d'actions'*, le déclencheur sera désamorcé après avoir été exécuté une fois. Il existe des actions pour amorcer et désamorcer les déclencheurs, c'est-à-dire que des déclencheurs peuvent tourner eux-mêmes et d'autres déclencheurs s'amorcer et se désamorcer, ce qui permet de définir un système complexe de déclencheurs dépendant de déclencheurs.

La plupart des chaînes du système de déclenchement sont compilées par Spr, c'est-à-dire que des paramètres substituables (sauf ceux qui changent d'état), des variables d'environnement, etc., peuvent être utilisés.

Tous les utilisateurs.
Les déclencheurs sont sauvegardés dans un fichier de configuration imposée, qui s'applique à tous les utilisateurs qui utilise cette installation de KeePass. Donc, vérifiez que tous les déclencheurs conviennent bien à tous les utilisateurs. Notammennt, que le déclencheur ne contienne pas de données sensible (pour des raisons de sécurité/de confidentialité).

Les données sensibles :
Certains événements/conditions/actions de déclenchement prennent en charge les champs pour les données potentiellement sensibles (par exemple : le champ mot de passe de l'action 'Ouvrir le fichier de la base de données'). Comme les déclencheurs sont enregistrés dans un fichier de configuration non chiffré, il n'est généralement pas recommandé de saisir directement des données sensibles dans les champs de déclencheur. Si une base de données est ouverte lorsque le déclencheur s'exécute, alors les données sensibles peuvent être stockées dans la base de données et le champ du déclencheur peut pointer vers les données à l'aide d'une référence de champ (que KeePass résout lors de l'évaluation du champ). De cette façon, seule la référence du champ apparaît dans le fichier de configuration et les données sensibles actuelles sont stockées dans le fichier de base de données chiffré.

Les déclencheurs spécifiques de l'utilisateur.
Afin de limiter un déclencheur à un ou plusieurs utilisateurs spécifiques, vous pouvez ajouter un condition de type 'Variable d'environnement'. Définissez le paramètre 'Nom' sur 'USERNAME' (sans les quotes). Dans le cas d'un seul utilisateur, sélectionnez "Égale" comme comparaison et définissez le paramètre 'Valeur' sur le nom d'utilisateur du système. Dans le cas de plusieurs utilisateurs, sélectionnez "Correspond à l'expression régulière" comme comparaison et définissez le paramètre 'Valeur' sur une expression régulière appropriée (par exemple, si vous spécifiez '`^(Michael|Tobias)$`', le déclencheur s'applique uniquement aux utilisateurs 'Michael' et 'Tobias'). Des informations sur les expressions régulières peuvent être trouvées ici : Mode de recherche 'Expression régulière'.

Propriétés de connexion d'E/S :
La plupart des actions de déclenchement ayant un paramètre chemin/URL du fichier permettent uniquement de spécifier le chemin/l'URL et éventuellement les accréditations (nom d'utilisateur et mot de passe) pour accéder au fichier ; les propriétés de connexion avancées (comme le délai d'attente - timeout - , l'agent utilisateur, le mode passif, etc.) ne peuvent pas être spécifiées ici. Si des propriétés de connexion avancées sont requises, alors ouvrir le fichier une fois (en utilisant 'Fichier' → 'Ouvrir') avec les propriétés de connexion souhaitées. Cela créera un élément dans la liste de fichiers 'Rouvrir' (qui mémorise les propriétés de connexion). Lorsqu'une action de déclenchement est exécutée, KeePass charge les propriétés de connexion à partir de l'élément correspondant (même chemin/URL) dans la liste de fichiers 'Rouvrir'.

Les événements

- **Application initialisée :**
  cet événement se produit lorsque KeePass a terminé l'initialisation, mais n'a pas encore effectué d'automatisation de la fenêtre principale (comme l'ouverture d'une base de données par défaut).
  - *Paramètres :* Aucun.
- **Application démarrée et prête :**
  cet événement se produit lorsque KeePass a démarré, a effectué des automatisations de la fenêtre principale (comme l'ouverture d'une base de données par défaut) et est prêt pour les actions de l'utilisateur.
  - *Paramètres :* Aucun.
- **Sortie de l'application :**
  cet événement se produit lorsque KeePass est sur le point de quitter. Les bases de données ont déjà été fermées, mais les ressources (comme les polices, etc.) sont toujours valides.
  - *Paramètres :* Aucun.
- **Le fichier de la base de données est ouvert :**
  cet événement se produit juste après qu'un fichier de base de données a été ouvert avec succès.
  - *Fichier/adresse (URL) :* un filtre d'événement facultatif. Si un filtre est spécifié (c'est-à-dire que quelque chose est entré dans *'Fichier/adresse (URL) - Filtre'*), le déclencheur n'est évalué que si le filtre correspond au chemin du fichier de la base de données en cours. Par exemple : si vous entrez *F:*\ comme chaîne de filtre et spécifiez *'Commence par'* comme méthode de comparaison, alors le déclencheur ne sera évalué que si le chemin de la base de données (qui vient juste d'être ouverte) commence par *F:*\.
- **Juste avant l'enregistrement du fichier de la base de données :**
  cet événement se produit juste avant l'enregistrement d'un fichier de base de données.
  - *Paramètres :* voir l'événement 'Le fichier de la base de données est ouvert'.
- **Le fichier de la base de données a été enregistré :**
  cet événement se produit juste après qu'un fichier de base de données a été enregistré avec succès.
  - *Paramètres :* voir l'événement 'Le fichier de la base de données est ouvert'.
- **Juste avant la synchronisation du fichier de la base de données :**
  cet événement se produit juste avant qu'un fichier de base de données ne soit synchronisé avec un autre fichier de base de données.
  - *Paramètres :* voir l'événement 'Le fichier de la base de données est ouvert'.
- **Le fichier de la base de données vient juste d'être synchronisé :**
  cet événement se produit juste après qu'un fichier de base de données a été synchronisé avec un autre fichier de base de données.
  - *Paramètres :* voir l'événement 'Le fichier de la base de données est ouvert'.
- **Fermeture du fichier de la base de données (avant l'enregistrement) :**
  cet événement se produit juste avant la fermeture du fichier de la base de données. Cela se produit avant que KeePass enregistre automatiquement la base de données ou demande à l'utilisateur s'il souhaite enregistrer les modifications non enregistrées.
  - *Paramètres :* voir l'événement 'Le fichier de la base de données est ouvert'.
- **Fermeture du fichier de la base de données (après l'enregistrement) :**
  cet événement se produit juste avant la fermeture d'un fichier de base de données. Le fichier de base de données était déjà enregistré automatiquement ou les modifications non enregistrées étaient enregistrées/abandonnées selon le choix de l'utilisateur.
  - *Paramètres :* Voir 'Fichier de la base de données est ouvert'
- **Les données de l'entrée sont copiées dans le presse-papiers :**
  cet événement se produit lorsque les données de l'entrée (nom d'utilisateur, mot de passe, etc.) sont copiées dans le presse-papiers de Windows.
  - *Valeur :* un filtre de valeur facultatif (données copiées).
- **Temps - Périodique :**
  cet événement se produit à des intervalles définis par l'utilisateur. L'événement n'est déclenché que si KeePass n'est pas occupé par une tâche différente (comme afficher une sous-boîte de dialogue).
  - *Intervalle :* Intervalle de temps entre les événements, en secondes.

  - *Redémarrer le timer sur l'activité KeePass :* si cette option est activée, une activité KeePass (interaction utilisateur, automatisation, sous-dialogue, activité de greffon, etc.) provoque un redémarrage du timer, c'est-à-dire qu'un intervalle complet doit s'écouler pour le prochain événement.
- **Clic sur un bouton personnalisé de la barre d'outils :**
  cet événement se produit lorsque l'utilisateur clique sur un bouton personnalisé de la barre d'outils. Des boutons personnalisés de la barre d'outils peuvent être créés à l'aide de l'action du déclencheur 'Ajouter un bouton personnalisé à la barre d'outils'.
  - *ID :* ID du bouton de la barre d'outils sur lequel il a fallu cliquer (voir Actions).

Les conditions

- **Variable d'environnement :**
  - *Nom :* nom de la variable d'environnement à vérifier. Le nom *ne* doit *pas* être entouré par des caractères pourcentage (%).
  - *Valeur :* la valeur que la variable d'environnement spécifiée doit avoir pour que la condition soit vraie.
- **Chaîne de caractères :**
  - *Chaîne de caractères :* une chaîne (KeePass Spr-compile cela, c'est-à-dire que vous pouvez, par exemple, utiliser des paramètres substituables)).
  - *Valeur :* la valeur que la chaîne évaluée spécifiée doit avoir pour que la condition soit vraie.
- **Le fichier existe :**
  - *Fichier :* le fichier qui doit exister pour que la condition soit vraie.
- **L'hôte distant est joignable (ping) :**
  - *Hôte :* l'hôte à qui envoyer le ping.
- **La base de données a des modifications non sauvegardées :**
  évalue à vrai, si la base de données spécifiée a des modifications non sauvegardées.
  - *Base de données :* la base de données pour vérifier les modifications non sauvegardées.

Les actions

- **Exécuter la ligne de commande ou l'adresse (URL) :**
  Le fichier/l'URL et les arguments sont analysés par le moteur Spr avant d'être envoyés au shell, c'est-à-dire que des paramètres substituables génériques et dépendants de la base de données peuvent être utilisés. Si vous souhaitez utiliser des commandes shell intégrées, comme `COPY`, alors veuillez consulter : L'exécution de commandes Shell intégrées.
  - *Fichier/adresse (URL) :* la chaîne qui doit être exécuter par le shell.
  - *Arguments :* facultatif. Si *'Fichier/adresse (URL)'* pointe vers un fichier exécutable, alors cette chaîne est envoyée à l'exécutable en tant qu'argument(s) de ligne de commande.
  - *Attendre pour quitter :* si cette option est cochée, alors KeePass attend indéfiniment la fin du processus démarré.
  - *Style de fenêtre :* spécifie comment la fenêtre principale du fichier/adresse (URL) exécuté(e) doit être affichée. Toutes les applications ne respectent pas ce paramètre.
  - *Verbe :* Spécifie l'action à effectuer. Une chaîne vide signifie utiliser le verbe par défaut. Certaines applications prennent en charge des verbes supplémentaires (par exemple : "Imprimer" pour imprimer le document spécifié). Lors de l'utilisation du verbe "RunAs", l'application est exécutée avec les droits d'administration (cela peut nécessiter une confirmation via la boîte de dialogue UAC).
- **Activer ou désactiver le déclencheur :**
  - *Nom du déclencheur :* nom du déclencheur cible dont l'état activé/désactivé doit être modifié. Si ce champ est laissé vide, alors le déclencheur cible est le déclencheur courant.
  - *Nouvel état :* spécifie le nouvel état du déclencheur cible.
- **Ouvrir le fichier de la base de données :**
  ouvre un fichier de base de données KDBX (dans un nouvel onglet). Si le fichier de base de données donné est déjà ouvert, alors KeePass le place au premier plan.
  - *Fichier/adresse (URL) :* le chemin du fichier de la base de données à ouvrir. S'il s'agit d'une

adresse, alors le protocole (préfixe) doit être spécifié.
    - *Connexion d'entrée/sortie - Nom d'utilisateur/Mot de passe :* accréditation facultative utilisée pour la connexion au système de fichiers cible (par exemple : nom d'utilisateur/mot de passe du compte FTP). Cette accréditation n'est pas utilisée pour déchiffrer la base de données.
    - *Mot de passe/Fichier clé/Compte utilisateur Windows :* accréditation facultative qui est utilisée pour déchiffrer le fichier de la base de données.
- **Enregistrer la base de données active :**
enregistre la base de données actuellement active. Cette action enregistre toujours la base de données, même s'il n'y a pas de modifications non enregistrées. Pour n'enregistrer que s'il y a des modifications non enregistrées, alors utilisez la condition du déclencheur 'La base de données a des modifications non sauvegardées'.
    - *Paramètres :* Aucun.
- **Synchroniser la base de données active avec un fichier ou une adresse (URL) :**
synchronise la base de données actuellement ouverte et active avec un fichier.
    - *Fichier/adresse (URL) :* le chemin du fichier de la base de données avec lequel synchroniser. S'il s'agit d'une URL, alors le protocole (préfixe) doit être spécifié. Plusieurs chemins d'accès/URL de fichiers peuvent être spécifiés en les encadrant chacun par des doubles quotes (si différentes informations d'identification de connexion E/S sont requises, alors utilisez plutôt plusieurs actions).
    - *Connexion d'entrée/sortie - Nom d'utilisateur/Mot de passe :* accréditation facultative utilisée pour la connexion au système de fichiers cible (par exemple : nom d'utilisateur/mot de passe du compte FTP). Cette accréditation n'est pas utilisée pour déchiffrer la base de données.
    - *En cas d'erreur - Silencieux :* Si cette option est activée, KeePass n'affiche pas de boîte de dialogue d'erreur en cas d'erreur lors de la synchronisation, sauf si l'enregistrement de la base de données active échoue.
    - *En cas d'erreur - Continuer :* Lors de la synchronisation de plusieurs fichiers, l'activation de cette option permet à KeePass de poursuivre la synchronisation même en cas d'erreur. Les fichiers qui n'ont pas été importés avec succès ne sont pas écrasés (c'est-à-dire que les données qu'ils contiennent ne sont pas perdues). Cette option n'a aucun effet sur l'exécution des autres actions déclenchées.
- **Importer dans la base de données active :**
importe un fichier dans la base de données actuellement ouverte et active.
    - *Fichier/adresse (URL) :* le chemin du fichier source à importer. S'il s'agit d'une URL, alors le protocole (préfixe) doit être spécifié.
    - *Format de fichier :* spécifie le format d'importation (voir la boîte de dialogue d'importation pour les valeurs possibles).
    - *Méthode :* spécifie le comportement des groupes/entrées qui existent à la fois dans la base de données actuellement active et dans le fichier en importation.
    - *Mot de passe/Fichier clé/Compte utilisateur Windows :* accréditation facultative qui est utilisée pour déchiffrer le fichier d'importation, si nécessaire. Si aucune accréditation n'est spécifiée, mais que le fichier d'importation est chiffré, alors KeePass affiche une boîte de dialogue d'invite de clé.
- **Exporter la base de données active :**
exporte la base de données actuellement ouverte et active vers un fichier.
    - *Fichier/adresse (URL) :* chemin du fichier cible vers lequel exporter. S'il s'agit d'une URL, alors le protocole (préfixe) doit être spécifié.
    - *Format de fichier :* spécifie le format d'exportation (voir la boîte de dialogue d'exportation pour les valeurs possibles).
    - *Filtre - Groupe :* spécifie le chemin du groupe à exporter (facultatif ; une chaîne vide signifie toute la base de données). Le chemin doit commencer par le caractère utilisé comme séparateur, et le nom du groupe racine de la base de données ne doit pas être spécifié. Par exemple : pour exporter un groupe 'B' qui est un sous-groupe du groupe 'A', alors spécifiez `/A/B` comme chemin de groupe.
    - *Filtre - Balise (tag) :* exporte uniquement les entrées qui ont la balise spécifiée (paramètre facultatif).
- **Fermer la base de données active :**
Fermez la base de données actuellement active.

    - *Paramètres :* Aucun.
- **Activer la base de données (sélectionner l'onglet) :**
- *Fichier/adresse (URL) :* le chemin de la base de données à activer. Il peut s'agir d'une sous-chaîne du chemin réel de la base de données. Par exemple : la spécification de `BaseDeDonnées` correspondrait à une base de données `C:\Documents\KeePass\BaseDeDonnées.kdbx`.
- *Filtre :* spécifie les bases de données qui sont prises en compte. Si 'Déclenchement' est sélectionné et que le champ 'Fichier/adresse (URL)' est vide, alors la base de données qui a déclenché l'événement est activée.

Attendre :
attend le laps de temps spécifié.
- *Intervalle de temps :* nombre de millisecondes à attendre.

Afficher la boîte de message :
Affiche une boîte de message.
- *Instruction principale :* première ligne du texte du message (qui s'affiche éventuellement avec une police plus forte).
- *Texte :* texte du message.
- *Icône :* l'icône qui s'affiche à côté du texte du message.
- *Boutons :* spécifie les boutons disponibles.
- *Bouton par défaut :* le bouton qui a initialement le focus.
- *Action - Condition :* spécifie la condition qui doit être remplie pour que l'action suivante soit exécutée. Par exemple : si 'Bouton OK/Oui' est sélectionné, alors l'action n'est effectuée que si l'utilisateur clique sur le bouton 'OK' ou 'Oui' de la boîte de message.
- *Action :* l'action à effectuer après l'affichage de la boîte de message.
- *Action - Paramètres :* paramètres de l'action spécifiée. Par exemple : si l'exécution d'une ligne de commande/adresse (URL) est spécifiée comme action, alors ce champ doit contenir la ligne de commande/adresse (URL).

Exécuter la saisie automatique globale :
exécute la saisie automatique globale (comme en appuyant sur la touche de raccourci clavier de la saisie automatique globale).
- *Paramètres :* Aucun.

Exécuter la saisie automatique avec l'entrée sélectionnée :
exécute la saisie automatique avec l'entrée actuellement sélectionnée comme contexte.
- *Séquence :* la séquence de frappes à envoyer. Si ce champ est vide, alors la séquence par défaut est utilisée.

Afficher les entrées par balise (tag) :
recherche toutes les entrées ayant la balise spécifiée et les affiche dans la liste des entrées de la fenêtre principale.
- *Balise (tag) :* balise que les entrées doivent avoir.

Ajouter un bouton personnalisé à la barre d'outils :
ajoute un bouton personnalisé à la barre d'outils de la fenêtre principale.
- *ID :* ID du bouton de la barre d'outils (voir le gestionnaire d'événements).
- *Nom :* texte qui est affiché sur le bouton de la barre d'outils.
- *Description :* texte qui s'affiche dans l'info-bulle du bouton.

Enlever le bouton personnalisé de la barre d'outils :
supprime le bouton personnalisé de la barre d'outils de la fenêtre principale.
- *ID:* ID du bouton de la barre d'outils (voir le gestionnaire d'événements).

Exemples

Consulter la page Trigger Examples.

Le champ d'adresse (URL)

Conseils et astuces d'utilisation :

Les capacités standard

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 dans les paramètres 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 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`, `main` function and command line arguments, 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 quotes.
- 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 'Remplacer l'adresse' (onglet 'Propriétés' dans la boîte de dialogue de l'entrée). Cela vous permet d'exécuter une URL spécifique, tout en utilisant le champ d'adresse pour (uniquement) stocker des données. 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 'Remplacer l'adresse') sera exécutée.

En utilisant un navigateur différent :
Si votre navigateur par défaut est Mozilla Firefox et que vous souhaitiez ouvrir un site spécifique avec Microsoft Edge, alors spécifiez les éléments suivants dans le champ de remplacement d'adresse :

```
cmd://{EDGE} "{URL}"
```

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

La modification globale du comportement de l'URL :
Si vous souhaitez modifier l'action d'URL *par défaut* pour un protocole d'URL (par exemple : `http://`, `https://` ou `ftp://`), alors vous pouvez définir un remplacement de protocole d'URL dans 'Outils' → 'Options' → onglet 'Intégration ' → 'Remplacer l'adresse (URL)'. Cela permet par exemple de spécifier un navigateur par défaut pour des sites Web (dans la boîte de dialogue, vous pouvez trouver plusieurs remplacements pour les navigateurs comme Microsoft Edge et Mozilla Firefox).

Les remplacements du protocole d'une adresse (URL) peuvent également être utilisés pour définir de nouveaux protocoles. Par exemple : si vous souhaitez définir un protocole `kdbx://` qui ouvre une autre base de données KeePass, alors spécifiez ce qui suit comme remplacement pour le protocole `kdbx` (sur Windows) :
`cmd://"{APPDIR}\KeePass.exe" "{BASE:RMVSCM}" -pw-enc:"{PASSWORD_ENC}"`
sur des systèmes de type Unix (Mono) :
`cmd://mono "{APPDIR}/KeePass.exe" "{BASE:RMVSCM}" -pw-enc:"{PASSWORD_ENC}"`
Si une entrée a maintenant une URL ressemblant à `kdbx://CheminVersVotreBaseDeDonnées.kdbx` et le mot de passe maître pour cette base de données dans le champ de mot de passe, alors double-cliquer sur l'URL de l'entrée dans la fenêtre principale ouvre l'autre base de données. Le paramètre de ligne de commande `-pw-enc` et le paramètre substituable `{PASSWORD_ENC}` permettent de transmettre le mot de passe maître de l'autre base de données sous forme chiffrée, c'est-à-dire que les moniteurs de processus et les utilitaires similaires ne peuvent pas lire le mot de passe maître.

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, tel 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'entrées principale
- Glisser&Déposer
- La saisie automatique
- Les greffons

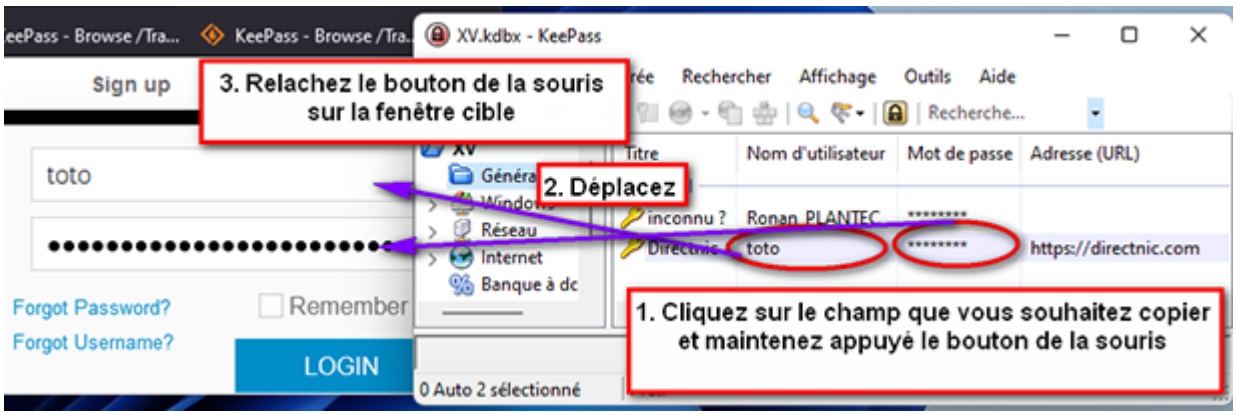
La liste d'entrées principale

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 greffons disponibles qui intègrent KeePass avec d'autres applications.

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

Remplacer XML

Remplacer XML

À propos de la fonctionnalité de remplacement XML.

- Les informations générales
- Exemples :
  - Remplacer le texte dans tous les titres et les remarques d'entrée
  - Remplacer toutes les adresses (URLs) HTTP par des adresses (URLs) HTTPS
  - Remplacer les icônes de groupe
  - Supprimer les chaînes d'entrée par nom
  - Supprimer les pièces jointes d'entrée par extension de nom
  - Réinitialiser les couleurs d'arrière-plan
  - La saisie automatique :
    - Désactiver la saisie automatique pour les entrées avec des champs vides
    - Convertir `{DELAY=` en majuscules
    - Ajouter `{DELAY=50}` à toutes les séquences sans un `{DELAY=`
    - Modifier les valeurs `{DELAY=`
    - Supprimer `{DELAY=x}` de toutes les séquences
    - Réinitialiser les séquences par défaut qui contiennent `{DELAY=`
    - Ajouter une association de saisie automatique à toutes les entrées
  - Copier les adresses (URLs) d'entrée dans les champs Titre
  - Copier les titres des entrées dans les champs Nom d'utilisateur vides
  - S'assurer que la première ligne n'est pas vide

Les informations générales

Remplacer XML est une fonctionnalité puissante qui modifie une base de données en manipulant sa représentation XML.

Il crée un DOM XML KeePass 2.x de la base de données actuelle en mémoire, effectue l'opération spécifiée par l'utilisateur (par exemple : supprimer des nœuds ou remplacer du texte), charge l'arborescence XML modifiée, et fusionne la base de données actuelle avec la base de données modifiée.

⚠ Il s'agit d'une fonction réservée aux experts. Utilisez-la avec précaution !

Remplacer XML peut être invoqué via 'Outils' → 'Outils de la base de données' → 'Remplacer XML...'.

Des informations sur XPath et les expressions régulières sont disponibles sur la page d'aide 'Rechercher'.

KeePass protège les entrées de l'historique ; XML Replace ne peut pas être utilisé pour les modifier. De plus, toute modification des propriétés de la base de données (nom/description de la base de données, etc.) peut être ignorée.

Exemples

Remplacer le texte dans tous les titres et les remarques d'entrée	
Sélectionner les nœuds :	`//Entry/String[(Key = 'Title') or (Key = 'Notes')]/Value`
Action :	Remplace les données
Données :	Le texte interne
Que rechercher :	*`LeTexteÀRechercher`*
Remplacer par :	*`LeRemplacement`*
Dans tous les titres et remarques d'entrée, cela remplace toutes les occurrences de *`LeTexteÀRechercher`* par *`LeRemplacement`*.	

Remplacer toutes les adresses (URLs) HTTP par des adresses (URLs) HTTPS	
Sélectionner les nœuds :	`//Entry/String[Key = 'URL']/Value`
Action :	Remplace les données
Données :	Le texte interne
Que rechercher :	`^http:`
Remplacer par :	`https:`
Options :	☑ Expression régulière
Dans tous les champs d'adresse (URL) d'entrée, cela remplace toutes les URL HTTP par des URL HTTPS.	

Remplacer les icônes de groupe	
Sélectionner les nœuds :	`//Group/IconID`
Action :	Remplace les données
Données :	Le texte interne
Que rechercher :	`^48$`
Remplacer par :	36
Options :	☑ Expression régulière
Cela assigne l'icône du package ZIP à tous les groupes qui ont actuellement un dossier fermé en tant qu'icône. Tous les ID d'icône peuvent être trouvés dans la boîte de dialogue du sélecteur d'icône.	

Supprimer les chaînes d'entrée par nom	
Sélectionner les nœuds :	`//Entry/String[Key = '`*`LeNom`*`']`
Action :	Supprime des nœuds
Supprime toutes les chaînes de caractères d'entrée nommées*LeNom*.	

Supprimer les pièces jointes d'entrée par extension de nom	
Sélectionner les nœuds :	`//Entry/Binary/Key[(string-length(.) >= 4) and (substring(., string-length(.) - 3) = '.jpg')]/..`
Action :	Supprime des nœuds
Supprime toutes les pièces jointes dont le nom se termine par « .jpg ».	

Réinitialiser les couleurs d'arrière-plan	
Sélectionner les nœuds :	`//Entry/BackgroundColor`
Action :	Supprime des nœuds
Positionne la couleur d'arrière-plan par défaut (transparent/alterné) à toutes les entrées.	

Désactiver la saisie automatique pour les entrées avec des champs vides	
Sélectionner les nœuds :	`//Entry/String[((Key = 'UserName') or (Key = 'Password')) and (Value = '')]/../AutoType/Enabled`
Action :	Remplace les données
Données :	Le texte interne
Que rechercher :	`True`
Remplacer par :	`False`
Désactive la saisie automatique pour toutes les entrées qui ont un champ Nom d'utilisateur ou un champ de mot de passe vide.	

Convertir `{DELAY=` en majuscules	
Sélectionner les nœuds :	`//DefaultSequence | //KeystrokeSequence`
Action :	Remplace les données
Données :	Le texte interne
Que rechercher :	`{DELAY=`
Remplacer par :	`{DELAY=`
Convertit tous les codes `{DELAY=` dans les substitutions et les associations de séquence de saisie automatique en majuscules (par défaut, l'option de sensibilité à la casse est désactivée, donc le texte 'Que rechercher' correspond à toutes les casses). Dans KeePass 2.x, les paramètres substituables sont insensibles à la casse. Cependant, cette opération de remplacement XML peut être utile pour préparer l'exemple suivant (qui correspond à `{DELAY=` d'une manière sensible à la casse).	

Ajouter `{DELAY=50}` à toutes les séquences sans un `{DELAY=`

Sélectionner les nœuds :	`(//DefaultSequence | //KeystrokeSequence)[not(contains(., '{DELAY=')) and (. != '')]`
Action :	Remplace les données
Données :	Le texte interne
Que rechercher :	`^(.*)$`
Remplacer par :	`{DELAY=50}$1`
Options :	☑ Expression régulière
Ajoute un `{DELAY=50}` à tous les remplacements et associations de séquence de saisie automatique qui ne contiennent déjà aucun `{DELAY=` et qui ne sont pas vides. Notez que la sélection du nœud est sensible à la casse (indépendamment de l'option de sensibilité à la casse des données), vous devez donc vous assurer que tous les codes `{DELAY=` sont en majuscules avant d'effectuer cette opération. Cela peut par exemple être fait à l'aide de l'opération de remplacement XML mentionnée ci-dessus.	

Modifier les valeurs `{DELAY=`	
Sélectionner les nœuds :	`//DefaultSequence | //KeystrokeSequence`
Action :	Remplace les données
Données :	Le texte interne
Que rechercher :	`\{DELAY=[\d\s]*\}`
Remplacer par :	`{DELAY=50}`
Options :	☑ Expression régulière
Positionne les valeurs de tous les codes `{DELAY=` dans les remplacements et les associations de séquence de saisie automatique à 50.	

Supprimer `{DELAY=`*x*`}` de toutes les séquences	
Sélectionner les nœuds :	`//DefaultSequence | //KeystrokeSequence`
Action :	Remplace les données
Données :	Le texte interne
Que rechercher :	`\{DELAY=[\d\s]*\}`
Remplacer par :	*(Laisser vide)*
Options :	☑ Expression régulière
Supprime tous les codes `{DELAY=`*x*`}` de toutes les séquences de saisie automatique.	

Réinitialiser les séquences par défaut qui contiennent`{DELAY=`	
Sélectionner les nœuds :	`//DefaultSequence[contains(., '{DELAY=')]`
Action :	Supprime des nœuds
Si une séquence a été spécifiée dans le champ 'Remplacer la séquence par défaut' (dans la boîte de dialogue de saisie automatique) et qu'elle contient `{DELAY=`, alors la séquence est réinitialisée, c'est-à-dire que l'option 'Hériter de la séquence de saisie automatique par défaut du groupe parent' est activée.	

Ajouter une association de saisie automatique à toutes les entrées	
Sélectionner les nœuds :	`//Entry/AutoType`
Action :	Remplace les données
Données :	XML externe
Que rechercher :	`</AutoType>\Z`
Remplacer par :	`<Association><Window>* - Notepad</Window><KeystrokeSequence>{PASSWORD}</KeystrokeSequence></Association></AutoType>`
Options :	☑ Expression régulière
Ajoute une association de saisie automatique à toutes les entrées : le titre de la fenêtre `* - Bloc-notes` est associé à la séquence `{PASSWORD}`.	

Copier les adresses (URLs) d'entrée dans les champs Titre	
Sélectionner les nœuds :	`//Entry`
Action :	Remplace les données
Données :	XML interne
Que rechercher :	`(?s)(<Key>Title</Key>\s*)(<Value>.*?</Value>|<Value\s*/>)(.*?<Key>URL</Key>\s*)(<Value>.*?</Value>|<Value\s*/>)`
Remplacer par :	`$1$4$3$4`
Options :	☑ Sensible à la casse ☑ Expression régulière
Copie l'adresse (URL) de l'entrée dans le champ Titre de l'entrée (en écrasant toutes les données existantes dans le champ Titre). Si vous souhaitez que l'adresse (URL) de l'entrée soit copiée seulement si le champ titre est vide, alors utiliser ce qui suit pour 'Sélectionner les nœuds': `//Entry/String[(Key = 'Title') and (Value = '')]/..`	

Copier les titres des entrées dans les champs Nom d'utilisateur vides	
Sélectionner les nœuds :	`//Entry/String[(Key = 'UserName') and (Value = '')]/..`
Action :	Remplace les données
Données :	XML interne
Que rechercher :	`(?s)(<Key>Title</Key>\s*<Value>)(.*?)(</Value>.*?<Key>UserName</Key>\s*)(<Value></Value>|<Value\s*/>)`
Remplacer par :	`$1$2$3<Value>$2</Value>`
Options :	☑ Sensible à la casse ☑ Expression régulière
Copie le titre de l'entrée dans le champ du nom d'utilisateur de l'entrée, si ce champ est vide.	

S'assurer que la première ligne n'est pas vide	
Sélectionner les nœuds :	`//Entry/String/Value`

Action :	Remplace les données
Données :	Le texte interne
Que rechercher :	`(?s)^(\r?\n)`
Remplacer par :	`--$1`
Options :	☑ Expression régulière

Pour tous les champs multilignes, cela insère '`--`' dans la première ligne de la valeur du champ, si cette ligne est vide et que la valeur a au moins deux lignes. Exemple :

```

Échantillon de données
```

est remplacé par

```
--

Échantillon de données
```

L'interface utilisateur

Les paramètres de la base de données

Les paramètres de la base de données

Décrit les différentes options de base de données.

Dans la boîte de dialogue des paramètres de la base de données, vous pouvez configurer divers paramètres liés à la base de données.

- Général
- Les options de sécurité
- Les options de compression
- Les modèles

Général

Sur cet onglet, vous pouvez spécifier des généralités comme le nom de la base de données et une description. De plus, vous pouvez définir diverses valeurs par défaut comme un nom d'utilisateur par défaut pour les nouvelles entrées (créées dans cette base de données).

Les options de sécurité

Sur cet onglet, vous pouvez spécifier divers paramètres liés au chiffrement. Ne modifiez ces paramètres que si vous savez vraiment ce que vous faites.

Algorithme de chiffrement :
Vous pouvez choisir l'algorithme utilisé pour chiffrer la base de données. Tous les algorithmes de chiffrement proposés par KeePass sont des algorithmes bien connus et sécurisés, consulter le chiffrement de la base de données.

Transformation de clé :
Consulter la protection contre les attaques par dictionnaire.

KeePass a un bouton sur cet onglet pour calculer le nombre de transformations de clé que votre ordinateur peut faire en 1 seconde. Si, par exemple, vous ne souhaitez attendre que 0,5 seconde, alors la moitié du nombre résulte du test de performance.

Les options de compression

Les bases de données de KeePass peuvent être compressées avant d'être chiffrées. La compression réduit la taille de la base de données, mais ralentit également un peu le processus de sauvegarde/chargement de la base de données.

Il est recommandé d'utiliser l'option de compression *GZip*. Cet algorithme est très rapide (vous ne remarquerez aucune différence par rapport à l'enregistrement de la base de données sans compression) et son taux de compression est acceptable.

Il *n*'est *pas* recommandé d'enregistrer les bases de données sans compression.

Sur les PC modernes, l'enregistrement de fichiers avec compression peut en fait être plus rapide que l'enregistrement sans compression, car le processus de compression est effectué par le processeur (qui est très rapide) et moins de données doivent être transférées depuis/vers le périphérique de stockage. Surtout lorsque l'appareil est lent (tel que l'enregistrement sur une clé USB), la compression peut réduire considérablement le temps d'enregistrement/de chargement.

Les modèles

Les modèles sont un excellent moyen de prédéfinir des noms d'utilisateurs ou des champs supplémentaires souvent utilisés, ou des combinaisons de chacun.

- Un modèle est une entrée KeePass normale avec toutes les données requises déjà saisies.
- Les modèles doivent être conservés dans un seul groupe.
- Ne placez pas d'entrées de données réelles dans le groupe de modèles.

Créez d'abord un groupe normal dans la fenêtre principale, puis positionnez-le comme groupe de modèles dans 'Fichier' → 'Paramètres de la base de données' → onglet *'Avancé'.*

Pour créer une nouvelle entrée basée sur un modèle, cliquez sur la flèche déroulante du bouton de la barre d'outils *'Ajouter une entrée...'* et choisissez le modèle à utiliser.

La boîte de dialogue de l'entrée

La boîte de dialogue de l'entrée

Éditer des entrées nouvelles ou déjà existantes.

- Général
- Avancé
- Propriétés
- La saisie automatique
- Historique
- Les outils
- L'édition de plusieurs entrées en une fois

Général

Sur l'onglet 'Général', vous pouvez spécifier les informations principales d'un compte.

Titre :
Dans le champ Titre, le nom du système/service doit être saisi.

Pour certains systèmes/services, il peut être judicieux de s'assurer que le titre de l'entrée se trouve dans le titre de la fenêtre cible, car cela permet à la saisie automatique d'associer l'entrée à la fenêtre cible. Pour plus de détails, voir saisie automatique globale. Cependant, si le titre de la fenêtre cible ne contient pas le nom du système/service (par exemple, '`Connexion - Nom du navigateur`'), alors il est recommandé de créer à la place une association fenêtre/séquence personnalisée.

Nom d'utilisateur :
Dans le champ Nom d'utilisateur, vous devez spécifier les données que vous saisissez lors d'une connexion afin de vous identifier. Il s'agit généralement d'un nom d'utilisateur, d'une adresse de courriel ou d'un numéro.

Il n'y a pas de champ d'adresse de courriel séparé par défaut, car cela réduirait la convivialité. Pour plus de détails, consultez la section 'un champ d'adresse de courriel peut-il être ajouté ?' dans la FAQ.

Lors de la saisie dans le champ du nom d'utilisateur, KeePass peut afficher une liste de suggestions pour le nom d'utilisateur. Cette liste est générée dynamiquement : lors de l'ouverture de la boîte de dialogue d'entrée, KeePass collecte les noms d'utilisateur de toutes les entrées stockées dans la base de données actuellement active. Si vous voyez un nom d'utilisateur incorrect dans la liste, alors vous devez rechercher ce nom d'utilisateur dans vos entrées (à l'aide de la fonction de recherche) et le corriger. Si les noms d'utilisateur ne sont pas affichés dans la fenêtre principale (cachés par des astérisques ou colonne désactivée), alors aucune suggestion n'est affichée dans la boîte de dialogue de saisie.

Dans les paramètres de la base de données (menu 'Fichier' → 'Paramètres de la base de données'), vous pouvez définir un nom d'utilisateur par défaut pour les nouvelles entrées.

Mot de passe :
Par défaut, KeePass génère un mot de passe pour une nouvelle entrée (cela peut être personnalisé/désactivé). Vous pouvez utiliser ce mot de passe ou le remplacer.

Il y a un bouton (à droite du champ de confirmation du mot de passe) qui ouvre le générateur de mot de passe.

De plus, il y a un bouton pour désactiver/activer l'estimation de la qualité du mot de passe pour l'entrée actuelle. La désactivation de l'estimation de la qualité du mot de passe pour une entrée exclut également l'entrée des rapports de qualité du mot de passe (menu 'Rechercher' → 'Qualité du mot de passe...').

Adresse (URL) :
Consulter la page d'aide 'Le champ d'adresse (URL)'.

Expire le :
Dans la liste des entrées de la fenêtre principale, une entrée expirée est affichée avec une icône **X** rouge et une police barrée. Les entrées expirées ne sont pas supprimées/déplacées automatiquement.

Vous pouvez rechercher des entrées expirées à l'aide du menu 'Rechercher' → 'Expiré'. Les entrées expirées peuvent également être affichées automatiquement lors de l'ouverture de la base de données (menu 'Outils' → 'Options' → onglet 'Avancé' → option 'Afficher les entrées qui ont expiré (le cas échéant)').

Avancé

Les champs personnalisés de chaîne de caractères :
Chaque entrée peut avoir un nombre arbitraire de champs personnalisés de chaîne de caractères. Un tel champ se compose d'un nom et d'une valeur. Le nom doit être unique (à l'intérieur de l'entrée).

Dans la fenêtre principale, la valeur d'un champ personnalisé de chaîne de caractères peut être copiée dans le presse-papiers en faisant un clic droit sur l'entrée, en pointant sur 'Autres données' et en cliquant sur le nom du champ de chaîne personnalisée (cela est également possible via le menu 'Entrée').

La valeur d'un champ personnalisé de chaîne de caractères peut également être utilisée dans une séquence de saisie automatique ; consulter la page d'aide des paramètres substituables. Par exemple : la valeur d'un champ personnalisé d'une chaîne de caractères nommé « BIC » (acronyme de Business Identifier Code) peut être insérée à l'aide du paramètre substituable '`{S:BIC}`'.

Dans les fichiers de base de données, les champs personnalisés de chaîne de caractères sont stockés sous forme chiffrée (voir « Le chiffrement de la base de données »). L'option 'Protéger la valeur dans la mémoire du processus' (dans la boîte de dialogue du champ personnalisé de la chaîne de caractères) permet d'activer/désactiver la protection de la mémoire de processus pour la valeur du champ personnalisé de chaîne de caractères. L'activation de cette protection induit certaines limitations (par exemple : la valeur doit être masquée par des astérisques pour que la protection soit efficace) et augmente le temps nécessaire aux différentes opérations. Par conséquent, il ne doit être activé que pour les données vraiment sensibles (par exemple : un deuxième mot de passe).

Fichiers joints :
Vous pouvez joindre des fichiers arbitraires à une entrée.

Les fichiers joints sont stockés dans le fichier de base de données sous forme chiffrée (voir 'Le chiffrement de la base de données'). Lors de l'importation d'un fichier en pièce jointe, KeePass ne supprime pas le fichier source ; vous devez le supprimer vous-même, si vous le souhaitez.

Cette fonctionnalité est destinée à stocker quelques/ou de petits fichiers (par exemple : des fichiers d'enregistrement, des fichiers de paires de clés publiques/privées, etc.). Chiffrer de nombreux/volumineux fichiers est considéré comme hors de portée d'un gestionnaire de mots de passe et il est recommandé d'utiliser un logiciel de chiffrement de fichiers spécialisé (par exemple VeraCrypt) pour cette tâche à la place (KeePass peut être utilisé pour stocker le mot de passe du conteneur de fichiers chiffrés).

Propriétés

Balises (tags) :
Vous pouvez affecter des balises arbitraires à une entrée. Plusieurs balises doivent être séparées par des virgules (ou des points-virgules). En cliquant sur le bouton à droite du champ de saisie des balises, un menu s'affiche qui permet d'ajouter des balises trouvées dans d'autres entrées.

Des balises peuvent également être ajoutées/supprimées dans la fenêtre principale : cliquez avec le bouton droit sur une ou plusieurs entrées→ 'Modifier l'entrée (rapidement)' → 'Ajouter une balise (tag)' ou 'Supprimer une balise (tag)'.

Un tag peut également être attribué à un groupe (dans la fenêtre principale, faites un clic droit sur le groupe → 'Éditer un groupe' → onglet 'Propriétés' → saisissez la balise dans le champ 'Balises (tags)'). Toutes les entrées de ce groupe ou de l'un de ses sous-groupes héritent de la balise.

Un cas d'utilisation courant consiste à marquer les entrées fréquemment utilisées (balise 'Favori').

Pour afficher toutes les entrées qui ont une balise spécifique, cliquez sur le bouton à trois touches [] dans la barre d'outils de la fenêtre principale (à droite du bouton de la barre d'outils 'Rechercher') et choisissez la balise. Alternativement, cette commande est également accessible via le menu principal : 'Rechercher' → 'Balise (tag)' → choisir la balise.

Si vous souhaitez voir toutes les entrées avec une balise spécifique (par exemple : 'Favori') lors de l'ouverture d'une base de données, alors vous pouvez créer un déclencheur pour cela : cliquez sur 'Outils' → 'Déclencheurs', ajoutez un nouveau déclencheur, entrez un nom (par exemple : 'Afficher les favoris lors de l'ouverture d'une base de données'), ajoutez un événement 'Le fichier de base de données est ouvert' et ajoutez une action 'Afficher les entrées par balise (tag)' avec le paramètre 'Balise (tag)' défini sur le nom de la balise (par exemple : "Favori").

Remplacer l'adresse (URL) :
Consulter ' La modification du gestionnaire d'adresse'.

UUID.
Un UUID est un nombre de 128 bits qui identifie uniquement un objet (une entrée dans ce cas-là).

À certains endroits (par exemple : dans les références de champ), un UUID a besoin d'être spécifié dans la forme hexadécimale. À D'autres endroits (par exemple : dans les fichiers XML KDBX), un UUID est stocké dans la forme Base64.

La boîte de dialogue de l'entrée affiche à la fois les formes (hexadécimale et Base64), ainsi vous pouvez directement copier la forme dont vous avez actuellement besoin.

La saisie automatique

Sur cet onglet, vous pouvez configurer le comportement de la saisie automatique pour l'entrée actuelle. Voir la page d'aide sur la saisie automatique.

Historique

Chaque entrée a sa propre histoire. Lors de la modification d'une entrée, KeePass crée automatiquement une entrée d'historique, qui contient les données précédentes. Les entrées de l'historique sont répertoriées sur l'onglet 'Historique' de la boîte de dialogue de l'entrée.

Par défaut, le nombre d'entrées d'historique par entrée et la taille de l'historique par entrée sont limités à des valeurs raisonnables. Vous pouvez modifier ces limitations dans la boîte de dialogue des paramètres de la base de données (menu 'Fichier' → 'Paramètres de la base de données').

Si vous souhaitez supprimer manuellement certaines entrées de l'historique, alors deux possibilités s'offrent à vous :

- Sur l'onglet 'Historique' de la boîte de dialogue de l'entrée, vous pouvez supprimer des entrées d'historique spécifiques.
- Dans 'Outils' → 'Outils de la base de données' → 'Maintenance de la base de données...', vous

pouvez supprimer toutes les entrées de l'historique qui sont antérieures à un nombre de jours spécifique.

Les outils

Lorsque vous cliquez sur le bouton 'Outils' (en bas à gauche dans la boîte de dialogue de l'entrée), un menu s'affiche et propose des commandes utiles.

Copiez le mot de passe initial.
Copie (dans le presse-papiers) le mot de passe qui était en cours lorsque la boîte de dialogue a été ouverte. Cette commande peut être utile par exemple lorsque vous essayez de changer le mot de passe et que le site Web/service demande le mot de passe précédent comme confirmation*après* avoir spécifié le nouveau mot de passe.

Commandes du champ Adresse (URL).
Ces commandes modifient le champ Adresse (URL).

Insérer une référence à un champ.
Lorsque vous cliquez sur l'une des commandes de ce sous-menu, une boîte de dialogue s'affiche qui permet de créer facilement une référence de champ dans le champ choisi.

Les paramètres du générateur OTP.
Affiche une boîte de dialogue pour modifier facilement les paramètres du générateur de mot de passe à usage unique de l'entrée.

L'édition de plusieurs entrées en une fois

La boîte de dialogue de l'entrée prend en charge l'édition d'entrées multiple en une fois. Pour cela, sélectionnez plusieurs entrées dans la liste d'entrées de la fenêtre principale et invoquez la commande 'Éditer les entrées'.

- Si les entrées contiennent différentes valeurs pour un champ (par exemple : si les entrées ont différents noms d'utilisateur), alors la boîte de texte dans la boîte de dialogue de l'entrée affiche "(valeurs multiples)". Si vous ne changez pas ceci, alors les valeurs pour ce champ ne seront pas modifiées. Si vous le changez, alors la nouvelle valeur sera assignée à toutes les entrées.
- Dans le cas d'une option booléenne, la case à cocher peut prendre en charge trois états :
  - Non coché. L'option est/sera désactivée pour toutes les entrées.
  - Coché. L'option est/sera activée pour toutes les entrées.
  - Indéterminé. Pour certaines entrées, l'option sera désactivée, tandis que pour les autres entrées, il sera activé. Les états ne seront pas modifiés.

Les contrôles pour les données qui ne peuvent pas être modifiées dans des entrées multiples en une fois (par exemple : les fichiers en pièces jointes) sont désactivés. De telles données ne seront pas modifiées.

Les options de l'interface

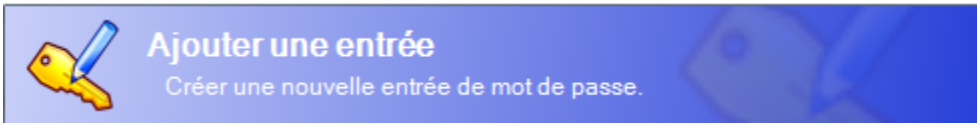
Les options de l'interface graphique de l'utilisateur
Expliquent diverses options de l'interface graphique de l'utilisateur.

- Les styles de bannières de la boîte de dialogue

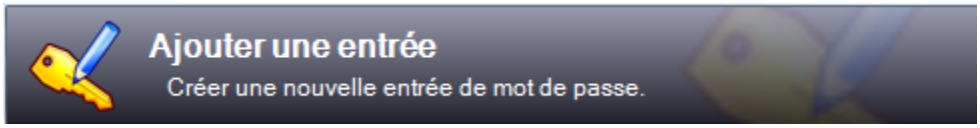
Les styles de bannières de la boîte de dialogue

KeePass prend en charge différents styles de bannières de la boîte de dialogue. Ces styles sont indépendants du système d'exploitation et peuvent être librement utilisés sur tous les systèmes.

Bleu :

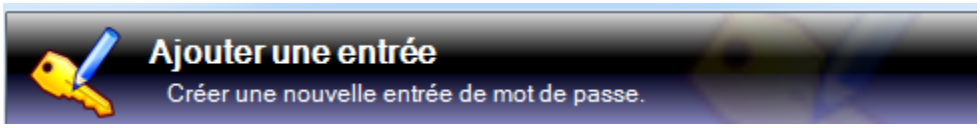


Sombre :



Clair :

Bleu carbone :



Charger/Enregistrer depuis/vers une adresse (URL)

Dans cette boîte de dialogue, vous pouvez spécifier une adresse (URL), à partir de/vers laquelle les données sont lues/écrites.

Par défaut, KeePass prend en charge **FTP**, **HTTP**, **HTTPS** et **WebDAV**. Plusieurs protocoles supplémentaires peuvent être disponibles sur votre système (si des fournisseurs spécifiques sont installés).

Le greffon IOProtocolExt ajoute la prise en charge de **SCP**, **SFTP** et **FTPS**.

Stockage dans le nuage :
Si vous souhaitez stocker votre fichier de base de données dans un stockage en nuage : pour la plupart des stockages en nuage, il existe une intégration avec le système de fichier local (c-à-d. vous pouvez accéder aux fichiers en utilisant l'explorateur de fichiers Windows). Par exemple : Dropbox, Microsoft OneDrive et Google Drive fournissent une telle intégration. Si une telle intégration est disponible, alors il est recommandé que vous accédiez au fichier de la base de données de cette façon ; ceci fonctionne souvent mieux qu'en y accédant par le protocole FTP ou WebDAV. Si une telle intégration n'est pas disponible et que le stockage en nuage n'est également pas accessible via un protocole standard, alors un greffon spécifique de KeePass pour le stockage en nuage devrait être disponible.

Exemple : en utilisant un serveur FTP

Afin de charger/enregistrer votre base de données depuis/vers un serveur FTP, vous devez d'abord charger le fichier de la base de données sur le serveur manuellement. Cela a seulement besoin d'être fait une fois.

Ensuite, démarrez KeePass et allez dans *'Fichier' → 'Ouvrir' → 'Ouvrir une adresse (URL)...'*. Entrez le chemin complet de la base de données et n'oubliez pas le préfixe `ftp://` ! Ce préfixe est obligatoire, sinon KeePass ne sait pas quel protocole utiliser. Saisissez l'accréditation (les informations d'identification) FTP et cliquez sur [OK]. KeePass téléchargera le fichier et l'ouvrira.

KeePass peut se souvenir de l'accréditation (les informations d'identification) FTP, si vous le souhaitez. Vous pouvez choisir entre se souvenir de tout (nom d'utilisateur et mot de passe), partiellement (nom d'utilisateur uniquement) ou ne pas se souvenir du tout de l'accréditation (les informations d'identification).

Quand vous appuyez sur le bouton 'Enregistrer', KeePass chargera automatiquement la nouvelle base de données sur le serveur (même emplacement que précédemment, c'est-à-dire en écrasant le précédent).

Les FAQ

La FAQ administrative

La FAQ administrative

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

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 bogues. 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, gravez 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 (2.x).

Qu'en est-il d'un serveur Internet de 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, respectez 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 KeePass 2.x ne s'exécute-t-il pas sur mon ordinateur ?
- Pourquoi KeePass 2.x tombe-t-il en panne lors de son démarrage à partir d'un lecteur/partage réseau ?
- Est-ce que KeePass 2.x utilise les implémentations d'algorithme validées FIPS ?
- Pourquoi le fichier d'aide CHM ne fonctionne-t-il pas ?
- Où puis-je trouver plus d'*icônes d'application* pour les raccourcis Windows ?
- Comment puis-je ajouter plus d'*icônes client* 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 ?
- Que faire en cas d'un conflit de raccourci clavier global ?
- Pourquoi KeePass essaie-t-il de se connecter à Internet ?
- Est-ce que l'interface graphique de l'utilisateur prend en charge les thèmes sombres ?
- Comment modifier la (taille) 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 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-t-elle 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 KeePass 2.x ne s'exécute-t-il pas sur mon ordinateur ?

Les symptômes : lorsque vous essayez d'exécuter KeePass 2.x sous Windows ≤ XP, un message d'erreur comme le suivant s'affiche :
"Un fichier .DLL est requis, MSCOREE.DLL, est introuvable" ou
"L'application n'a pas réussi à s'initialiser correctement (0xc0000135)" .

La cause : KeePass 2.x nécessite Le Framework .NET ≥ 3.5 de Microsoft.

La résolution : installer le Framework .NET 3.5 ou supérieur de Microsoft. Il est disponible en téléchargement gratuit sur le site Web de Microsoft : Microsoft .NET Framework. Alternativement, vous pouvez l'installer via Windows Update (le framework est un composant facultatif).

KeePass 1.x ne nécessite pas ce framework.

Pourquoi KeePass 2.x tombe-t-il en panne lors de son démarrage à partir d'un lecteur/partage réseau ?

Les symptômes : lorsque vous essayez d'exécuter KeePass 2.x à partir d'un lecteur/partage réseau, vous obtenez un message d'erreur comme celui-ci :
"L'application a généré une exception qui n'a pas pu être gérée" ou
"KeePass a rencontré un problème et doit fermer".

La cause : la stratégie de sécurité par défaut stricte du Framework .NET de Microsoft interdit l'exécution d'applications .NET à partir d'un lecteur/partage réseau.

La résolution recommandée : copier/installer KeePass 2.x sur un disque dur local et exécuter la copie.

La résolution alternative non recommandée : configurez la stratégie de sécurité pour autoriser l'exécution d'applications .NET à partir de lecteurs/partages réseau. Demandez à votre administrateur de le faire (des droits d'administrateur sont requis). Si vous disposez des droits administrateur et que vous souhaitez le faire vous-même, alors vous pouvez utiliser l'outil de stratégie de sécurité d'accès au code (Caspol.exe) fourni avec le framework .NET (des instructions utiles peuvent être trouvées ici et ici).

Est-ce que KeePass 2.x utilise les implémentations d'algorithme validées FIPS ?

KeePass utilises plusieurs algorithmes. Cette FAQ répond en se concentrant sur les algorithmes utilisés pour le chiffrement/déchiffrement d'un fichier de base de données. Typiquement, KeePass utilise principalement AES-256, SHA-256, HMAC-SHA-256 et SHA-512 ici (sauf si l'utilisateur a spécifié un autre algorithme de chiffrement ou une autre fonction de dérivation de clé dans les paramètres de la base de données). Pour ces algorithmes, le Framework .NET fournit les classes, et KeePass les utilises.

Depuis la version 4.8, le Framework .NET prend en charge les implémentations des algorithmes validés FIPS ci-dessus (see 'Qu'est-ce qu'il y a de nouveau dans le Framework .NET 4.8 ?').

Pour une compatibilité avec les versions anciennes du Framework .NET, KeePass ignore le mode FIPS par défaut. Si tous vos PC ont le Framework .NET 4.8 ou supérieur d'installé, alors vous pouvez activé l'utilisation des implémentations d'algorithme validés FIPS en ouvrant le fichier 'KeePass.exe.config' à l'aide

d'un éditeur de texte et effacer la ligne '`<enforceFIPSPolicy enabled="false" />`'.

Les implémentations d'autres algorithmes (tels que ChaCha20 et Argon2) ne sont pas validées FIPS. Si Microsoft fournira des implémentations validées de ces algorithmes dans le futur, alors nous considérons que nous les utiliserons.

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 d'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 clientes 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.

Vous pouvez importer vos propres icônes dans les bases de données de KeePass. Pour cela, cliquez sur le bouton *'Ajouter...'* dans la boîte de dialogue du sélecteur d'icônes.

Les formats pris en charge sont BMP, EMF, GIF, ICO, JPEG, PNG, TIFF et WMF.

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

Les fonctions peuvent être bloquées/forcées en utilisant un fichier de configuration forcée.

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

Cela ne s'applique pas à KeePass 2.x.

Que faire en cas d'un conflit de raccourci clavier global ?

Par défaut, la touche de raccourci global accomplissant une saisie automatique est Ctrl+Alt+A. Cependant, il existe quelques modèles de clavier où cette combinaison de touches est utilisée pour saisir un caractère. Par exemple, il existe une disposition de clavier français où cette combinaison de touches

produit le caractère 'æ', et il ya une disposition de clavier polonais où il produit le caractère 'ą' En cas d'un tel conflit, vous avez besoin de décider si vous voulez que la combinaison de touche ontinue d'être une touche de raccourci global ou si vous voulez la changer.

Dans KeePass 2.x, les touches de raccourci globales peuvent être modifiées dans 'Outils' → 'Options' → onglet 'Intégration'.

Pourquoi l'impression ne fonctionne pas dans KeePass 1.x ?

Les symptômes : lorsque vous essayez d'imprimer une liste de mots de passe dans KeePass 1.x, rien ne se passe après avoir cliqué sur OK dans la boîte de dialogue 'Options d'impression'.

La cause : KeePass 1.x utilise l'application associée aux fichiers `.html` pour imprimer la liste des mots de passe. Si cette application ne prend pas en charge le verbe shell "print" (comme Mozilla Firefox), alors rien ne se passe.

La résolution : Associez les fichiers `.html` à une autre application qui prend en charge le verbe shell "print" (telle qu'Internet Explorer).

La résolution alternative/la solution de contournement : cliquer sur *"Fichier" → 'Aperçu avant impression'* dans KeePass 1.x et imprimez manuellement le document dans l'application qui vient d'ouvrir le fichier.

Pourquoi KeePass essaie-t-il de se connecter à 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.

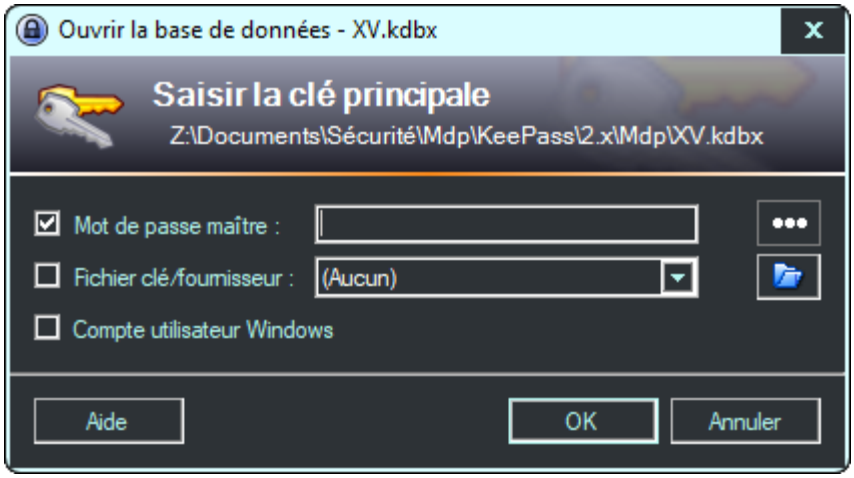
Quans on démarre KeePass pour la première fois, le logiciel demande si la vérification de la mise à jour automatique soit être activée (recommandée). Elle peuvt être activée/désactivée dans 'Outils' → 'Options...' → onglet 'Avancé'.

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

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

- Sur Windows 11, un thème (sombre) peut être sélectionné dans les paramètres Windows → 'Accessibilité' → 'Thèmes de contraste'.
- Sur Windows 10, un thème (sombre) peut être sélectionné dans les paramètres Windows → 'Personnalisation' → 'Thèmes' → 'Paramètres de contraste élevé'.
- Sur Windows 7, 8 et 8.1, un thème (sombre) peut être sélectionné dans le panneau de configuration → 'Apparence et personnalisation' → 'Personnalisation'.

Exemple (Windows 11, thème 'Crépuscule') :



Option 'Choisir votre mode (application par défaut) ' → 'Sombre'.
Windows 11 possède une option 'Choisir votre mode' (sur Windows 10, c'est nommé 'Choisir votre mode d'application par défaut'), qui peut être positionnée à 'Sombre'. Remarquer que cette option s'applique seulement aux applications UWP, et non aux applications Windows régulières. Windows permet l'option UWP pour contredire le thème du système (c-à-d. un thème de système claire peut être actif même si l'option UWP est positionnée à 'Sombre'). KeePass est une application Windows régulière, et non pas une application UWP, donc il suit le thème du système, pas celui de l'option UWP. C'est le comportement attendu ; KeePass n'a rien à voir avec le les options UWP.

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

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

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

- Sur Windows 11, la taille de la police peut être changée dans les paramètres Windows → 'Système' → 'Affichage' → 'Mise à l'échelle & disposition' → option 'Mise à l'échelle'. Redémarrer Windows après avoir modifié cette option.
  ⚠ *N*'utilisez *pas* cette option 'Taille du texte' (dans les paramètres Windows → 'Accessibilité' → 'Vision'), parce que cette option ne met pas proprement tous les textes à l'échelle.
- Sur Windows 10, la taille de la police peut être modifiée dans les paramètres Windows → 'Système' → 'Écran' → 'Mise à l'échelle et disposition' → option 'Modifier la taille du texte, des applications et d'autres éléments'. Redémarrer Windows après avoir modifié cette option.
  ⚠ *N*'utilisez *pas* l'option 'Agrandir le texte' (dans les paramètres Windows → 'Option d'ergonomie' → 'Écran'), parce que cette option ne met pas proprement tous les textes à l'échelle.
- Sur Windows 7, 8 et 8.1, la taille de la police peut être modifiée dans le panneau de configuration Windows → 'Apparence et Personnalisation' → 'Affichage'.
- Sur les systèmes Linux avec KDE 5 ou supérieur, la police peut être modifiée dans les paramètres du système → 'Polices'.
- Sur les systèmes Linux avec GNOME 3 ou supérieur, la police peut être modifiée en utilisant GNOME Tweaks → 'Polices'.

En supplément pour le support de ces paramètres système, KeePass permet de personnaliser la taille qui est utilisée dans les listes et pour les mots de passe (dans la boîte de dialogue des options ; ces paramètres affectent seulement KeePass et aucune autre application).

Si vous voulez juste changer la police de l'interface graphique de KeePass (ce qui n'est généralement pas une bonne idée) : le greffon KeeUIExt fournit une option pour cela. Cependant, il est recommandé d'utiliser les paramètres ci-dessus à la place.

La fonction de saisie automatique résiste-t-elle aux enregistreurs de frappes ?

Par défaut : non. La méthode de saisie automatique de KeePass 2.x fonctionne de la même manière que celle de 1.x et n'est donc pas sécurisée pour les enregistreurs de frappes.

Cependant, KeePass propose une méthode alternative appelée obfuscation de saisie automatique à deux canaux (TCATO), qui rend les enregistreurs de frappes inutiles. Il s'agit d'une fonctionnalité opt-in (car elle ne fonctionne pas avec toutes les fenêtres) et doit être activée manuellement pour les entrées. Consulter la documentation TCATO pour plus de détails.

Est-ce la saisie automatique peut localiser les commandes 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 chiffrement ... à KeePass ?

AES (Rijndael) et ChaCha20 sont pris en charge. Il existe divers greffons qui prennent en charge des algorithmes de chiffrement supplémentaires, y compris, mais sans s'y limiter, Twofish, Serpent et GOST.

Si vous souhaitez implémenter un algorithme, jetez un œil à l'exemple de greffon *ArcFourCipher*.

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-t-elle 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) ?

KeePass dispose d'un éditeur intégré qui permet de travailler facilement avec de grandes quantités de textes (formatés).

Pour ajouter un long texte à une entrée, alors importez le fichier en tant que pièce jointe (ou cliquez sur 'Joindre' → 'Créer une pièce jointe vide'). L'éditeur intégré prend en charge les fichiers *.TXT (texte simple) et *.RTF (texte formaté).

Pour modifier une pièce jointe, faites un clic droit sur l'entrée dans la fenêtre principale, pointez sur "Pièces jointes" et cliquez sur '*"VotreFichier.*"*. Alternativement, si le fichier texte est la seule pièce jointe, alors vous pouvez l'ouvrir en double-cliquant simplement dessus dans la fenêtre principale (activer l'affichage de la colonne de pièce jointe dans 'Affichage' → 'Configurer les colonnes' → 'Pièces jointes'). Alternativement, il est également possible de cliquer sur le nom de la pièce jointe dans la vue des détails de l'entrée de la fenêtre principale.

Pour les fichiers TXT, l'éditeur intégré prend en charge les opérations standard telles que couper, copier, coller, annuler, renvoyer à la ligne, etc. Pour les fichiers RTF, des commandes de formatage standard supplémentaires sont disponibles : choix de la police, taille de la police, gras, italique, souligné, barré, couleurs du texte et de l'arrière-plan, alignement gauche/centre/droite, etc.

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 soit 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 (2.x)

KeePass 2.x propose diverses options permettant aux administrateurs réseau de personnaliser l'apparence et le comportement du programme.

- Les préliminaires
- Les exigences minimales du mot de passe maître
- La spécification d'états d'éléments de l'interface utilisateur
- Davantage d'options

Les préliminaires

La plupart des options ci-dessous sont configurées en modifiant directement le fichier de configuration KeePass.config.xml. Si vous envisagez de déployer une version personnalisée de KeePass, alors vous devez bien comprendre tout le système de configuration de KeePass, en particulier comment appliquer certains paramètres et laisser les autres aux utilisateurs ?

Notez que KeePass propose un cadre de greffons riche. S'il n'y a pas d'élément dans le fichier XML pour configurer ce à quoi vous pensez, alors vous pouvez écrire un greffon.

Les exigences minimales du mot de passe maître

Vous pouvez spécifier plusieurs propriétés que les mots de passe maîtres doivent avoir pour être acceptés (longueur, qualité estimée, etc.). Reportez-vous à la section spécifications des propriétés minimales du mot de passe maître.

La spécification d'états d'éléments de l'interface utilisateur

L'état (activé, désactivé, visible, masqué) de plusieurs éléments de l'interface utilisateur (UI) peut être spécifié à l'aide de la valeur `UIFlags` du nœud `UI` dans le fichier de configuration. Il peut s'agir d'une combinaison au niveau du bit d'un ou plusieurs des indicateurs (flags) suivants :

Indicateur (Hex)	Indicateur (Dec)	Description
0x0	0	Ne forcer aucun état (par défaut).
0x1	1	Désactiver l'élément de menu 'Outils' → 'Options'.
0x2	2	Désactiver l'élément de menu 'Outils' → 'Greffons'.
0x4	4	Désactiver l'élément de menu 'Outils' → 'Déclencheurs'.
0x8	8	Désactiver les contrôles pour spécifier après combien de jours la clé principale devrait/doit être changée.
0x10	16	Masquer les barres de progression de la qualité du mot de passe et les étiquettes d'information.
0x20	32	Désactiver l'élément de menu 'Aide' → 'Vérifier les mises à jour...'.
0x40	64	Désactiver l'élément de menu 'Outils' → 'Outils de base de données' → 'Remplacer XML...'.
0x80	128	Désactiver l'élément de menu 'Fichier' → 'Paramètres de la base de données...'.
0x10000	65536	Masquer les profils intégrés dans le menu contextuel du générateur

		de mot de passe de la boîte de dialogue d'édition d'entrée.
0x20000	131072	Afficher les éléments UI liés aux derniers temps d'accès. *Remarque :* Les bases de données ne sont pas marquées comme modifiées lorsqu'un temps de dernier accès change. Ainsi, lorsque seuls les derniers temps d'accès sont modifiés et que l'utilisateur ferme la base de données (sans enregistrer manuellement au préalable et sans sauvegarde forcée par exemple par un déclencheur ou un greffon), les modifications apportées aux derniers temps d'accès sont perdues.
0x40000	262144	N'affiche pas les boîtes de dialogue d'informations lors de la création d'une nouvelle base de données.
0x80000	524288	Ne pas afficher les boîtes de dialogue d'informations sur la compatibilité de l'obfuscation de saisie automatique.
0x100000	1048576	Ne pas effacer la liste des termes de recherche rapide lors de la fermeture/du verrouillage d'une base de données. *Remarque :* même si cet indicateur est positionné, alors la liste est effacée lorsque vous quittez KeePass. Si vous effectuez fréquemment les mêmes recherches, envisagez d'utiliser des balises ou des profils de recherche.
0x200000	2097152	Activer l'éditeur de méthode d'entrée (IME) sur les bureaux sécurisés. ⚠ Cela peut entraîner des problèmes (écran noir, processus IME/CTF

		avec une utilisation élevée du processeur, etc.). Voir 'Why does the Input Method Editor (IME) not work?'.
0x400000	4194304	Ajuste automatiquement la faiblesse des paramètres de la transformation de clé aux valeurs par défauts courants, sans boîte de dialogue d'un avertissement/confirmation. Si ce bit `UIFlags` est positionné, l'option 'Montrer un avertissement quand la transformation de clé est faible' (qui est activée par défaut) n'a aucun effet. Quand on ajuste les paramètres de la transformation de clé, la base de données est marquée comme modifiée.

La valeur de `UIFlags` doit être spécifiée en notation décimale.

Par exemple : si vous souhaitez désactiver les éléments de menu 'Options' et 'Vérifier les mises à jour...', alors vous devez spécifier 33 comme valeur pour le nœud `UIFlags` (0x1 + 0x20 = 1 + 32 = 33).

Davantage d'options

- **Configuration/Application/ConfigSave** :
  Si cette option est définie sur `false` (faux), alors KeePass n'enregistre aucun paramètre de configuration (c'est-à-dire que la configuration est chargée normalement, mais les modifications apportées à celle-ci sont abandonnées lors de la fermeture de KeePass).
- **Configuration/Application/ExpirySoonDays** :
  Spécifie le nombre de jours pendant lesquels les entrées sont considérées comme expirant "bientôt". La valeur par défaut est 7.
- **Configuration/Application/HelpUrl** :
  Spécifie l'URL qui est ouverte pour une page d'aide. Cela remplace toutes les autres sources d'aide (locales et en ligne). Compilé par Spr ; le chemin relatif de la page d'aide est inséré par `{BASE}`. Cet élément est utilisé seulement si il est enregistré dans le fichier de configuration imposée.
- **Configuration/Defaults/WinFavsBaseFolderName** :
  Pour l'exportation des 'Favoris Windows' : nom du dossier racine ; la valeur par défaut est 'KeePass'.
- **Configuration/Defaults/WinFavsFileNamePrefix** :
  Pour l'exportation des 'Favoris Windows' : préfixe pour le titre de chaque favori ; la valeur par défaut est une chaîne vide.
- **Configuration/Defaults/WinFavsFileNameSuffix** :
  Pour l'exportation des 'Favoris Windows' : suffixe pour le titre de chaque favori ; la valeur par défaut est une chaîne vide.
- **Configuration/Integration/AutoTypeInterKeyDelay** :
  Spécifie le délai par défaut (en ms) entre deux pressions de touches envoyées par la saisie automatique. Le minimum est de 1 ms. Notez que de très petits délais peuvent empêcher les applications cibles de traiter correctement les touches pressées.
- **Configuration/Integration/AutoTypeAbortOnWindows** :
  Ce nœud peut contenir un ou plusieurs nœuds `Window` qui spécifient des fenêtres cibles de type

automatique non autorisées (la valeur de chaque nœud doit être un filtre de fenêtre cible). Par exemple : la configuration suivante interdit la saisie automatique dans le Bloc-notes et LibreOffice Writer :

```
<AutoTypeAbortOnWindows>
    <Window>* - Bloc-notes</Window>
    <Window>* - LibreOffice Writer</Window>
</AutoTypeAbortOnWindows>
```

- **Configuration/Security/ProtectProcessWithDacl** :
  Si cette option est positionnée à `true` (vrai), alors KeePass protège son processus avec une liste de contrôle d'accès discrétionnaire (DACL).
  ⚠ Veuillez noter que cela empêche également d'autres logiciels légitimes (outils liés à l'accessibilité tels que Windows Narrator, d'autres produits de sécurité tels que des programmes antivirus ou des pare-feux, des outils fournissant des améliorations de l'interface utilisateur, etc.) de fonctionner avec KeePass. En outre, divers problèmes tels que des blocages d'applications, des exceptions et des plantages peuvent survenir. Par conséquent, cette option est désactivée par défaut et ne peut être activée qu'en éditant manuellement le fichier de configuration. Il ne fonctionne raisonnablement que dans des scénarios d'utilisation très spécifiques et limités, puis n'est pas recommandé pour la plupart des utilisateurs.
  Cette option ne fonctionne que sur Windows et nécessite la bibliothèque KeePassLibN (incluse dans les installations et packages par défaut).
- **Configuration/UI/TrayIcon/ShowOnlyIfTrayedEx** :
  Si cette option est positionnée à `true` (vrai), alors l'icône de KeePass dans la zone de notification s'affiche uniquement si la fenêtre principale a été réduite à la barre des tâches.
  ⚠ L'activation de cette option peut entraîner des problèmes de déni de service. Si vous souhaitez masquer l'icône KeePass, alors il est recommandé de le configurer plutôt dans les paramètres système voir 'Customize the Taskbar in Windows (Personnaliser la barre des tâches dans Windows)'.

La création de greffons

La création de greffons (2.x)

Comment développer des greffons pour KeePass 2.x ?

Cette documentation s'applique aux greffons de KeePass 2.x. Les greffons 2.x sont fondamentalement différents des greffons 1.x. Les greffons 1.x ne peuvent pas être chargés par KeePass 2.x.

- Les exigences
- Le tutoriel pas à pas
- Les opérations communes :
  - La fourniture d'éléments de menu
- Les conventions d'un greffon
- La vérification de la mise à jour
- Est-ce que les greffons de KeePass 2.x peuvent être écrits en C++ non managé ?
- Les fichiers PLGX

Les exigences

Avant de pouvoir commencer à développer un greffon KeePass, vous avez besoin des prérequis suivants :

- Le dernier package portable KeePass ZIP. Vous pouvez l'obtenir sur le site Web de KeePass.
- Un IDE de développement C# (≥ 2.0) (par exemple : Microsoft Visual Studio ou SharpDevelop).

Le tutoriel pas à pas

Démarrez votre IDE préféré et créez un nouveau projet de *bibliothèque de classes C#* (pour le Framework .NET, et non pas pour le Standard/Core .NET). Dans ce tutoriel, l'exemple de greffon que nous développons s'appelle `SimplePlugin`. La première chose que vous devez faire maintenant est d'ajouter

une *référence* à KeePass : accédez à la boîte de dialogue des références et sélectionnez le fichier `KeePass.exe` (à partir du package ZIP portable). Après avoir ajouté la référence, les espaces de noms `KeePass` et `KeePassLib` devraient être disponibles.

Il est important que vous fassiez référence à un `KeePass.exe` officiel, et non à un instantané de développement ou à votre propre build, car sinon votre greffon sera incompatible avec les builds officiels de KeePass.

Tous les greffons KeePass doivent dériver d'une classe de `greffon` d'un KeePass de base (un greffon dans l'espace de noms KeePass.Plugins). En remplaçant les méthodes et les propriétés de cette classe, vous pouvez personnaliser le comportement de votre greffon.

Un greffon minimal ressemble à ceci :

```
using System;
using System.Collections.Generic;

using KeePass.Plugins;

namespace SimplePlugin
{
public sealed class SimplePluginExt : Plugin
{
private IPluginHost m_host = null;

public override bool Initialize(IPluginHost host)
{
if(host == null) return false;
m_host = host;
return true;
}
}
}
```

Vous pouvez trouver une version entièrement documentée et étendue de ce greffon simple sur la page Web des greffons de KeePass.

Ce greffon ne fait exactement rien, mais il montre déjà quelques conventions importantes, qui doivent être suivies par tous les greffons :

- namespace (l'espace de noms) doit être nommé comme le fichier DLL sans extension. Notre fichier DLL s'appelle `SimplePlugin.dll`, donc namespace doit s'appeler `SimplePlugin`.
- La classe principale du greffon (que KeePass instanciera lorsqu'il chargera votre greffon) doit être appelée exactement de la même manière que le namespace plus "Ext". Dans ce cas : "SimplePlugin" + "Ext" = "SimplePluginExt".
- La classe de greffon principale doit être dérivée de la classe de base `KeePass.Plugins.Plugin`.

La fonction `Initialize` est la plus importante et vous la remplacerez probablement toujours. Dans cette fonction, vous obtenez une interface vers les composants internes de KeePass : une référence d'interface `IPluginHost`. Grâce à cette interface, vous pouvez accéder au menu principal de KeePass, à la base de données actuellement ouverte, etc. La fonction `Initialize` est appelée immédiatement après que KeePass a chargé votre greffon. Toute initialisation doit être effectuée dans cette méthode (**pas** dans le constructeur de votre classe de greffon !). Si vous avez tout initialisé avec succès, alors vous devez retourner `true`. Si vous retournez `false`, alors KeePass déchargera immédiatement votre greffon.

Une seconde fonction dont vous aurez très souvent besoin est la méthode `Terminate` :

```
public override void Terminate()
{
}
```

Cette fonction est appelée peu de temps avant que KeePass ne décharge votre greffon. Vous ne pouvez pas interrompre ce processus (c'est juste une notification et votre dernière chance de nettoyer toutes les ressources utilisées, etc.). Immédiatement après votre retour depuis cette méthode, KeePass peut décharger votre greffon. Il est fortement recommandé de libérer toutes les ressources dans cette méthode (**pas** dans le destructeur de votre classe de greffon !).

Nous avons presque terminé ! Nous devons maintenant dire à KeePass que notre fichier est un greffon

KeePass. Cela se fait en éditant *le bloc d'informations de version* du fichier. Ouvrez la boîte de dialogue d'édition de la version du fichier (dans Visual Studio 2005 : cliquez avec le bouton droit sur le nom du projet → *'Propriétés'* → bouton *'Informations sur l'assemblage'*). Tous les champs peuvent être attribués librement à l'exception du champ *Nom du produit* (pour plus d'informations, voir Les conventions d'un greffon). Ce champ doit être positionné à "`KeePass Plugin`" (sans les doubles quotes).

C'est ça ! Essayez maintenant de compiler votre greffon et de copier le fichier DLL résultant dans le répertoire KeePass. Si vous démarrez KeePass et accédez à la boîte de dialogue des greffons, alors vous devriez voir votre greffon dans la liste des greffons chargés.

La fourniture d'éléments de menu

De nombreux greffons fournissent des éléments de menu (avec des sous-éléments, si nécessaire) dans des emplacements bien en vue comme le menu 'Outils', le menu contextuel d'entrée, etc. Un tel élément de menu peut être fourni à KeePass en remplaçant la méthode `GetMenuItem` de votre classe de greffon (qui dérive de la classe de base du `greffon`). Dans cette méthode, le greffon peut construire et renvoyer un `ToolStripMenuItem`, que KeePass affichera ensuite à l'emplacement approprié.

Les utilisateurs doivent pouvoir associer l'élément de menu à votre greffon. En règle générale, les greffons positionnent le texte de l'élément de menu sur le nom du greffon ou sur une chaîne de caractères commençant par le nom du greffon. Par exemple, un greffon 'Abcd' qui veut fournir un seul élément de menu (pour l'accès aux options du greffon) pourrait positionner le texte de l'élément de menu sur 'Options Abcd'. Si le greffon prend en charge plusieurs commandes, alors positionnez le texte de l'élément de menu sur le nom du greffon (par exemple 'Abcd') et ajoutez un sous-élément pour chaque commande.

La méthode `GetMenuItem` doit toujours construire et retourner un nouveau `ToolStripMenuItem`. Ne mettez pas en cache l'élément de menu ou l'un de ses sous-éléments à des fins ultérieures (KeePass peut invoquer la méthode `GetMenuItem` plusieurs fois et afficher les éléments de menu à plusieurs endroits ; si votre greffon mettait en cache un élément de menu, alors essayer de l'afficher à plusieurs endroits entraînerait des problèmes, car un `ToolStripMenuItem` ne peut avoir qu'un seul élément parent). Si vous souhaitez mettre à jour l'état des sous-éléments (comme désactiver certains éléments ou afficher des coches), alors vous pouvez le faire par exemple dans une méthode anonyme qui gère l'événement `DropDownOpening` de l'élément de menu renvoyé (de cette façon, vous n'avez pas besoin de vous souvenir manuellement des références de l'élément de menu); voir SamplePlugin pour un exemple.

KeePass prend possession de l'élément de menu renvoyé (et de ses sous-éléments). Le greffon ne doit pas ajouter ou supprimer l'élément à/depuis n'importe quel menu lui-même ; KeePass le fera.

Si votre greffon ne fournit pas d'élément de menu à l'emplacement spécifié par le paramètret de `PluginMenuType` , alors, renvoyez `null`.

Exemple:

```
public override ToolStripMenuItem GetMenuItem(PluginMenuType t)
{
// Provide a menu item for the main location(s)
if(t == PluginMenuType.Main)
{
ToolStripMenuItem tsmi = new ToolStripMenuItem();
tsmi.Text =   "Abcd Options";
tsmi.Click +=   this.OnOptionsClicked;
return tsmi;
}

return null; // No menu items in other locations
}

private void OnOptionsClicked(object sender, EventArgs e)
{
// Called when the menu item is clicked
}
```

Pour un exemple sur comment créer un élément de menu avec des sous-éléments (et de mise à jour dynamique de leurs états), consultez l'exemple de greffon SamplePlugin.

Les conventions d'un greffon

Bloc d'informations sur la version du fichier :

KeePass utilise le bloc d'informations sur la version du fichier pour détecter si un fichier DLL est un greffon KeePass et il en récupère les informations à afficher dans la boîte de dialogue des greffons. Les champs sont utilisés comme suit :

- **Title:** doit contenir le nom complet du greffon.
- **Description:** doit contenir une courte description (pas plus de 5 lignes) de votre greffon.
- **Company:** doit contenir le nom de l'auteur du greffon.
- **Product name:** doit être positionné à `"KeePass Plugin"` (sans les doubles quotes).
- **Copyright:** non utilisé par KeePass ; librement assignable par le greffon.
- **Trademarks:** non utilisées par KeePass ; librement assignable par le greffon.
- **Assembly version:** doit être positionné à la version de votre greffon.
- **File version:** doit être positionné à la version de votre greffon. C'est à vous de décider comment vous versionnez vos versions de greffon, mais cela devrait être un schéma qui permet des comparaisons de version (en comparant les composants de version). *N*'utilisez *pas* d'astérisques pour créer un numéro de version au moment de la génération.
- **GUID:** non utilisé par KeePass ; librement assignable par le greffon.

Name, namespace et class name :

Si vous souhaitez utiliser le nom (name) "KeePass" en tant que partie du nom de votre greffon, alors préfixez/ajoutez directement un préfixe/suffixe non numérique. Par exemple, "KeePassSync" est correct, mais "KeePass Sync" ne l'est pas.

L'espace de noms (namespace) doit être nommé comme le fichier DLL sans extension. Par exemple, si le fichier DLL est nommé `SecretImporter.dll`, alors vous devez appeler l'espace de noms `SecretImporter`.

La classe du greffon doit être nommée comme l'espace de noms plus "Ext". Pour le greffon SecretImporter, ce serait `SecretImporterExt`.

La vérification de la mise à jour

La vérification des mises à jour de KeePass ≥ 2.18 peut également vérifier les mises à jour des greffons. La prise en charge de la vérification des mises à jour est facultative ; les greffons n'ont pas à prendre en charge les vérifications de mise à jour.

Afin de prendre en charge les vérifications de mise à jour, les développeurs de greffon doivent effectuer les opérations suivantes :

- **Fournir le fichier d'informations de version :** lorsqu'un utilisateur final appelle une vérification de mise à jour, KeePass télécharge un fichier d'informations de version, qui spécifie les numéros de version actuels d'un ou plusieurs greffons. Chaque auteur de greffon héberge son propre fichier d'informations de version. Le format du fichier d'informations de version est décrit en détail ci-dessous.
- **Laisser KeePass savoir :** afin de pouvoir vérifier la version du greffon, KeePass doit savoir où se trouve votre fichier d'informations de version. Pour informer KeePass, remplacez la propriété de chaîne `UpdateUrl` de votre classe de greffon (celle dérivée de Plugin) pour renvoyer l'URL complète et absolue de votre fichier d'informations de version. Il doit s'agir d'une URL `https://` (pour la rétrocompatibilité, KeePass prend également en charge`http://` et `ftp://`, mais pour des raisons de sécurité, `https://` devrait être utilisé).

Les développeurs de greffon doivent mettre à jour leur fichier d'informations de version chaque fois qu'ils publient de nouvelles versions de leurs greffons.

Format de fichier d'informations de version :

- Le fichier est un simple fichier texte. Il doit être encodé en UTF-8 sans marque d'ordre d'octet (KeePass ≥ 2.21 prend en charge les BOM UTF-8 dans les fichiers d'informations de version, mais pour la compatibilité avec KeePass < 2.21, il est recommandé de ne pas utiliser de BOM). Toutes les fins de ligne sont prises en charge.
- La première ligne du fichier doit commencer par un caractère séparateur de votre choix. Le caractère de séparation peut être n'importe quel caractère, mais il ne doit pas apparaître dans les noms et les versions de greffon. Il est suggéré '`:`'.
- Chacune des lignes suivantes spécifie un nom de greffon et sa version actuellement disponible,

séparés par le caractère de séparation spécifié dans la ligne d'en-tête.

- Comme nom de greffon, la valeur du champ 'Title' dans le bloc d'informations de version du greffon doit être spécifiée. Pour les greffons gérés, il s'agit de la valeur spécifiée à l'aide de l'attribut d'assemblage `AssemblyTitle`.
- Comme numéro de version, la valeur de la version du fichier dans le bloc d'informations de version du greffon doit être spécifiée. Pour les greffons gérés, il s'agit de la valeur spécifiée à l'aide de l'attribut d'assemblage `AssemblyFileVersion`. Le .0 à la fin peut être supprimé (par exemple, spécifiez `1.3` au lieu de `1.3.0.0`).
- Le fichier doit se terminer par une ligne contenant uniquement le caractère de séparation.
- Vous pourriez éventuellement compresser votre fichier d'informations de version à l'aide de GZip (notez que ce n'est pas la même chose que Zip). Le nom du fichier doit alors se terminer par "`.gz`".

Exemple : supposons que vous développiez deux greffons : *MonGreffon1* (version 1.5) et *MonGreffon2* (version 1.13.2.17). Ensuite, votre fichier d'informations de version pourrait ressembler à ceci :

```
:
MonGreffon:1.5
MonGreffon:1.13.2.17
:
```

Si vous avez développé plusieurs greffons, alors il est recommandé de créer un fichier d'informations de version, de répertorier tous vos greffons dans ce fichier et de spécifier l'URL du fichier dans tous vos greffons. Lorsque KeePass vérifie les mises à jour, il ne télécharge votre fichier d'informations de version qu'une seule fois. Cela réduit le trafic réseau et est plus rapide que de télécharger un fichier d'informations de version pour chaque greffon séparément.

Signature : depuis KeePass 2.34, vous pouvez *éventuellement* signer numériquement votre fichier d'informations de version à l'aide de RSA/SHA-512.

- Une paire de clés RSA peut par exemple être générée comme suit :
```
using(RSACryptoServiceProvider rsa = new RSACryptoServiceProvider(4096))
{
rsa.PersistKeyInCsp =  false;
Console.WriteLine("Private key: " + rsa.ToXmlString(true));
Console.WriteLine("Public key: " + rsa.ToXmlString(false));
}
```
  Toutes les longueurs de clé prises en charge par `RSACryptoServiceProvider` sont prises en charge par KeePass (jusqu'à .NET 4.5, soit 384 à 16384 bits par pas de 8 bits). Nous recommandons au moins 2048 bits ; le fichier d'informations de version principal (contenant la version KeePass) utilise 4096 bits.
- Afin de dire à KeePass d'accepter un fichier d'informations de version spécifique uniquement lorsqu'il est vérifiable avec une clé publique spécifique, votre greffon doit appeler la méthode `UpdateCheckEx.SetFileSigKey` pour associer l'URL spécifiée à la clé publique spécifiée. La clé publique doit être une chaîne XML au format renvoyé par la méthode `RSACryptoServiceProvider.ToXmlString`. Ne stockez pas la clé privée dans votre greffon, uniquement la clé publique.
- Pour signer un fichier d'informations de version non signé, hachez toutes les lignes non vides coupées entre l'en-tête et la ligne de pied de page à l'aide du codage SHA-512, UTF-8, chaque ligne se terminant par `'\n'` (et non `"\r\n"`). Signez le hachage à l'aide de la clé privée (si vous utilisez `RSACryptoServiceProvider` : alors chargez la clé privée à l'aide de sa méthode `FromXmlString`, puis calculez la signature à l'aide de la méthode `SignData`). Encodez le hachage à l'aide de Base64 et ajoutez-le à la première ligne du fichier d'informations de version.

Est-ce que les greffons de KeePass 2.x peuvent être écrits en C++ non managé ?

Oui et non. Vous pouvez écrire la logique de votre greffon en C++ non managé (des API Win32 natives peuvent être utilisées). Cependant, vous devez fournir une interface managée à votre greffon, c'est-à-dire que vous devez exporter une classe managée dérivée de la classe de base du `Greffon` comme décrit dans le tutoriel. De plus, le C++ managé est nécessaire pour modifier les éléments internes de KeePass (les entrées, les groupes, la fenêtre principale, etc.).

Pour un exemple d'utilisation d'API non gérées dans un assemblage de greffon en C++ géré, consultez l'exemple de greffon SamplePluginCpp.

Il est fortement recommandé de développer des greffons en C#, et non en C++, pour des raisons de compatibilité (dans le cas des greffons natifs, des versions 32 et 64 bits distinctes sont nécessaires ; les greffons natifs ne fonctionnent pas sur des systèmes de type Unix ; etc.).

Les fichiers PLGX

PLGX est un format de fichier de greffon *optionnel* pour KeePass ≥ 2.09. Au lieu de compiler votre greffon dans un fichier DLL, les fichiers de code source du greffon peuvent être empaquetés dans un fichier PLGX et KeePass compilera le greffon lui-même lors de son chargement.

Le principal avantage de l'appoche PLGX est la compatibilité avec les versions de KeePass personnalisées. Un greffon DLL fait référence à une version officielle de KeePass, et à moins qu'il y ait un changement dans KeePass qui casse le greffon, le greffon est également compatible avec toutes les futures versions de KeePass qui sont compilées avec la même clé de signature d'assemblage (nom fort). Cela s'applique à tous les systèmes d'exploitation. En particulier, un greffon DLL qui n'utilise aucune fonction spécifique à Windows fonctionne correctement sous Linux avec une version KeePass du package ZIP portable officiel. Cependant, certains packages Linux compilent KeePass à partir du code source ; ces constructions ne sont pas signées du tout ou sont signées avec une clé de signature d'assemblage différente et sont donc incompatibles avec les greffons DLL. En revanche, les greffons PLGX sont compatibles avec les versions (builds) de KeePass personnalisées, car KeePass peut ajuster la référence KeePass du greffon avant de le compiler.

Un autre avantage de l'approche PLGX est une forte détection de compatibilité. Dans le cas d'un greffon DLL, une incompatibilité (causée par un changement d'API dans KeePass) est détecté par le runtime lorsque le greffon essaie d'appeler/accéder à la méthode/classe, pas au moment du chargement. Ainsi, une incompatibilité est détectée tardivement et peut planter KeePass. En revanche, lors de l'utilisation du format PLGX, une incompatibilité est détecté immédiatement au moment du chargement : en cas de problème, le le processus de compilation échoue et KeePass peut afficher une information message d'incompatibilité du greffon à l'utilisateur. Pour les greffons DLL, KeePass effectue sa propre vérification de compatibilité, qui ne détecte cependant pas toutes les incompatibilités ; PLGX est supérieur ici.

En ce qui concerne la sécurité, les plugins DLL sont meilleurs, car ils peuvent être signé numériquement (Authenticode). De plus, les plugins DLL sont généralement chargés légèrement plus rapidement (parce qu'ils peuvent être chargés directement ; pas cache des greffons).

Pour les utilisateurs, la procédure d'installation d'un greffon DLL est exactement la même que pour un greffon PLGX ; les deux doivent être copiés dans le dossier 'Plugins'.

Comparaison :

	DLL	PLGX
Compatibilité avec les versions (builds) personnalisées (Linux)	✗ Partielle.	✓
Vérification de compatibilité	✗ Faible.	✓ Forte.
Prise en charge de la signature Authenticode	✓	✗
Pas de compilation sur le système de l'utilisateur	✓	✗
Pas de cache de greffon	✓	✗

Ainsi, les deux formats ont des avantages et des inconvénients uniques.

Package double : vous pouvez expédier un greffon à la fois sous forme de DLL et de PLGX dans un seul package (par exemple : 'SecretImporter.dll' et 'SecretImporter.plgx' à l'intérieur du même dossier). KeePass chargera le fichier le plus approprié (si KeePass a été signé avec la clé officielle de signature d'assemblage, alors il chargera la DLL, sinon le PLGX). Si KeePass charge la DLL, le PLGX est ignoré.

Recommandations : Dans tous les cas, fournissez un fichier DLL (pour des raisons de sécurité). Si vous souhaitez prendre en charge les builds KeePass personnalisés, fournissez également un fichier PLGX (c'est-à-dire fournir un package double).

La création de fichiers PLGX : les fichiers PLGX peuvent être créés à partir des sources de greffon en appelant `KeePass.exe` avec l'option de ligne de commande `--plgx-create`. Si vous passez en plus un chemin vers le répertoire des sources du greffon (sans séparateur de fin), alors KeePass utilisera celui-ci ; sinon, il affichera une boîte de dialogue de navigation de dossiers pour vous permettre de sélectionner le répertoire. Si vous souhaitez transmettre l'emplacement du répertoire à l'aide de la ligne de commande, alors assurez-vous de spécifier un chemin d'accès complet et absolu ; les chemins relatifs ne fonctionneront pas.

Afin de garder la taille du fichier PLGX petite, il est recommandé de nettoyer le répertoire des sources du greffon avant de compiler le PLGX. Supprimez tous les fichiers binaires inutiles (fichiers dans les répertoires `bin` et `obj`) ; en particulier, supprimez toute DLL d'assemblage de greffon que vous avez compilée vous-même. Les fichiers temporaires de l'IDE (tels que les fichiers `.suo` et `.user`) peuvent également être supprimés.

Les fonctionnalités PLGX :

- Format de fichier extensible et orienté objet.
- Prise en charge de la compression (les fichiers de données sont compressés à l'aide de GZip).
- Prise en charge de `.csproj`. KeePass récupère toutes les informations nécessaires à la compilation de l'assemblage du greffon à partir du fichier `.csproj` dans les sources du greffon.
- Prise en charge des ressources embarquées.
- Prise en charge des assemblages .NET référencés. L'information de références est lue à partir du fichier `.csproj`.
- Prise en charge des assemblages personnalisés référencés. Les assemblages tiers requis par le greffon (références aux DLL) sont pris en charge, à condition que l'assemblage tiers se trouve dans le répertoire du code source du greffon (ou tout sous-répertoire de celui-ci).
- Prise en charge de ResX. Les fichiers `.resx` sont automatiquement compilés en fichiers binaires `.resources`.
- Le cache PLGX. Les fichiers PLGX sont compilés une seule fois et l'assemblage généré est stocké dans un cache. Pour tous les démarrages de KeePass suivants, aucune compilation n'est requise.
- Maintenance du cache PLGX. La taille du cache PLGX peut être vue dans la boîte de dialogue des greffons KeePass. Ici, le cache peut également être marqué pour être effacé (il sera effacé lors du prochain démarrage de KeePass). Une option pour supprimer automatiquement les anciens fichiers du cache est prise en charge et activée par défaut.

Les limites de PLGX :

- Seul C# est pris en charge (pas Visual Basic ou tout autre langage .NET).
- Le compilateur inclus dans le .NET Framework prend en charge au maximum C# 5. Afin d'éviter d'utiliser les fonctionnalités d'une version plus récente de C#, il est donc recommandé de définir la version C# de votre projet de greffon sur 5 :
  - Dans Visual Studio 2017 et versions antérieures , ouvrez les propriétés du projet → onglet 'Version' → bouton 'Avancé' → définissez l'option 'Version du language' sur 'C# 5'.
  - Dans Visual Studio 2019 et versions ultérieures, le fichier XML du projet doit être modifié : l'élément '`LangVersion`' doit contenir '5'. Pour plus de détails, consultez Gestion des versions du langage C# (C# Language Versioning).
- Les ressources liées (dans différents assemblages) ne sont pas prises en charge.
- Les dépendances sur d'autres projets ne sont pas prises en charge (réorganisez votre projet pour utiliser à la place des références d'assemblage personnalisées).

Définition des prérequis : vous pouvez *éventuellement* spécifier une version minimale de KeePass, un framework .NET installé au minimum, un système d'exploitation et la taille minimale d'un pointeur (x86 contre x64) en utilisant les options `--plgx-prereq-kp:`, `--plgx-prereq-net:`, `--plgx-prereq-os:` et `--plgx-prereq-ptr:` de ligne de commande. Si l'une des conditions préalables du greffon n'est pas remplie, alors KeePass affiche un message d'erreur détaillé à l'utilisateur final (au lieu d'un message générique d'incompatibilité du greffon). Exemple de construction :

```
KeePass.exe --plgx-create C:\VotreRépertoireDeGreffon --plgx-prereq-kp:2.09 --plgx-prereq-net:3.5
```

Les valeurs de système d'exploitation valides sont `Windows` et `Unix`. Lorsqu'il s'exécute sur un système d'exploitation inconnu, KeePass est par défaut Windows. Les tailles de pointeur (vérification de x86 par

rapport à x64) sont spécifiées en octets ; par exemple, pour autoriser uniquement l'exécution sur x64, vous spécifiez `--plgx-prereq-ptr:8`.

Générer des commandes : vous pouvez *éventuellement* spécifier des commandes de préconstruction et de post-construction à l'aide de `--plgx-build-pre:` et `--plgx-build-post:`. Ces commandes sont intégrées dans le fichier PLGX et exécutées lors de la compilation du greffon sur le système de l'utilisateur final.

Dans les commandes de génération, le paramètre substituable `{PLGX_TEMP_DIR}` spécifie le répertoire temporaire (incorporant un séparateur de fin), dans lequel les fichiers ont été extraits. Dans la commande de post-construction, `{PLGX_CACHE_DIR}` est remplacé par le répertoire de cache du greffon (incorporant un séparateur de fin), dans lequel l'assemblage généré a été stocké.

Ces commandes de construction peuvent par exemple être utilisées pour copier des fichiers supplémentaires dans le répertoire de cache. Exemple :
```
KeePass.exe --plgx-create C:\VotreRépertoireDeGreffon --plgx-build-post:"cmd /c COPY """{PLGX_TEMP_DIR}MonFichier.txt""" """{PLGX_CACHE_DIR}MonFichier.txt"""
```

Afin de spécifier une double quote sur la ligne de commande, elle doit être encodée à l'aide de trois doubles quotes (c'est le standard Windows, voir "https://docs.microsoft.com/en-us/windows/win32/api/shellapi/ns-shellapi-shellexecuteinfow MSDN: `SHELLEXECUTEINFOW`). Ainsi, la ligne de commande ci-dessus intégrera en fait la commande post-build `cmd /c COPY "{PLGX_TEMP_DIR}MonFichier.txt" "{PLGX_CACHE_DIR}MonFichier.txt"` dans le PLGX, ce qui est correct. Il est fortement recommandé d'encadrer les chemins contenant des espaces réservés PLGX à l'aide de doubles quotes, sinon la commande ne s'exécutera pas correctement si le chemin contient un espace (ce qui arrive très souvent).

Si vous devez exécuter plusieurs commandes, alors écrivez-les dans un fichier batch et exécutez-le (avec `cmd`). Si vous avez besoin d'effectuer des tâches de construction plus complexes, alors écrivez votre propre exécutable de construction et exécutez-le à l'aide des commandes de construction (il est généralement utile de transmettre les emplacements des répertoires en tant qu'arguments à votre exécutable de construction), par exemple :
```
KeePass.exe --plgx-create C:\VotreRépertoireDeGreffon --plgx-build-post:"{PLGX_TEMP_DIR}MonBuild.exe {PLGX_TEMP_DIR} {PLGX_CACHE_DIR}"
```

Le débogage PLGX : lorsque l'option de ligne de commande `--debug` est transmise et qu'un greffon PLGX ne parvient pas à se compiler, alors la sortie de tous les compilateurs essayés est enregistrée dans un fichier temporaire.

Écrire des scripts

Scénariser (2.x)

Comment automatiser KeePass 2.x ?

Afin d'automatiser KeePass, vous avez besoin soit du greffon/extension KPScript soit de PowerShell.

- Vous pouvez trouver la dernière version de KPScript sur la page des greffons de KeePass. Le fichier `KPScript.exe` doit être copié dans le répertoire où KeePass est installé (qui contient le fichier `KeePass.exe`).
- Une version PowerShell adaptée est incluse dans Windows 10/11. Sur d'autres systèmes d'exploitation, vous devrez peut-être l'installer au préalable.

Il existe trois façons d'automatiser KeePass :

- KPScript - Les opérations de commande unique :
  KPScript peut être appelé à l'aide de commandes uniques. En transmettant l'emplacement de la base de données, sa clé, une commande et éventuellement certains paramètres, des opérations simples comme l'ajout d'une entrée peuvent être effectuées. La syntaxe est très simple, aucune connaissance en script n'est requise. Cette méthode est idéale lorsque vous souhaitez apporter rapidement de petites modifications à la base de données. Il n'est pas recommandé lorsque vous devez effectuer de nombreuses opérations, car pour chaque commande, la base de données doit être chargée à partir du fichier, déchiffrée, modifiée, chiffrée et réécrite dans le fichier.
- KPScript - Les fichiers de script KPS :
  Ces fichiers sont beaucoup plus puissants que les opérations de commande unique, mais sont

également plus compliqués. Vous devez avoir une expérience de la programmation C# et des composants internes de KeePass 2.x.

- PowerShell :
  Avec PowerShell, vous pouvez charger l'assemblage `KeePass.exe` et faire tout ce que KeePass peut faire.
  Télécharger les exemples de scripts PowerShell de KeePass.