KeePass

KeePassXC ist ein Programm zur Verwaltung von persönlichen Passwörtern, ein sogenannter **Password-Manager**. Mit einem solchen Programm können Sie beliebig viele Passwörter, inkl. Anmerkungen dazu, sicher speichern. Dadurch wird es praktikabel, für alle Zugänge unterschiedliche, lange und sichere Passwörter zu verwenden, da Sie sich die Passwörter **nicht merken** müssen – nur das eine für die Passwort-Datenbank.

Die Passwörter werden in einer mit sehr **starker Verschlüsselung** gesicherten Datenbank-Datei, auch als **“Container”** bezeichnet, abgelegt. Diese Datenbank-Datei können Sie wie eine normale Datei an mehreren Orten speichern, um einem möglichen Verlust vorzubeugen. Sie müssen dann allerdings auch manuell dafür sorgen, dass alle Kopien der Datei aktuell gehalten werden. Die Ablage im Cloudstorage der TU Braunschweig ist sinnvoll, da dort ein automatisches Backup erfolgt und Sie jederzeit auf die Passwortdatei zugreifen können, auch von außerhalb Ihres Büros.

Das Programm bietet viele Komfort-Funktionen zum Umgang mit Passwörtern. Am wichtigsten in der täglichen Arbeit ist die sogenannte Auto-Type bzw. **AutoFill-Funktion**. Damit können Sie durch eine selbst definierte Tastenkombination (Standard ist Strg-Alt-A (Windows)) automatisch die richtigen Zugangsdaten für einen Zugang ausfüllen lassen.

Darüber hinaus ist ein **Passwort-Generator** zur Erzeugung sicherer Passwörter eingebaut sowie ein Test, wie sicher ein spezielles Passwort ist. Und natürlich können Sie die Datenbank auch durchsuchen.

Außerdem ist es möglich, mehrere Datenbank-Dateien gleichzeitig geöffnet zu haben, beispielsweise für Team-Passwörter (siehe weiter unten in dieser Anleitung).

KeePassXC ist **kostenfreie OpenSource-Software** und ist für Windows, macOS und Linux verfügbar. Für Android und iOS gibt es jeweils Apps (siehe separate Anleitungen), die dieselbe Datenbank-Datei verwenden können.

> **Achtung:** Die Sicherheit der Passwortdatei hängt wesentlich davon ab, wie sicher Ihr selbst gewähltes Passwort für die Datenbank-Datei selbst ist. Denn wenn jemand die Datenbank unbefugt zugreifen will, so hat der Angreifende beliebig viele Versuche, das Passwort zu knacken. Verwenden Sie also bitte für die Datenbank-Datei selbst ein besonders langes und sicheres Passwort (mindestens 20 Zeichen, gerne auch noch länger) und schreiben Sie sich dieses Passwort zur Sicherheit auch auf und verwahren Sie diese Papier-Kopie an einem sicheren Ort. Auch der (zusätzliche) Einsatz einer Schlüsseldatei ist möglich.

>

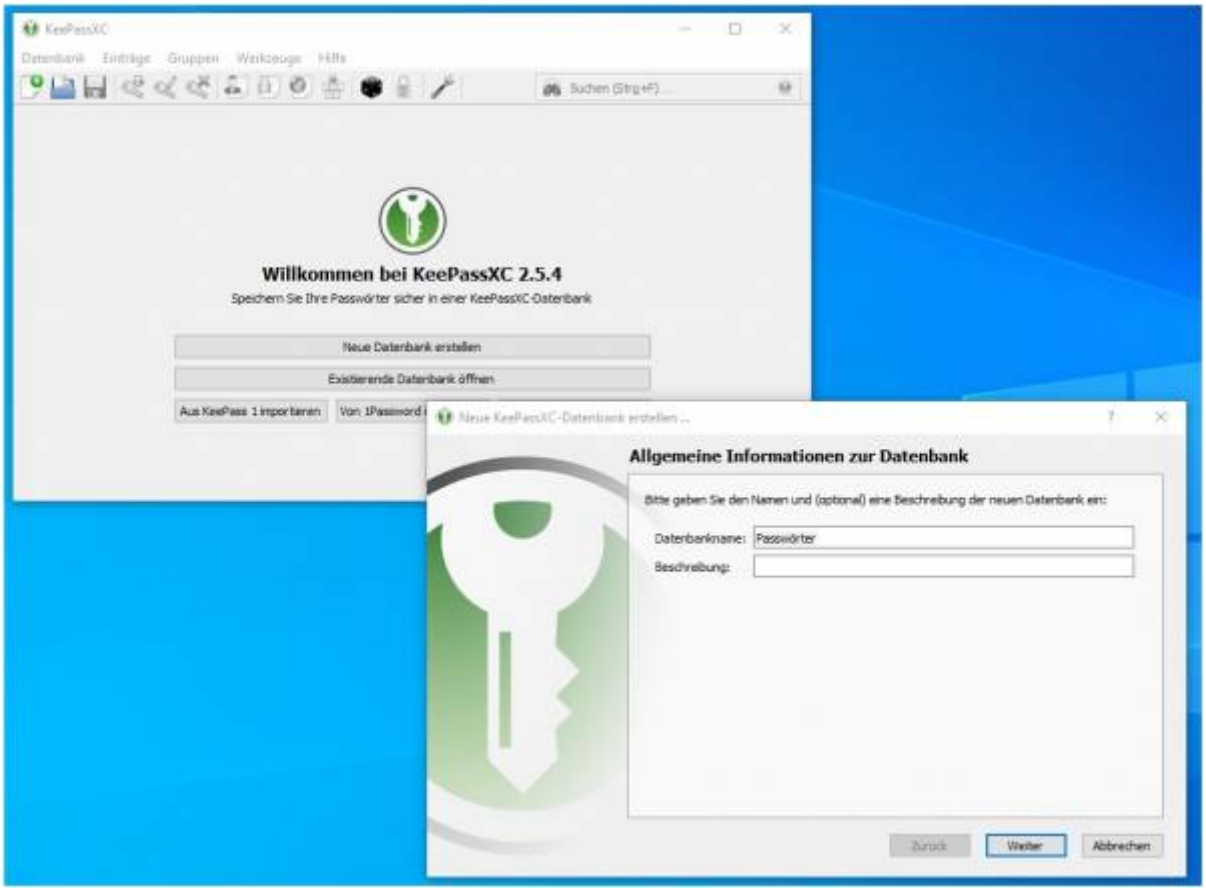
> Bitte beachten Sie ebenfalls, dass es bei Verlust des Passworts zur Datenbank oder der eventuell eingesetzten Schlüsseldatei nicht mehr möglich ist, auf die Passwort-Datenbank zuzugreifen. Auch der IT-Service-Desk kann Ihnen in dem Fall nicht weiterhelfen!

Falls Sie bereits KeePass (ohne XC) einsetzen sollten, so können Sie die Datenbank unverändert auch mit KeePassXC weiterverwenden.

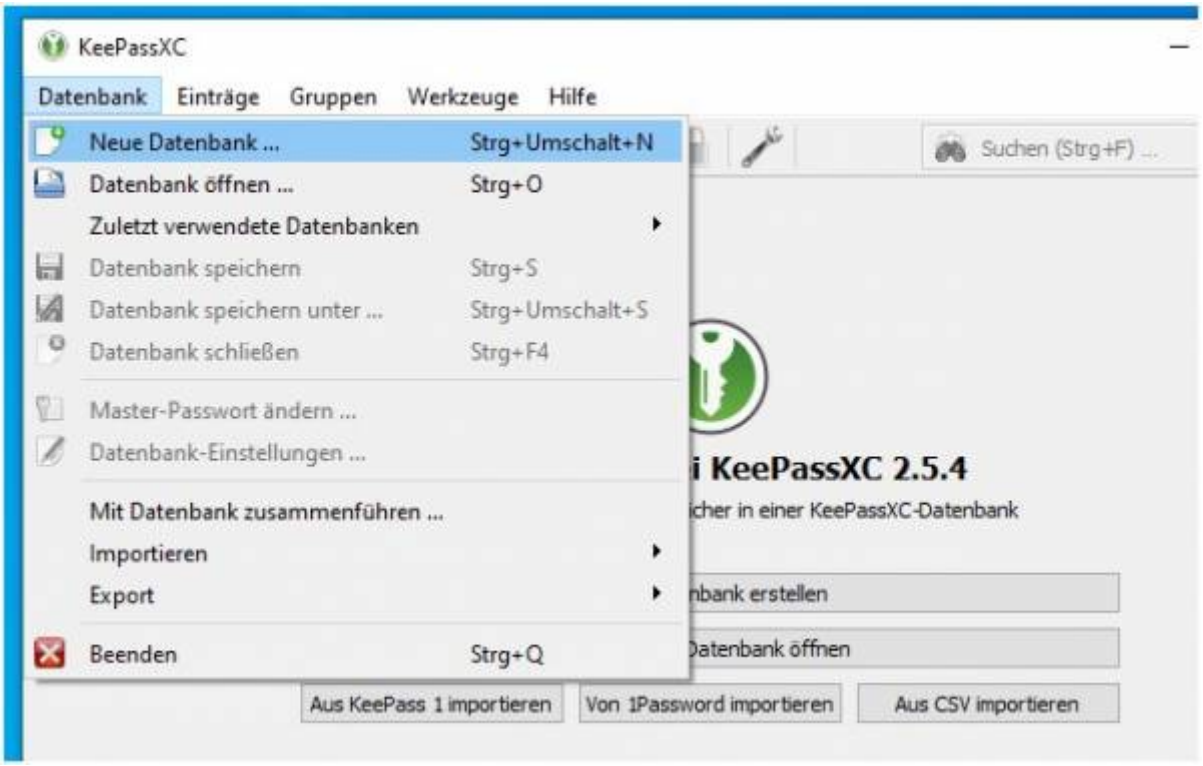
Anlegen einer KeePass Datenbank

Mit Passwortschutz (Masterpasswort)

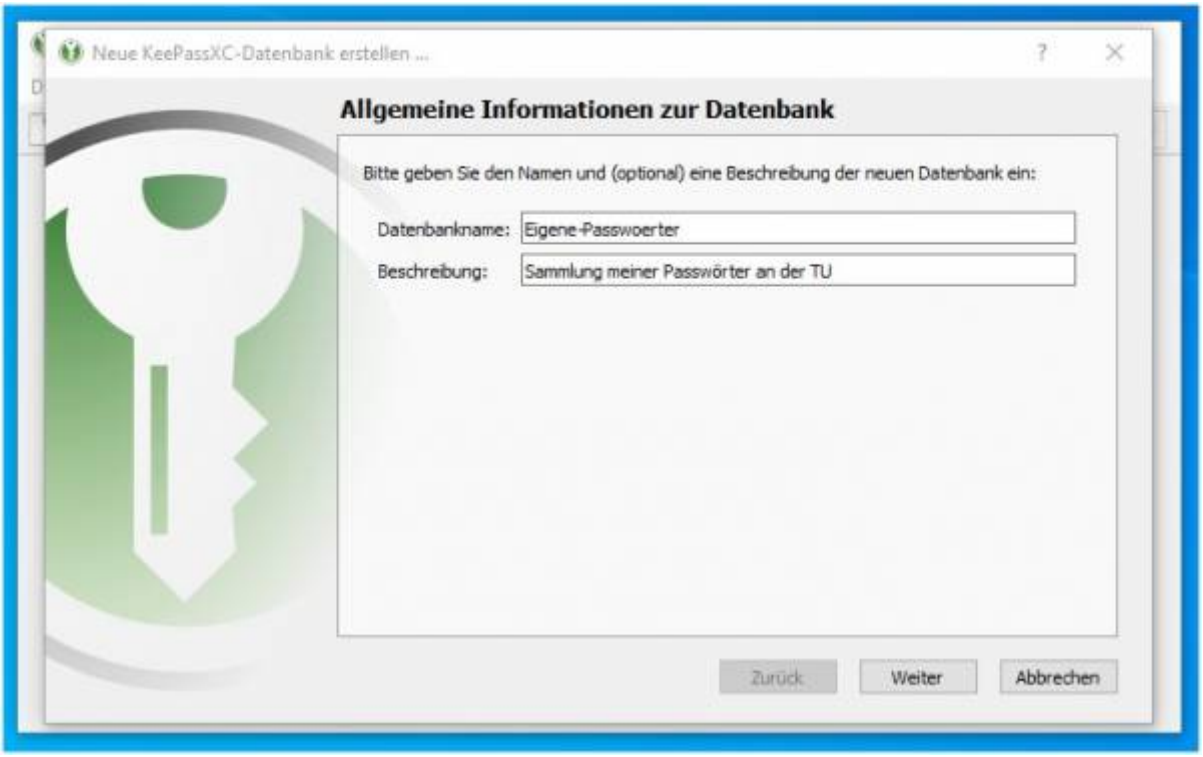
1. Öffnen Sie KeePassXC



2. Klicken Sie auf **[Datenbank]** erstellen. Ist bereits eine Datenbank geöffnet, wird der Button also nicht gezeigt, klicken Sie auf Datenbank in der Menüleiste und dann auf **[Neue Datenbank …]**.



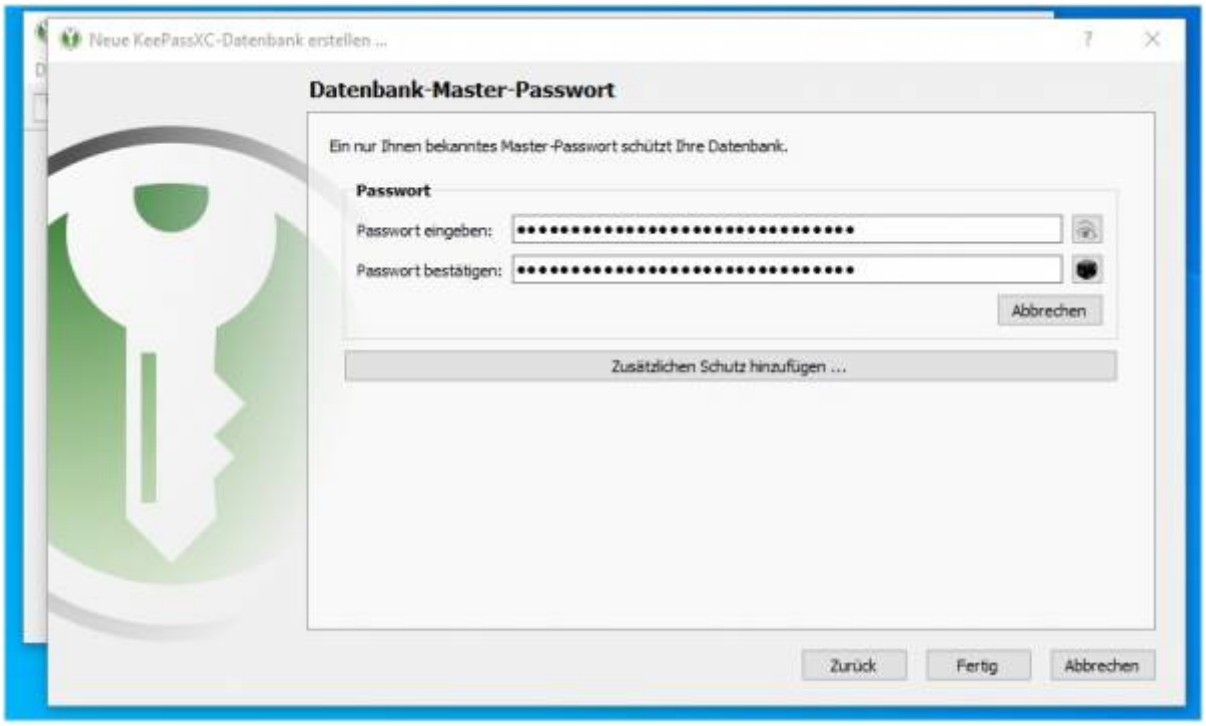
3. Vergeben Sie der Datenbank einen eindeutigen Namen und fügen Sie eine Beschreibung hinzu.



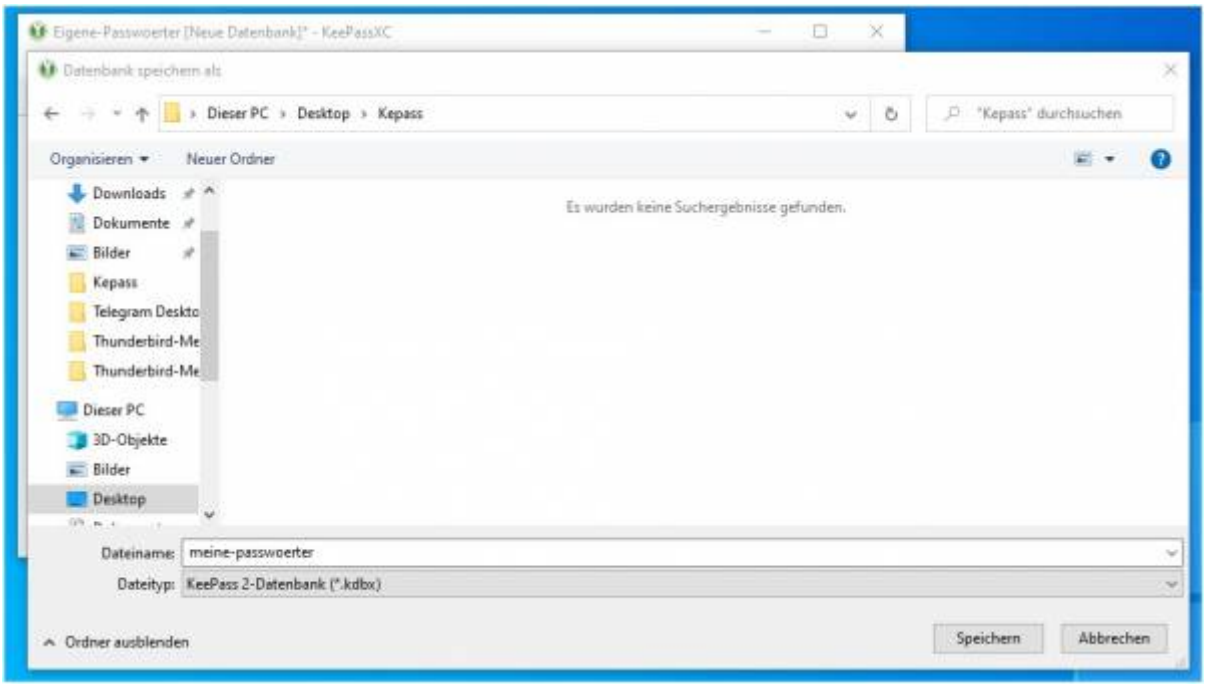
4. Belassen Sie die Verschlüsselungseinstellungen auf den Standardeinstellungen. Klicken Sie auf **[Weiter]**.

5. Vergeben Sie der Datenbank ein sicheres Kennwort. Sicherheitshalber notieren Sie dieses und hinterlegen Sie es an einem sicheren Ort. Passwortlängen mit mehr als 20 Zeichen sind üblich.

> **Bedenken Sie:** Das Entschlüsseln Ihrer Passwortdatenbank gibt einem Angreifer Zugang zu all Ihren Konten!

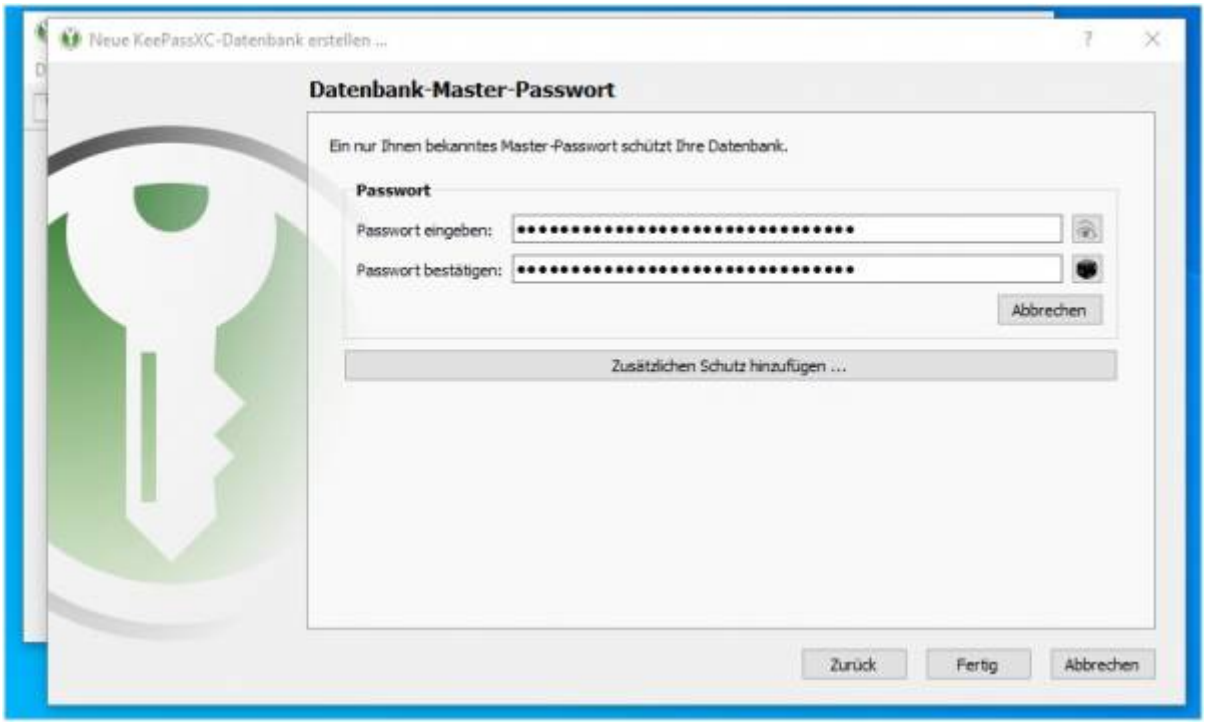


6. Speichern Sie die Datenbank-Datei an einem sicheren Ort auf Ihrem Gerät, auf dem Netzlaufwerk (T:) oder in einem Synchronisationsordner für Cloudstorage. Vergeben Sie auch hier einen eindeutigen Dateinamen.



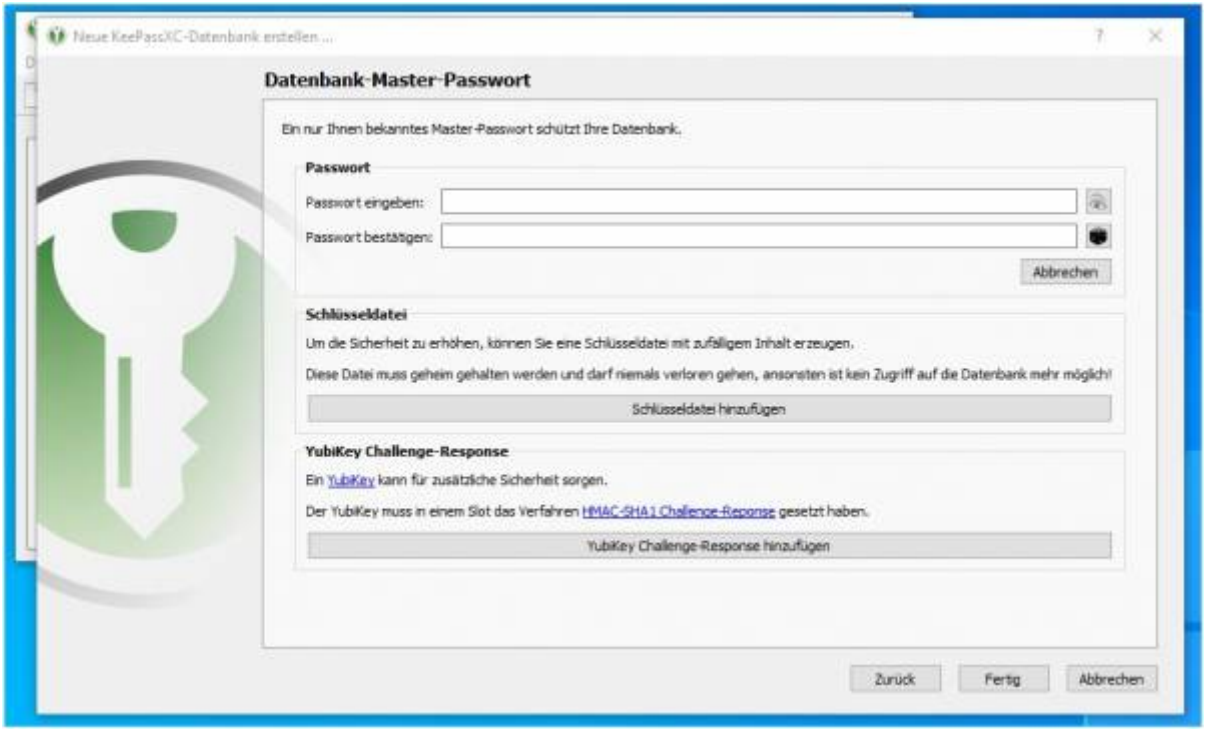
Mit Schlüsseldatei

1. Der Vorgang ist in den meisten Punkten identisch mit dem Vorgang zur Erstellung mit einem Masterpasswort. Befolgen Sie bitte die Punkte 1-4 der Anleitung Mit Passwortschutz (Masterpasswort) bei der Erstellung und folgen danach dieser Anleitung.

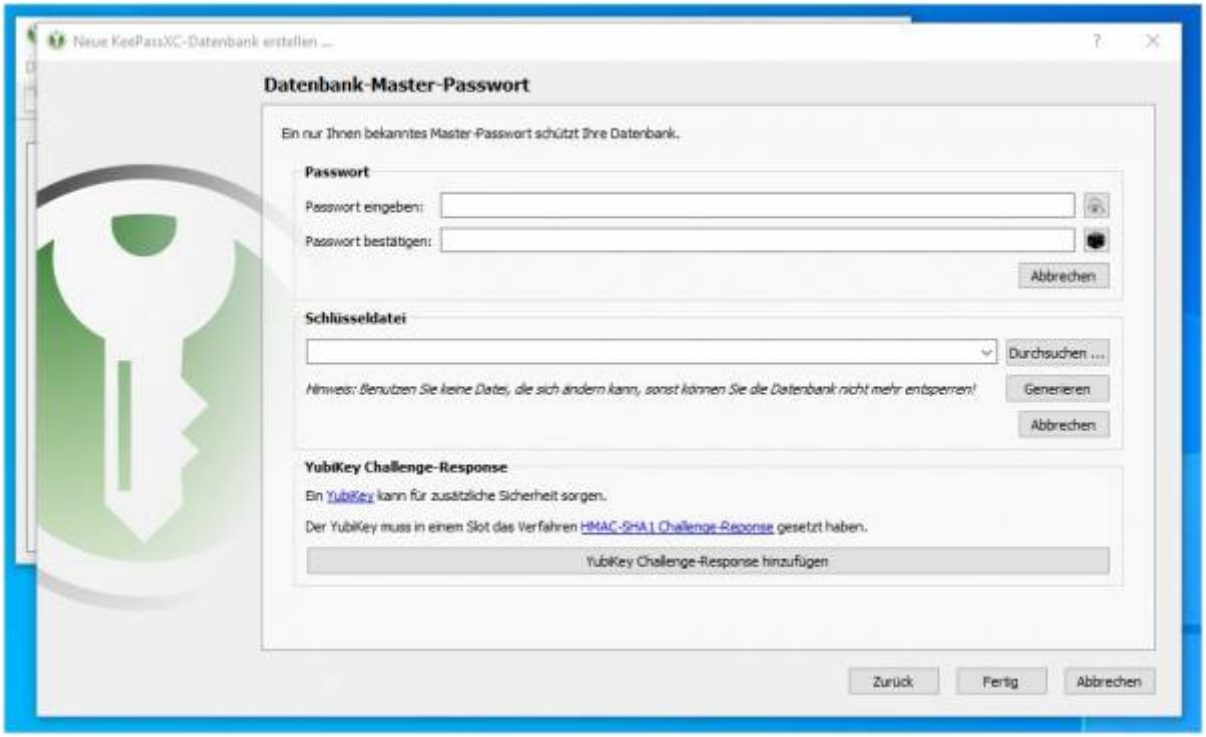


2. Wählen Sie **[Zusätzlichen Schutz hinzufügen …]**.

3. Klicken Sie auf **[Schlüsseldatei hinzufügen]**.

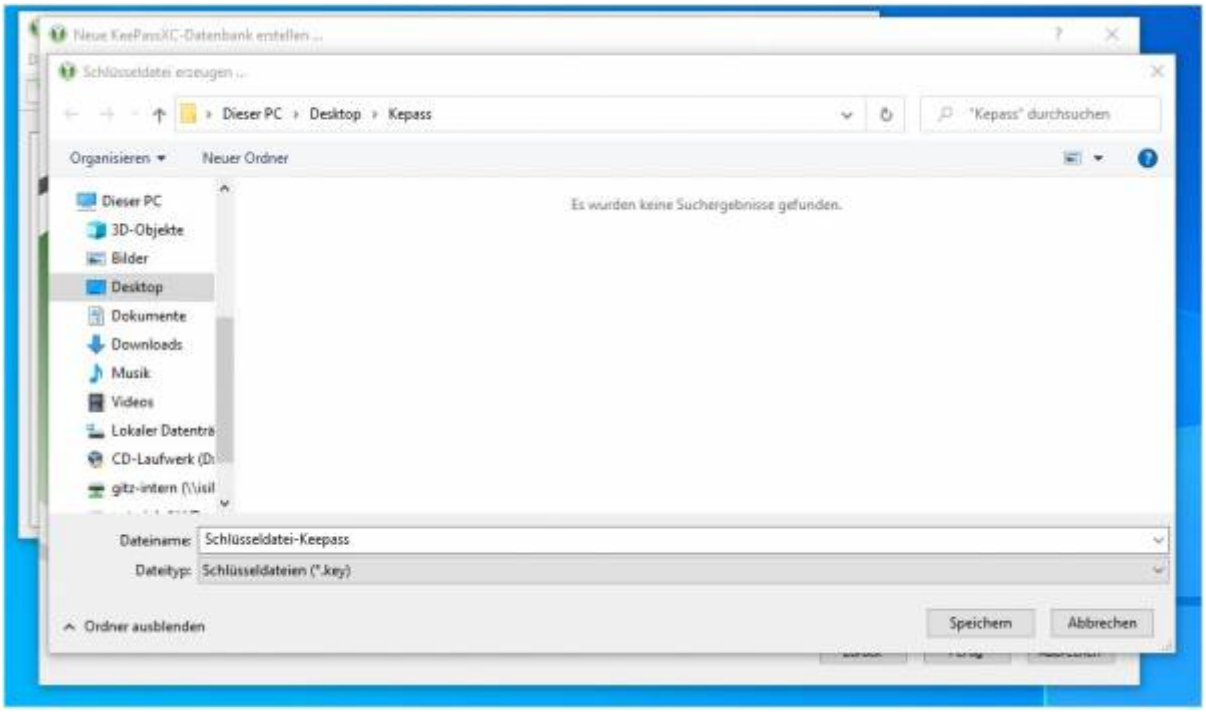


4. Sie können eine vorhandene Schlüsseldatei auswählen. Mit Klick auf **[Generieren]**, erstellen Sie eine neue Schlüsseldatei.



5. Speichern Sie die Schlüsseldateien an einem dedizierten Ort auf Ihrer Festplatte.

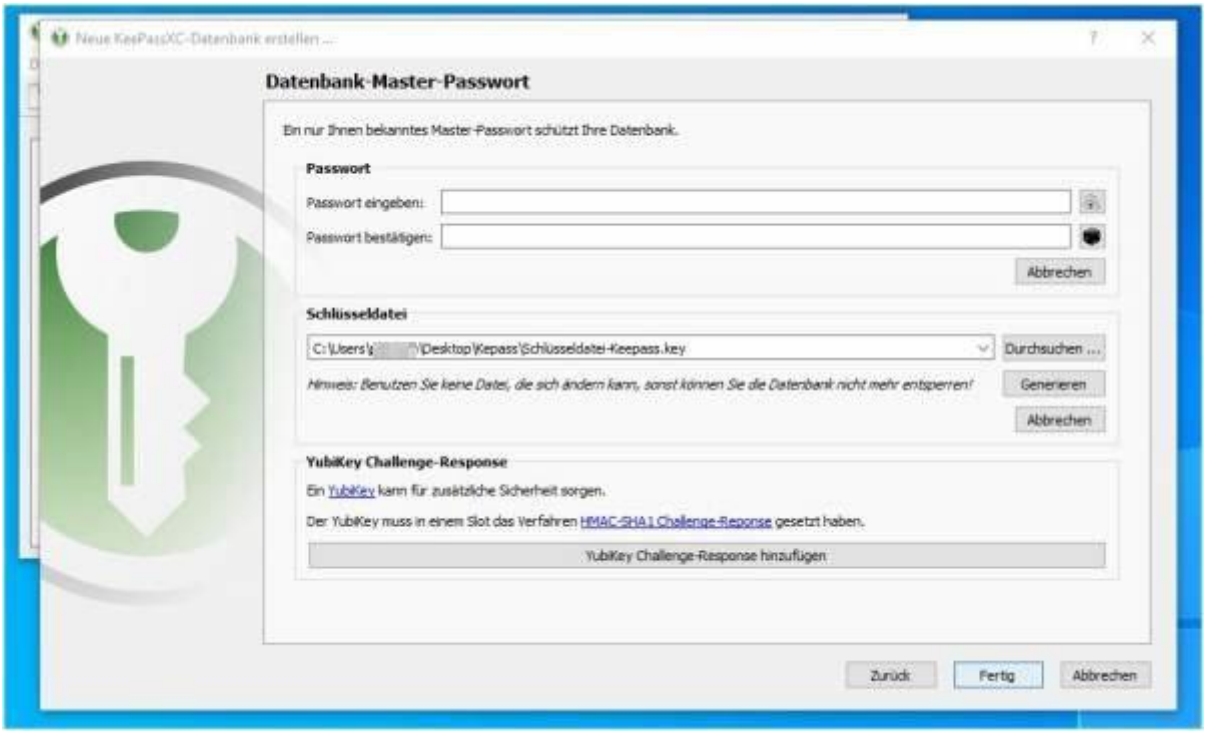
> Idealerweise vergeben Sie **NICHT** den **gleichen Namen** wie der Passwortdatenbank und speichern die Schlüsseldatei **NICHT** am **selben Ort** wie die Passwortdatenbank.



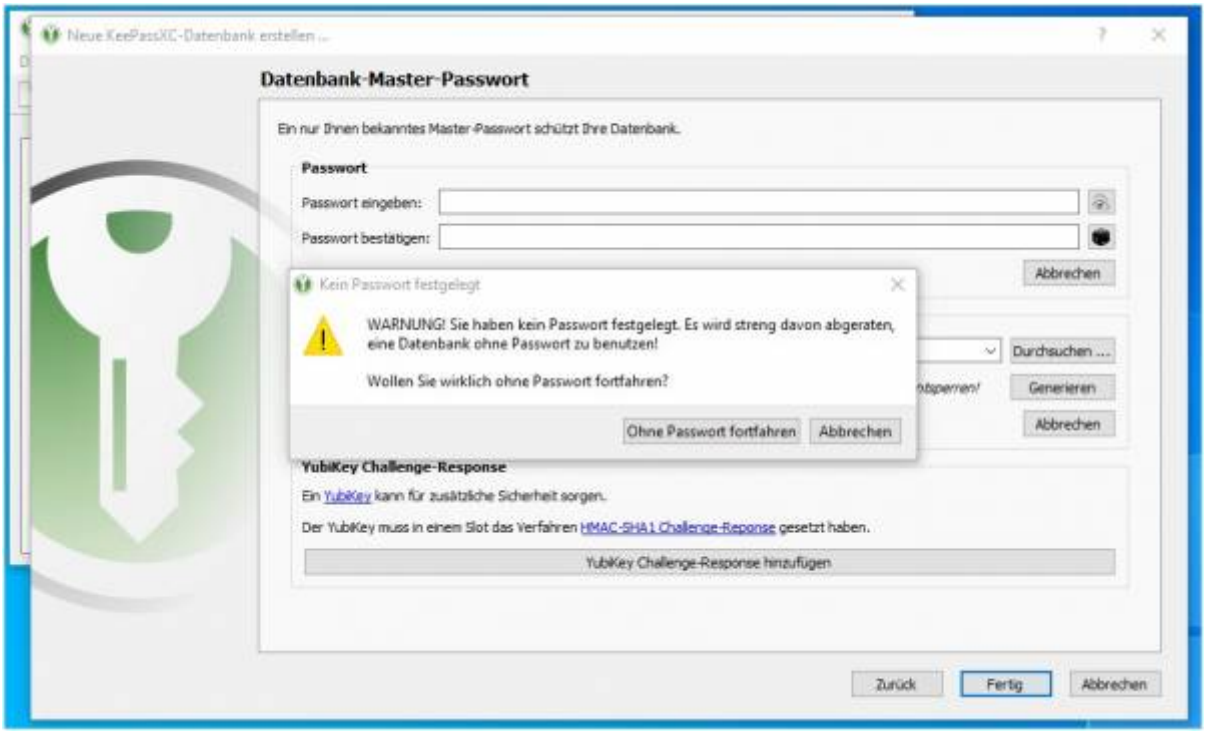
- Sichern Sie die Schlüsseldatei **zusätzlich an einem zweiten** Ort.

> **Achtung:** Der Verlust, die Veränderung oder eine Zerstörung dieser Schlüsseldatei macht die Passwortdatei unwiederbringlich unzugänglich! Auch der IT-Service-Desk kann in einem solchen Fall nicht helfen.

6. Klicken Sie auf **[Fertig]**.



7. Bestätigen Sie den Vorgang mit Klick auf **[Ohne Passwort fortfahren]**. Die Passwortdatenbank wird dadurch lediglich mit Zugriff auf die Schlüsseldatei gesichert.



Mit Masterpasswort und mit Schlüsseldatei

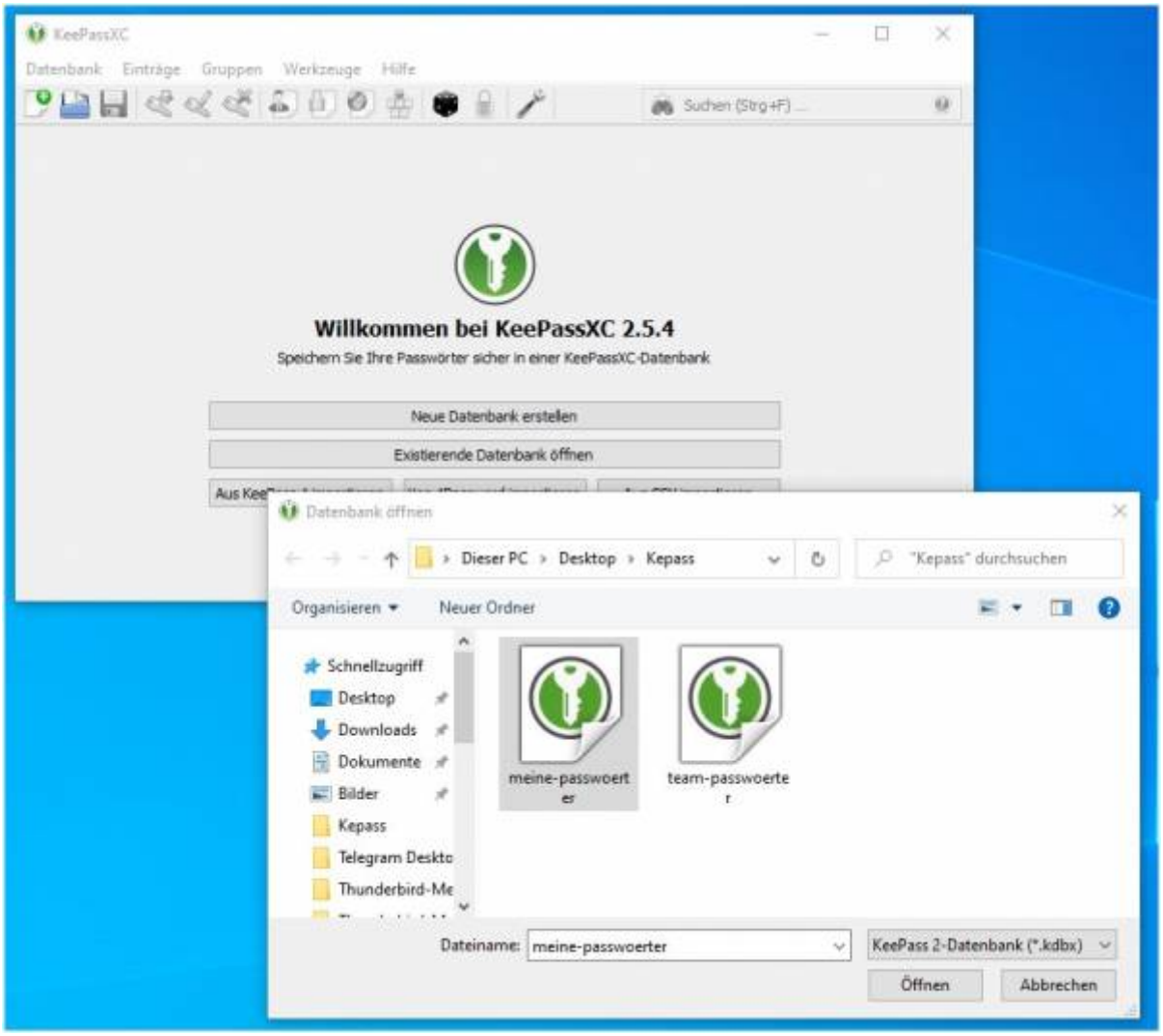
Die Passwortdatenbank kann sehr wohl auch mit einem kombinierten Schutz gesichert werden. In diesem Fall folgen Sie der Anleitung Mit Schlüsseldatei, vergeben aber im Schritt **2.2.6.** zusätzlich ein Passwort.

> Ein doppelter Schutz ist gerade bei hochsensiblen Passwortdatenbanken eine Möglichkeit den unbefugten Zugang zu diesen unwahrscheinlicher zu gestalten.

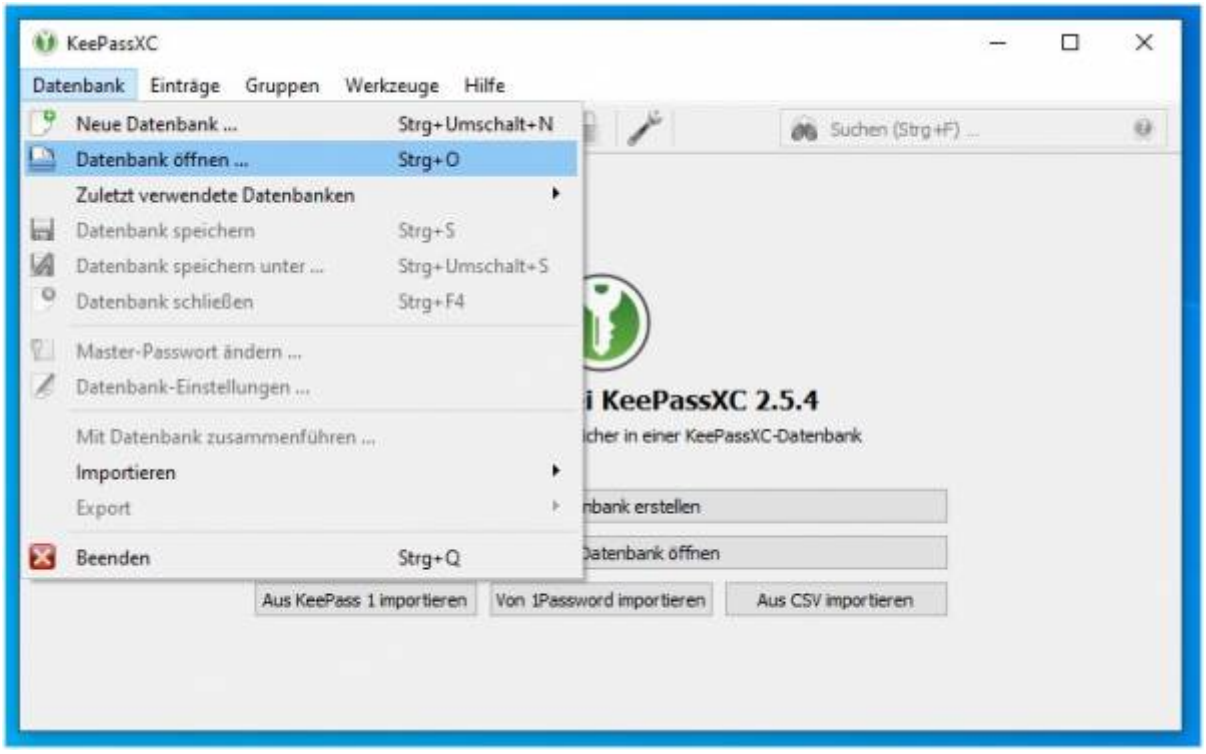
Öffnen einer vorhandenen KeePass-Datenbank

Öffnen einer KeePass-Datenbank mit Masterpasswort

1. Starten Sie KeePassXC

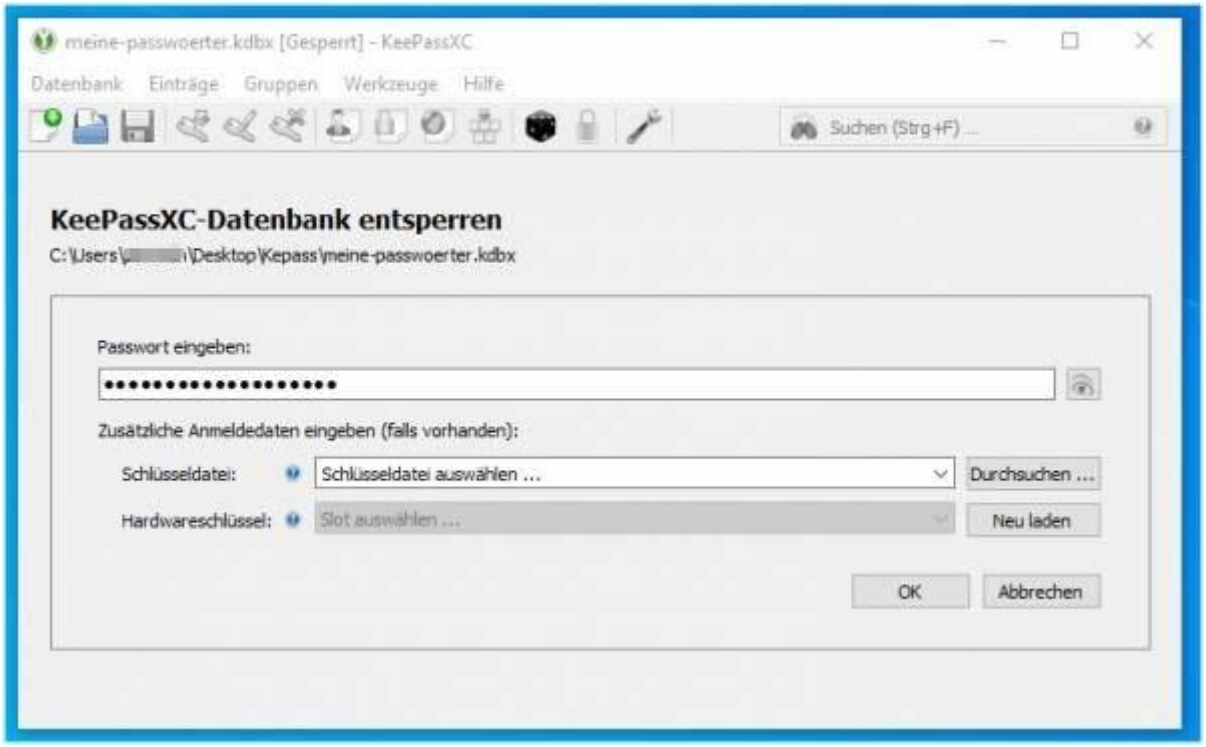


2 Klicken Sie auf **[Existierende Datenbank öffnen...]**.



> Ist die Willkommensanzeige nicht zu sehen, ist bereits eine weitere KeePass-Datenbank geöffnet, klicken Sie auf Datenbank in der Menüleiste und dann auf **[Datenbank öffnen...]**.

3. Geben Sie das Passwort ein und bestätigen Sie mit **[OK]**.



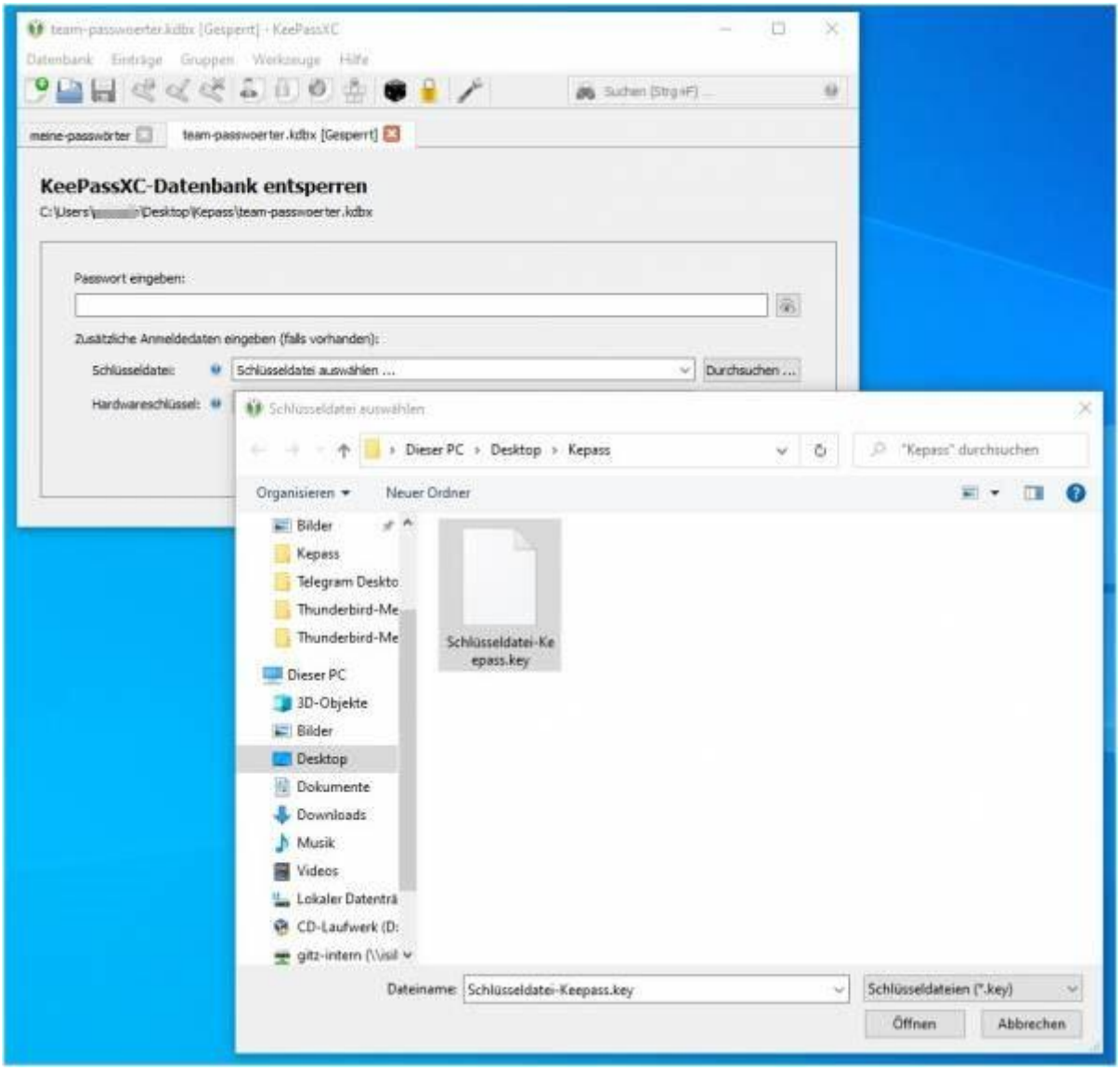
4. Die Datenbank ist nun geöffnet und Sie können Ihre Passwörter nutzen oder bearbeiten.

Öffnen einer KeePass-Datenbank mit Schlüsseldatei

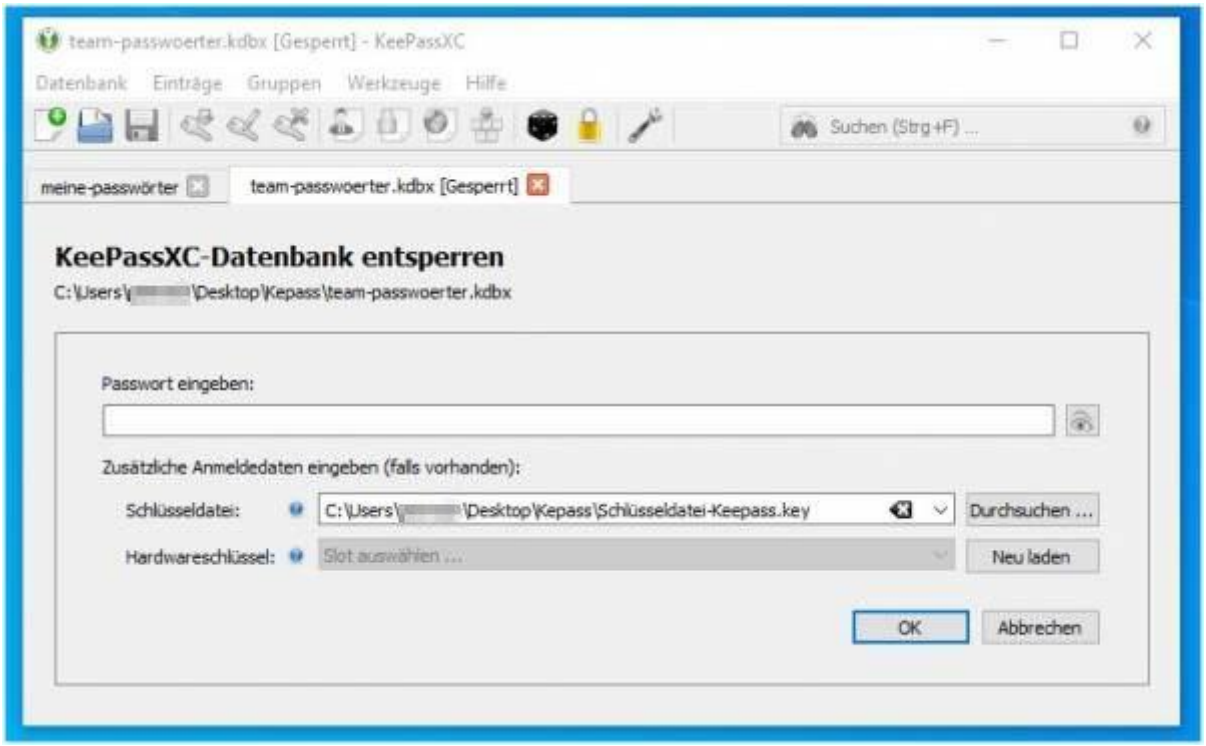
Befolgen Sie zum Öffnen der KeePass-Datenbank zunächst die ersten drei Punkte der Anleitung Öffnen einer KeePass-Datenbank mit Masterpasswort und folgen Sie danach dieser Anleitung.

1. Wählen Sie **[Durchsuchen ...]**.

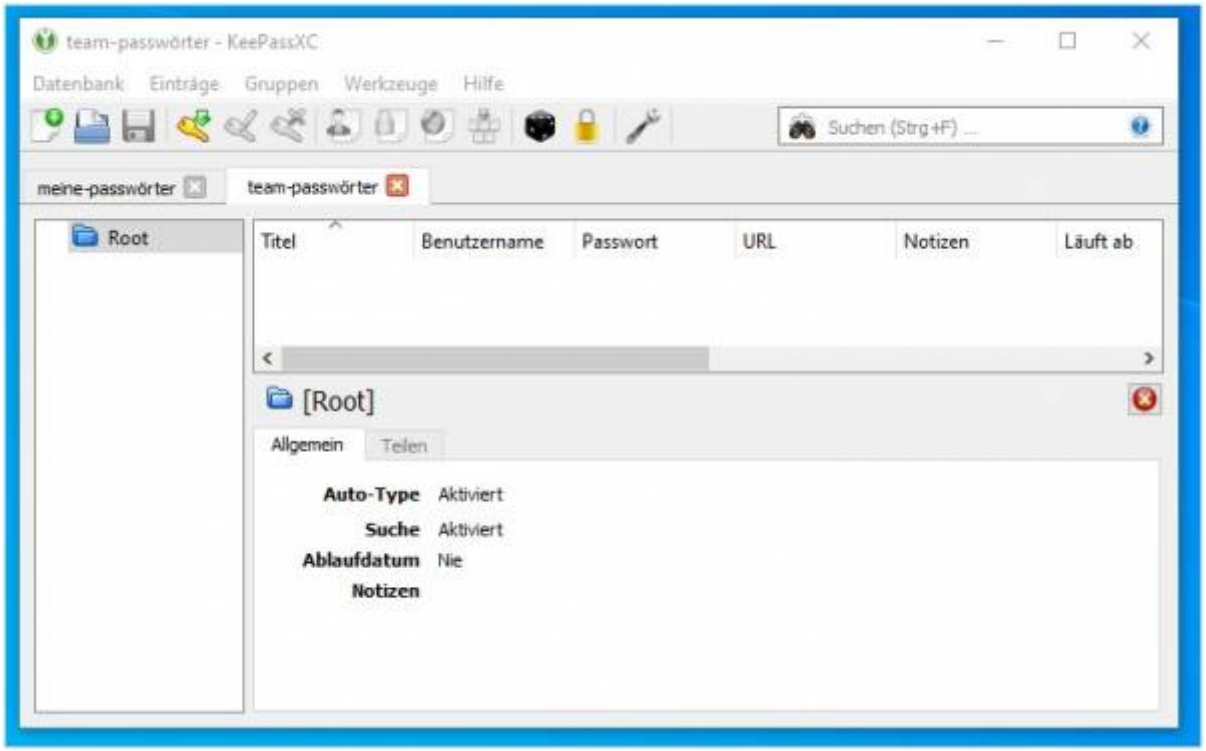
2. Navigieren Sie zu der passenden Schlüsseldatei und bestätigen Sie Ihre Auswahl mit **[Öffnen]**.



3. Bestätigen Sie mit **[OK]**.



4. Die KeePass-Datenbank ist nun nutzbar.

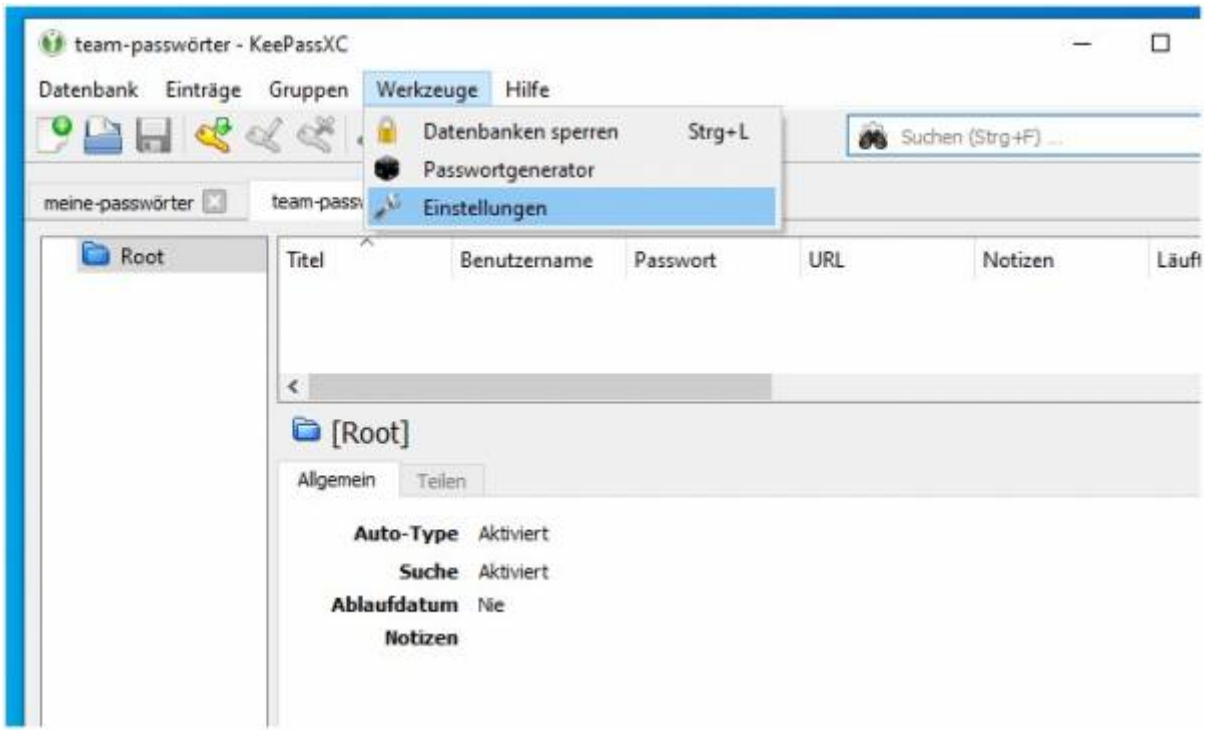


> Wie Sie hier sehen ist es auch möglich mehrere Datenbanken gleichzeitig geöffnet zu haben. Sie können zwischen den Datenbanken über die Reiter-Zeile, die in KeePassXC als Tabs dargestellt werden, durchschalten.

Arbeiten mit KeePass-Datenbank

Empfohlene Einstellungen

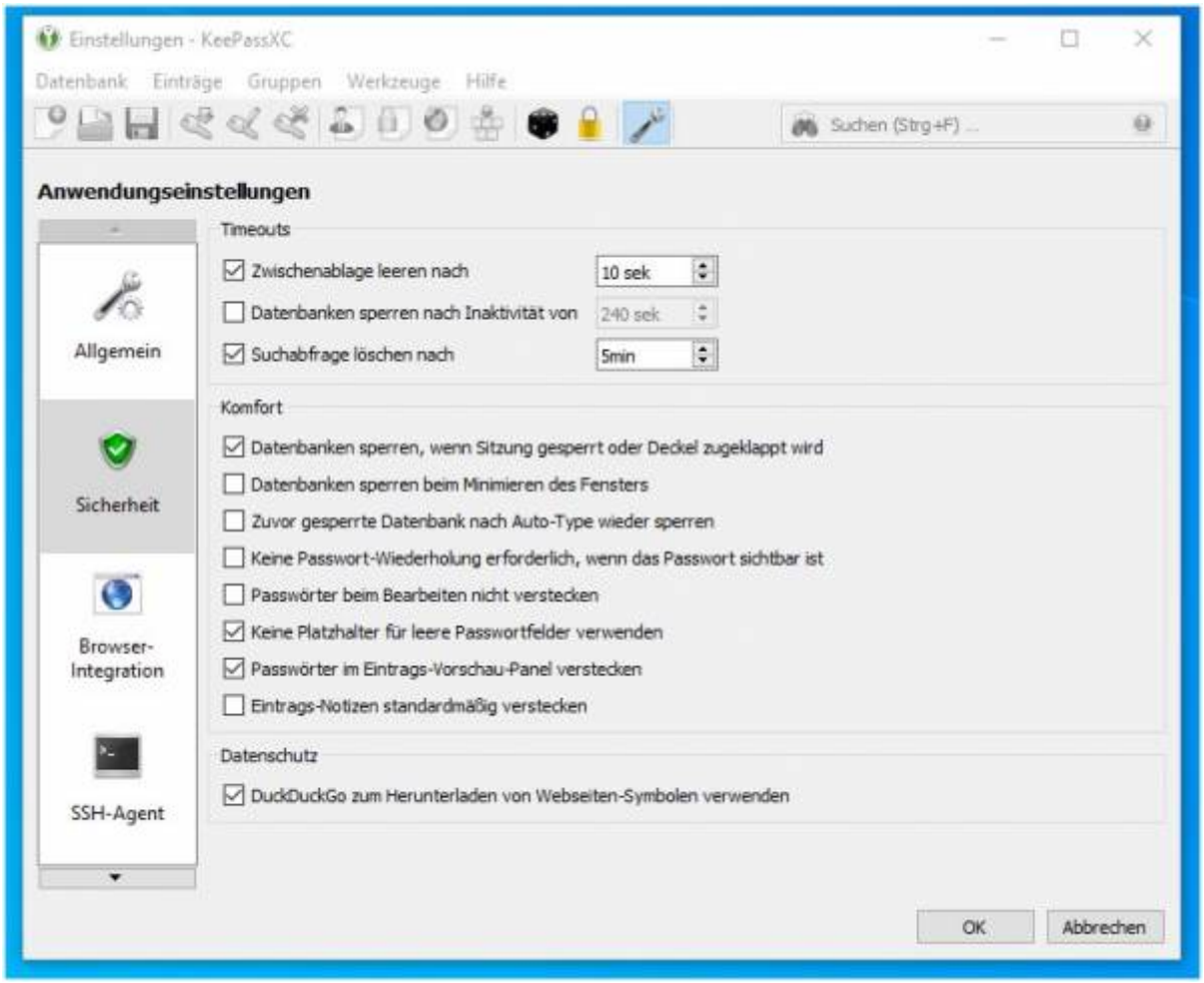
1. Öffnen Sie die KeePassXC Einstellungen.



Herunterladen von Webseiten-Symbolen

Oftmals ist es schneller zugehörige Passwörter mithilfe von Webseiten-Symbolen zu finden. KeePassXC unterstütz dies als zusätzliche Option. Damit zu der jeweiligen Seite das passende Icon angezeigt wird, gehen Sie folgendermaßen vor:

Nach öffnen der Einstellungen (wie unter Empfohlene Einstellungen), wechseln Sie zu dem Bereich **[Sicherheit]**, wie in der Abbildung zu sehen ist.

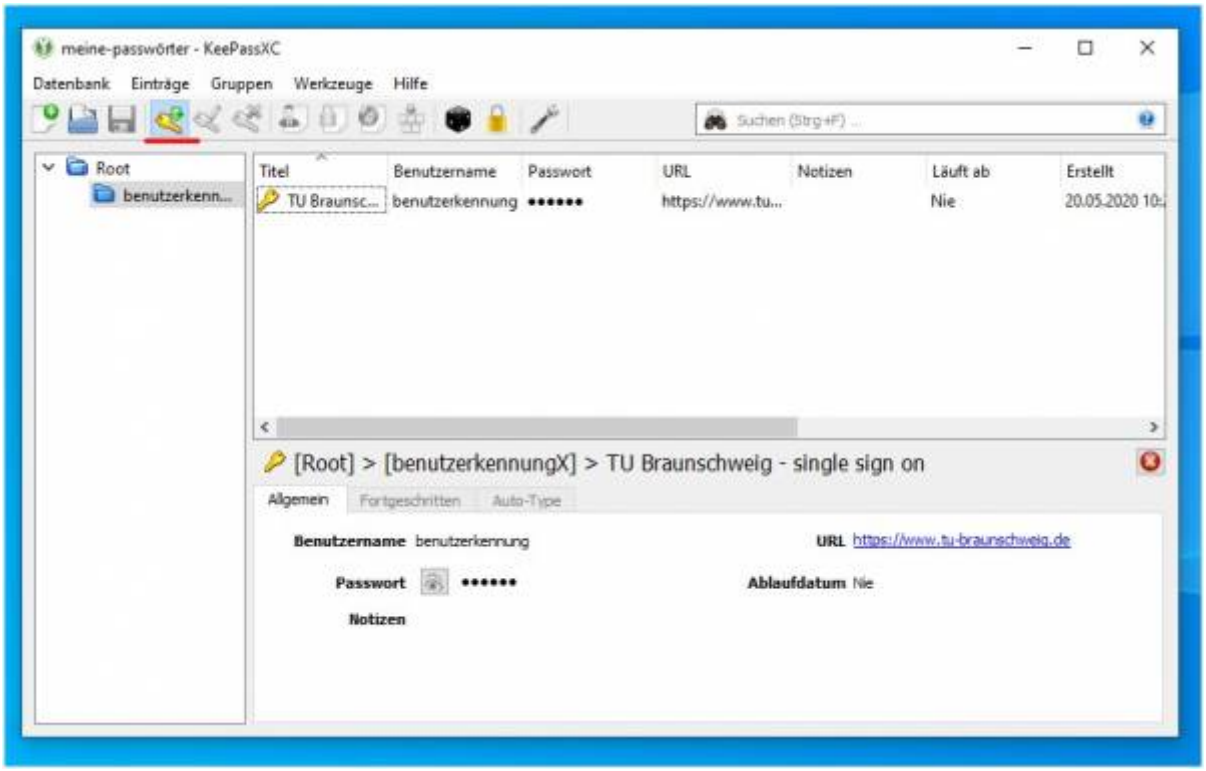


Im Abschnitt Datenschutz aktivieren Sie den Haken bei „DuckDuckGo zum Herunterladen von Webseiten-Symbolen verwenden“.

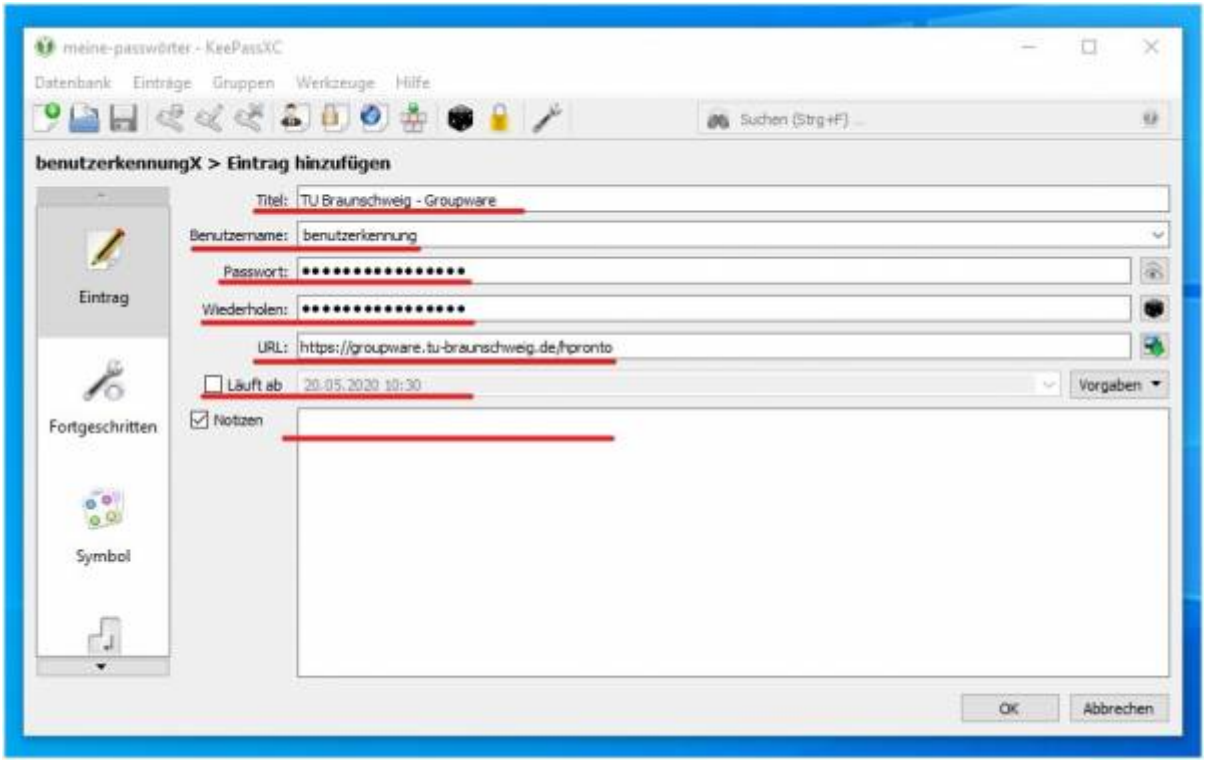
Erzeugen eines Eintrags

Manueller Eintrag

1. Um einen neuen Datenbankeintrag zu machen, klicken Sie auf das (in der Abbildung rot markiert) **[Eintrag Hinzufügen]**-Symbol.



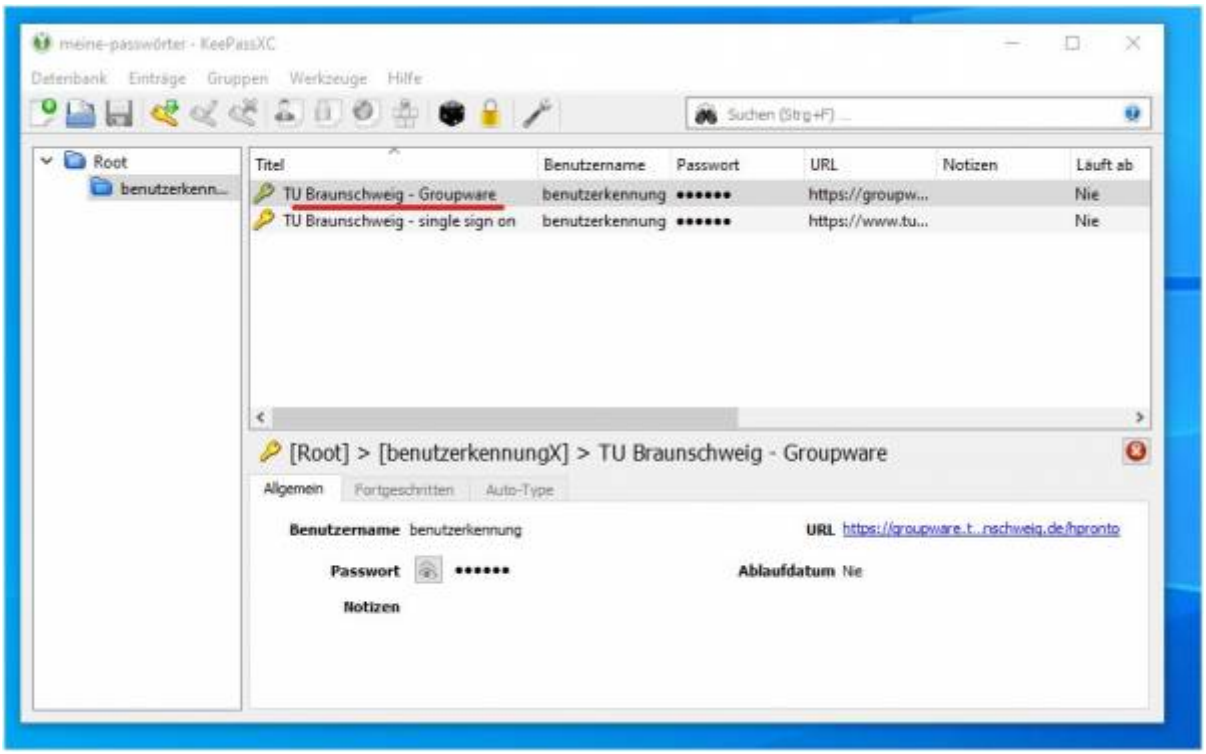
2. Geben Sie die aktuellen Benutzerinformationen ein.



- Vergeben Sie einen aussagekräftigen **Titel** – gerne den genauen Titel der Anwendung/Webseite
- **Benutzerkennung** (GITZ-/Mitarbeiterkennung)

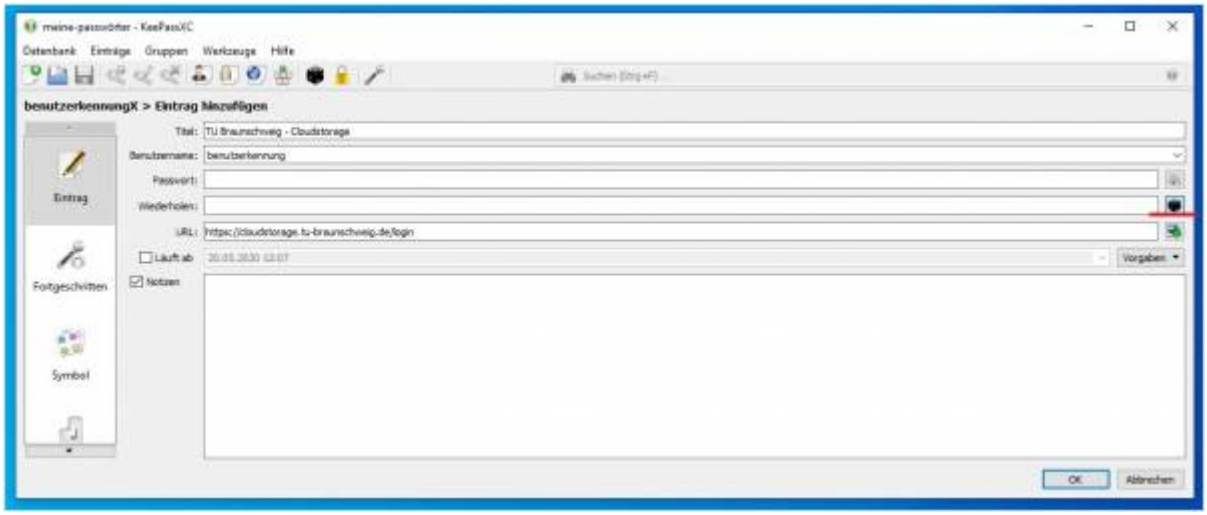
- Das zugehörige **Passwort** (2X)
- Im Falle einer Webseite, die genaue **Webseiten-URL** der Anmeldeseite
- Sie können optional ein **Ablaufdatum** eingeben. Das entspräche dem Ablaufdatum Ihres Kennworts.
- Sie können gerne **Notizen** hinzufügen. Dieses Feld ist ebenfalls optional.
- Mit **[OK]** legen Sie den Datenbankeintrag an.

3. Der Eintrag ist nun in der entsprechenden Liste der Einträge zu sehen.

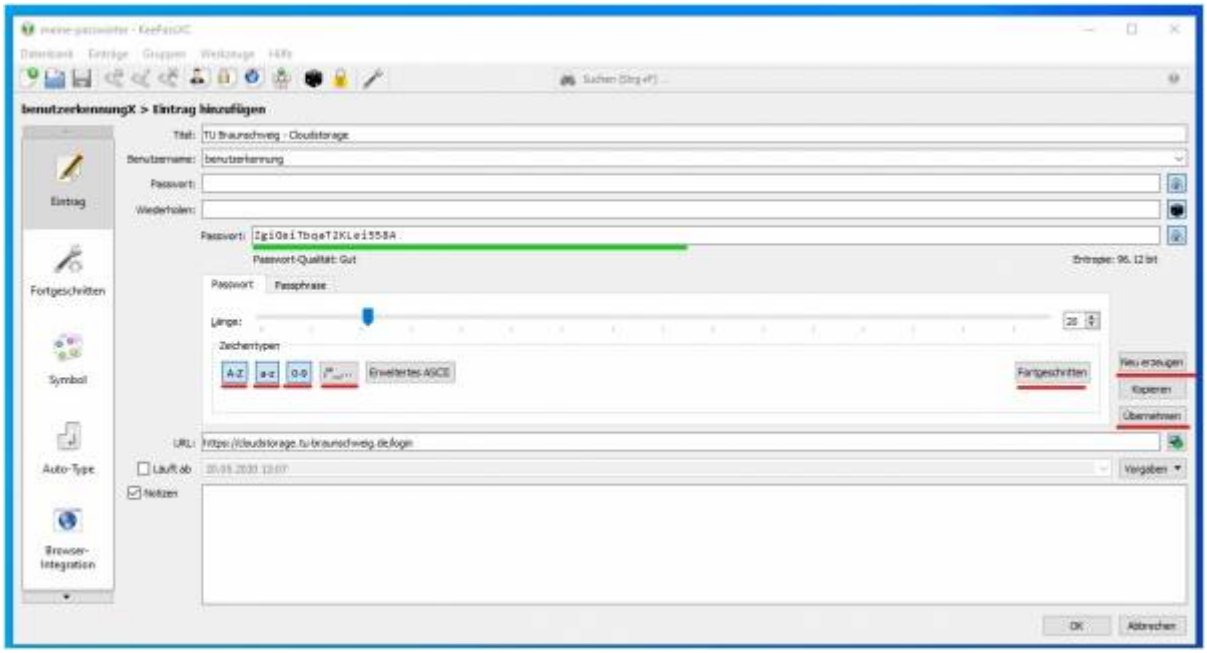


Nutzen des Passwortgenerators

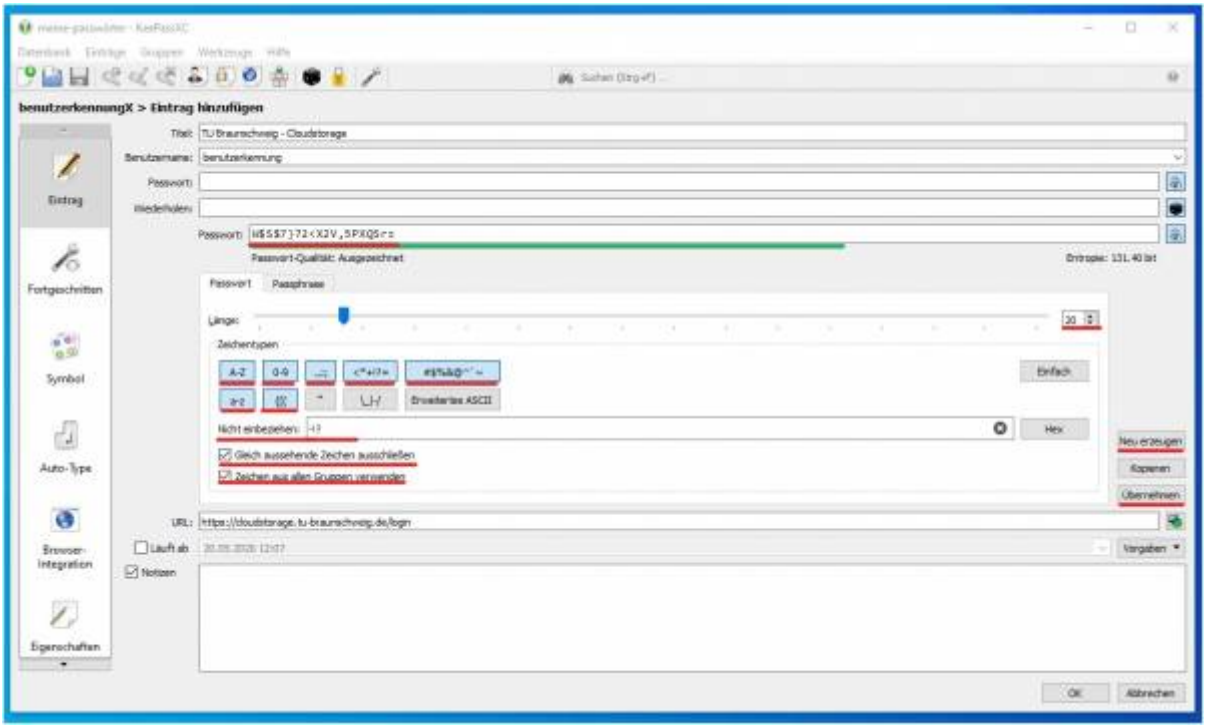
1. KeePassXC bietet einen integrierten Passwort Generator. Dazu klicken Sie beim Anlegen oder beim Bearbeiten eines Eintrags auf das Würfel-Icon.



2. In der Einfachen Darstellung können Sie die Passwortlänge bestimmen sowie Standard Zeichengruppen aktivieren.

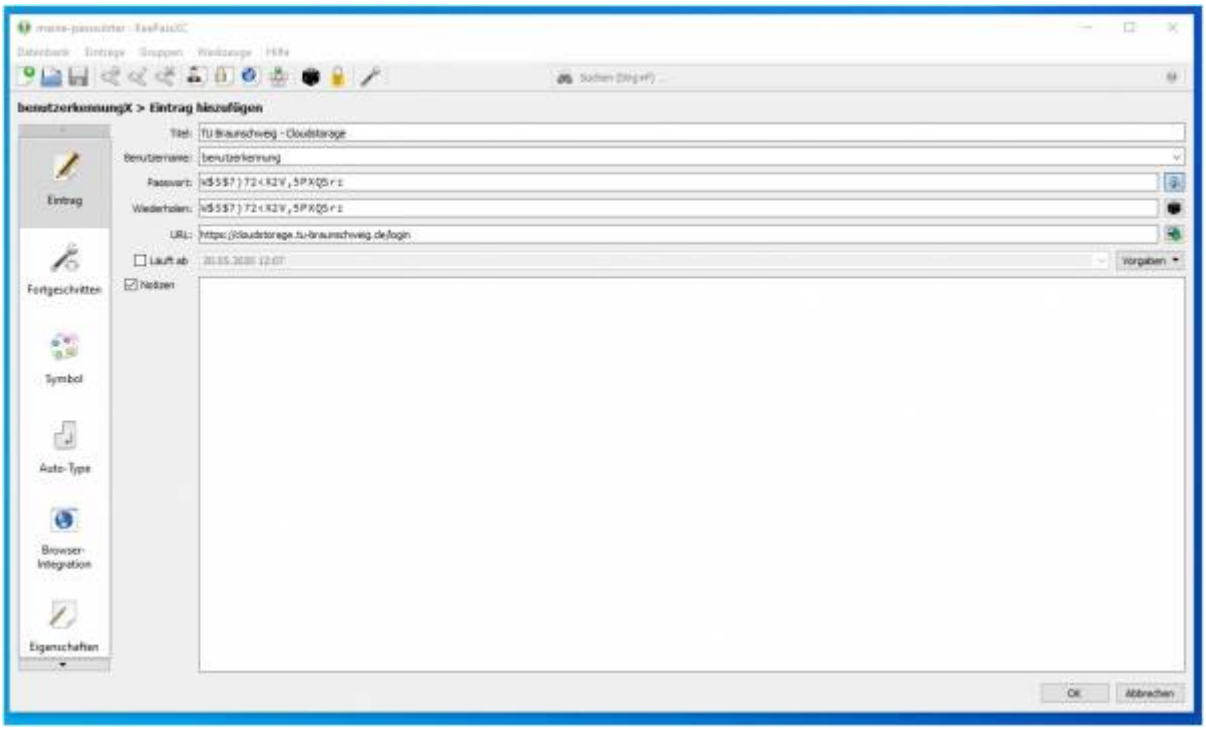


3. Klicken Sie in der Einfachen Darstellung auf **[Fortgeschritten]**, können Sie die Zeichengruppen justieren. Das ist für viele Anwendungen nützlich, da oftmals nicht jedes Zeichen im Passwort erlaubt ist.



- Bspw. Können Sie für das Passwort Ihrer TU-Mitarbeiterkennung keine „?“- oder „ „-Zeichen verwenden.
- Anschließend klicken Sie auf **[Übernehmen]**.

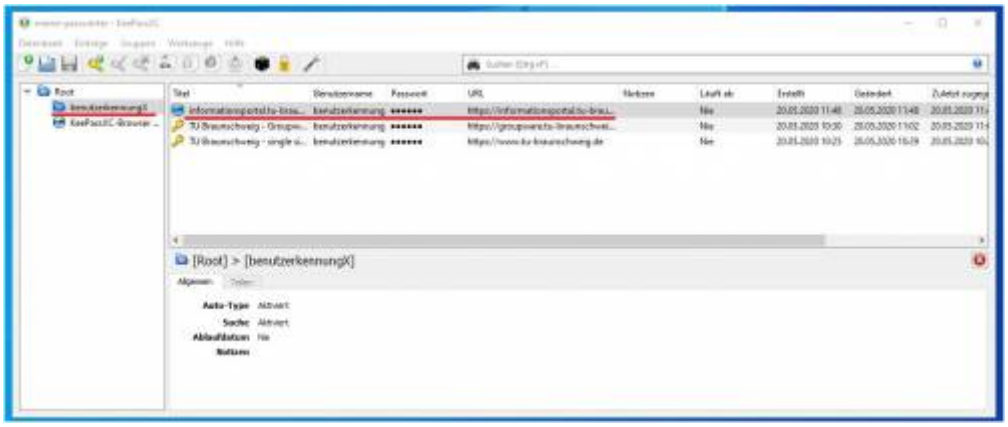
4. Das Passwort wurde übernommen. Speichern Sie den Eintrag nun mit **[OK]**.



Aufrufen eines bestehenden Eintrags

Passwort per Copy&Paste, Abtippen eingeben

1. Sie können mit einem Doppelklick auf das maskierte Passwort oder die Benutzerkennung das Passwort kopieren.



2. Fügen Sie die kopierte Information in der Anmeldemaske einer Webseite oder Applikation ein. Das Passwort ist dabei nicht sichtbar.

Passwort automatisch eingeben (Tastenkombination Strg-Alt-A)

Klicken Sie in ein Feld in einer Anmeldemaske, so wird es aktiv. Drücken Sie nun die Tasten **[Strg]+[Alt]+[A]**, werden Ihre Benutzerdaten automatisch eingegeben. Dies funktioniert auch, wenn die Eingabemaske von der Browserintegration, dem Add-On nicht als solches erkannt wird (Quasi, wenn das KeePassXC Icon nicht angezeigt wird).

Team-Passwörter

Ein besonderer Anwendungsfall ist das sichere Speichern von **gemeinsam genutzten Passwörtern**. Dies kann nötig sein beispielsweise für den Zugang zu einem gemeinsam genutzten Zugang, zu einem Fachzeitschriften-Abonnement oder ähnlicher externer Quellen oder auch als Möglichkeit, im Vertretungsfall der Zugang zu einem Funktionskonto durch organisatorisch berechtigte Personen zu gewährleisten.

Für jede Arbeitsgruppe bzw. jeden Zugange ist jeweils ein **eigener Passwort-Container** zu pflegen. Die Passwort-Container sollen ausschließlich Passwörter enthalten die dringend innerhalb der Gruppe benötigt werden.

Anlegen einer Team-Passwort-Datenbank

In diesem Fall wird organisatorisch festgelegt, dass für jeden solchen Zugang (bzw. für jeden Personenkreis mit identischen Zugängen) eine **separate Password-Datenbankdatei** angelegt wird. Diese Datei ist entsprechend wiedererkennbar zu benennen. Diese Team-Passwort-Dateien sollen **ohne Masterpasswort**, aber unbedingt mit einer **Schlüsseldatei** gesichert werden - siehe weiter oben in dieser Anleitung.

Die Schlüsseldatei darf nicht genauso benannt werden wie die Passwortdatenbankdatei. Die Schlüsseldatei ist auf jeden Fall getrennt von der Passwortdatenbankdatei zu speichern und muss so gespeichert werden, dass keine unbefugten Personen Zugang zu dieser Datei erhalten können - die Passwortdatenbankdatei selbst darf aber durchaus auf z.B. dem Abteilungslaufwerk zugänglich für alle eventuell berechtigten Personen abgelegt werden - ohne die Schlüsseldatei kann ja niemand darauf zugreifen.

Verteilung der Schlüsseldatei

Die Verteilung der Schlüsseldatei an die jeweils befugten Personen sollte persönlich erfolgen, idealerweise in Form der persönlichen Übergabe eines USB-Sticks, der nur und ausschließlich die Schlüsseldatei enthält und **nicht** als solcher gekennzeichnet ist. Dabei ist, wenn möglich ein gebrauchter, nicht als “wichtig” erkennbarer und keinesfalls beschrifteter USB-Stick zu verwenden.

Sofern keine persönliche Übergabe möglich ist, wird folgendes Verfahren empfohlen:

Der Austausch der Passwort-Container soll über zentrale, zugriffsbeschränkte Datenlaufwerke, bspw. rein interne Netzwerklaufwerke oder den TU-eighenen Cloudstorage, erfolgen. Die Zugriffsberechtigungen auf die Datenspeicherorte der Container sind auf das minimal notwendige zu beschränken und die Nutzendenberechtigung sind periodisch zu überprüfen und zu aktualisieren.

Es muss für jede Schlüsseldatei (also jede Team-KeePass-Datenbankdatei) eine Liste der berechtigten Personen, die einen USB-Stick erhalten haben, mit Ausgabedatum geführt werden.

Auf keinen Fall darf die Schlüsseldatei zusammen mit der KeePass-Datenbankdatei in einem Ordner oder auf einem Medium (USB-Stick, CD, …) gespeichert werden!
Die Schlüsseldateien sind zu jeder Zeit vor dem Zugriff durch unbefugte Personen zu schützen!

Austausch von Masterkennwörtern

Sofern der Austausch von (Master-) Kennwörtern für Passwort-Container notwendig ist, so sollte er über sichere Kanäle erfolgen. Zu präferieren sind nicht-technisch gestützte Übergaben der Masterpasswörter.

Dazu sollten zentrale, sichere Ablageorte in den Organisationseinheiten definiert werden, etwa in einem verschlossenen Safe im jeweiligen Sekretariat. Erfolgt die Übergabe der Masterpasswörter über IT-Systeme ist unbedingt auf eine Ende-zu-Ende-Verschlüsselung zu achten. *Damit entfällt im Regelfall das Versenden per E-Mail.*

Es ist zu vermeiden, lokale Kopien von Passwort-Containern anzulegen, speziell ist es nicht gestattet, Passwort-Container auf privaten Geräten vorzuhalten.

Tipps und Tricks

Tastenkombinationen

[Strg][Alt][A]: Mit dieser Tastenkombination füllen Sie automatisch Anmeldeinformationen aus. Diese Tastenkombination ist mit der linken Hand ausführbar. *Dies ist die bereits eingestellte Standardeinstellung.*

[Strg][Alt][P]: Fühlen Sie sich dabei wohler mit zwei Händen zu tippen, führt diese Kombination die gleiche Aktion aus. Dabei können Sie die Taste P mit der rechten Hand bedienen. **Dies müssen Sie, wenn gewünscht selbst einstellen.**

Eigene Tastenkombinationen

In den Einstellungen können Sie unter **[Tastenkombinationen]** Tastenkombinationen verändern oder weitere Kombinationen für andere Aktionen anlegen.

Revision #27
Created 23 May 2024 09:24:13 by Dennis Lukas
Updated 24 May 2024 13:33:00 by Dennis Lukas