***Technische Notiz***
***Jürgen Meißburger***

20.2.2007

# KeePass Password Safe

### Automatisches Web-Login mit verschlüsselten Passwörtern

## 1. Einleitung

Jeder, der im Internet einkauft oder seine Bankgeschäfte erledigt, benötigt seine Login-Informationen wie Benutzerkennung oder Kontonummer und ein dazugehöriges Passwort bzw. PIN. Unter dem Aspekt der Sicherheit ist es am besten, alle diese Informationen ausschließlich im (eigenen) Kopf zu speichern! Leider verlässt jedoch den Normalsterblichen im Laufe der Zeit schon mal sein Gedächtnis, wenn die Zahl der zu merkenden Informationen stetig wächst und wächst ..... Fehlversuche, Kontosperrungen oder Schlimmeres sind die Folge!

Aufschreiben der Passwörter an einem geheimen Ort (unter der Tastatur, unter der Schreibtischschublade, im Geldbeutel oder in der Bettlektüre .... ;-) löst nicht wirklich das Problem, falls man unerwartet Besuch von Bösewichten oder "Freunden" erhält.

Aus diesem Grunde existieren Programme, die solch sensitiven Informationen "gut verschlüsselt" auf dem Rechner (weniger empfehlenswert) oder auf einem externen Datenträger (besser) ablegen. Hierfür eignen sich vor allem USB-Sticks, die sich auch mal bequem im Banktresor oder in der Brieftasche verstauen lassen. Besonders bequem sind sogenannte U3-Sticks, bei denen der Zugriff auf den Datenträger selbst nochmals Passwort-geschützt ist.

Eines dieser Programme, das beliebige Zugangsinformationen verschlüsselt aufbewahren und auch den Login-Vorgang automatisieren kann, **ist KeePass Password Safe von Dominik Reichl**. Wichtig dabei ist, dass zu keiner Zeit, auch nicht bei geöffnetem Programm, die Passwortinformation unverschlüsselt etwa im Speicher oder auf dem Bildschirm steht und durch Spionage-Programme ausgelesen werden könnte.


Dank einer eingebauten Auto-Type-Funktion, die durch eine einfache Script-Sprache praktisch jedem Login-Vorgang angepasst werden kann, kann das Login im Netz automatisiert werden, so dass auch das lästige und ebenfalls nicht ganz ungefährliche Tippen der Passwörter (Keylogger!) entfällt.

Und das beste: Das Programm ist kostenlos (gegen eine kleine und freiwillige Spende hat der Autor sicher nichts einzuwenden) und kann unter der Adresse

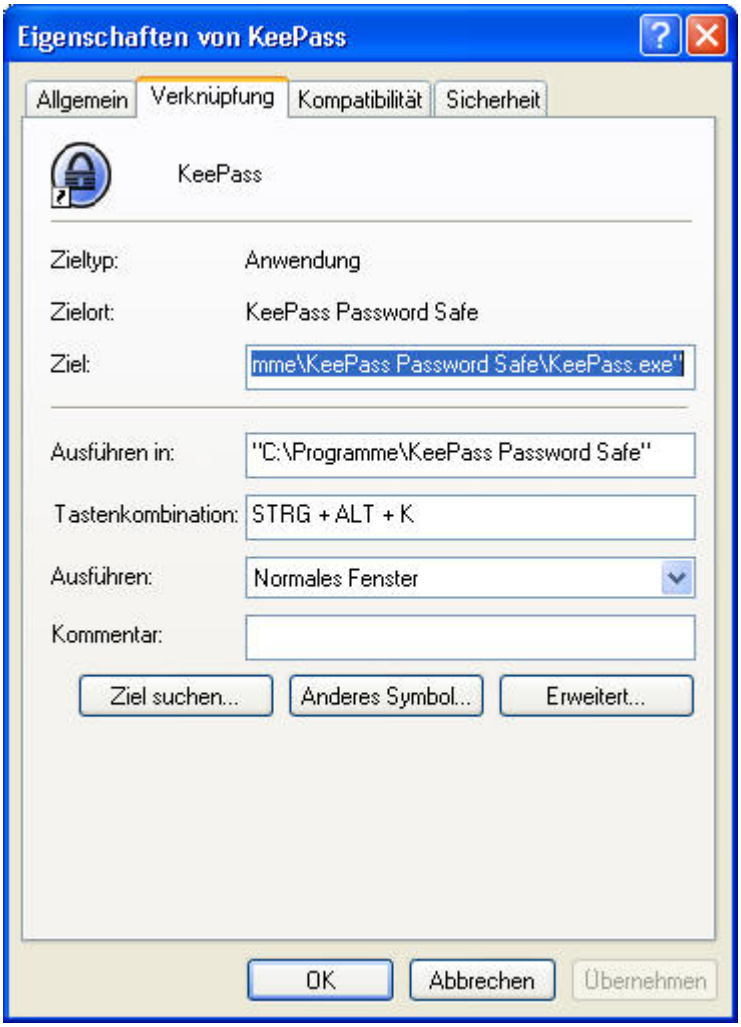
**http://keepass.info**

heruntergeladen werden.

## 2. Installation

Nach Herunterladen der Datei **KeePass-xxxx-Setup.exe** diese ausführen und den Installationsanweisungen folgen. Das Programm kann problemlos jederzeit wieder in der "Systemsteuerung - Software" deinstalliert werden.

Wer die Installation ganz vermeiden möchte, sollte statt dessen das ZIP-Archiv **KeePass-xxxx.zip** herunterladen und beispielsweise in den Ordner C:\Programme\KeePass entpacken. Das Programm wird dann einfach durch Löschen dieses Ordners wieder deinstalliert.

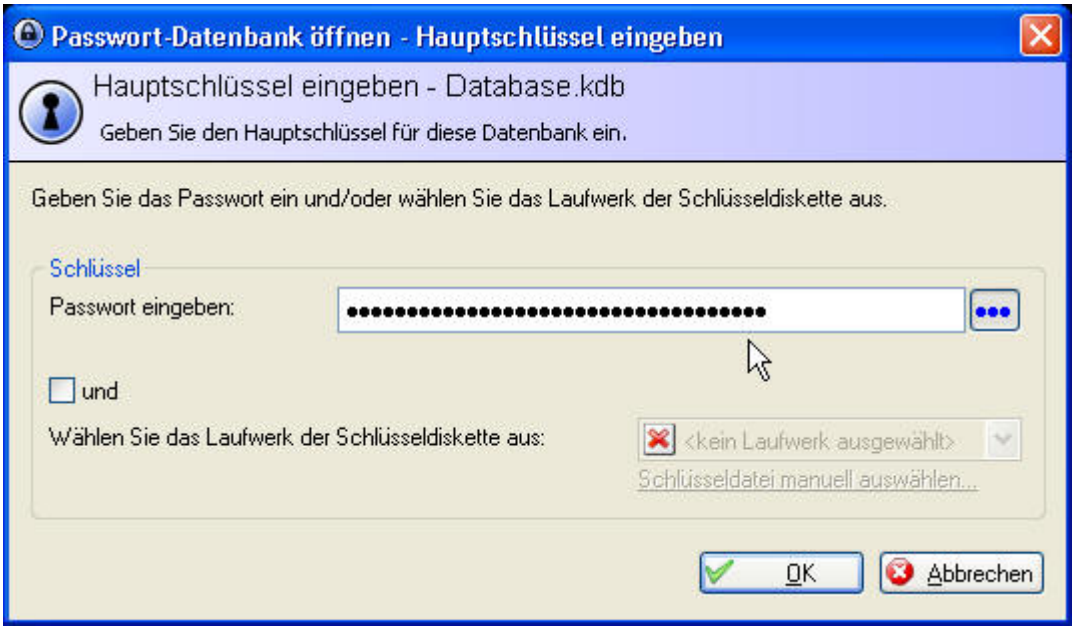



Auf dem Desktop oder in der Schnellstartleiste kann dann noch mit "Rechte Maustaste - Verknüpfung erstellen" eine Startverknüpfung mit dem Programm **KeePass.exe** erstellt werden, um das Programm einfach zu starten.

KeePass selbst versucht den Hotkey **<Ctrl>-<Alt>-K** für seinen Start zu registrieren. Falls dies nicht von selbst funktionieren sollte, kann man diesen Hotkey mit "RM - Eigenschaften - Tastenkombination" in das Programmlink für KeePass Password Safe eintragen. Dies ermöglicht einen Start des Programms im Hintergrund auch bei "vollem" Bildschirm, wenn die Startsymbole nicht sichtbar sind.

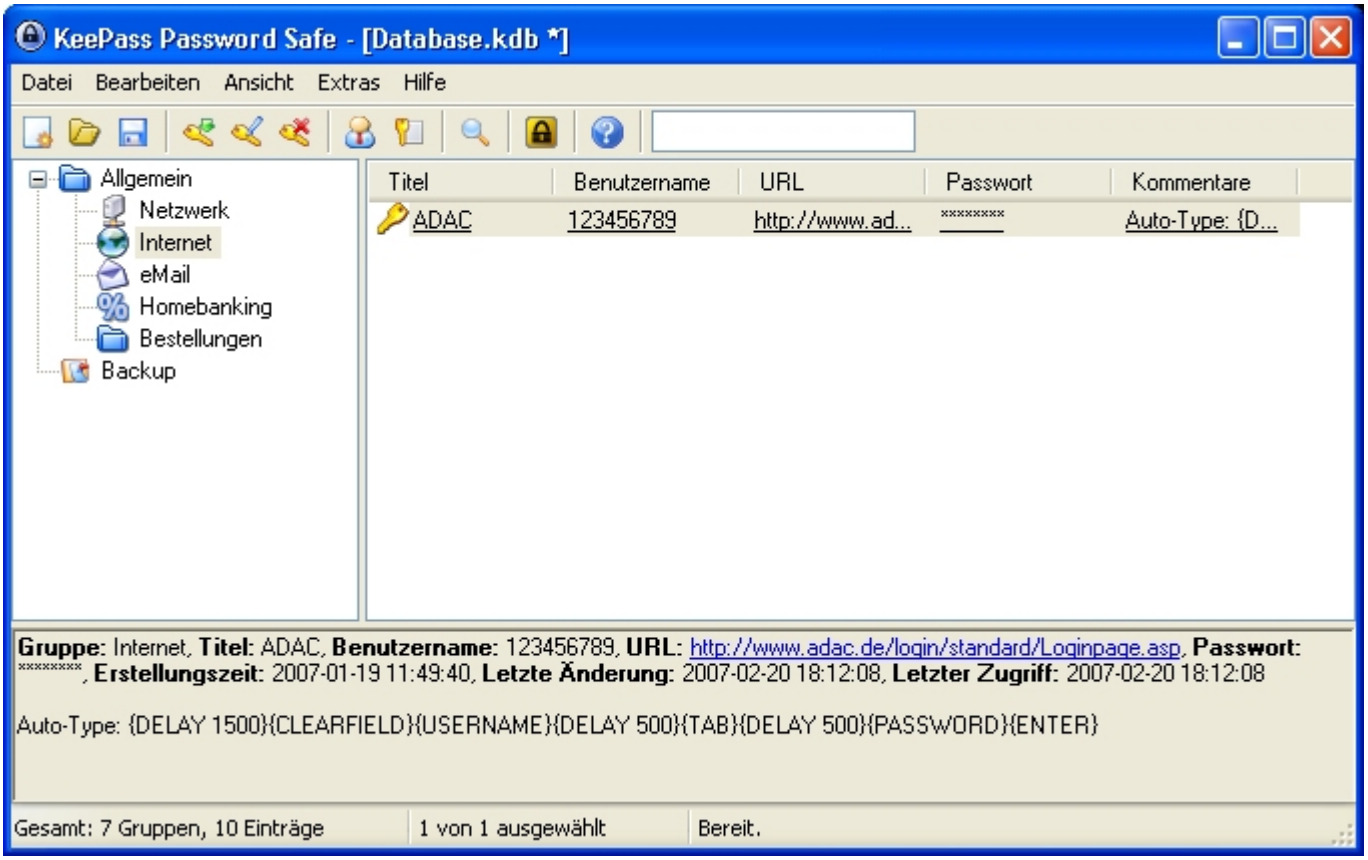
## 3. Start und Einrichten der Datenbank

Beim ersten Start wird man aufgefordert, ein Master-Passwort für eine neue Datenbank anzugeben. Hier sollte man sich einen längeren, gut merkbaren Satz (auch mit Sonderzeichen und Umlauten) ausdenken, der zur Verschlüsselung all der in der Datenbank gespeicherten Informationen dient. **Man muss sich in Zukunft also nur diesen einen Satz merken, den man tunlichst auch nicht vergessen sollte!** (Ein Backup des Satzes in einem verschlossenem Couvert im Bankfach ist vielleicht keine schlechte Idee ;-)



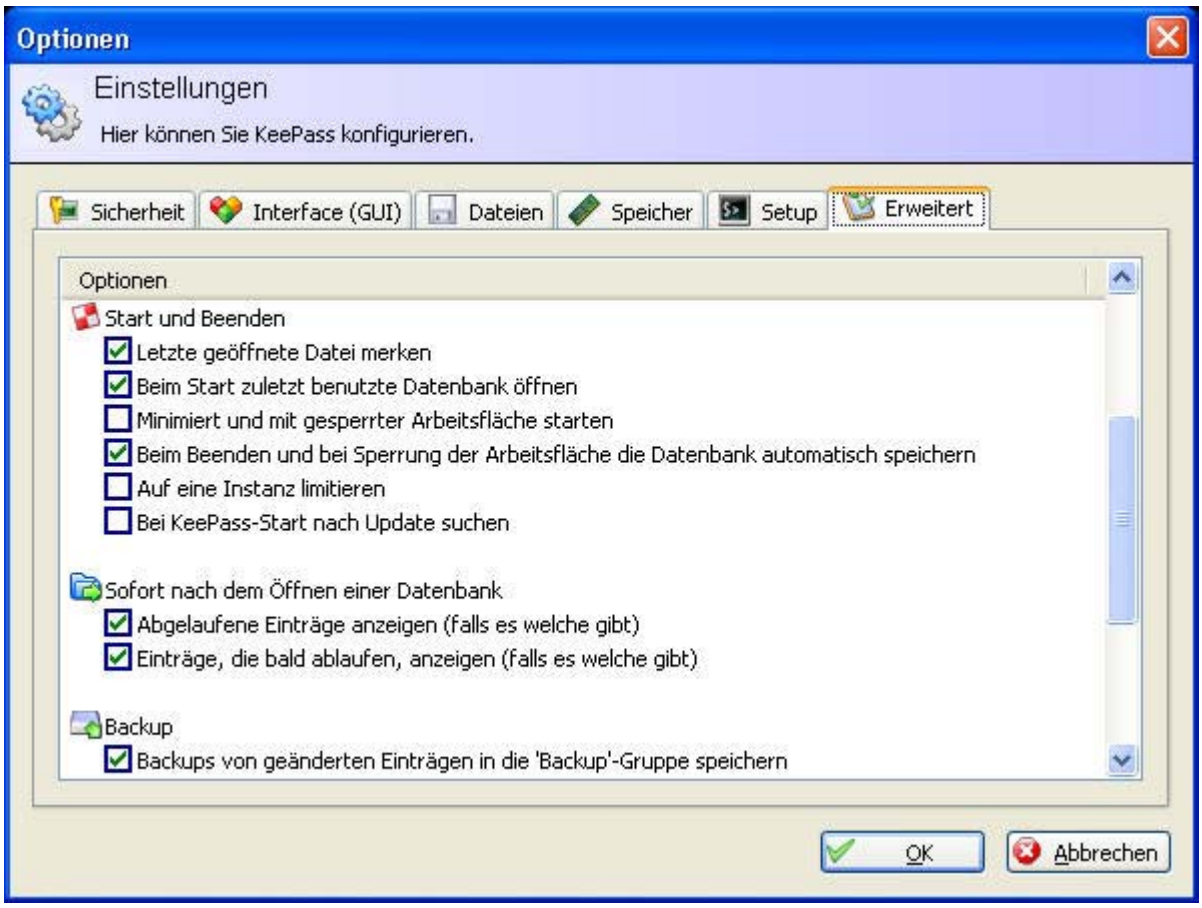

Wer noch höhere Sicherheit wünscht, kann in diesem Dialog noch eine Schlüsseldatei angeben, die auf einem anderen Laufwerk, etwa einem USB-Stick, liegen kann. Der Zugang zur Datenbank ist dann nur mit dem Master-Passwort und gleichzeitigem Zugriff auf die Schlüsseldatei (also physikalischem Besitz des Datenträgers mit der Schlüsseldatei) möglich.

Im Hauptfenster des Programms:



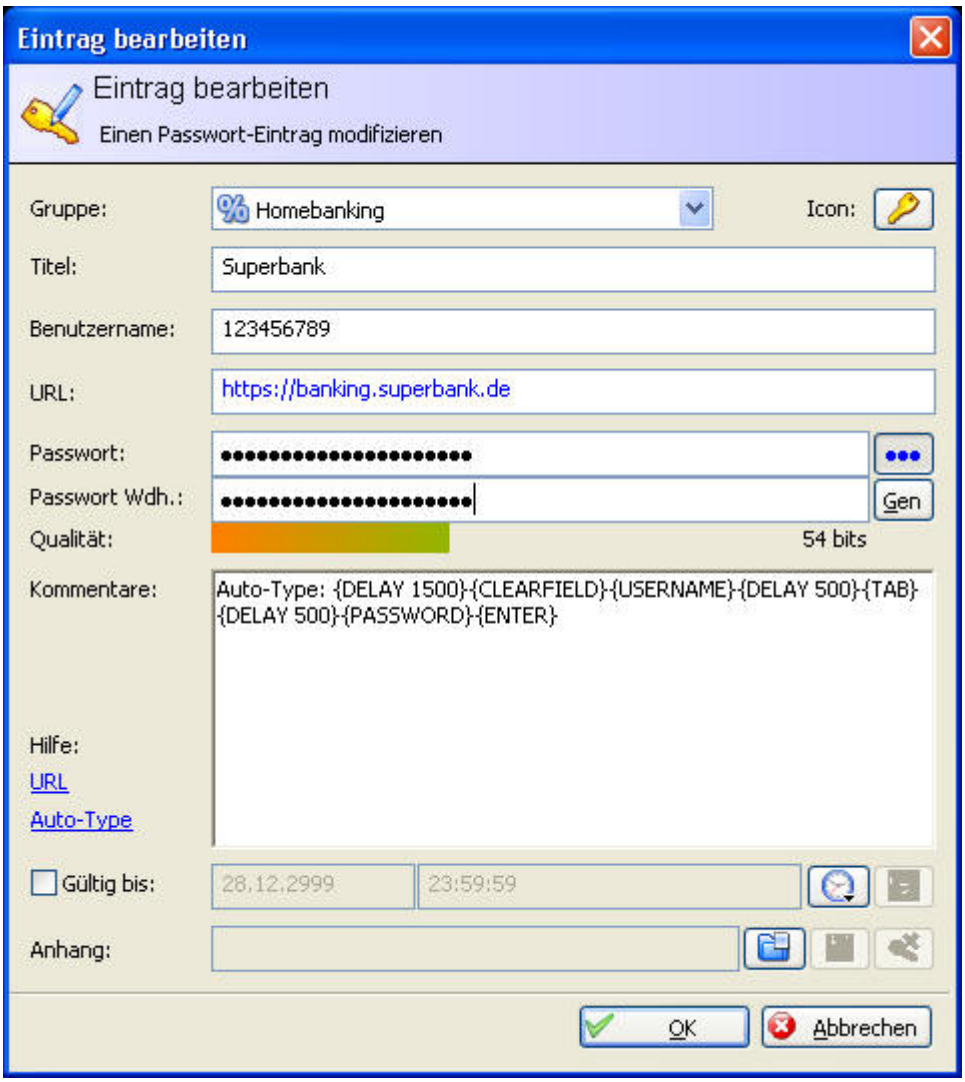

wird dann die neu erzeugte Datenbank mit "Datei - Speichern unter...." auf der Festplatte abgespeichert (Default ist **Database.kdb**). Man sollte diese Datenbank vielleicht nicht direkt unter "Eigene Dateien", sondern an einem etwas unverfänglicheren Platz ablegen und in regelmäßigen Abständen eine Sicherungskopie erstellen.

Unter "Ansicht - Sprache ändern" lässt sich die gewünschte Menü-Sprache einstellen, und mit "Extras - Einstellungen - Erweitert" lassen sich einige Optionen für eine flottere Bedienung angeben:



# 4. Benutzung mit Auto-Type

Mit "Eintrag hinzufügen" bzw. "Eintrag bearbeiten" werden nun neue Zugangsdaten in die Datenbank eingetragen. Um bei etwas langsameren Webseiten die Zugangsdaten sicher in die Formularfelder der Login-Seite einzutragen, kann man die Skript-Fähigkeiten von PasswordSafe zu nutzen und mit "Eintrag bearbeiten" etwa folgende Skriptzeile einzutragen:




Die **URL:** ist die URL der Login-Seite des Webanbieters, also etwa der Bank oder des on-line-Shops (Achtung: Sollte immer SSL-verschlüsselt sein, d.h. mit **https://.....** beginnen !).

Der Benutzername ist der Login-Name oder bei Banken häufig die Konto-Nummer,

und das Passwort ist schließlich das eigentliche Passwort oder eine PIN für den Kontenzugang.

Die Auto-Type-Zeile bewirkt jeweils eine kleine Verzögerung beim Ausfüllen der Felder und zu Beginn ein Löschen des ersten Feldes.

Der Vorgang des Auto-Login läuft dann wie folgt ab:

- Die gewünschte Verbindung im rechten, oberen Fenster auswählen und unten auf das blau markierte Link der Login-Seite klicken. Damit öffnet sich der Standard-Browser mit dem Login-Bildschirm.
- Dann unten in der Taskleiste auf das Kästchen für KeePass klicken, so dass PasswordSafe wieder in den Vordergrund kommt.
- und mit <Ctrl>V das Login ausführen. Nach 1.5 Sekunden sollten dann die Felder in der Login-Maske des Browsers automatisch ausgefüllt und das Login durchgeführt werden.