Keepass-Passwortsafe
Benutzeranleitung

Inhaltsverzeichnis

Allgemeine Informationen

Bitte lesen Sie diesen Abschnitt vor der Einrichtung des Keepass vollständig durch.

Was ist Keepass?

Keepass ist ein Passwortsafe, in welchem Kennwörter sicher und einfach verwalten werden können. Die Kennwörter werden im Passwortsafe in einer nicht lesbaren Form abgelegt.
Beim Start eines Programms kann man das Passwort per Paste & Copy in die Anmeldemaske des Programms einfügen.
Sowohl browserbasierte als auch lokal installierte Programme lassen sich direkt aus Keepass aufrufen.

Warum sollte man Keepass nutzen?

Die Schwierigkeit, ein Passwort zu knacken, wächst mit dessen Länge exponentiell an. Darum sollte ein Passwort mindestens 12 Zeichen lang sein.

Des Weiteren sollte es auch eine gewisse Komplexität aufweisen, also nicht aus einer Zahlenreihefolge oder dem eigenen Namen plus Geburtsjahr bestehen. Komplexität lässt sich herstellen durch die Kombination mehrerer Zeichentypen (Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen).
Beispiel 1: Fußb@ll-WM_!974

Oder durch die Akronymisierung eines längeren Satzes (von jedem Wort wird der Anfangsbuchstabe verwendet).
Beispiel 2: IaadPhLB-s2015 → entstanden aus: ich arbeite an der PH Ludwigsburg – seit 2015

Allerdings bietet kein noch so gutes Kennwort absoluten Schutz, da es beispielsweise durch Phishing von einem Angreifer erbeutet werden kann. Wenn man nun für alle Anwendungen und Systeme dasselbe Passwort verwendet, kann ein Angreifer mit dem einen gestohlenen Kennwort in alle Anwendungen eindringen.

Daher sollte für jede Anwendung ein separates Passwort verwendet werden. Angesichts der vielen Anwendungen kann man sich natürlich nicht alle Kennwörter merken. Diese vielen Kennwörter abrufbar zu speichern, ist der Zweck eines Passwortsafes.

Zur sicheren Benutzung von Keepass

Hierbei sind zwei extrem wichtige Gesichtspunkte zu beachten.

1. Das Passwort für Keepass selbst.
Da Keepass tendenziell alle Kennwörter eines Anwenders enthält, ist es natürlich ein attraktives Ziel für Angreifer. Darum muss das Passwort für Keepass besonders lang und besonders komplex sein, damit es nicht erraten werden kann.

Des Weiteren – und das ist beinahe noch wichtiger – muss es immer verfügbar sein.
Mit anderen Worten: es darf niemals vergessen werden!
Da Keepass eine rein individuelle Anwendung ist, kann es nicht per Ticket zurückgesetzt werden.

Um die Verfügbarkeit sicherzustellen, kann man das Passwort auf einen Zettel schreiben und diesen an einem sicheren Ort aufbewahren. Die Schreibtischschublade und der Platz unter der Tastatur sind definitv keine sicheren Orte. Besser ist es, den Zettel in ein Buch einzulegen oder das Passwort gleich mit Bleistift ins Buch einzutragen oder es auszudrucken und es mitten in einem vollen Ordner abzuheften. Besser ist es freilich, ein Teil des Passworts sich selbst per Mail zuschicken oder es in einer Datei mit einem unverfänglichen Namen (Bsp.: Keepassdoku.docx oder KP_Info.docx) abzuspeichern.

Da man sich auf die Funktionalität von Keepass verlässt, kann man sich wahrscheinlich nur an wenige Passwörter der Anwendungen erinnern, die im Keepass gespeichert werden, weshalb kein Zugriff auf diese Anwendungen und deren Daten mehr möglich ist.
Allerdings: Auch wenn das Keepass-Kennwort vergessen wurde, ist nicht alles verloren. Man kann für die Anwendungen neue Kennwörter beantragen. Das ist aber mühsam und zeitraubend und sollte unbedingt vermieden werden.

2. Ebenso wichtig ist, die im Keepass enthaltenen Kennworteinträge zu sichern.
Diese werden in einer Datenbank gespeichert. Wird die Datenbank beschädigt oder gelöscht, sind alle gespeicherten Kennwörter verloren, was die gleichen Folgen hat wie das Vergessen des Keepass-Passworts.

Darum muss mindestens ein, besser zwei Backups der Datenbank gespeichert werden. Ein Backup sollte dabei unbedingt auf einem zentralen Laufwerk wie dem Homedir liegen, weil dieses täglich gesichert wird.

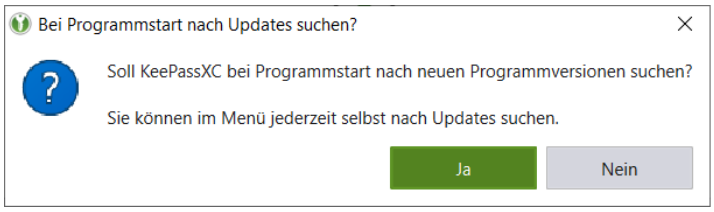
Einrichtung und Verwendung

Einrichtung

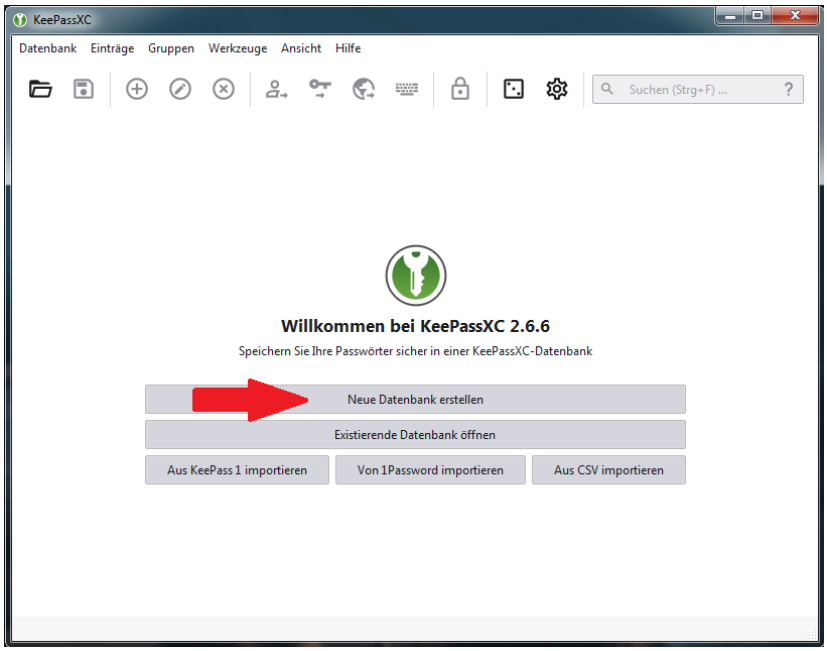
Keepass wird über unser Software-Verteilungssystem „Baramundi“ automatisch auf jedem Rechner installiert.

Es muss aber individuell konfiguriert werden. Hierzu gehen Sie wie folgt vor:

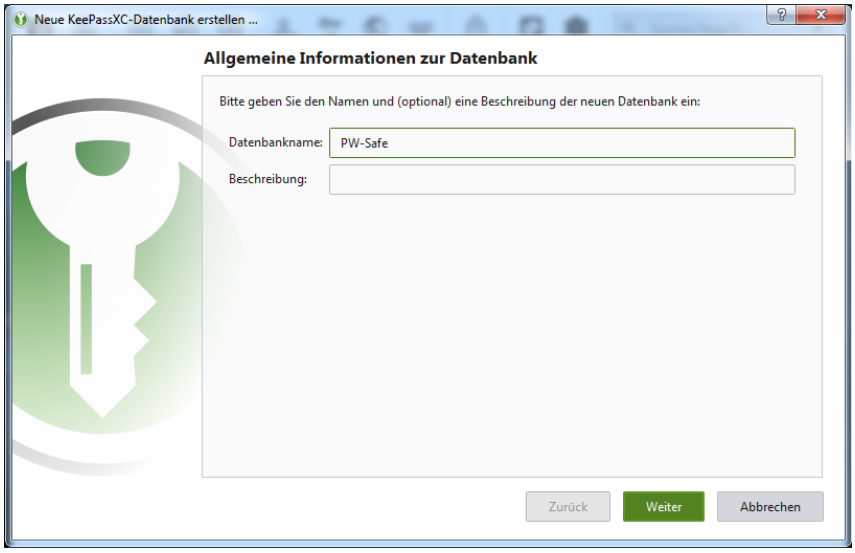
- Keepass im Startmenü oder über das auf dem Desktop liegende Icon starten.
- Es erscheint die Abfrage, ob bei jedem Programmstart nach Updates gesucht werden soll. Bitte wählen Sie hier „Nein“ aus (Die Sicherheitsupdates für diese Software werden wir Zentral Installieren).



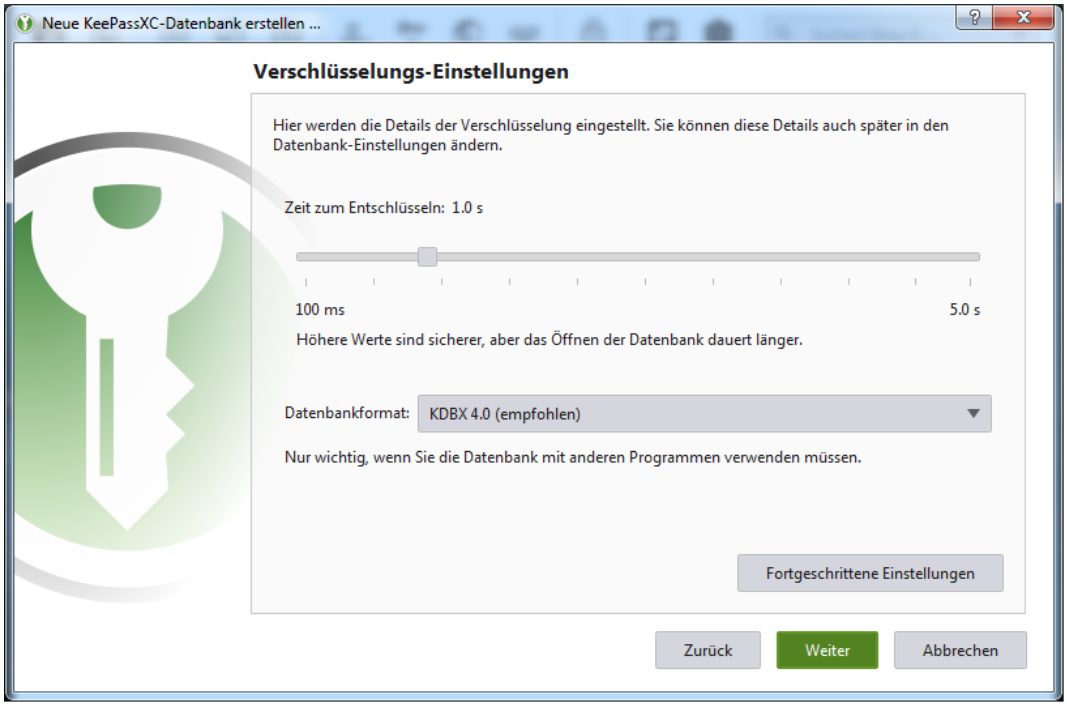
- Im Einstiegsbildschirm der Konfiguration den Punkt „Neue Datenbank erstellen“ auswählen



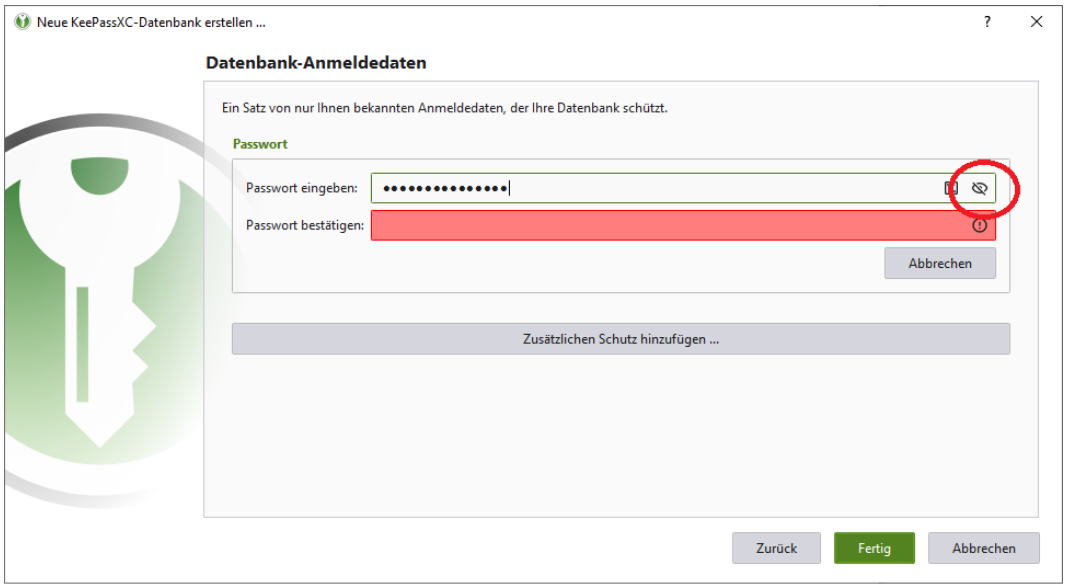
- Als Datenbankname wird „Passwörter“ vorgeschlagen. Da diese standardmäßige Bezeichnung Angreifern bekannt ist und evtl. auf einem infiltrierten PC bewusst nach dieser Zeichenfolge gesucht wird, empfiehlt es sich aus Sicherheitsgründen den Namen durch eine sinnvolle Alternative zu ersetzen. Im Beispiel ist dies „PW-Safe“



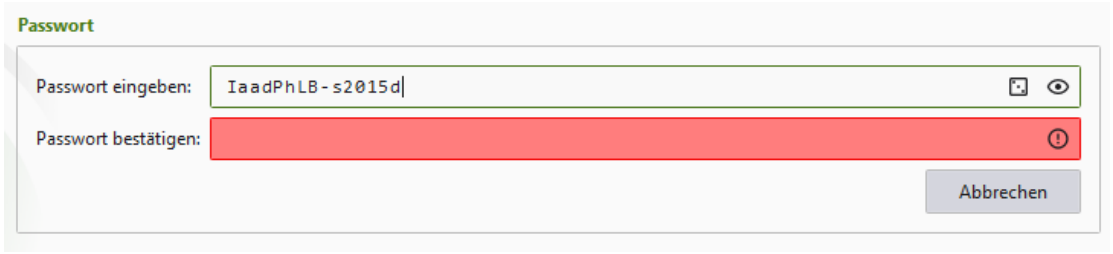
- Die nachfolgenden Verschlüsselungs-Einstellungen können belassen werden.



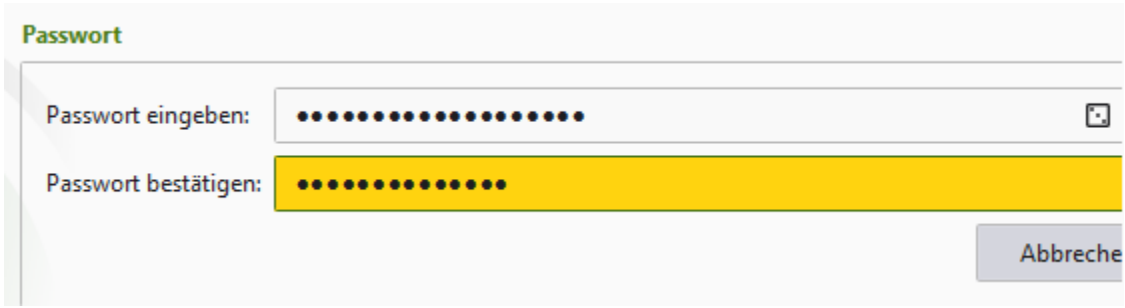
- Jetzt wird das Passwort für den Start von Keepass eingegeben. Dieses muss, wie eingangs beschrieben, besonders lang und besonders komplex sein.



- Da die Passworteingabe zur Kontrolle wiederholt werden muss, was bei einem langen und komplexen Wort, dessen Zeichen nur als Punkte dargestellt werden, zu Fehlern führen kann, kann man mit dem Augensymbol in der rechten oberen Ecke (im Bildschirmfoto rot umkreist) sich die Eingabe im Klartext anzeigen lassen:



- Als weiteren Komfort unterlegt Keepass die zweite Eingabezeile mit gelber Farbe, so lange die Eingabe derer im oberen Eingabefeld entspricht. Die Farbe wechselt auf Rot, wenn die zweite Eingabe von der ersten abweicht:



- Die fertig erstellte Konfiguration wird nun in der Keepass-Datenbank abgespeichert. Obwohl man zu Beginn der Konfiguration die Default-Bezeichnung auf „PW-Safe“ geändert hat, wird hier wieder „Passwörter“ angezeigt:

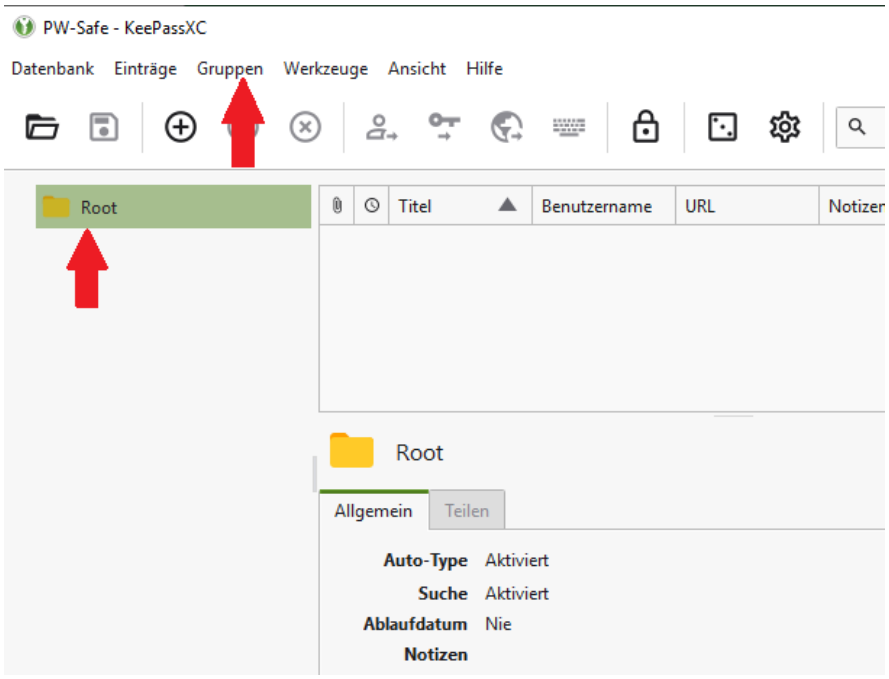
- Man muss den Eintrag also manuell auf die gewünschte und anfänglich festgelegte Bezeichnung ändern:

Gruppen anlegen

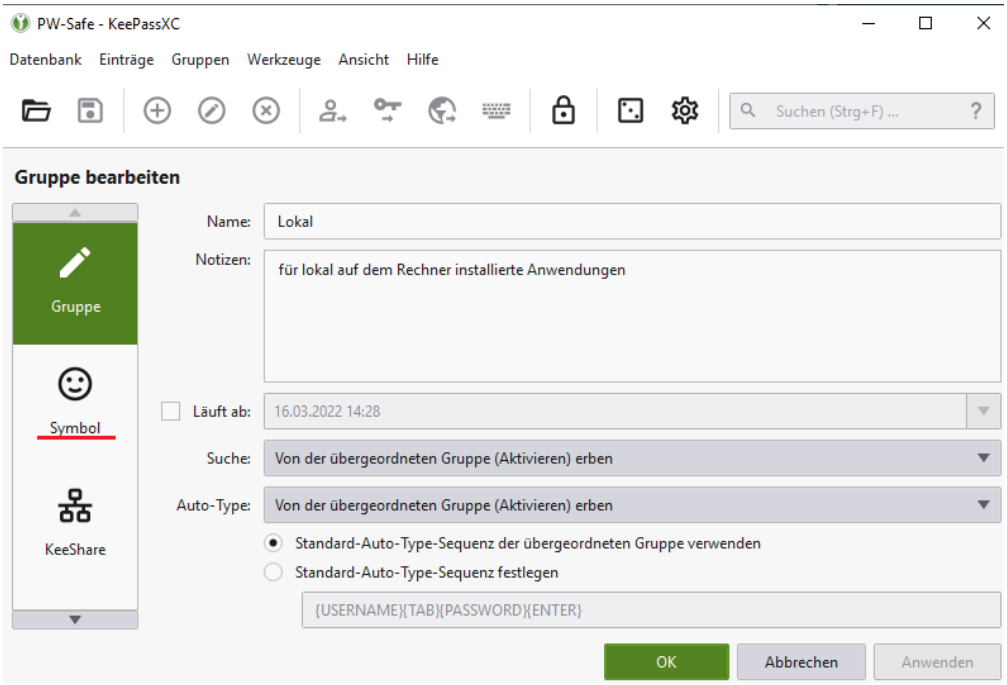
Wenn Keepass erstmals gestartet wird, erhält man einen leeren Ordner.

Es empfiehlt sich, insbesondere wenn viele Programme verwaltet werden müssen, eine Unterteilung vorzunehmen.
Dies macht man mittels „Gruppen“, welche den Ordnern in einem Dateisystem entsprechen.

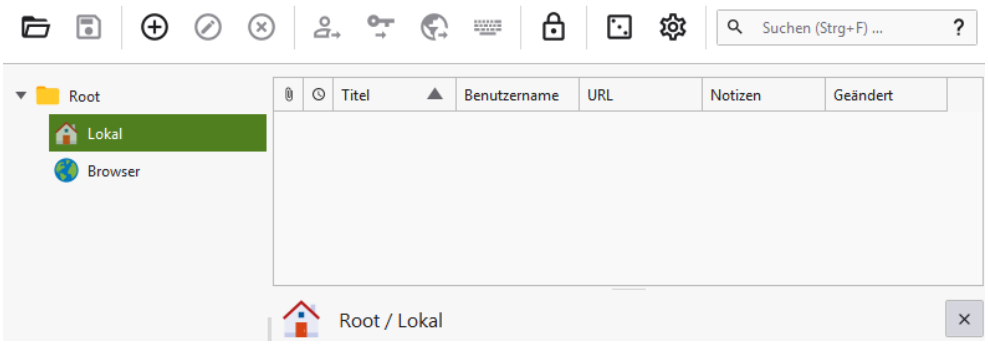
- Eine Gruppe kann man auf zweierlei Weise anlegen: entweder mit rechtem Mausklick auf „Root“ oder im Menü den Punkt „Gruppen“ anwählen.



- Nach Festlegung eines Namens kann man zusätzlich noch Notizen eintragen und ein Symbol auswählen:

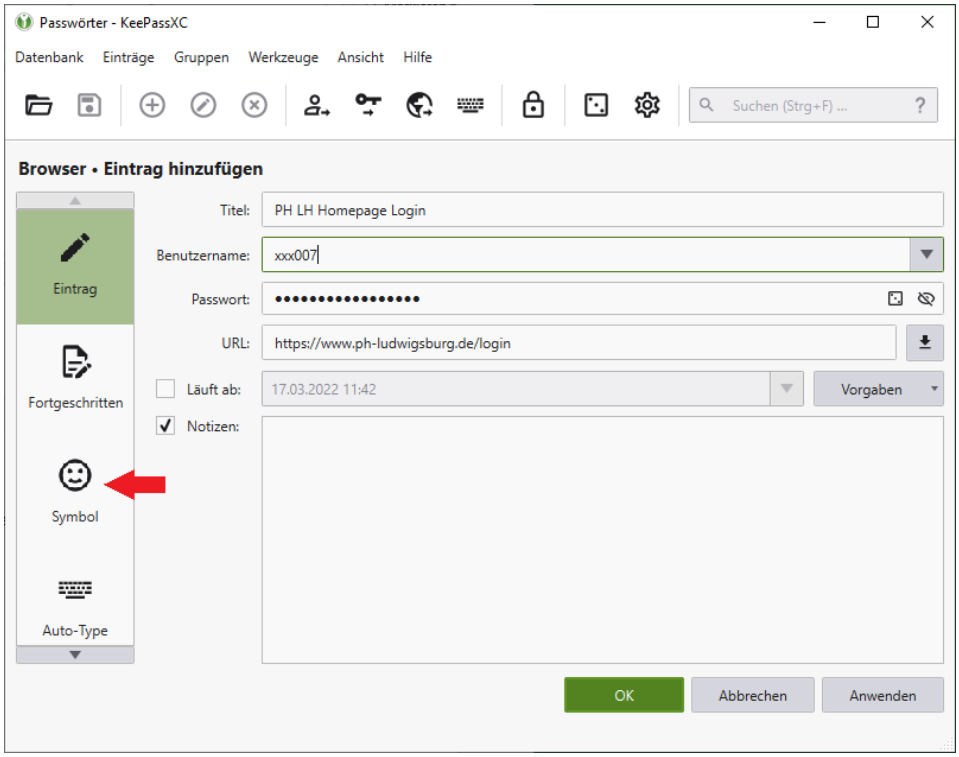


- Das Ergebnis sieht dann wie folgt aus:

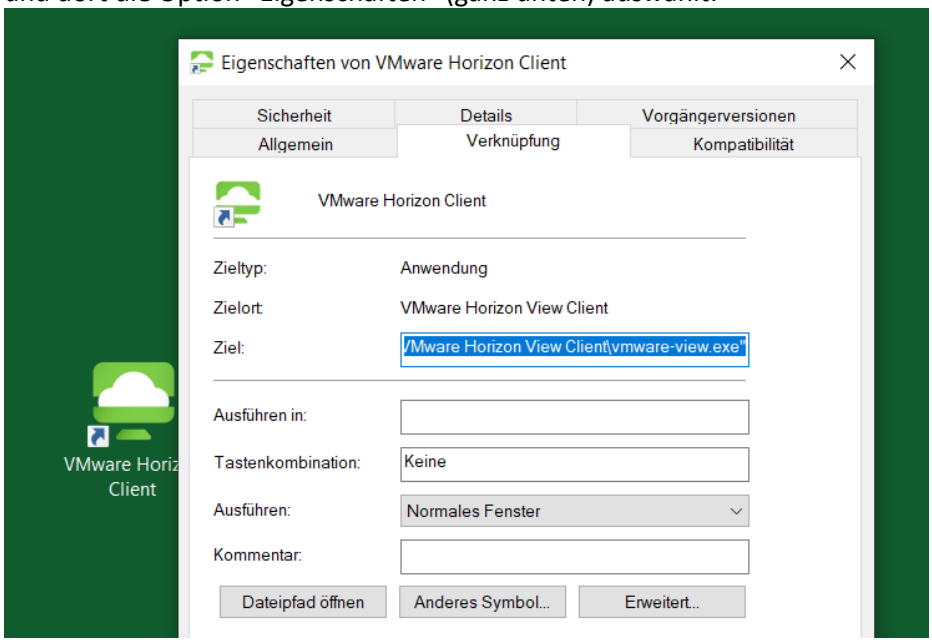


Einen Eintrag hinzufügen

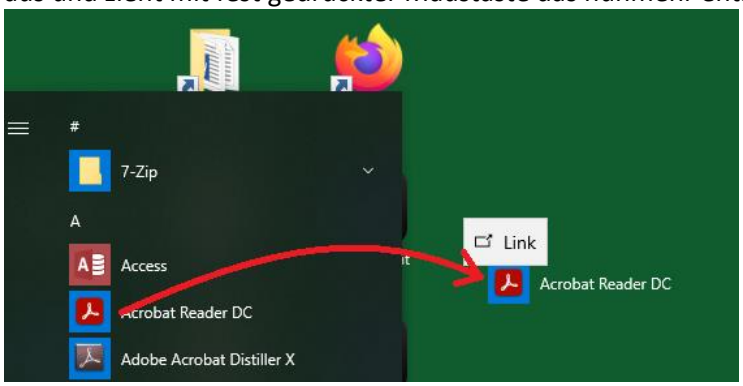
Im Menü auf „Einträge“ gehen und „Neuer Eintrag“ wählen.
Der Titel ist wahlfrei, sollte aber natürlich die auszuwählende Anwendung erkennen lassen.
Unter „Benutzername“ und „Passwort“ sind die entsprechenden Anmeldedaten einzutragen, also beim Benutzernamen entweder die user id oder Domäne\user id oder die Emailadresse.



Unter URL gibt man bei Browseranwendungen naturgemäß die URL an, indem man die Anwendung im Browser startet und die Adresse in der Menüzeile kopiert. Bei lokal installierten Anwendungen gibt man den Dateipfad an. Beispiel für die Anwendung VMWare Horizon:
URL: C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe
Den Dateipfad sieht man, ewnn man mit der rechten Maustaste das Icon auf dem Desktop anklickt und dort die Option “Eigenschaften” (ganz unten) auswählt:



Allerdings geht es nicht immer so einfach, wie gerade eben dargestellt. Um zu den Eigenschaften zu gelangen, muß ein Icon auf dem Desktop liegen, damit man mit der rechten Maustaste die Eigenschaften auswählen kann. Um ein Icon auf den Desktop zu bringen, öffnet man das Windows-Startfnster (das Fenstersymbol auf dem Bildschirm ganz links unten), wählt die gewünschte Anwendung aus und zieht mit fest gedrückter Maustaste das nunmehr entstandene kleine Icon auf den Desktop.



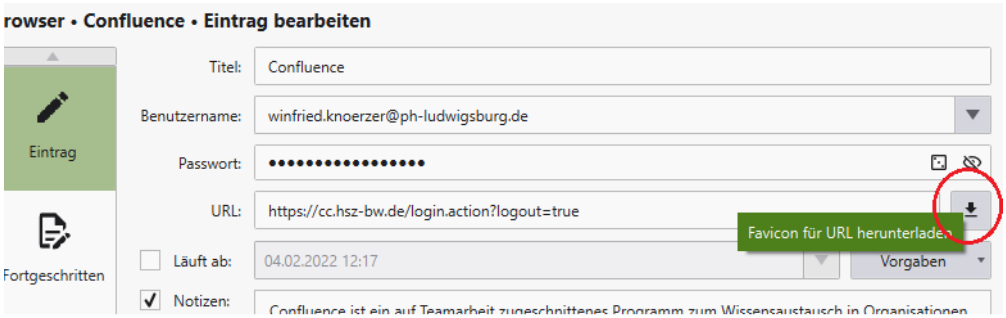
Bei manchen Programmen ist der Dateipfad, sofern er Leerzeichen enthält, von Anführungszeichen umgeben. Diese Anführungszeichen müssen noch entfernt werden.

Hinweis: diese beiden Maßnahmen, das Erzeugen eines Desktop-Icons und eventuell das Entfernen der Anführungszeichen, sind nicht erforderlich, wenn man Keepass nur als Aufbewahrungsort für die Kennwörter verwenden will. Man braucht das nur durchzuführen, wenn man die Anwendungen direkt aus Keepass starten will. Das aber ist, wie gesagt, nur eine Zusatzfunktion. Wenn man nur ds Passwort herauskopieren möchte, um es in die Anmeldemaske einer Anwendung einzufügen, kann die URL-Zeile leer bleiben.

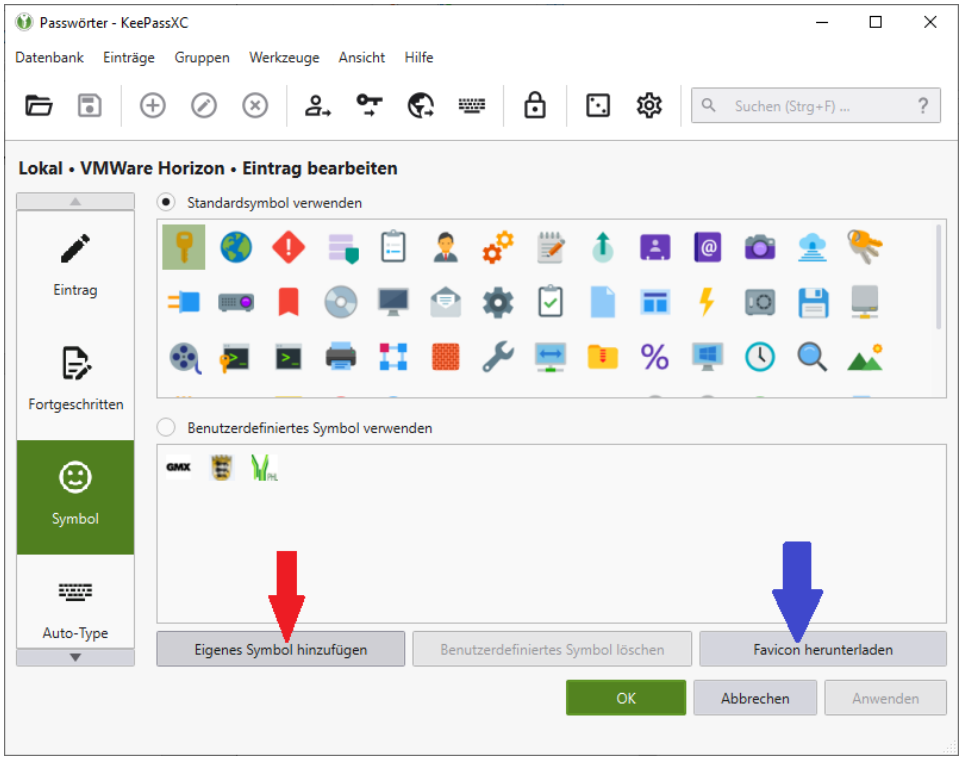
Programmsymbole

Zur besseren Übersicht trägt die Verwendung eines Symbols bei. Um einem Eintrag ein Symbol zuzuweisen, gibt es mehrere Möglichkeiten:

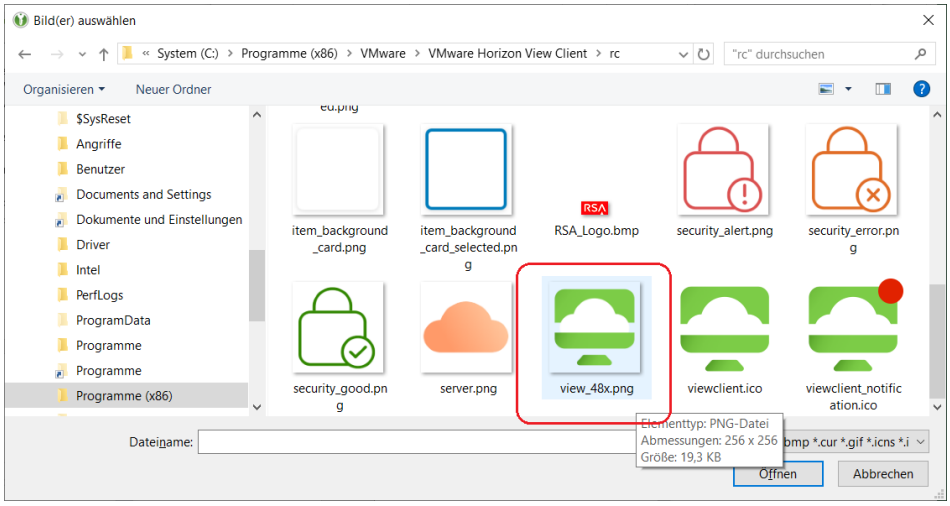
1. Man klickt auf das Pfeil-nach-unten-Symbol rechts von der URL-Eingabezeile, wodurch ein sogenanntes Favicon heruntergeladen und zugewiesen wird. Ein Favicon ist ein Programmicon, ein kleines Symbol, anhand dessen ein Programm identifiziert werden kann. Dieses automatische Herunterladen funktioniert leider nur relativ selten, weil Keepass ein solches Icon meistens nicht finden kann.



2. Falls – was vor allem bei lokal installierten Programmen zutrifft – irgendwo im Programmverzeichnis ein solches Icon vorhanden ist, kann dieses manuell zugeordnet werden. Man geht links auf das Icon „Symbol“ (s.o. roter Pfeil bei „Eintrag hinzufügen“) und gelangt zu folgendem Fenster:

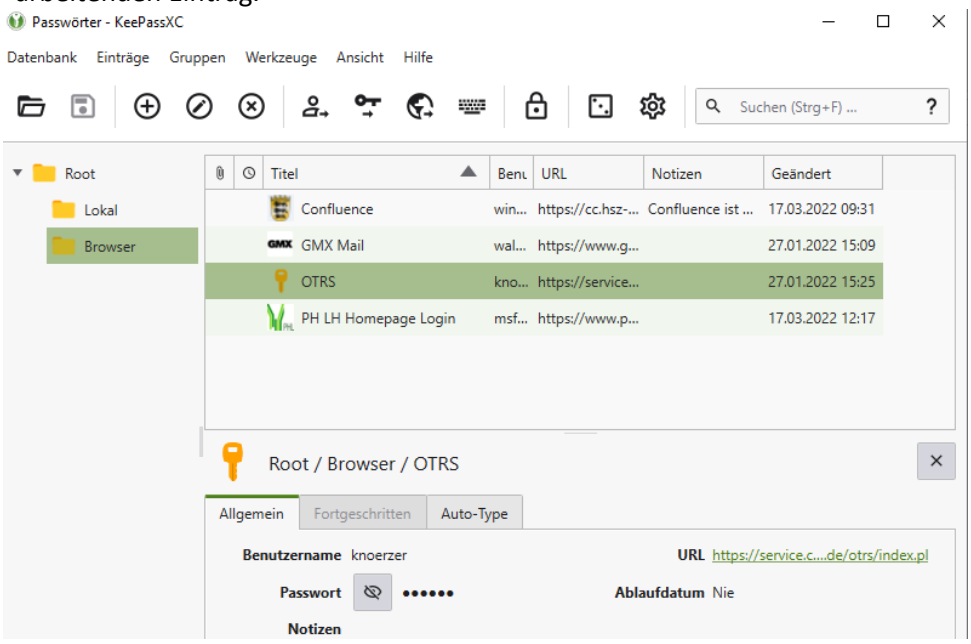


Hier „Eigenes Symbol hinzufügen“. Im Programmverzeichnis sucht man nach einem geeigneten Symbol:



Dieses neue Symbol wird im unteren Auswahlfeld plaziert. Dort kann man es auswählen und die Auswahl mit OK bestätigen.

3. Man kann auch nachträglich ein Favicon herunterladen. Dazu wählt man im Menü unter „Einträge“ die Option „Eintrag bearbeiten“ aus oder doppelklickt im Hauptbildschirm auf den zu bearbeitenden Eintrag.



Anschließend wieder das Icon „Symbol“ anklicken und dort den Schalter „Favicon herunterladen“ betätigen.

Das Passwort festlegen

Man kann, was sich insbesondere bei bereits seit längerem gebrauchten Programmen anbietet, ein bestehendes Passwort in die entsprechende Eingabezeile (vgl. Bild: Eintrag hinzufügen auf S. 11) eintragen.

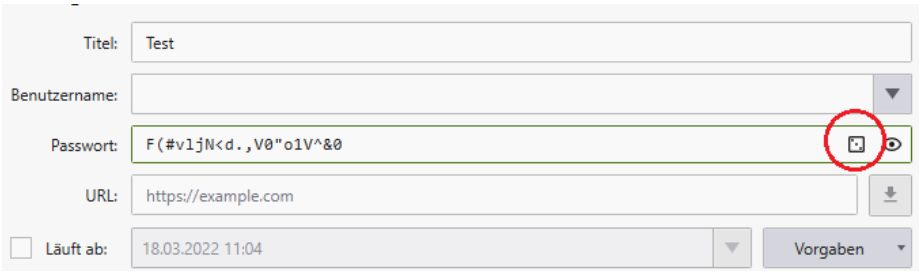
In diesem Fall wird man Keepass nur als Reserve einsetzen, weil man – wie bisher – darauf vertraut, sich das Passwort merken zu können und auf Keepass nur zuzugreifen beabsichtigt, wenn man doch einmal das Kennwort vergessen haben sollte.

Das hat den Vorteil, eine Anwendung auch dort (auf einem fremden Rechner) starten zu können, wo die eigene Keepass-Datenbank nicht zur Verfügung steht.

Aber das ist nicht der eigentliche Zweck eines Passwort-Managers. Dieser besteht darin, so komplexe, lange und unterschiedliche Passwörter zu verwenden, dass man diese sich nicht mehr merken kann und deshalb eines Passwort-Managers bedarf.

Diese Zielsetzung unterstützt Keepass mit der Funktion der automatisierten, zufallsgesteuerten Passwortgenerierung.

Wenn man in der Passwort-Eingabezeile auf das rot umkreiste quadratische Symbol klickt, startet ein kleiner Passwortgenerator.



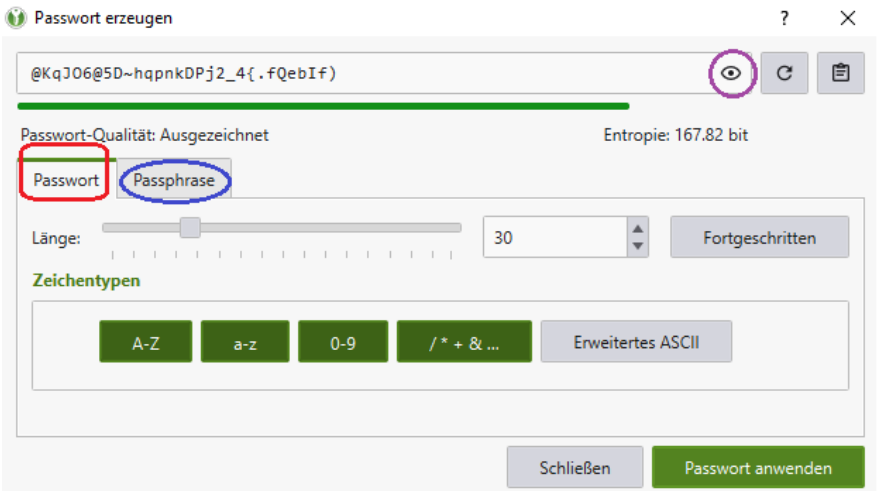
Hier stehen zwei verschiedene Verfahren zur Auswahl: Passwort und Passphrase.

Eine *Passphrase* ist ein kompletter Satz, den man entweder selber eingeben oder von Keepass erzeugen lassen kann.
Der Vorteil besteht darin, dass dadurch ein sehr langes Passwortobjekt entsteht; ein gewisser Nachteil ist, dass nur Klein- oder nur Großbuchstaben verwendet werden können – also nur ein von zwei Buchstabentypen, keine Ziffern und keine Sonderzeichen.

Was man hinsichtlich der Länge gewinnt, verliert man an Komplexität.

Da die Passwort-Richtlinien der PH aber die Verwendung von mindestens 3 dieser 4 Zeichenkategorien vorschreiben, kommt für den Dienstgebrauch die Funktion „Passwortphrase“ eh nicht in Betracht.

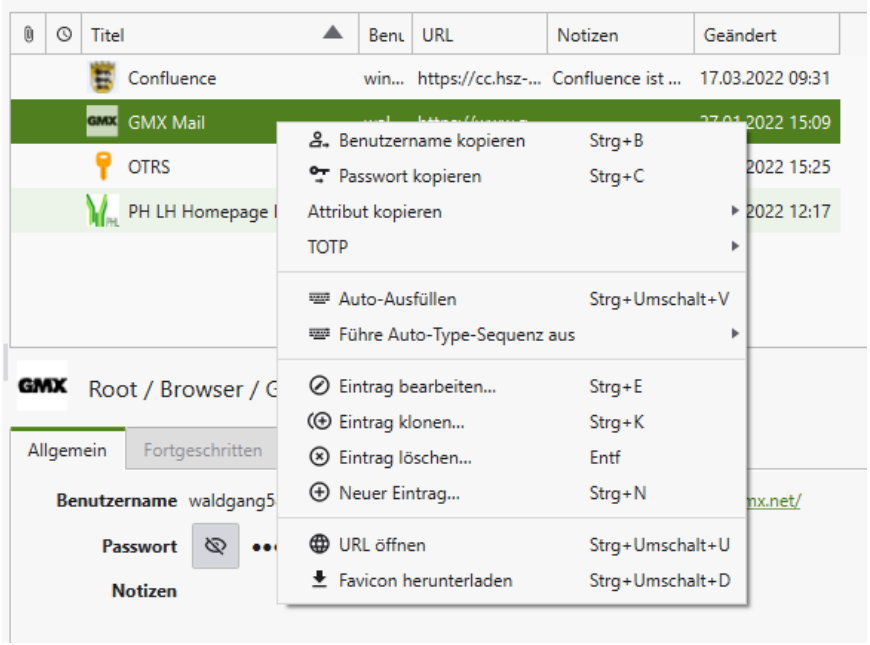
Wie man auf dem Bildschirmfoto für *Passwort* sehen kann, ist im Beispiel eine Passwortlänge von 30 Zeichen eingestellt.
Das Ergebnis sieht man oben, wenn man das Augensymbol (violett umrandet) aktiviert hat. Ergebnis wird mit dem Schalter „Passwort anwenden“ bestätigt.



Eine Anwendung starten

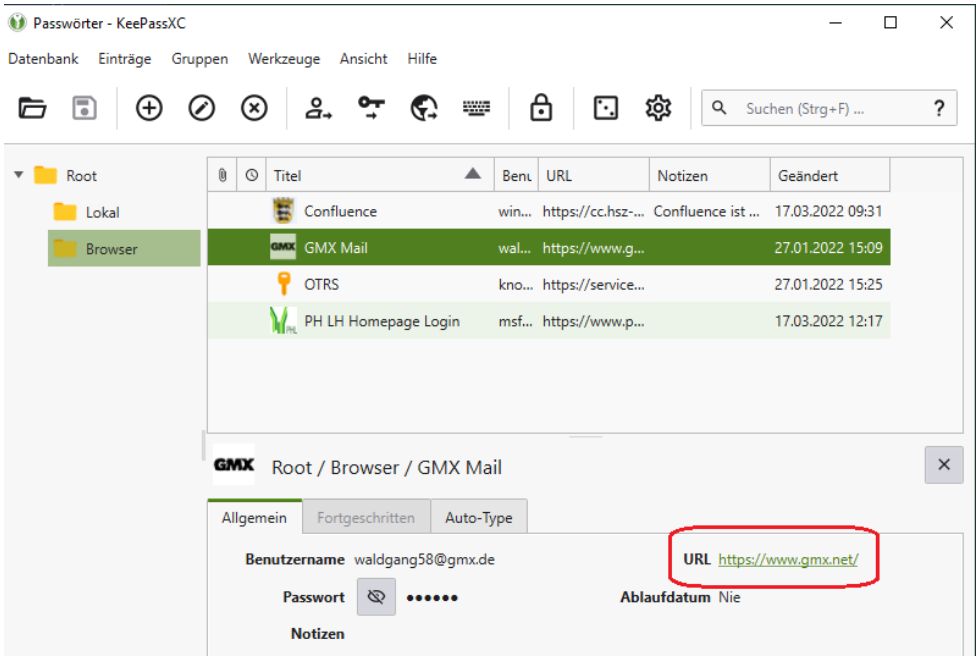
Man kann eine Anwendung ganz normal über das Startmenü, über ein Desktop-Icon oder im Browser über ein Lesezeichen starten und danach Keepass wechseln und mit Rechtsklick auf die Anwendung die Funktionen „Benutzernamen kopieren“ und „Passwort kopieren“ anwenden.

Das Passwort (bzw. der Benutzername) wird in die Zwischenablage übertragen, wo es 10 Sekunden lang aufbewahrt wird. In diesem Zeitrahmen kann es in die Anmeldemaske eingefügt werden.



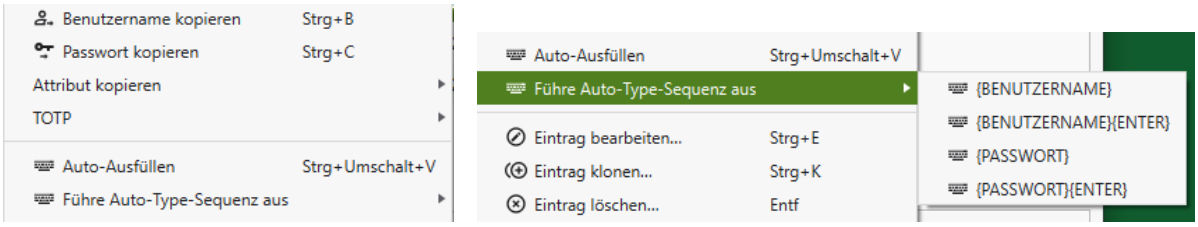
Man kann Keepass aber auch als Startplattform für die wichtigsten Anwendungen nutzen.

Man betätigt den Link rechts unten bei URL, wodurch die Anwendung aufgerufen wird. Das weitere Vorgehen bzgl. Benutzername und Passwort ist identisch mit dem oben beschriebenen manuellen Verfahren.



Sicherheitshinweise

Kein Autoausfüllen, kein Autotype verwenden!

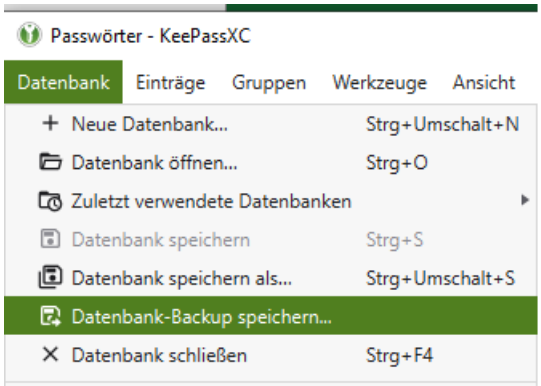


Mit dieser Funktion werden automatisch die Werte dort eingetragen, wo der Cursor steht – entweder Benutzername und zugleich Passwort oder einzeln, wie man auf dem kleinen Bild rechts sieht.

In der Theorie hört sich das komfortabel an, die Praxis aber hat Tücken.

Man weiß nie mit absoluter Sicherheit, wo sich der Cursor gerade befindet. Steht er in Word, so werden dort die Anmeldedaten im Klartext [sichtbar!] wiedergegeben, was natürlich äußerst unerwünscht ist, wenn sich eine andere Person in der Nähe befindet.
Aus diesem Grund raten die meisten Einführungen/Ratgeber zu Keepass von dieser Funktion ab.

Datenbank Backup:
Wie eingangs erwähnt, sollte die Datenbank mit den Gruppen und Einträgen der Anwendungen in mindestens doppelter, besser dreifacher Form vorliegen: einmal lokal, dann auf zwei verschiedenen Verzeichnissen im Homedir.



Es muss auch daran gedacht werden, Veränderungen auf der Basis-Datenbank (also derjenigen, die man standardmäßig verwendet) in den Backup-Versionen nachzuziehen oder die Datenbankdatei regelmäßig zu kopieren.

Zum Abschluss sei noch einmal daran erinnert, das Kennwort für den Aufruf von Keepass unbedingt verfügbar zu haben. Auch wenn man es täglich gebraucht wird, kann es leicht passieren, dass es wegen seiner Länge und Komplexität nach einem Urlaub vergessen wird. Darum ist es am besten, es an einer sicheren Stelle (digital in einer Datei mit einem unverfänglichen Namen oder analog auf einem Papier, das beispielsweise in ein Buch eingelegt wird) zu verwahren.

Dr. Winfried Knörzer
Informationssicherheitsbeauftragter

MIT - Zentrum für Medien und Informationstechnologie
Pädagogische Hochschule Ludwigsburg
Reuteallee 46, 71634 Ludwigsburg
Telefon: (07141) 140 – 1449; Raum 1A.110
E-mail: winfried.knoerzer@ph-ludwigsburg.de