

Passwörter verwalten mit KeePass 2

Anleitung für MitarbeiterInnen und Studierende

Zuletzt aktualisiert: März 2016

Inhalt

Allgemeines zu KeePass 2.....	1
Warnende Worte zu Passwort-Safes.....	1
Installation der portablen Version unter Windows	1
Änderung der Standardsprache (optional).....	2
Anlegen einer Passwortdatenbank	4
Erstellen von Passworteinträgen am Beispiel email.uni-graz.at	6
Verwendung des Passwort-Safes	7

Allgemeines zu KeePass 2

KeePass 2 ist ein weitverbreitetes Open Source Programm, das u.a. in einer portablen Version für Windows und Linux vorliegt. Es wird unter der GPL-Lizenz vertrieben und kann frei genutzt werden. Die Einrichtung eines Passwort-Safes ist aufwändig und erst ab einer hohen Anzahl an Passwörtern sinnvoll.

Warnende Worte zu Passwort-Safes

Die Verwendung von Passwort-Safes ist leider nicht unproblematisch. Durch die Nicht-Eingabe des Passworts merkt man sich keine Passwörter mehr. Daher ist mit dem Verlust (Verloren, Diebstahl, Defekt) des USB-Sticks oder des Gerätes auf dem Passwörter gespeichert sind ohne weitere Vorkehrungen ein Totalverlust der Passwörter verbunden. **Machen Sie daher immer eine Sicherheitskopie des Passwort-Safes!**

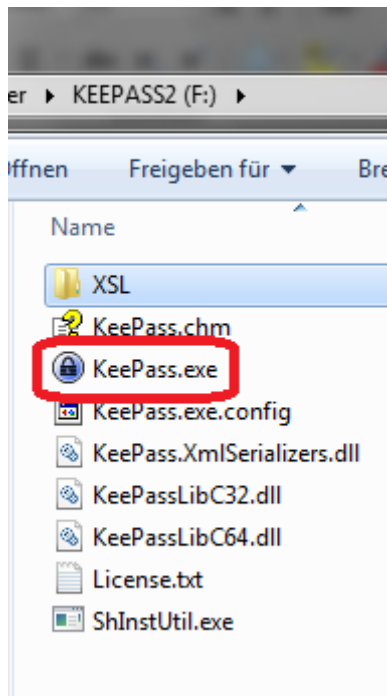
Installation der portablen Version unter Windows

Laden Sie sich die aktuelle portable Version von KeePass 2 von einer vertrauenswürdigen Homepage (z.B. <http://keepass.info/download.html>) herunter. Extrahieren Sie die den Inhalt der zip-Datei in ein Verzeichnis eines (mobilen) Datenträgers. Der mobile Datenträger ist sinnvoll, da Passwörter mitunter auch außerhalb Ihres Arbeitsplatzes benötigt werden.

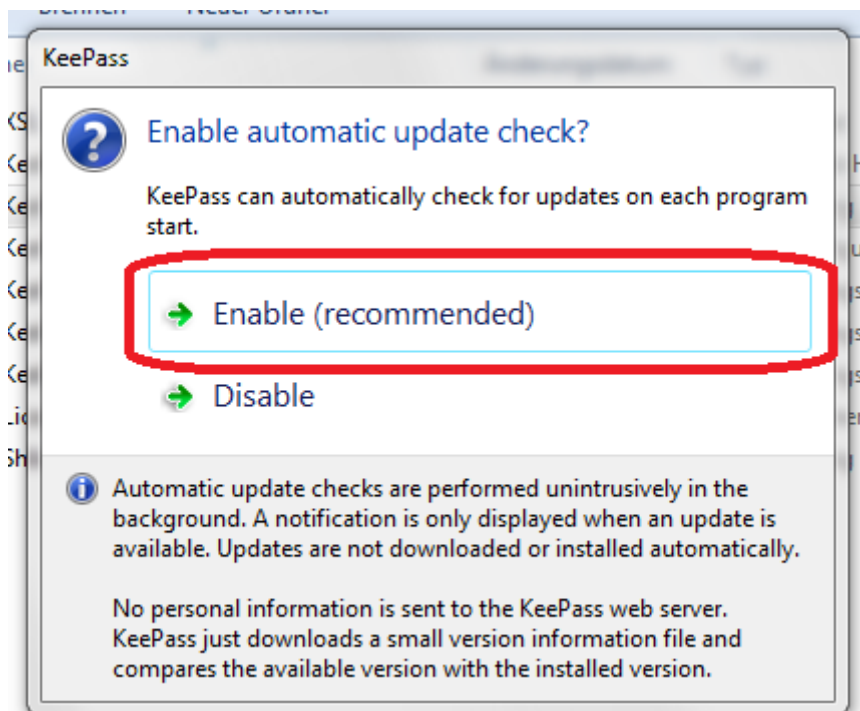
Sollten Sie KeePass 2 ausschließlich am Arbeitsplatz verwenden, gibt es ein entsprechendes Baramundi-Paket für die fertige Installation inkl. deutschem Sprachpaket (Anforderung über Servicedesk).

Änderung der Standardsprache (optional)

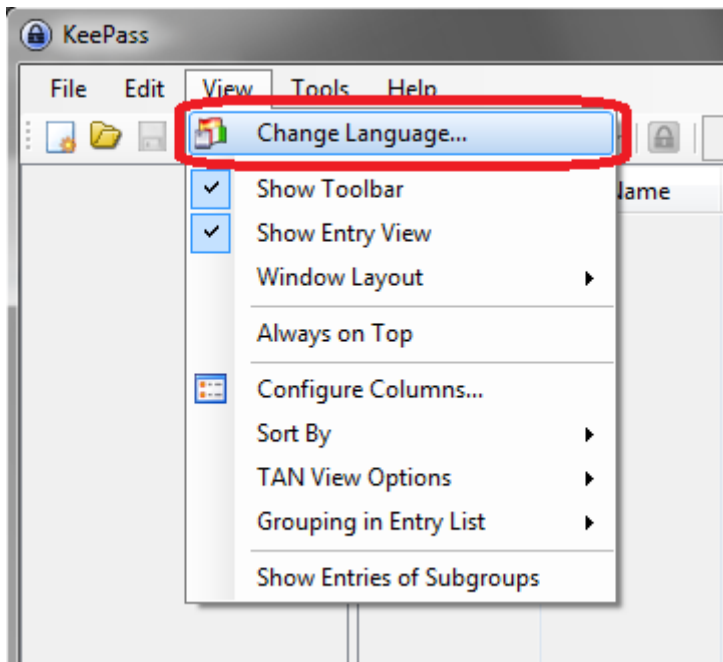
Starten Sie nun KeePass 2 mit einem Doppelklick auf *KeePass.exe*.



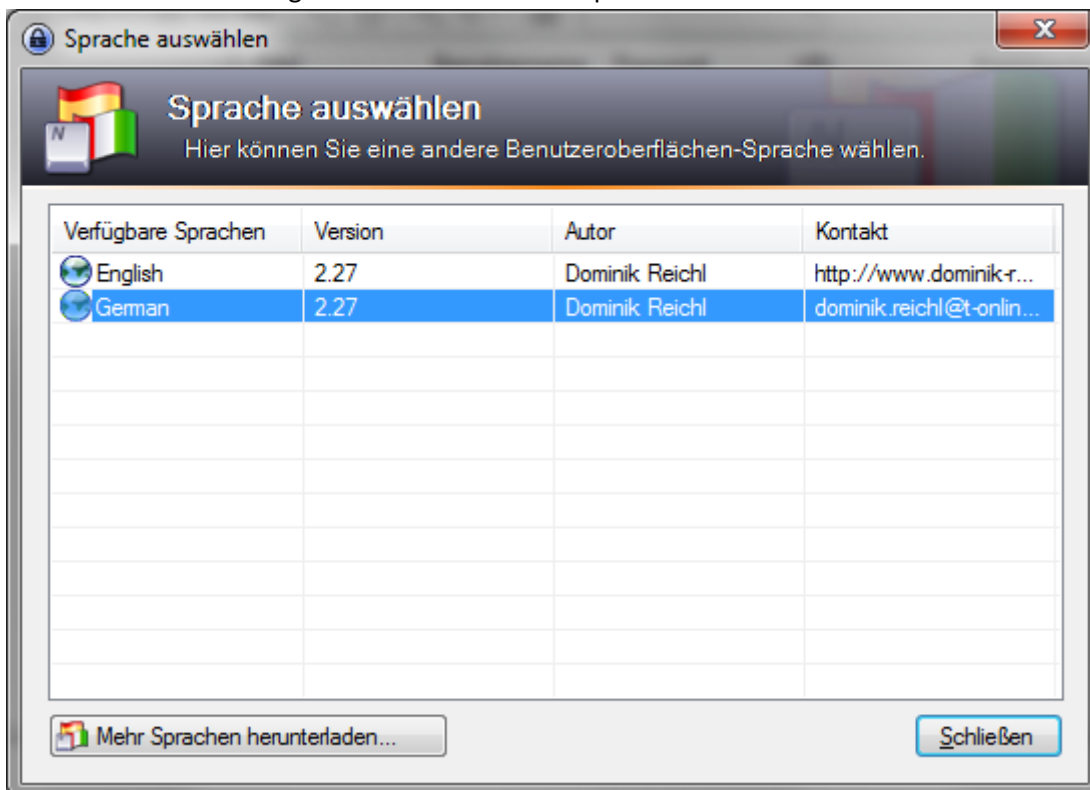
Die folgende Abfrage zur Aktivierung automatischer Updateüberprüfung beantworten Sie am besten mit der empfohlenen Einstellung. Auch sichere Software hat Sicherheitslücken und muss aktualisiert werden.



Nun startet KeePass 2. Bei Bedarf können Sie über das Menü *View » Change Language...* Ihre bevorzugte Sprache einstellen.



Damit laden Sie mit Unterstützung von KeePass 2 die zip-Datei mit der entsprechenden Sprache herunter. Entpacken Sie die Datei in das Verzeichnis, in das Sie zuvor KeePass 2 abgelegt haben. Nach einem Neustart des Programms steht dann Ihre Sprache im Menü zur Auswahl.

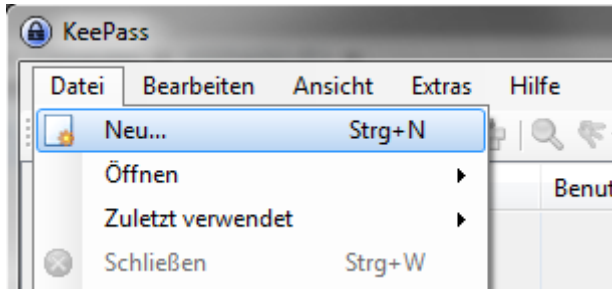


Nach dem Schließen erscheinen alle Menüs in der gewählten Sprache.

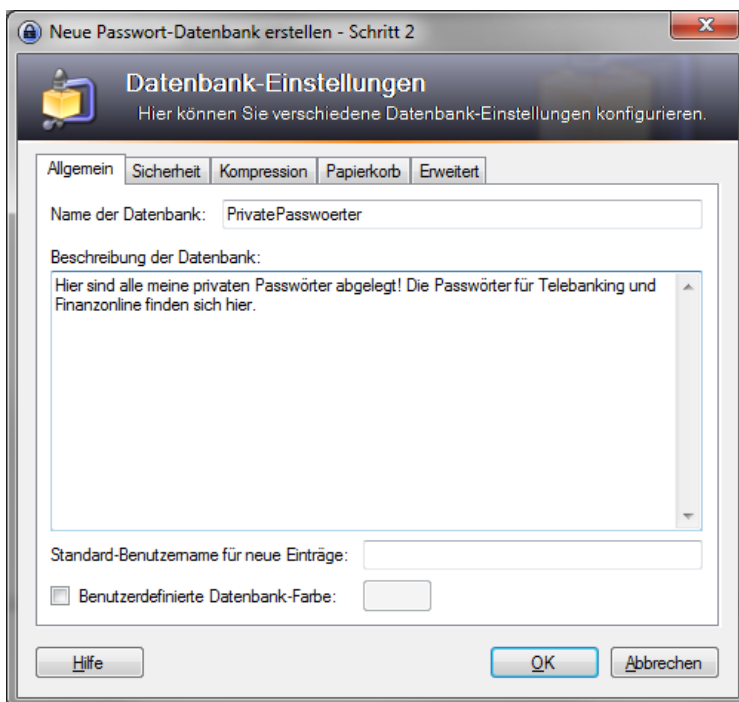
Anlegen einer Passwortdatenbank

Mit dem Anlegen einer Passwortdatenbank wird eine verschlüsselte Datei erstellt, in der Ihre Passwörter abgelegt werden. **Diese Datei ist daher besonders WICHTIG und sollte nach jeder Änderung (neues Passwort eingespeichert) auch gesichert werden!**

Zum Erstellen der Datenbank wählen Sie den Menüpunkt *Datei » Neu* oder drücken Sie *Strg+N*.



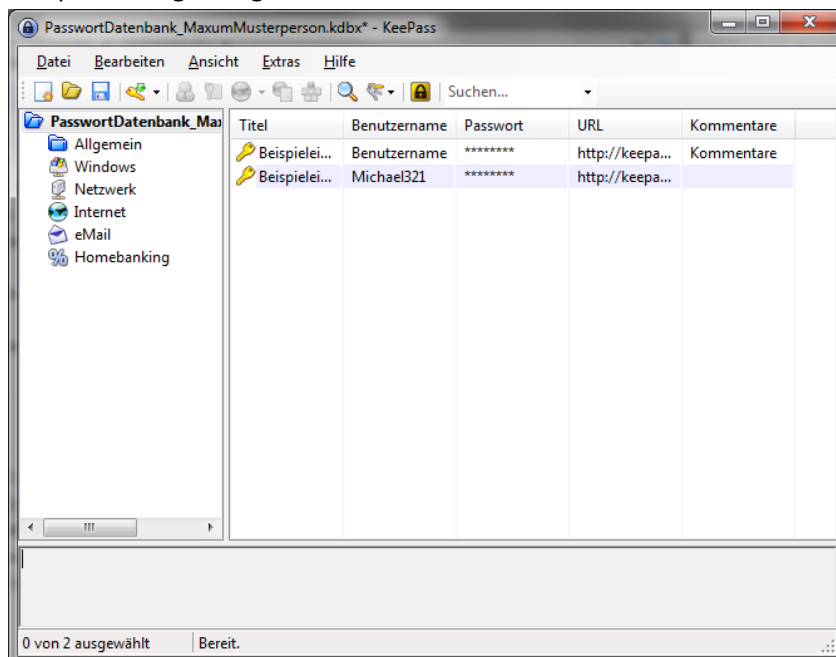
Im folgenden Pop-Up **Datenbank-Einstellungen** geben Sie den Namen und eine kurze Beschreibung der Datenbank ein.



Nach dem Bestätigen mit *OK* werden Sie nun nach dem Security Token für die Datenbank gefragt. Es gibt verschiedene Varianten, aber am einfachsten wählen Sie ein ausreichend langes Hauptpasswort aus. **Dieses Passwort ist der Schlüssel zu Ihrer Passwortdatenbank und darf nicht verloren gehen!** Das Passwort muss auch sehr sicher gewählt sein, damit Ihre gespeicherten Passwörter gut geschützt sind.



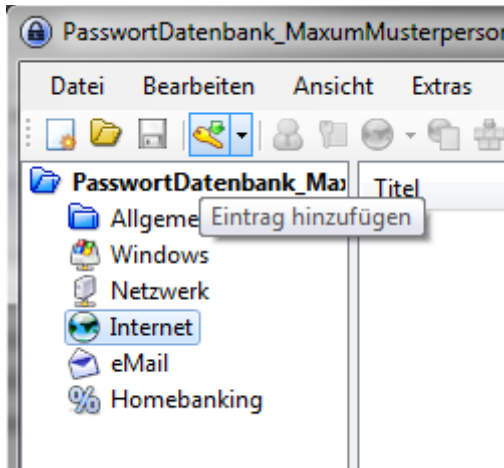
Mit dem Bestätigen auf *OK* sind sie nun fertig. Die neue Datenbank mit einer Beispielstruktur und Beispieleinträgen liegt vor.



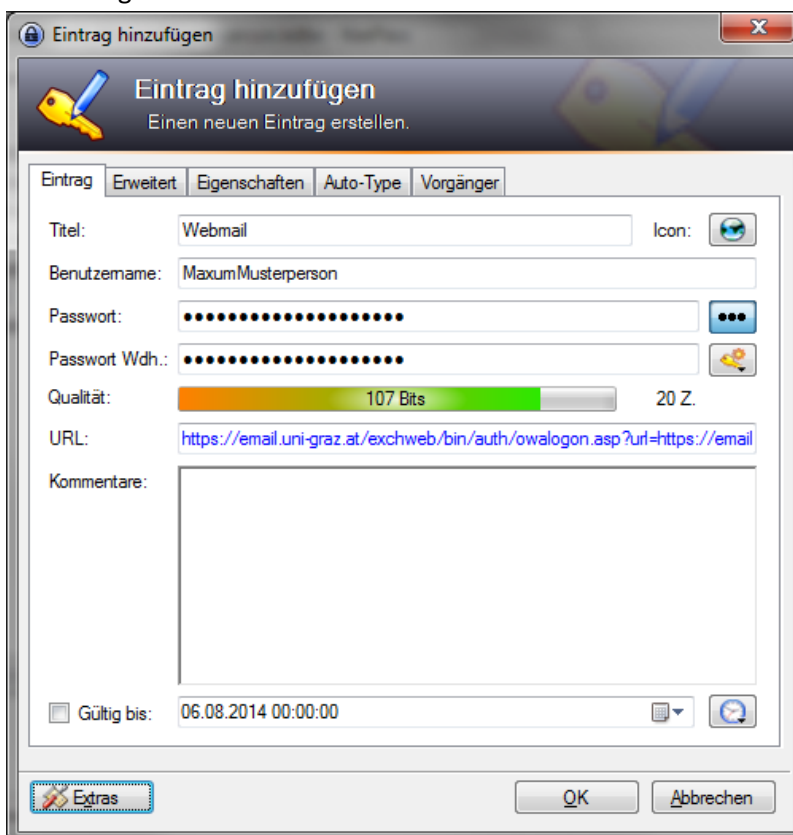
Erstellen von Passworteinträgen am Beispiel email.uni-graz.at

Nach dem Erstellen der Passwortdatenbank können Sie nun Passworteinträge erstellen.

Wählen Sie das Symbol für einen neuen Schlüssel.

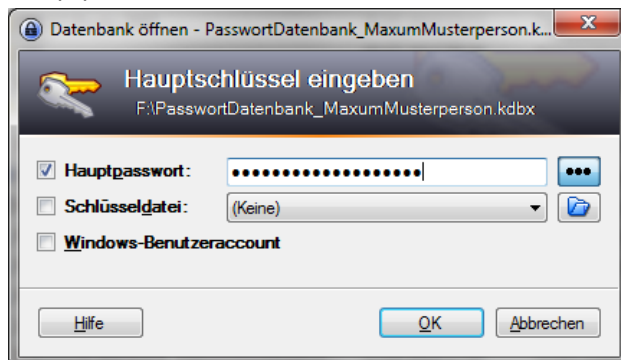


Im folgenden Fenster tragen Sie den Titel des passwortgeschützten Systems (im folgenden Beispiel „Webmail“) und die Zugangsdaten *Benutzername*, *Passwort* und *URL* (die Adresse des Zielsystems) ein. Sie können sich Passwörter generieren lassen, müssen diese aber dann natürlich auch im Zielsystem ändern. Den URL kopieren Sie am besten aus der Webseite heraus, um Tippfehlern vorzubeugen.

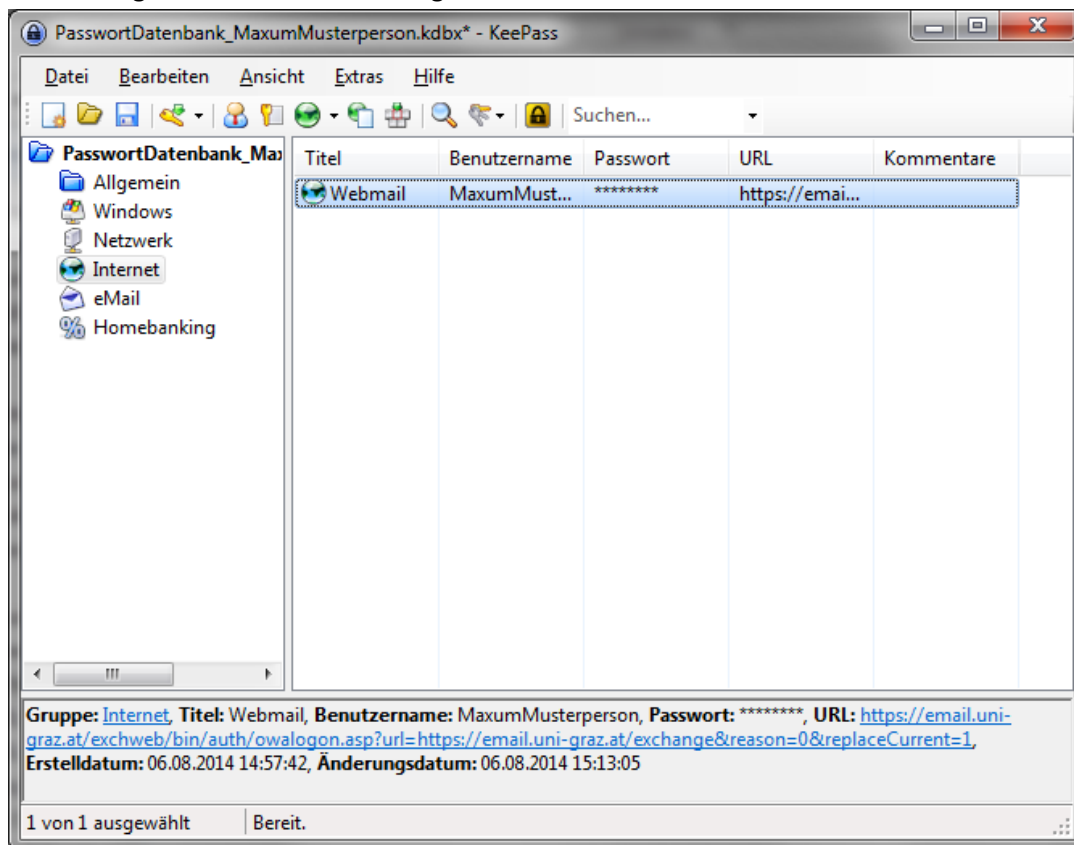


Verwendung des Passwort-Safes

Für die erste Verwendung schließen Sie nun KeePass 2. Nach dem Neustart von KeePass 2 erscheint die Aufforderung, Ihren Hauptschlüssel einzugeben. Geben Sie dort das vorher gewählt Hauptpasswort zum Entschlüsseln der Datenbank ein.



Nach erfolgreicher Authentifizierung erscheint nun Ihre Passwortdatenbank in KeePass 2.



Klicken Sie nun auf den Link für den Eintrag „Webmail“ in der Fußzeile des Fensters um die Seite im Browser zu öffnen. *Strg+V* kopiert die Zugangsdaten automatisch in das Browserfenster und meldet Sie an.

Klicken Sie mit der rechten Maustaste auf den Webmail-Eintrag, finden Sie auch weitere Optionen zur Bearbeitung des Datensatzes.