KeePass, votre coffre-fort de mots de passe

Jean-Daniel.Bonjour@epfl.ch, EPFL-ENAC-IT, responsable informatique, chargé de cours

How to store safely all your precious digital IDs and use them in a convenient way? If you don't already have an application for this purpose, then it's time for you to consider software developed under the KeePass free project!

Comment stocker de façon robuste tous vos précieux sésames d'accès au monde numérique et les utiliser efficacement? Si vous n'avez pas encore d'application pour cela, il est alors grand temps de vous intéresser aux logiciels libres de la famille KeePass!

Fiche descriptive

Domaine
- Gestionnaire de mots de passe (et d'autres informations personnelles)

Licence	langue	version
GPLv2+	multilingue	1.19 et 2.15

Autres alternatives libres
- Password Safe

Alternatives non libres
- LastPass
- Password Agent
- et beaucoup d'autres...

Sites Web
- projet KeePass: keepass.info

Plates-formes

Problématique des mots de passe

Pour l'usager EPFL standard, il est aujourd'hui devenu possible d'accéder à la plupart des applications informatiques proposées dans notre École avec un seul compte, son compte Gaspar[1]. En effet, la plupart des applications Web authentifiées de l'EPFL s'appuient sur le système Tequila[2] qui vous demande votre identifiant et mot de passe Gaspar[3]. Le monde Windows, la messagerie et les prestations de stockage dépendent du service d'annuaire Active Directory, dont les comptes sont par défaut synchronisés sur Gaspar. Il en est de même en ce qui concerne les mondes Linux et MacOSX (avec les services d'annuaires LDAP et Open Directory) ainsi que les services réseau (avec Radius). Plus personne n'a donc d'excuse à ne pas utiliser un **mot de passe robuste** (unique) pour accéder à l'ensemble de ces services.

Mais le monde numérique ne se limite pas à notre univers professionnel. Presque chaque mois ou semaine qui passe nous amène à créer de nouveaux comptes et retenir de nouveaux mots de passe: e-mail privé, réseaux sociaux, blogs, forums, stockage dans le *cloud*, services bancaires, commerce en ligne, voyages, partage de documents, de photos ou de vidéos, etc. Donc autant d'identités numériques que de services... dans l'attente de solutions d'authentification globales et mutualisées entre plusieurs prestataires[4]. Notre premier conseil de sécurité est de **ne surtout pas utiliser le même identifiant et mot de passe pour plusieurs services fournis par des prestataires différents**[5]! Celui qui respecte cette règle peut être tenté d'utiliser des mots de passe simples pour les mémoriser facilement tous... mais ils ne résisteront pas longtemps en cas de tentatives de deviner le mot de passe par *force brute*[6]. S'agissant des mots de passe complexes et donc solides, il faut s'aider d'algorithmes mentaux pour les retenir, ce qui ne convient pas à tout le monde. Quant à la liste de mots de passe sur papier au fond du tiroir ou dans un fichier texte sur votre ordinateur ou smartphone, c'est fort peu commode à utiliser et bien trop vulnérable.

Il est donc essentiel d'opter pour des mots de passe robustes et différents pour chaque service... et pour survivre, il nous faut une solution permettant de les conserver, les gérer et les utiliser de manière sûre, souple et efficace. Trois catégories d'outils existent pour cela.

Stockage d'identifiants par le navigateur Web

Depuis quelques années, les navigateurs Web sont en mesure de conserver les informations relatives aux formulaires (c'est même leur comportement par défaut), donc typiquement les informations de *login* des services Web authentifiés. S'agissant des champs de type `mots de passe`, un réglage permet de désactiver cette fonctionnalité[7]. Si vous la laissez activée, il est absolument essentiel de protéger l'ensemble des mots de passe ainsi enregistrés (ainsi que vos éventuelles clés privées de navigateur) par un *mot de passe principal*, sinon n'importe qui ayant accès à votre machine (ou aux fichiers de configuration de votre navigateur)

[1] Gestionnaire de comptes EPFL Gaspar: gaspar.epfl.ch
[2] Module libre d'authentification Web développé à l'EPFL par C. Lecommandeur (tequila.epfl.ch)
[3] Ce qui permet le *single sign-on*, c'est-à-dire la possibilité de naviguer d'un site authentifié à un autre en ne s'authentifiant que sur le premier
[4] Tel que OpenID (fr.wikipedia.org/wiki/OpenID) qui semble la plus prometteuse
[5] Faute de quoi, si l'un des mots de passe était intercepté, l'accès aux autres services serait compromis
[6] fr.wikipedia.org/wiki/Attaque_par_force_brute
[7] Sous Firefox, avec `Outils>Options` ou `Édition>Préférences`, puis onglet `Sécurité` et option `Enregistrer les mots de passe`

pourra récupérer vos mots de passe[8]. En activant la protection par mot de passe principal, lorsque vous redémarrerez votre navigateur, la première tentative d'authentification à un service sécurisée déclenchera la demande de saisie de ce mot de passe. Les mécanismes de synchronisation via internet des paramètres du navigateur[9] vous permettent en outre de synchroniser automatiquement, entre plusieurs navigateurs/machines, non seulement vos bookmarks mais également vos mots de passe. Cette technique facilite donc grandement l'authentification et vous permet d'utiliser des mots de passe robustes que vous n'avez pas besoin de mémoriser, mais elle présente les inconvénients suivants:

- elle se limite à l'authentification de services Web;
- elle n'est bien entendu pas envisageable sur une machine qui n'est pas la vôtre (sur le poste d'un ami, dans un cybercafé...);
- peut-être ne souhaitez-vous pas synchroniser des mots de passe via le *cloud*[10], même cryptés.

Notez qu'il existe des extensions permettant d'exporter vos mots de passe d'un navigateur vers un gestionnaire de mots de passe[11], voire l'inverse (importation).

Trousseau de clés du système d'exploitation

Chaque système d'exploitation propose en standard un mécanisme de gestion de *trousseaux de clés*[12] permettant d'enregistrer les informations d'accès à d'autres services *(credentials)*, et les protéger par un mot de passe principal. Cette méthode a cependant aussi des limites:

- pas de prise en charge de l'authentification de services Web;
- mécanisme intimement lié à la machine sur laquelle on travaille.

Gestionnaire de mots de passe

Bien que les deux mécanismes qui viennent d'être décrits puissent être considérés comme des *gestionnaires de mots de passe*, il existe une troisième catégorie d'outils spécifiques, correspondant à ce terme et dont KeePass fait partie, permettant à l'utilisateur d'enregistrer manuellement l'ensemble de ses identifiants et mots de passe[13] dans une base de données protégée par un mot de passe unique afin de n'avoir plus qu'un seul sésame robuste à mémoriser.

Exigences d'un gestionnaire de mots de passe

Il existe un grand nombre de gestionnaires de mots de passe, mais rares sont ceux qui satisfont à l'ensemble des exigences suivantes qui nous semblent essentielles pour un domaine aussi critique:

- le mécanisme de **chiffrage** doit être robuste, afin de rendre quasi impossible le décryptage de vos informations par celui qui aurait dérobé votre fichier de base de données; lorsque le logiciel tourne, les mots de passe doivent en outre être cryptés en mémoire pour éviter l'interception par des logiciels espions;
- le logiciel doit être libre et **open source**; du point de vue des spécialistes en sécurité (et des défenseurs du libre !), la possibilité d'examiner le code de l'application est la seule façon de s'assurer que le logiciel est robuste, et la seule garantie qu'il n'implémente pas de mécanisme malveillant;
- il doit être **commode à utiliser**, notamment s'agissant de la transmission des identifiants aux applications authentifiées (copier/coller, mécanisme *auto-type*); lorsque le logiciel tourne, les mots de passe doivent apparaître de façon masquée (au cas où quelqu'un lorgnerait par-dessus votre épaule);
- il doit être **flexible** en terme d'organisation de la base de données (mise en place d'arborescences de comptes) et permettre le stockage d'autres attributs (URL, notes, éventuel fichier attaché, etc.);
- il devrait en outre être utilisable de façon mobile (typiquement depuis une clé USB), c'est-à-dire conçu de façon **portable** *(stand-alone)*;
- il devrait être **multiplate-forme**, permettant d'accéder depuis tout type d'équipement (laptop ou desktop Windows/Linux/MacOSX, smartphone, tablette...) à ces informations que l'on est susceptible d'utiliser n'importe où;
- la **synchronisation** de la base de données entre les différents équipements que vous utiliserez doit être possible et offrir la robustesse nécessaire pour s'appuyer sur des mécanismes de type internet *(cloud)*.

Le logiciel libre **KeePass** et ses adaptations sur les différents systèmes d'exploitation et équipements constitue probablement le seul projet qui réunit toutes ces caractéristiques !

Installation de KeePass

À l'origine, **KeePass Password Safe**[14] est un projet libre de développement de gestionnaire de mots de passe sous Windows. À partir de celui-ci ont été implémentées des versions pour toutes les plates-formes courantes: **KeePassX** sous Linux et MacOSX, **KeePassDroid** sous Android (smartphones et tablettes), **MyKeePass** (et **iKeePass** limité à USA/Canada) sous iOS (iPhone, iPad), **7Pass** sous Windows Phone 7, **KeePassMobile** pour téléphones basés J2ME (Java 2 Micro Edition), etc.

Il est important de préciser ici que **deux versions** de KeePass évoluent en parallèle, toutes deux libres en licence GPLv2+, mais différentes en terme de portabilité et de fonctionnalités[15]:

[8] Sous Firefox, dans la même fenêtre de réglage: option `Utiliser un mot de passe principal`, et bouton `Mots de passe enregistrés`

[9] Par exemple l'extension **Xmarks** sous Firefox et Chrome, ou le module Mozilla **Firefox Sync** (anciennement dénommé Weave) entièrement intégré au navigateur Firefox depuis la version 4 (voir l'onglet `Sync` sous `Outils>Options` ou `Outils>Préférences`)

[10] Noter cependant que Xmarks permet de synchroniser via un espace WebDAV quelconque (voir **ditwww.epfl.ch/SIC/SA/SPIP/Publications/spip.php?article2063**), et que la technologie libre **Firefox Sync** permet d'implémenter son propre serveur de synchronisation (basé PHP, JSON, MySQL...)

[11] Par exemple, l'extension **Password Exporter** sous Firefox qui ajoute un bouton `Importer/Exporter les mots de passe` dans l'onglet `Sécurité` des options Firefox

[12] **Keychain** sous MacOS, **GNOME Keyring** sous Linux/GNOME, **KWallet** sous Linux/KDE, etc.

[13] Ainsi que d'autres attributs comme: adresses internet associées, notes, informations confidentielles telles que PIN-code, etc.

[14] Site principal **keepass.info**, et voir aussi **fr.wikipedia.org/wiki/KeePass**

[15] Pour une présentation détaillée des différences, voir **keepass.info/compare.html**

- branche **1.x** (KeePass *Classic*, écrit en C++): version la plus répandue, installable sans prérequis sur les 3 systèmes d'exploitation Windows, Linux et MacOSX
- branche **2.x** (KeePass *Professional*, écrit en C#): nécessite Microsoft .NET Framework ≥ 2 sous Windows [16], et Mono ≥ 2.6 supérieur sous Linux ou MacOSX [17]; offre des fonctionnalités additionnelles qui ne sont cependant pas vitales, notamment:
  - sous Windows: mécanisme additionnel de protection de la base de données en la liant au compte utilisateur Windows,
  - possibilité de définir des champs supplémentaires pour chaque entité,
  - possibilité d'attacher plus d'un fichier à une entité,
  - gestion d'un historique pour chaque entité,
  - mécanisme plus robuste de protection par rapport aux *keyloggers (two channels auto-type obfuscation)*,
  - possibilités de scripting.

Les **formats de bases de données** de ces deux versions sont différents et **non interopérables**. Ces fichiers portent les extensions `.kdb` pour la version 1.x, et `.kdbx` pour la version 2.x. bien que le passage d'une version à l'autre soit possible, il consiste plutôt en une migration [18]. Étant donné les prérequis de la version 2.x et surtout le fait qu'elle n'est pas disponible sur toutes les plates-formes, il est actuellement nécessaire d'**opter pour la version 1.x** [19] si vous souhaitez exploiter une base de données KeePass en parallèle sur plusieurs équipements dont les systèmes d'exploitation sont différents (laptop/desktop, smartphones et tablettes).

Une fois la décision prise quant à la version, vous pouvez passer à l'**installation**:

- Sous Windows: depuis la page **keepass.info/download.html**, vous pouvez choisir entre une installation basée *installeur* (type Setup.exe) ou déballage d'une archive ZIP. Le résultat sera le même dans les deux cas, et l'application installée sera portable, c'est-à-dire déplaçable/exploitable sur n'importe quel autre média de stockage (pas de trace de clé de registre ni de fichier INI dans le système). Il est bien clair que si vous avez opté pour la version 2.x, son usage via clé USB sur une machine ne disposant pas du Framework .NET ne sera pas possible.
- Sous Linux: vous pourriez installer KeePassX depuis la page **www.keepassx.org**, mais il est préférable (et plus facile) d'utiliser le gestionnaire de paquetage de votre distribution Linux. Le paquetage s'appelant `keepassx`, vous pouvez passer la commande: `sudo apt-get install keepassx` (Debian/Ubuntu) ou `yum install keepassx` (Red Hat/Fedora), et accepter l'installation des éventuels paquets dépendants. Vous accéderez ensuite à l'application depuis le menu `Applications>Accessories>KeePassX`.
- Sous MacOSX: depuis la page **www.keepassx.org/downloads/**, sous la rubrique MacOS X, téléchargez le fichier-image `KeePassX-version.dmg`, ouvrez-le, et déplacez le fichier KeePassX qui se trouve dans le dossier Applications.
- Sur smartphone ou tablette Android: installez l'application nommée KeePassDroid depuis le Market de Google.
- Sur iPhone ou iPad: installez l'application nommée MyKeePass depuis l'AppStore iTunes de Apple.

L'**interface utilisateur** diffère d'une plate-forme à l'autre. Quasiment identique entre Linux et MacOSX, l'organisation des menus est différente sous Windows (ainsi que selon la version 1.x ou 2.x). Bien entendu c'est toute autre chose sur smartphone ou tablette où l'interface graphique est adaptée à une interface de type tactile. Ceci n'empêche pas ces différentes implémentations KeePass d'être interopérables, c'est-à-dire partager le même fichier de base de données (pour autant que l'on s'en tienne à la même famille, donc soit 1.x soit 2.x).

Si vous souhaitez changer la **langue** de l'interface utilisateur:

- Sous Linux et MacOSX: le logiciel est multilingue, et vous pouvez changer de langue avec `Extra>Settings` (Linux) ou `KeePassX>Preferences` (Mac), puis allez dans la catégorie `Languages`, sélectionnez la langue désirée, cliquez `Apply` et relancez KeePassX.
- Sous Windows: KeePass s'installe par défaut en langue anglaise seulement. Si cela ne vous convient pas, faites `View>Change Language`, puis cliquez sur `Get more languages` [20], téléchargez le fichier correspondant à votre version et à la langue désirée, dézippez-le, déposez-le simplement dans le dossier d'installation KeePass et relancez l'application.

Dans les explications ci-dessous, nous présenterons les deux versions (1.x et 2.x) mais nous nous baserons sur la langue par défaut (anglaise). Sur Mac, traduisez bien entendu les raccourcis `<ctrl-xxx>` que nous indiquerons en `<cmd-xxx>`.

Prise en main sous Windows/Linux/Mac

Création d'une base de données

KeePass sauvegarde vos *entrées* (comptes avec identifiant, mots de passe, etc.) dans une base de données chiffrée qui consiste en un seul fichier. Celui-ci est accessible moyennant la saisie d'un **mot de passe principal** *(master password)* qui peut être facultativement complété par un fichier de clé (*Key file*, voir plus loin dans cet article).

La toute première fois que vous lancez KeePass, il vous faut commencer par créer une base de données avec `File>New`: vous êtes alors appelé à saisir puis confirmer le mot de passe principal (voir fig. 1). Choisissez un mot de passe robuste [21], car il protégera l'ensemble de tous vos autres mots de passe, et c'est le seul que vous

[16] .NET fait partie de Windows 7, mais doit être installé sous Windows XP

[17] Mono (**www.mono-project.com**) est une implémentation libre de .NET

[18] Le passage 1.x à 2.x s'effectue sous KeePass 2.x par importation KDB dans un fichier KDBX. Le retour 2.x à 1.x s'effectuerait sous KeePass 2.x par export des données en KDB

[19] Version qui ne devrait pas disparaître au profit de 2.x, voir **keepass.info/devstatus.html**

[20] Ce qui ouvrira la page web **keepass.info/translations.html**

[21] Un mot de passe robuste devrait être très éloigné d'un mot de dictionnaire et composé de 12 à 15 caractères mélangeant majuscules, minuscules, chiffres et caractères spéciaux. Dans la version Windows de KeePass, tant que l'indicateur en-dessous du champ Master password ne vire pas au vert, durant le processus de saisie du mot de passe, c'est qu'il est jugé trop risqué.

aurez à mémoriser. Il est **primordial de s'en souvenir**, sous peine de perdre l'accès à toutes les informations contenues dans la base de données. Il sera vain d'appeler au secours si vous l'avez oublié, car il n'y a vraiment aucune solution pour le récupérer. C'est du reste l'un des facteurs garantissant la sécurité de cet outil !

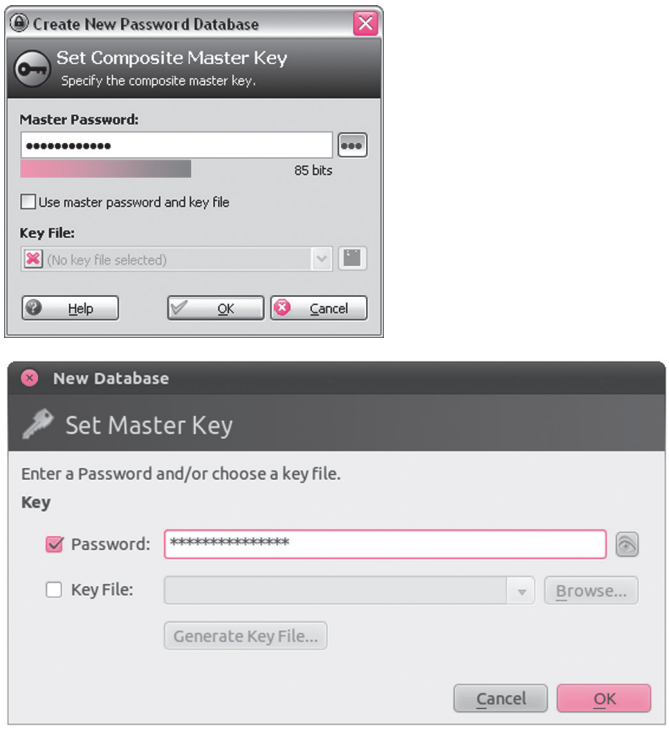

fig. 1 – fenêtres de saisie du mot de passe principal, sous Windows (1.x) et Linux/Mac

La première fois que vous sauvegarderez la base de données (`File>Save`), KeePass vous demandera, comme toute application, de spécifier l'emplacement et le nom de fichier, qui sera complété par l'extension `.kdb` sous la version 1.x, et `.kdbx` sous 2.x. Les prochaines fois que vous lancerez KeePass, il se souviendra de la dernière base de données utilisée et l'ouvrira après vous avoir demandé de saisir le mot de passe principal.

Pour changer après coup le mécanisme de protection (mot de passe principal et/ou fichier de clé), faites `File>Change Master Key`. Le logiciel vous demandera alors de re-sauvegarder la base de données afin de la réencrypter sur la base de ces nouveaux paramètres.

Disponible uniquement dans la version 2.x sous Windows, une option `Windows user account` permet de lier la protection de la base de données au compte utilisateur Windows courant. Il peut être dangereux de recourir à cette option, car elle vous empêchera d'ouvrir la base de données depuis d'autres machines, sauf si elles sont intégrées au même domaine Active Directory. En outre, la destruction du compte utilisateur Windows rendrait impossible l'utilisation de votre base de données.

Notez la présence, à droite du champ de saisie de mots de passe (et c'est aussi valable lorsque vous définirez dans un instant des entrées), d'un bouton avec 3 points (sous Windows) ou un œil (sous Linux/Mac) que vous pouvez désenfoncer pour afficher le mot de passe en clair lors de la saisie.

Gestion des groupes et entrées

Une fois la base de données ouverte, vous vous trouvez devant une fenêtre analogue à celles des figures 2 (Windows) ou 3 (Linux/Mac).

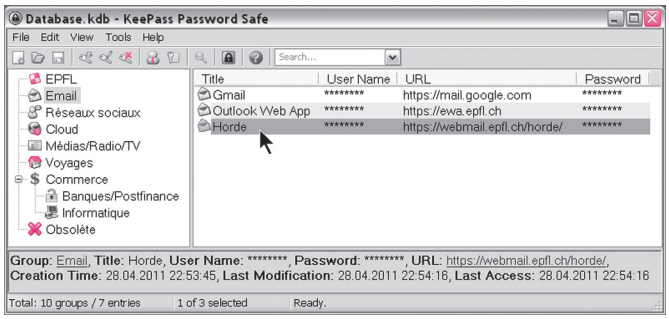

fig. 2 – fenêtre principale KeePass, sous Windows

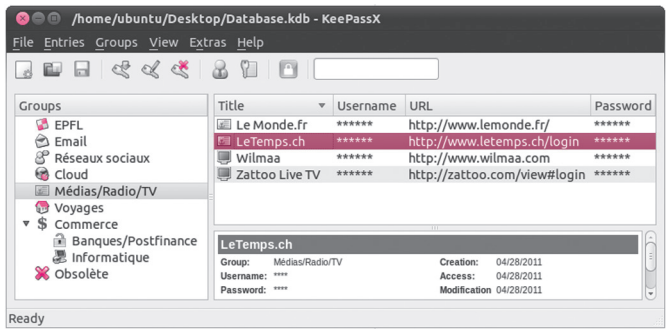

fig. 3 – fenêtre principale KeePassX, sous Linux ou MacOSX

On y distingue les zones suivantes:

- sous la barre de titre: les menus et une barre d'outils.
- à gauche: une arborescence de `groupes` et `sous-groupes`;
- dans la partie supérieure droite: la liste des `entrées` du groupe couramment sélectionné à gauche;
- dans la partie inférieure: l'affichage des **attributs** de l'entrée couramment sélectionnée dans la liste du dessus.

Les groupes permettent de classer par catégories et organiser hiérarchiquement vos codes d'accès (identifiant, mot de passe et autres attributs) dénommés entrées. Des icônes explicites peuvent être associées aux groupes et aux entrées afin de les identifier plus facilement.

On trouve par défaut, dans une nouvelle base de données, un certain nombre de **groupes** prédéfinis. Sous KeePass Windows: un groupe General contenant les sous-groupes Windows, Network, Internet, eMail et Homebanking. Sous KeePassX Linux/Mac: deux groupes Internet et eMail. Mais vous êtes entièrement libres de les détruire et définir votre propre hiérarchie à l'aide des commandes se trouvant dans le menu `Edit` (Windows) ou `Groups` (Linux/Mac).

Pour saisir une **nouvelle entrée**, sélectionnez d'abord le groupe dans lequel vous désirez la placer, puis faites `Edit>Add Entry` (Windows) ou `Entries>Add New Entry` (Linux/Mac), ou procédez par clonage d'une entrée existante (`Duplicate Entry` sous Windows, `Clone Entry` sous Linux/Mac). Apparaît alors la fenêtre de saisie des attributs de l'entrée (fig. 4). Vous n'êtes pas obligé de remplir tous les champs. Associez à l'entrée une icône représentative. Le champ Notes/Comment permet d'insérer librement tout autre type d'information. Vous pouvez même attacher à chaque entrée un fichier qui sera donc intégré de façon cryptée dans la base de données !

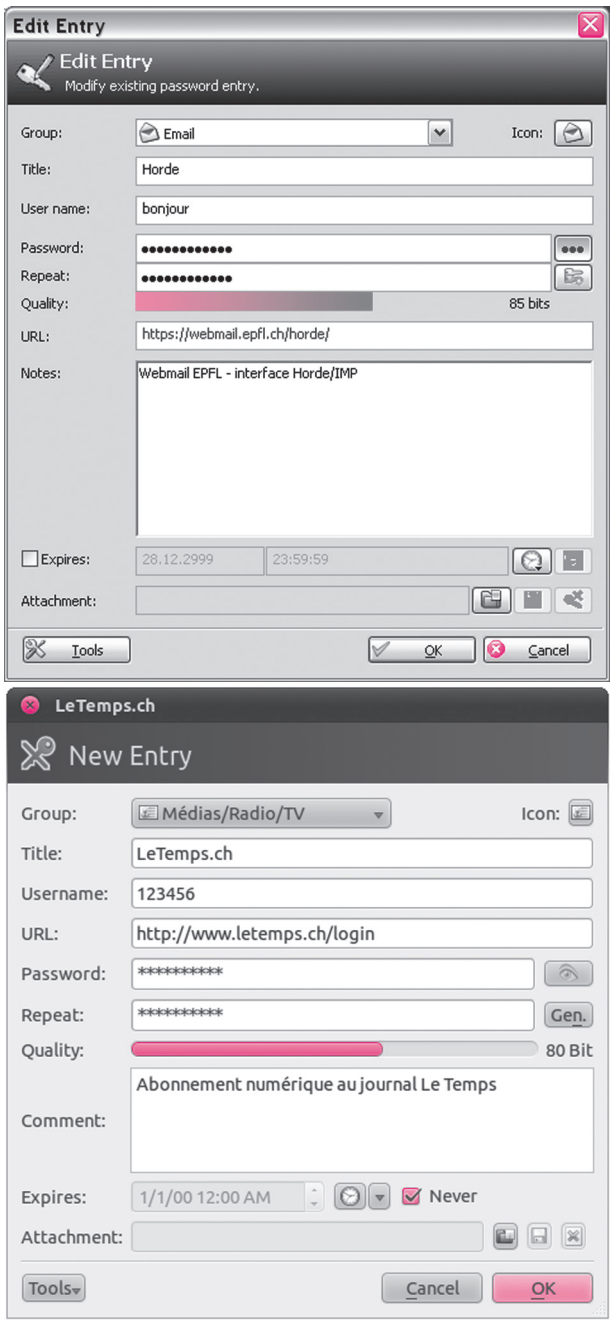

fig. 4 – fenêtres de saisie/modification des attributs d'une entrée, sous Windows (1.x) et sous Linux/Mac

Pour **éditer/modifier** après coup une entrée, vous pouvez double-cliquer sur son Title, ou la sélectionner et frapper <enter> (Windows) ou encore `Entries>View/Edit Entry` (Linux/Mac). Et finalement, pour réorganiser les entrées et groupes, procédez simplement par glisser/déposer.

Vous pouvez agir sur le type d'affichage en mode liste, ce qui est utile pour masquer certaines informations aux personnes qui pourraient voir votre écran:

- faire apparaître ou masquer certaines colonnes: `View>Show Columns` (Windows), `View>Columns` (Linux/Mac),
- faire apparaître ou masquer (par des *****) les usernames et passwords: `View>Hide Usernames` et `View>Hide Passwords` (commandes-bascules), ou encore `<ctrl-J>` et `<ctrl-H>` (Windows),
- ainsi que masquer la zone du bas présentant l'ensemble des attributs d'une entrée: `View>Show Entry View/Details`.

Notez finalement que les **menus contextuels** sont très bien implémentés sous KeePass. Ils apparaissent lorsque vous cliquez avec `<droite>` (ou `<ctrl-clic>` sur Mac) sur des entrées ou des groupes.

Utilisation des entrées de la base de données

À ce stade de notre présentation, votre base de données n'est qu'un répertoire de comptes avec attributs. Mais la puissance de KeePass va bien au-delà !

En premier lieu, lorsqu'une entrée dispose d'une URL, vous pouvez ouvrir celle-ci automatiquement (basculement automatique dans votre navigateur Web préféré) en la sélectionnant et frappant `<ctrl-U>` (ou `Edit>Open URLs` sous Windows, et `Entries>Open URL` sous Linux/Mac). Pour gagner du temps, associez donc l'URL correspondant à la page de *login* du service.

Il s'agit maintenant de **transférer votre identifiant** et **mot de passe** à cette page. Plusieurs techniques sont possibles:

- La bonne vieille technique du copier/coller: KeePass vous permet, depuis la liste de vos entrées, de récupérer dans le presse-papier le username ou password d'une entrée ainsi:
  - copie du username: sélectionnez l'entrée et faites `<ctrl-B>`, ou double-cliquez sur le champ *username*,
  - copie du password: sélectionnez l'entrée et faites `<ctrl-C>`, ou double-cliquez sur le champ *password*,
- Le **glisser/déposer** *(drag and drop)*: il est possible de glisser/déposer le *username* ou le *password* entre la fenêtre KeePass et les champs correspondants de votre page Web de *login*.
- Le mode **auto-type**: bien plus efficace que les méthodes ci-dessus, cette technique n'est cependant disponible que sous Windows et Linux et fonctionne ainsi:
  - assurez-vous d'abord que, dans la page de *login* de l'application sécurisée, le curseur d'insertion se trouve dans le champ username (c'est généralement le cas pour toutes les pages d'authentification bien conçues),
  - revenez ensuite dans KeePass, et frappez simplement le raccourci `<ctrl-V>` (ou la commande `Edit>Perform Auto-Type`, ou à l'aide du menu contextuel sous KeePass 2.x); ce raccourci va magiquement basculer dans la fenêtre précédente et y coller la séquence: USERNAME `<tab>` PASSWORD `<enter>`[22], et vous serez authentifiés !
  - si les champs de formulaire de la page d'authentification sont organisés différemment, il est possible d'indiquer à KeePass quelle séquence d'envoi spécifique effectuer[23].
- Le **global auto-type**: hélas pas non plus disponible sous MacOSX, cette méthode constitue vraiment le nec plus ultra. La logique est inverse par rapport à l'auto-type classique, puisqu'on déclenche l'opération d'injection du *username* et *password* directement depuis l'application authentifiée avec le raccourci `<ctrl-alt-A>`. Mais comment cela peut-il bien fonctionner ?
  - il faut bien entendu que KeePass soit préalablement démarré et tourne en arrière-plan avec la base de données

[22] Le <tab> passe du champ username au champ password, et <enter> valide la connexion

[23] Voir keepass.info/help/base/autotype.html

ouverte (si celle-ci est *lockée*, KeePass vous demandera d'abord le mot de passe pour la déverrouiller);
- il intercepte alors le raccourci passé depuis l'application authentifiée et récupère le titre de la fenêtre;
- il recherche, dans la base de données, l'entrée dont le champ *Title* correspond partiellement ou totalement au titre de la fenêtre d'authentification, puis lui envoie la séquence auto-type correspondante.

Pour que ce mode *global auto-type* fonctionne correctement, veillez aux points suivants:
- sous KeePassX (Linux/Mac), il n'est pas activé par défaut; allez dans `Extra>Settings` puis dans la catégorie `Advanced`, définissez le raccourci `<ctrl-alt-A>` (frappez cette séquence de touches) dans le champ `Global Auto-Type Shortcut`, activez l'option `Use entries title to match the window for Global Auto-Type`, et validez avec `Apply OK`;
- s'agissant de l'authentification de services Web, veillez à ce que le champ Title de l'entrée KeePass contienne bien le texte figurant dans la barre de titre de la page de *login* du service (titre fourni par la balise HTML <title>).

La puissance des modes auto-type KeePass réside dans le fait que cela fonctionne quel que soit votre navigateur Web et sans qu'il soit nécessaire d'installer une extension spécifique !

Si vous êtes maintenant convaincus par KeePass et souhaitez abandonner le système que vous utilisiez jusqu'ici, sachez qu'il est très facile de récupérer dans KeePass les identifiants et mots de passes que vous gériez différemment jusqu'ici. Commencez par les exporter depuis votre ancien outil au format TXT, CSV ou XML, puis **importez**-les dans KeePass avec `File>Import`.

Si vous exploitez KeePass sur un seul équipement, vous n'êtes pas à l'abri d'un crash disque ou d'un vol. N'oubliez donc pas de sauvegarder votre base de données sur un média externe. Vous pouvez aussi utiliser la bonne vieille technique de la liste papier en **imprimant** tous vos comptes avec `File>Print` (Windows seulement)... mais déposez-la en lieu sûr ! Notez que le processus d'impression, sous la version 1.x, passe par la génération d'un fichier HTML qu'il ne faut pas oublier de jeter après impression, car il contient les mots de passe en clair !

Fonctions plus avancées

Vous accédez aux nombreux réglages et préférences KeePass sous `Tools>Options` (Windows), `Extra>Settings` (Linux) ou `KeePass>Preferences` (Mac).

Sous KeePass 1.x (toutes plates-formes), vous constaterez que chaque fois que vous éditez une entrée, une copie de l'ancienne entrée est conservée dans un groupe nommé `Backup`. Vous pouvez désactiver cette fonctionnalité en décochant l'option `Save backups of modified entries into the Backup group` dans la catégorie de réglages `Advanced` sous Windows, ou dans la catégorie `General(2)` sous Linux/Mac, puis en supprimant ce groupe. Sous KeePass 2.x, cette fonctionnalité de backup n'existe pas, car les différentes versions d'une entité sont gérées au niveau de l'**historique** (voir onglet `History` dans la fenêtre d'édition d'une entité).

La sécurité de KeePass peut être paramétrée via diverses options dans la catégorie de réglages `Security`. Notez en particulier qu'il est possible de limiter la durée de validité des données déposées par KeePass dans le presse-papier (par défaut **auto-clear** après 10 à 20 secondes), et verrouiller automatiquement la base de donnée après un certain temps d'inactivité ou lorsque l'on minimise la fenêtre. Vous pouvez aussi **verrouiller** la base manuellement (p.ex. lorsque vous vous éloignez de votre poste) avec `File>Lock Workspace`, puis la déverrouiller avec `File>Unlock Workspace`, ou par le raccourcis `<ctrl-L>` ou encore le bouton cadenas (ce sont des bascules).

Pour renforcer encore la sécurité d'accès à la base de données, la solution consiste à la crypter en combinant deux techniques: le mot de passe principal *(master password)* et un **fichier de clé** *(key file)* qui constituent ensemble ce que KeePass appelle une Composite master key. Comme vu plus haut (fig. 1), faites `File>Change Master Key` et activez l'option `User master password and key file` (KeePass 1.x Windows) ou `Key File` (KeePassX Linux/Mac et KeePassX 2.x Windows). Vous devrez définir l'emplacement et nom de ce fichier de clé (mettez-lui l'extension `.key`), ensuite un générateur aléatoire fabriquera avec votre assistance la clé dans ce fichier. Vous pourriez opter pour un contrôle d'accès à la base de données basé sur le fichier de clé uniquement (donc sans mot de passe principal), mais ce n'est vraiment pas recommandé [24] ! Dans tous les cas, notez bien que si vous perdez ensuite le fichier de clé, le mot de passe principal n'est pas suffisant pour accéder aux informations de votre base de données.

Si vous êtes amené à gérer plusieurs bases de données KeePass, il peut être utile, sous Windows, d'associer les extensions `.kdb` ou `.kdbx` au logiciel pour pouvoir lancer KeePass par double-clic sur ces fichiers. Pour cela, dans l'onglet `Setup` (KeePass 1.x) ou `Integration` (2.x), cliquez simplement sur `Create Association`. Sous Linux et MacOSX, l'association des fichiers KDB à KeePassX est déjà faite.

Vous découvrirez que l'architecture KeePass est ouverte et permet l'usage de **plugins**. Faites cependant attention au fait que ces extensions, développées par des tierces parties, ont accès à votre base de données, ce qui peut donc compromettre la sécurité de KeePass !

Sachez finalement que KeePass Windows est en mesure de gérer des TAN *(Transaction Authentication Numbers)*, c'est-à-dire des **mots de passe à usage unique** (jetables) [25].

KeePass sur smartphone

Cela vous est sûrement arrivé (par exemple en voyage) de devoir accéder à une prestation authentifiée alors que vous n'avez pas le mot de passe sous la main, et cela vous a donné l'idée de stocker ces informations sur l'appareil qui ne vous lâche plus, votre smartphone. Avec le risque élevé de se faire voler son appareil, c'est bien entendu la pire idée qui soit si ces données sont dans un fichier en clair ! Mais KeePass, implémenté sur toutes les plates-formes mobiles, va vous sortir de ce mauvais pas !

Nous nous bornerons ici à vous présenter, par les figures 5 à 9, l'implémentation **KeePassDroid** sur smartphone et tablette An-

[24] Quiconque mettant la main sur votre Key file pourrait alors ouvrir votre base de données

[25] Voyez `Tools>TAN Wizard`

fig. 5 – sélection de la base de données et saisie du mot de passe principal sous KeePassDroid

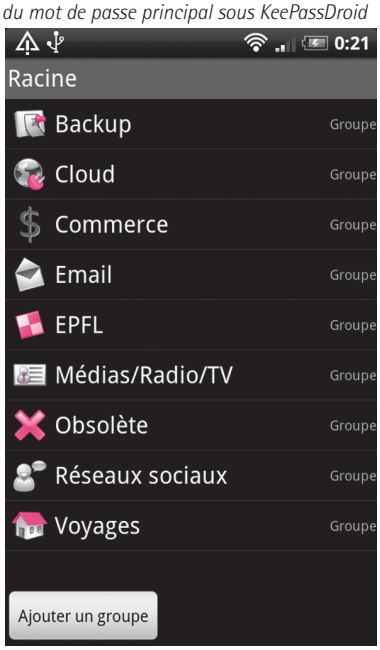

fig. 6 – affichage des groupes sous KeePassDroid

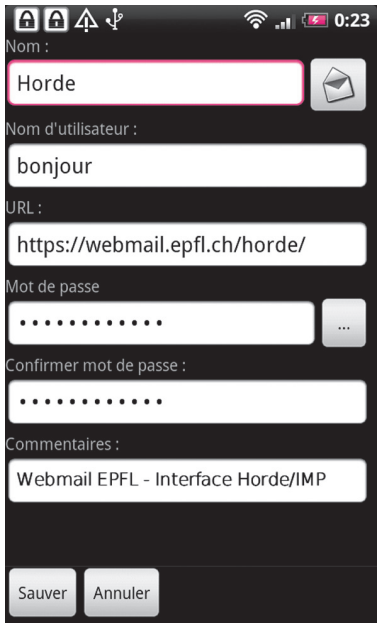

fig. 7 – saisie d'une entrée sous KeePassDroid

fig. 8 – sélection d'une icône de groupe ou d'entrée sous KeePassDroid

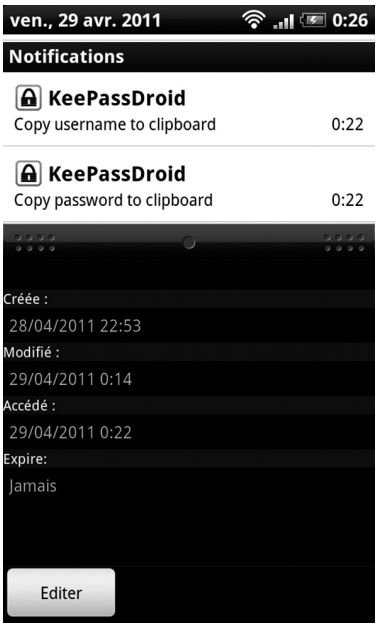

fig. 9 – affichage d'une entrée et récupération du username et password sous KeePassDroid

droid afin d'illustrer la simplicité de son **interface tactile**. Pour les personnes familières d'Android, remarquez, dans la figure 9, le mécanisme tactile implémenté via la barre supérieure de notification (ici dépliée) permettant de récupérer les username et password pour les coller dans l'application ou page Web authentifiée.

Synchronisation entre plusieurs postes

La base de données KeePass étant constituée d'un seul fichier, elle peut être facilement copiée à des fins de backup ou pour en disposer sur une autre machine. Vous pouvez aussi vous déplacer avec ce fichier **sur une clé USB** et l'exploiter directement sur celle-ci, mais faites-en une copie de sécurité ailleurs, une clé USB étant vite égarée ! Si vous souhaitez travailler sur des machines Windows où KeePass n'est pas installé, déposez également sur la clé USB l'application KeePass Windows. Nous vous rendons cependant attentif au danger inhérent à toute saisie de mot de passe: le mot de passe principal de votre base de données est susceptible d'être intercepté par un logiciel espion tel qu'un *keylogger*. Il faut être conscient de ce risque lorsque l'on travaille sur un poste qui n'est pas digne de confiance (cybercafé…). Dans une telle situation, la sécurité peut être renforcée par l'usage combiné du mot de passe principal avec un fichier de clé stocké sur votre clé USB (et bien entendu sauvegardé chez vous) et non sur le PC hôte.

Si vous utilisez KeePass sur plusieurs postes de travail ou équipements mobiles, les modifications de votre base de données devraient être répercutées sur tous ces équipements. L'automatisation de ce processus s'appelle la **synchronisation**. Pour l'instant, seul KeePass 2.x implémente un tel mécanisme en s'appuyant sur les protocoles FTP ou HTTP/WebDAV (voyez `File>Synchronize with URL`). Mais vous pouvez aussi recourir, quelle que soit la version de KeePass, à l'une des nombreuses solutions de synchronisation *génériques* de fichiers en **mode cloud** [26] supportées par vos appareils, telles que Dropbox [27], Wuala [28], SugarSync [29], Ubuntu One [30], MobileMe [31], Box.net [32], etc. La figure 10 présente une architecture de synchronisation KeePass entre plusieurs équipements à l'aide d'un tel service de stockage en *cloud*.

[26] Voir par exemple la liste wikipedia en.wikipedia.org/wiki/Comparison_of_file_hosting_services
[27] Dropbox (www.dropbox.com) est l'ancêtre de toutes ces solutions et le plus répandu
[28] Wuala (www.wuala.com) de La Cie offre une sécurité supplémentaire par rapport à Dropbox en ce sens qu'il y a un cryptage côté client avant l'envoi dans le *cloud*
[29] SugarSync (www.sugarsync.com) est un nouveau venu, dans le monde du *cloud*, très riche en fonctionnalités
[30] Ubuntu One (https://one.ubuntu.com/), solution de Canonical pour Linux/Ubuntu, très prochainement disponible sous Windows, Android, iOS
[31] MobileMe (www.apple.com/fr/mobileme/) de Apple est actuellement vieillot… et payant
[32] Box.net (www.box.net)

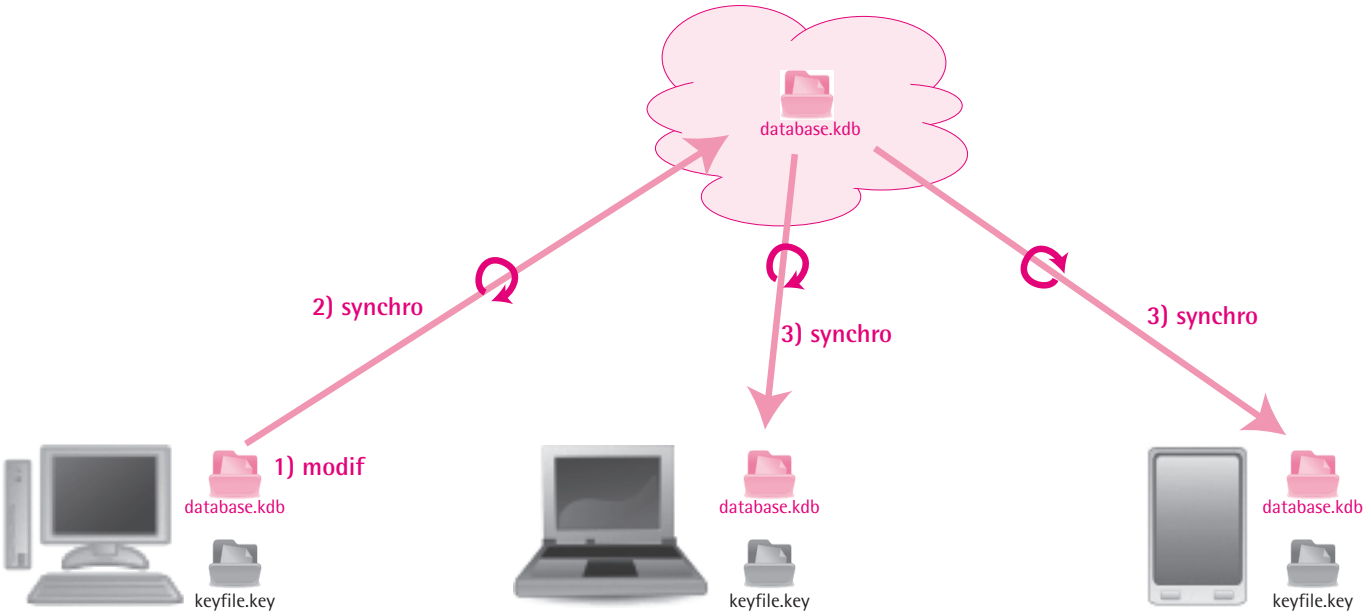

fig. 10 – architecture sécurisée de synchronisation KeePass via un service de cloud

On obtient un bon niveau de sécurité lorsque la base de données (`database.kdb`) est protégée par l'usage combiné d'un mot de passe principal et d'un fichier de clé (`keyfile.key`) déposé sur chaque machine. La synchronisation s'effectue ainsi:

1. on modifie la base de données depuis une machine (ici le desktop),
2. la base se synchronise alors automatiquement dans le *cloud*,
3. puis, de là, se synchronise vers les autres équipements.

Si la sécurité de l'espace de stockage en cloud est compromise, celui qui déroberait votre base de données ne pourra rien en faire sans posséder le fichier clé qui se trouve uniquement sur les machines. Celui qui vole une machine (contenant la base de données et le fichier clé) ne pourra rien faire non plus sans connaître votre mot de passe principal.

Avec une telle architecture, il est possible d'accéder à la base de données même lorsque l'on ne dispose provisoirement pas de connexion internet (p.ex. sur le smartphone). Si l'on modifie la base de données, la synchronisation de celle-ci dans le cloud s'effectuera automatiquement lorsque la connexion réseau sera rétablie. Il faut veiller à ne pas modifier simultanément la base de données depuis plusieurs équipements. Cela ne risque pas de se produire si vous êtes seul à exploiter cette base de donnée[33].

Références

Pour davantage d'informations sur l'utilisation des logiciels de la famille KeePass, voyez:

- l'aide intégrée au logiciel: menu `Help`
- la homepage de KeePass pour Windows: **keepass.info**
  - l'aide en ligne: **keepass.info/help/**
  - la FAQ technique: **keepass.info/help/base/faq_tech.html**
  - les forums de discussion: **https://sourceforge.net/projects/keepass/forums**
- la homepage de KeePassX pour Linux/MacOSX: **www.keepassx.org**
- pour d'autres liens voir: **keepass.info/links.html**.

[33] KeePass implémente du reste un mécanisme de lock-file qui vous informerait d'une telle situation