Passwortmanager nutzen - Beispiel anhand von KeePassXC

Hinweise zur Nutzung des Passwortspeichers im Browser Firefox finden Sie hier

Kurzübersicht

- KeePassXC (open source) als Passwortmanager-Software
- Ablage/Synchronisation der Passwortdatei mittels Sciebo
- Nutzung des Passwortmanagers in Browser und verknüpfter Datenbank auf dem Smartphone/Tablet möglich

- **Aber Vorsicht: die sichere Nutzung stellt gewisse Anforderungen an die Nutzer.**

Nützliche Links

- Häufig gestellte Fragen: https://keepassxc.org/docs/
- Offizielle Dokumentation: https://keepassxc.org/docs/KeePassXC_UserGuide.html
- Anleitung der TU Braunschweig: https://doku.rz.tu-bs.de/doku.php?id=software:keepassxc

Inhalt

Warum Passwortmanager?

Sie sollten **für jede Anwendung verschiedene** und gleichzeitig sichere Passwörter nutzen. Sollte ein Passwort an einer Stelle kompromittiert werden, müssen die Folgen für Logins an anderer Stelle möglichst gering bleiben. Außerdem sollten Passwörter möglichst stark sein - oft führt das zu schlechter zu merkenden Passwörtern. Viele Dienste/Websites haben außerdem unterschiedliche Vorgaben bezüglich Groß/Kleinschreibung, Sonderzeichen und Länge. Schließlich (aber nicht abschließend) bietet die Autotype-Funktion von Passwortmanagern einen gewissen Komfort.

Passwortmanager können die Sicherheit von Zugangsdaten/Passwörtern erhöhen, weil sie es ermöglichen, für verschiedene Dienste und Websites verschiedene und sehr starke Passwörter zu nutzen. Zudem müssen Sie sich auf diese Weise nur noch ein Passwort merken. *Ein richtiger Umgang mit Passwortmanagern ist dabei aber Grundvoraussetzung*.

Hinweis für Mac

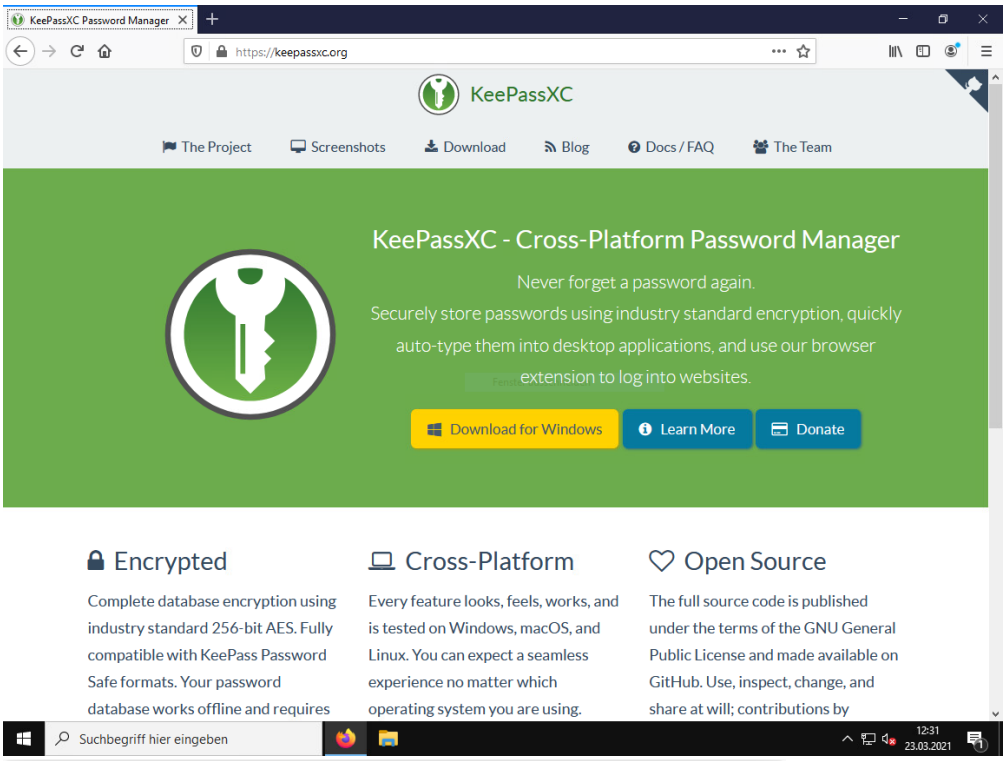
Mit der **Schlüsselbundverwaltung** bzw. gar der **iCloud Keychain** stellt Apple den Nutzern mit "Bordmitteln" einen sehr komfortablen Passwortmanager bereit, der allerdings **zwei nennenswerte Nachteile** hat. Erstens ist es nicht möglich, die dort abgelegten Passwörter mit einem nicht-Apple-System zu synchronisieren oder sie ohne größeren Aufwand dorthin zu portieren, es kommt zu einem Vendor Lock-In. Zweitens werden die Passwörter im Falle der iCloud Keychain auf den Servern von Apple gespeichert, sodass man als Nutzer darauf vertrauen muss, dass Apple mit den Passwörtern korrekt umgeht und sie richtig schützt.

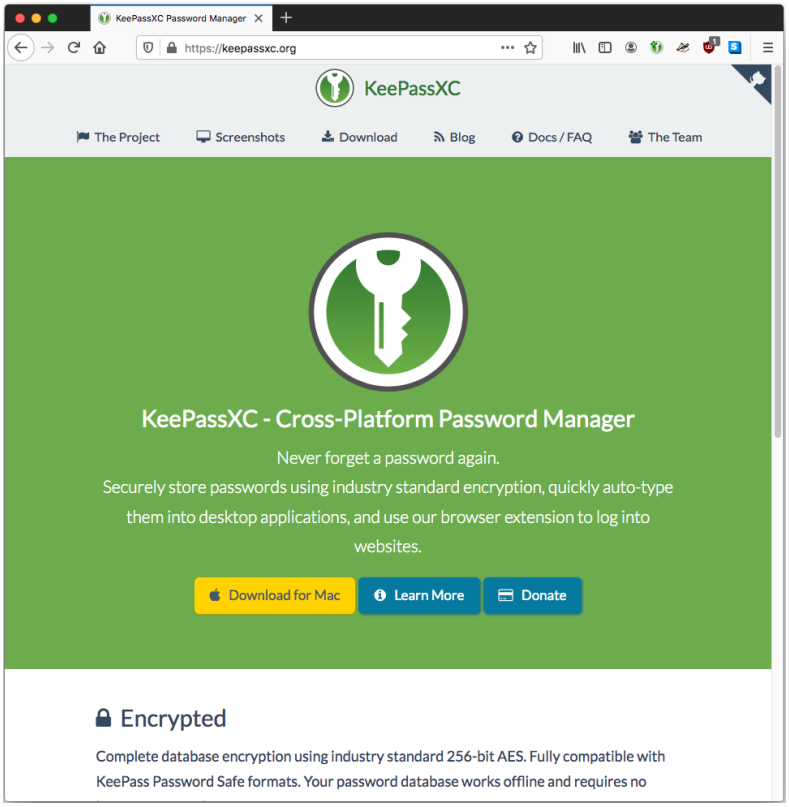
Der KeePass-Standard kann auch innerhalb der Apple-Produktwelt als Alternative zur Keychain sinnvoll und komfortabel genutzt werden. Unter macOS funktioniert KeePassXC zusammen mit Firefox; auf iOS-Geräten Programme wie Keepassium oder Strongbox selbst mit Safari.

Es folgt eine exemplarische Kurzanleitung anhand von KeePassXC, einem Open Source-Passwortmanager. Eine detailliertere, englischsprachige Dokumentation findet sich auf der Projektwebsite: https://keepassxc.org/docs/KeePassXC_GettingStarted.html

Installation von KeePassXC auf einem PC/Mac

KeePassXC darf ausschließlich von der offiziellen Projektwebsite (oder über ein vertrauenswürdiges Repo) bezogen werden: https://keepassxc.org/

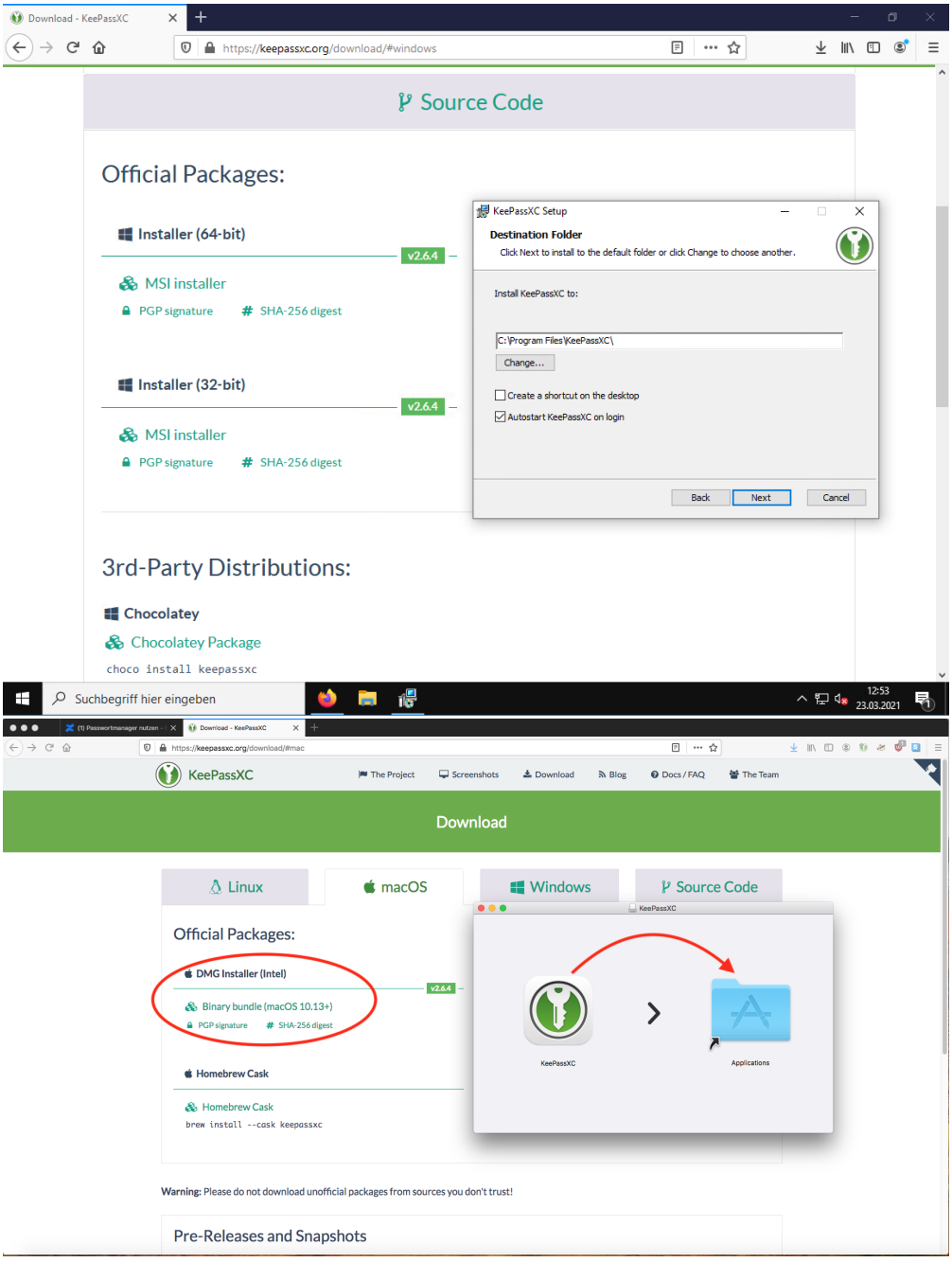




Die portable Version eignet sich für Umgebungen, in denen man als Anwender keine Administratorrechte für den genutzten PC hat.

Betriebssystemspezifische Hinweise

- Windows: Es sollte möglichst die 64 bit-Version verwendet werden.
- Mac: Die Nutzung von KeePassXC anstelle der Apple Schlüsselbundverwaltung bietet sich an, wenn Passwörter betriebssystemübergreifend synchronisiert werden sollen.

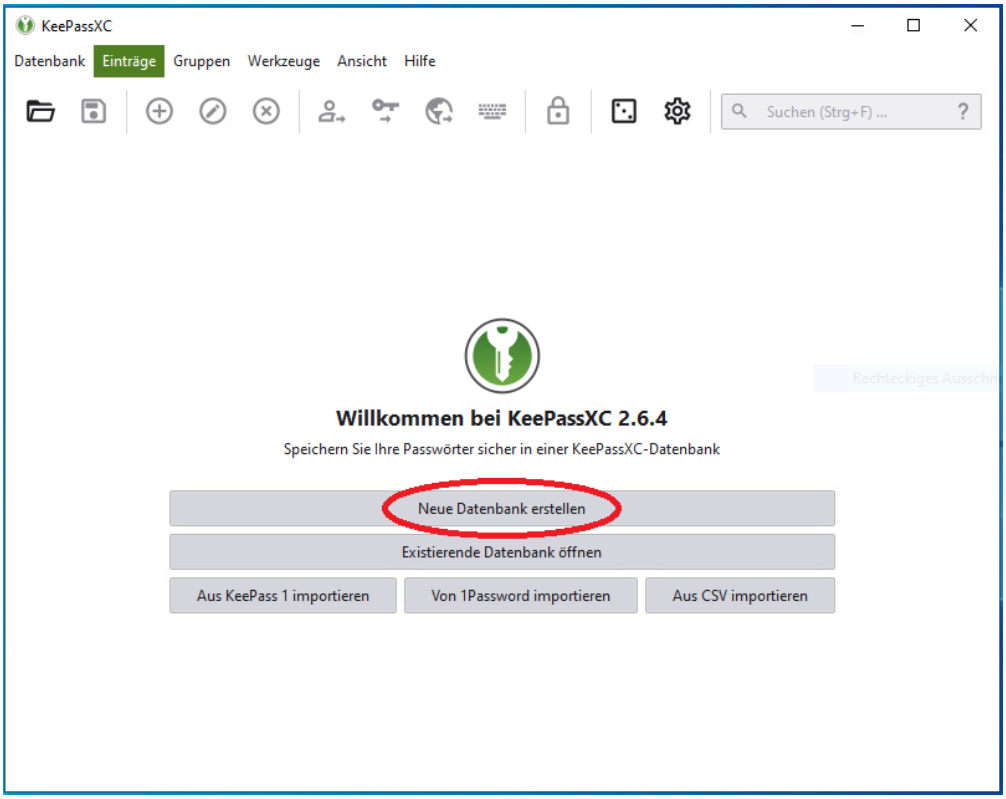


Einrichtung von KeePassXC

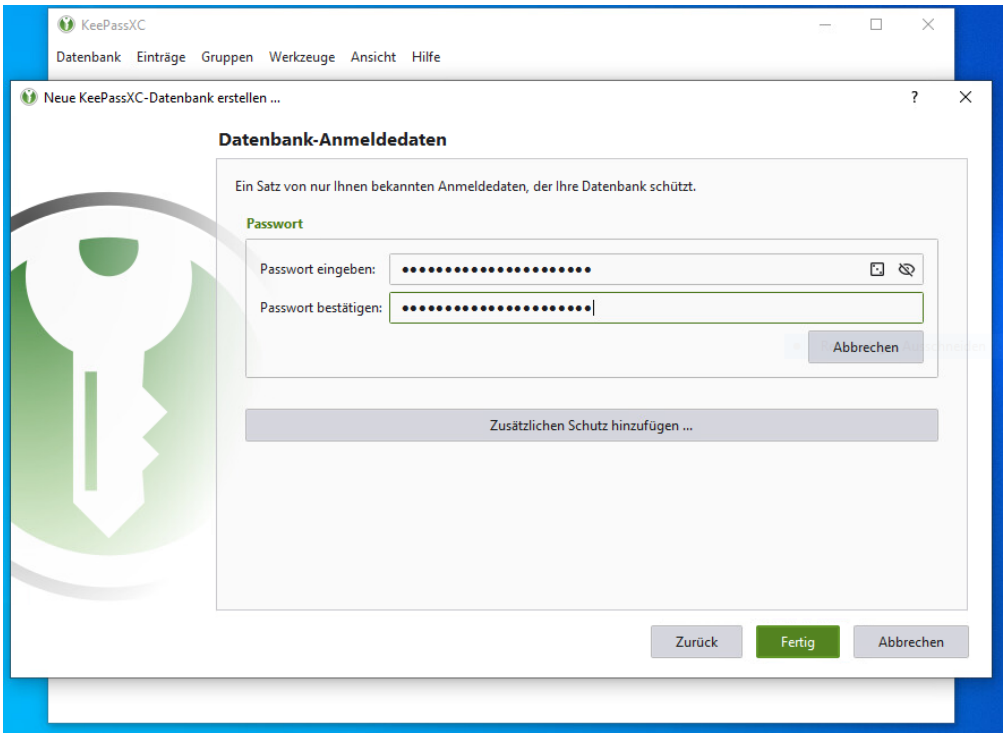
Neuerstellung einer Passwortdatei und Ablage im Sciebo-Ordner

An dieser Stelle wird vorausgesetzt, dass Sciebo bereits auf dem PC/Mac eingerichtet ist. (Falls dies nicht der Fall ist, könnte, allerdings nur eingeschränkt empfehlenswert, die Passwortdatei bei einem anderen Cloudanbieter gelagert oder mittels USB-Stick transportiert werden.)

Beim ersten Start fragt KeePassXC, ob eine neue Datenbank angelegt werden soll. Dies können wir mit einem Klick auf **Neue Datenbank erstellen** bestätigen

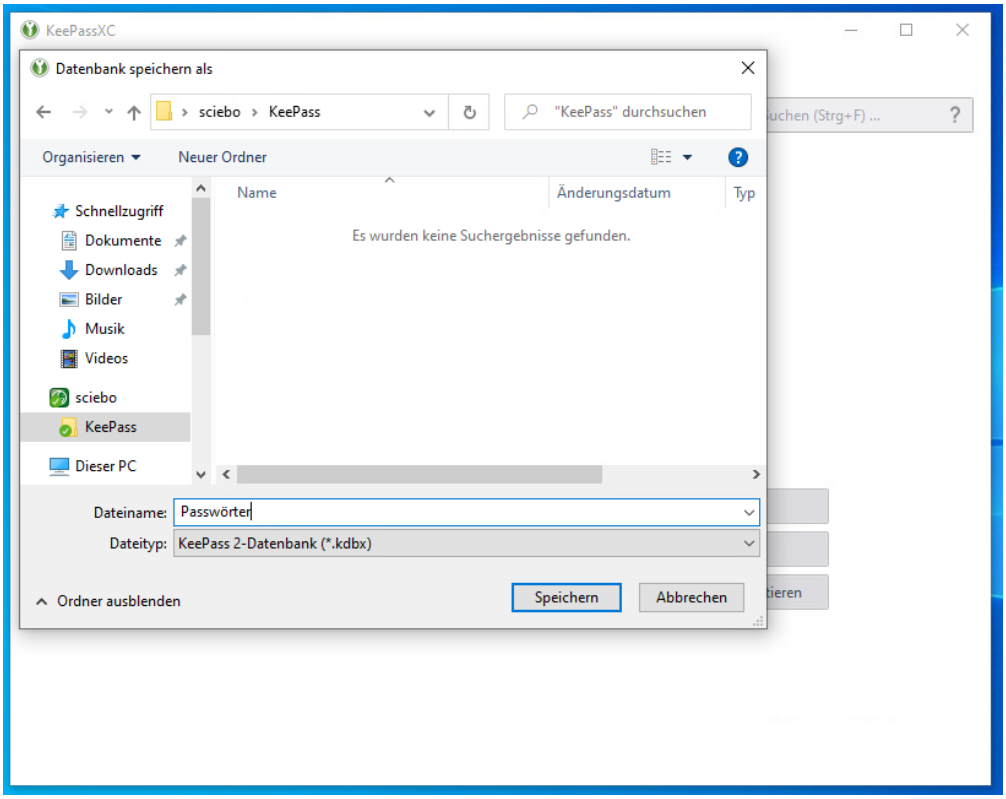


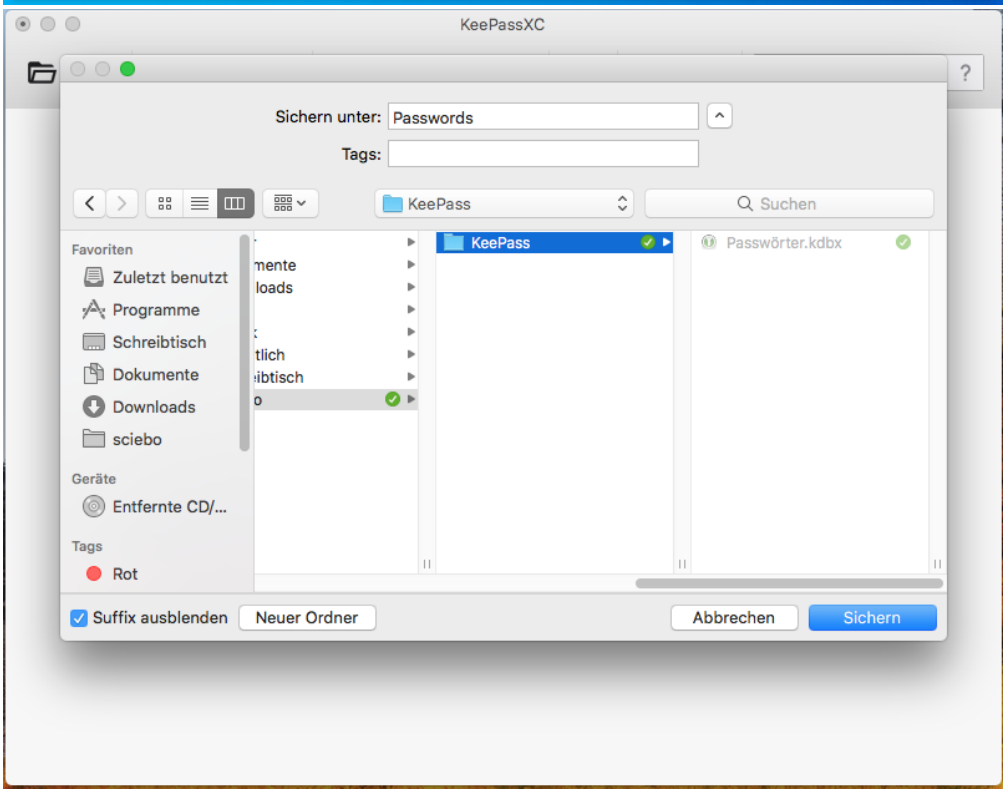
Klicken Sie sich durch das Menü, bis Sie im Fenster **Datenbank-Anmeldedaten** aufgefordert werden ein Master-Passwort festzulegen. Geben Sie hier zwei Mal ein **einzigartiges und sehr starkes Passwort** ein. Hinweise zum Erstellen von Passwörtern finden Sie hier: Ein sicheres Passwort setzen / Create a strong password



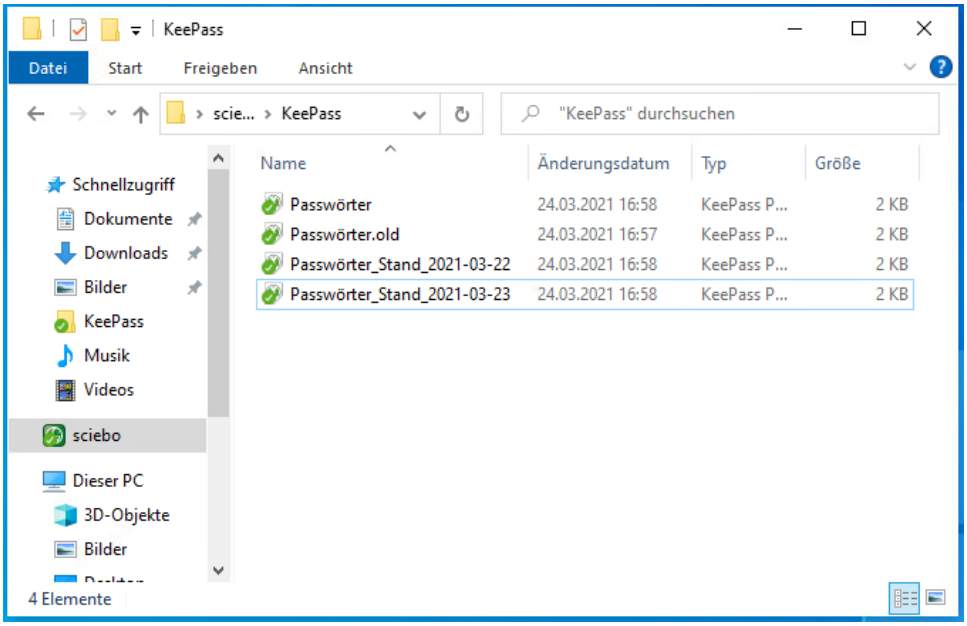
An dieser Stelle ist es möglich, die Sicherheit der Passwortdatenbank weiter zu erhöhen, indem man sich neben dem Master-Passwort zusätzlich mit einem Zertifikat oder einen Hardware-Token authentifiziert, um die Passwortdatenbank zu öffnen.

Im vorliegenden Fall legen wir die Passwortdatei im Sciebo-Ordner (dort in unserem Unterordner KeePass) ab, um sie PC-übergreifend nutzen zu können.



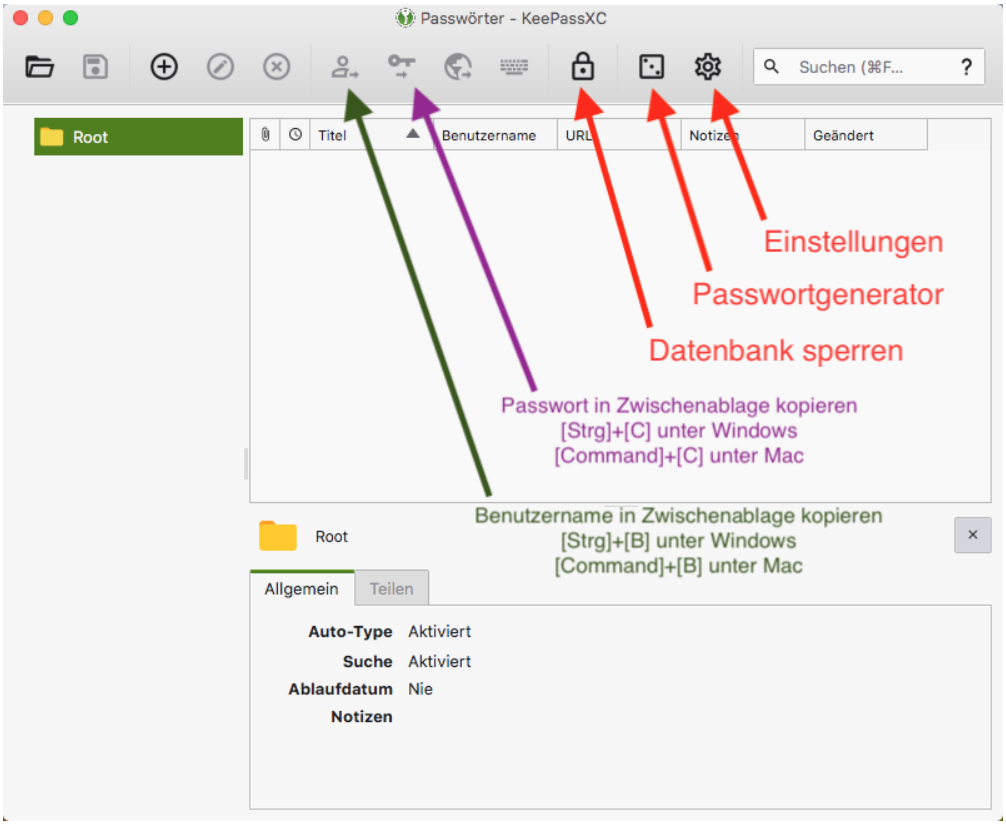


Hinweis: falls Sie für sich persönlich noch keine Backupstrategie entwickelt haben, so erzeugen Sie zumindest gelegentlich eine Sicherungskopie Ihrer Passwortdatenbank, beispielsweise wöchentlich oder nach (größeren) Änderungen, Beispiel:



Feintuning von KeePassXC für größeren Komfort

In den Einstellungen von KeePassXC (im *Hauptfenster* unter *Werkzeuge Einstellungen*) können recht viele Einstellungen vorgenommen werden, die den alltäglichen Komfort bei der Nutzung von KeePassXC verbessern. Das zusätzliche Aktivieren der unten genannten Optionen hat sich bewährt.



KeePassXC-Feintuning unter Windows

Im Menü **Einstellungen** ...

... ist das Aktivieren folgender, zusätzlicher Einstellungen empfehlenswert:

Programmstart

- KeePassXC beim Systemstart automatisch starten

Dateiverwaltung

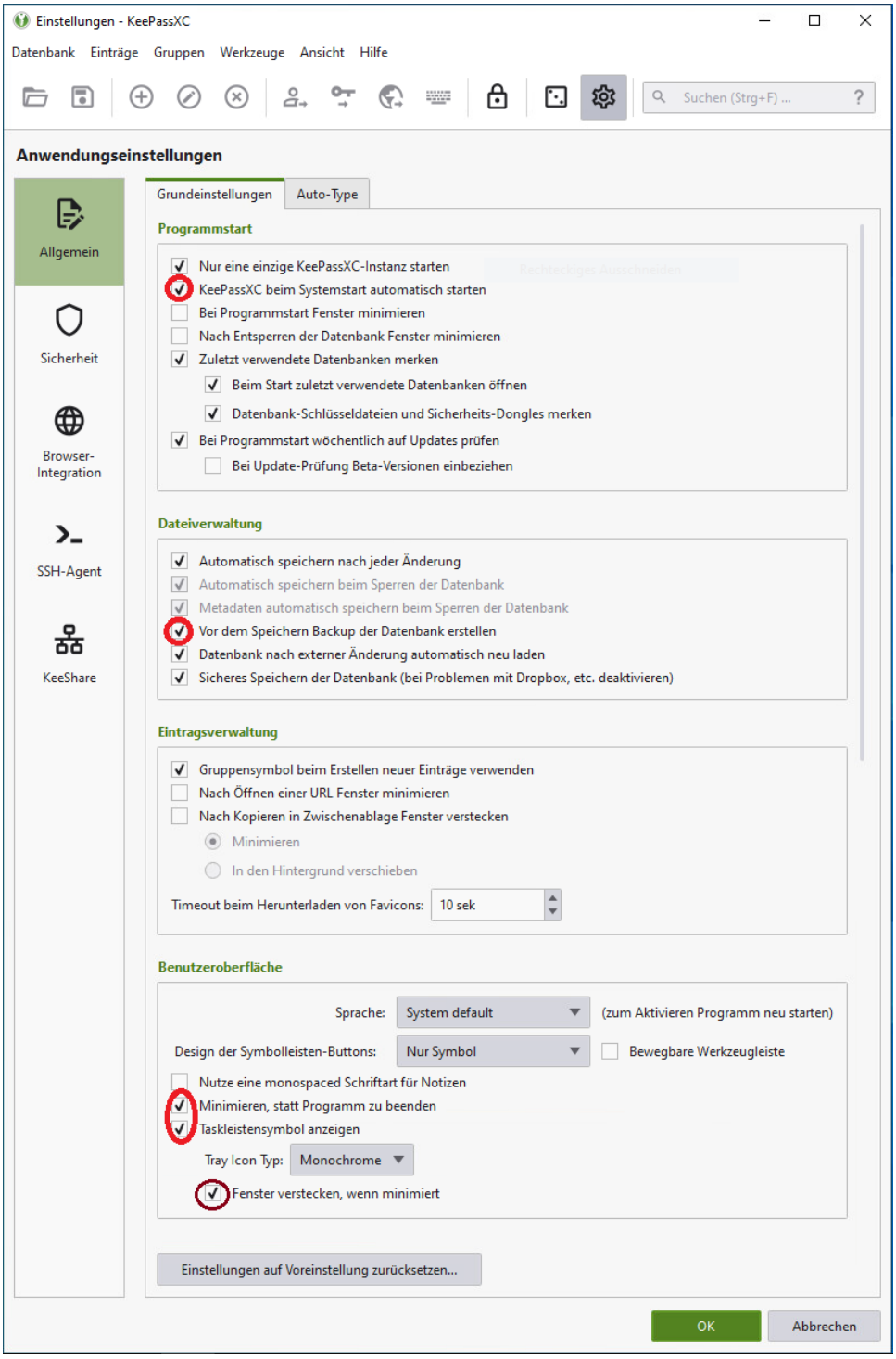
- Vor dem Speichern Backup der Datenbank erstellen

Benutzeroberfläche

- Minimieren, statt Programm zu beenden
- Taskleistensymbol anzeigen
- ggf.: verstecken, wenn minimiert (KeePassXC läuft dann im Hintergrund in der Statusleiste neben der Uhr)

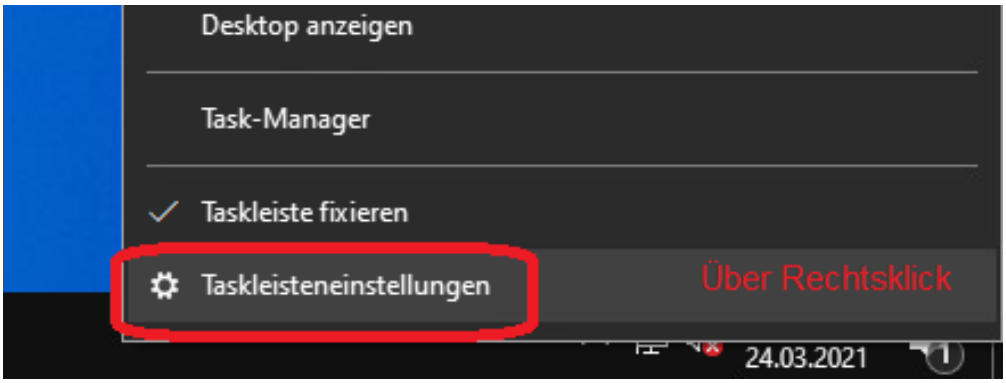
Browserintegration

- Browserintegration aktivieren
  - Firefox
  - ggf. andere Browser (abhängig davon, welche Browser Sie nutzen)

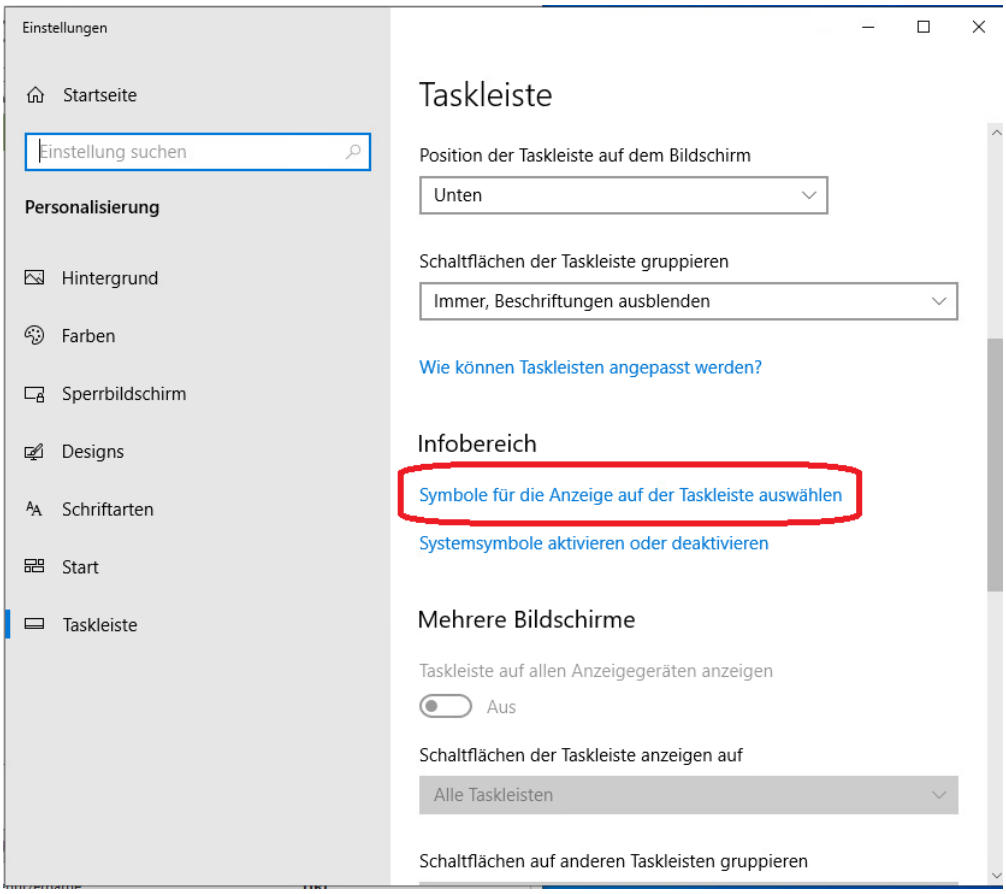


KeePassXC-Symbol in der Statusleiste (links von der Uhr) immer anzeigen lassen:

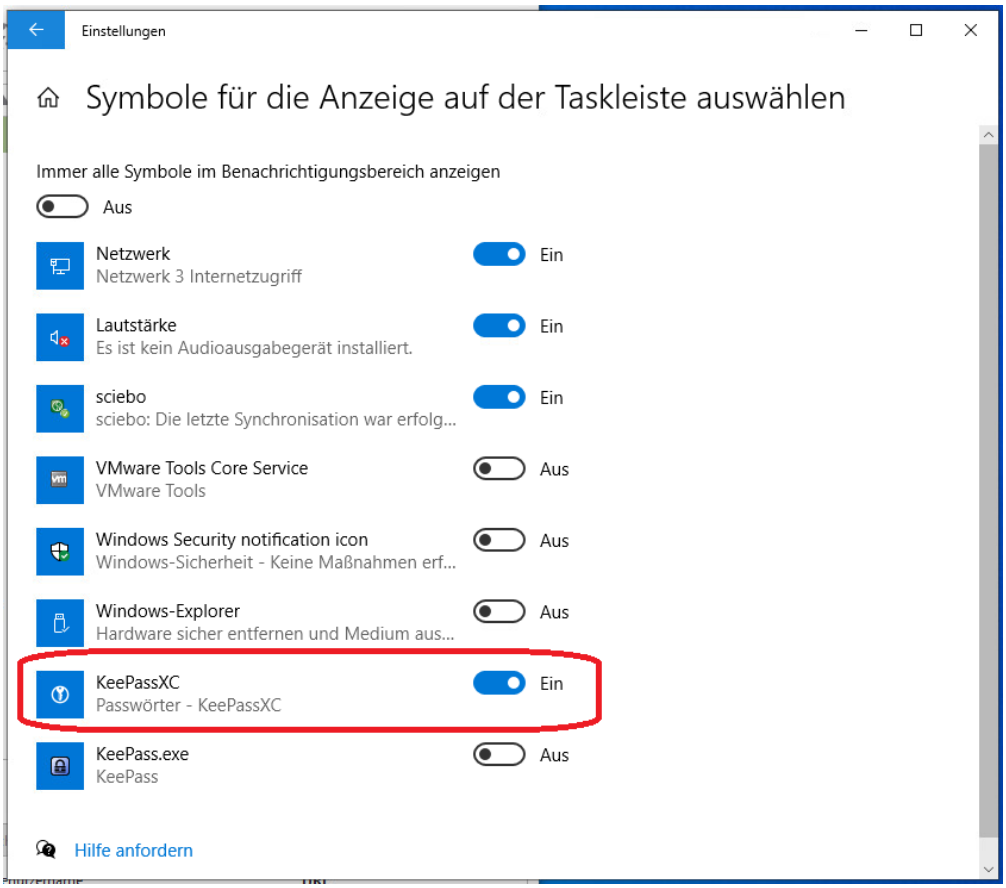
Rechtsklick auf die Taskleiste unten



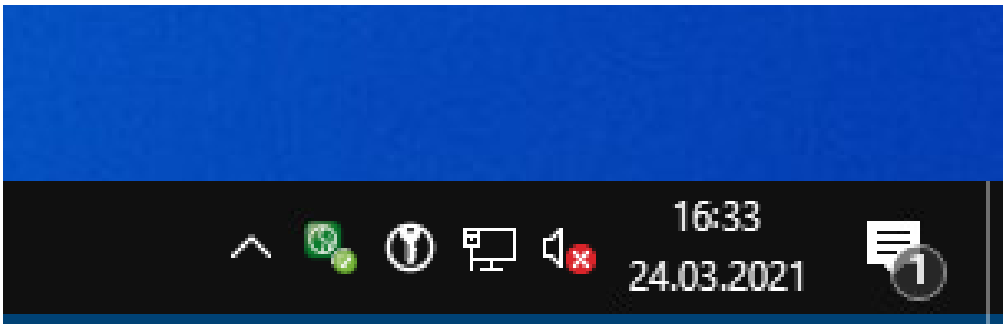
Runterscrollen, dann auf "Symbole für die Anzeige auf der Taskleiste auswählen" klicken:



Schalter neben KeePassXC einschalten:

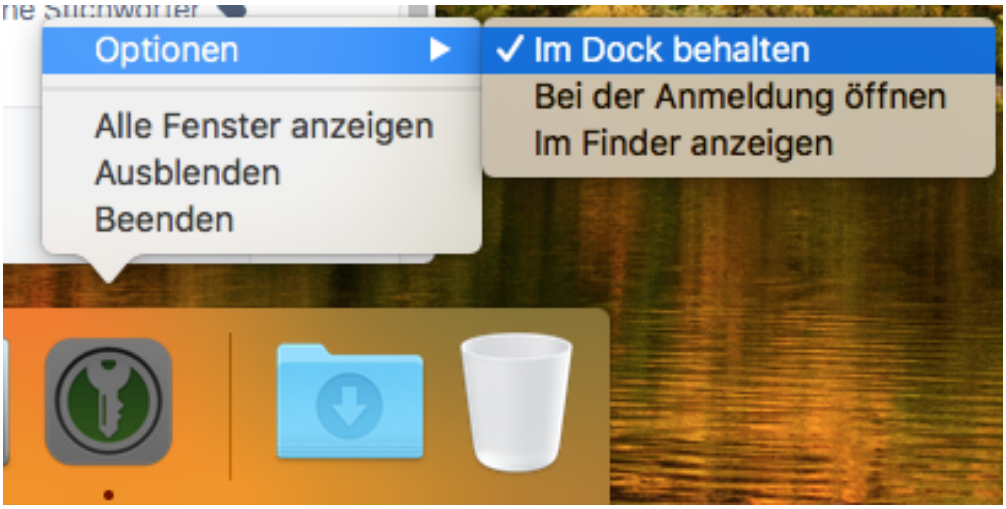


Das Symbol für KeePassXC befindet sich dann neben der Uhr:



KeePassXC-Feintuning unter macOS

KeePassXC-Symbol im Dock behalten:



Im Menü **Einstellungen** ...

... ist das Aktivieren folgender, zusätzlicher Einstellungen empfehlenswert:

Programmstart

- KeePassXC beim Systemstart automatisch starten

Dateiverwaltung

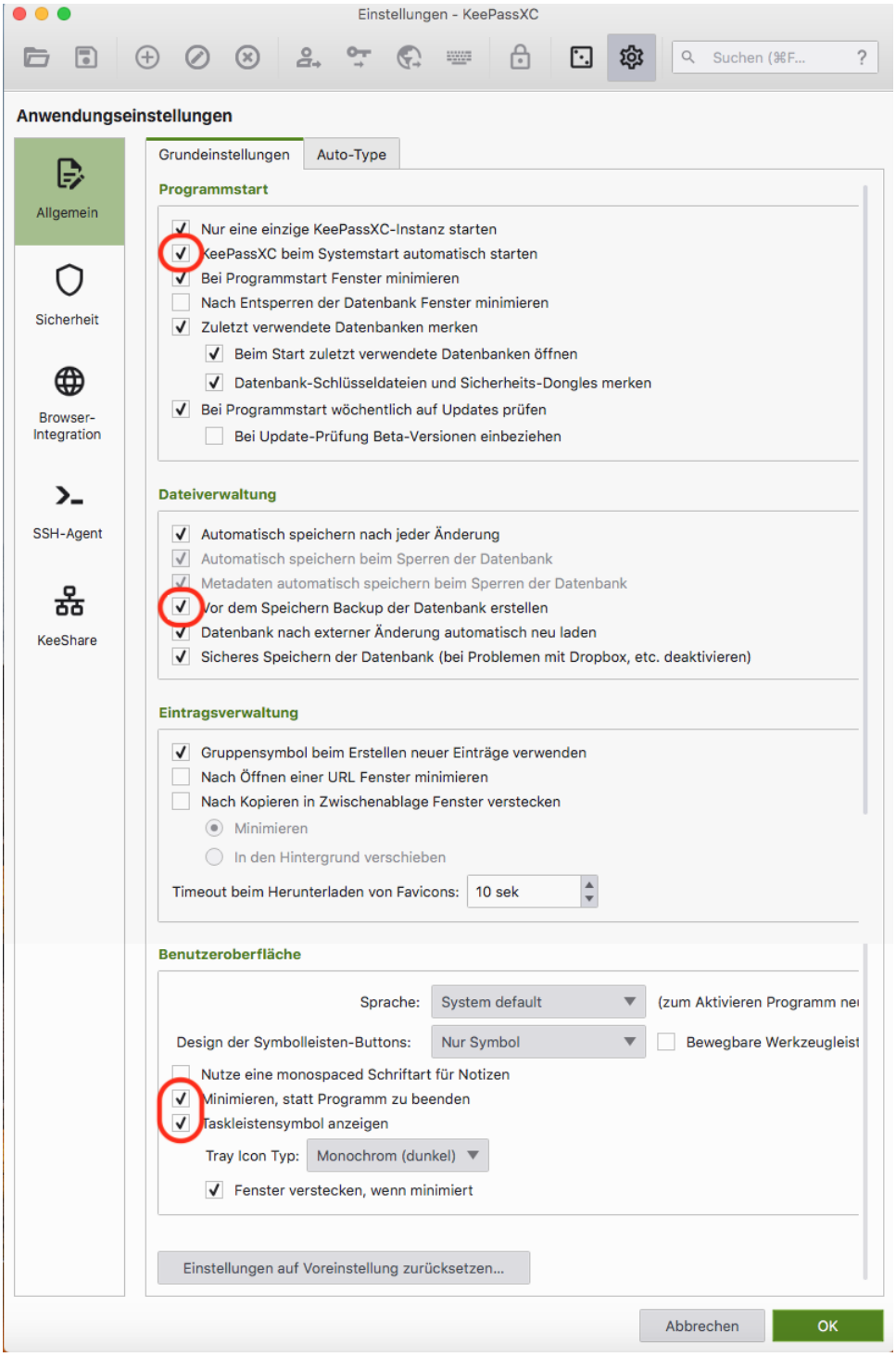
- Vor dem Speichern Backup der Datenbank erstellen

Benutzeroberfläche

- Minimieren, statt Programm zu beenden
- Taskleistensymbol anzeigen
- ggf.: verstecken, wenn minimiert
  (KeePassXC läuft dann im Hintergrund in der Statusleiste neben der Uhr)

Browserintegration

- Browserintegration aktivieren
  - Firefox
  - ggf. andere Browser (abhängig davon, welche Browser Sie nutzen)

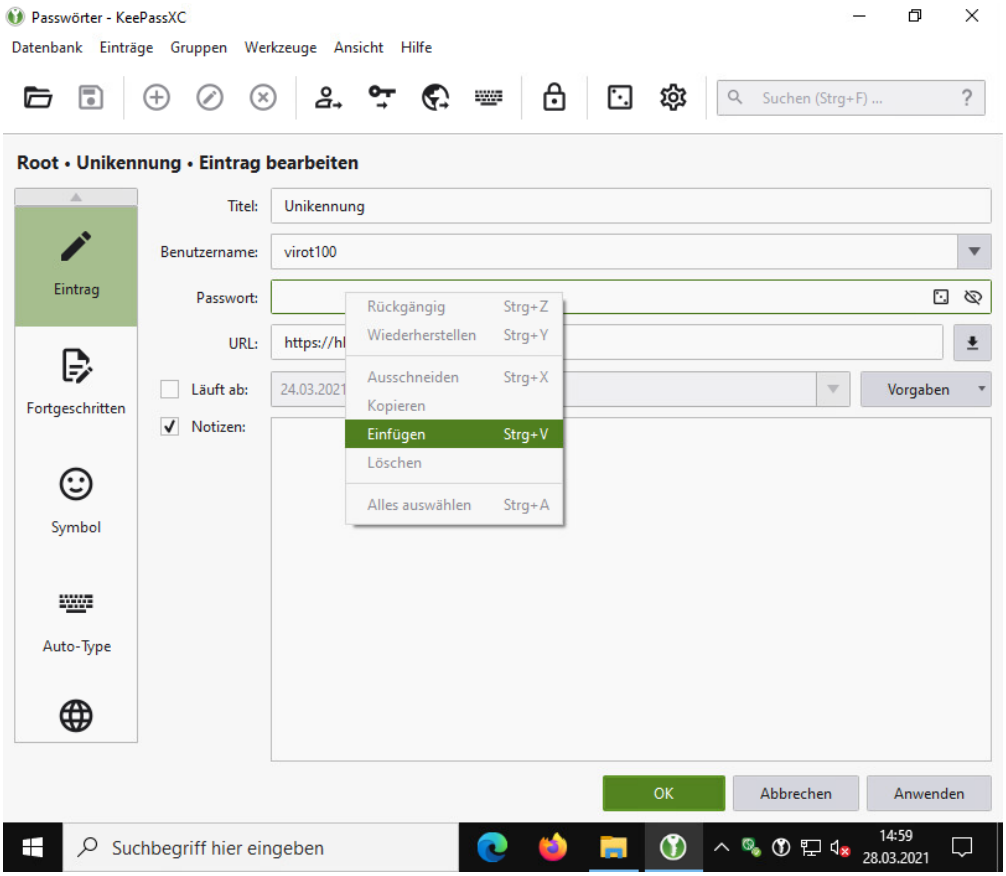


KeePassXC verwenden

Eintrag manuell erzeugen

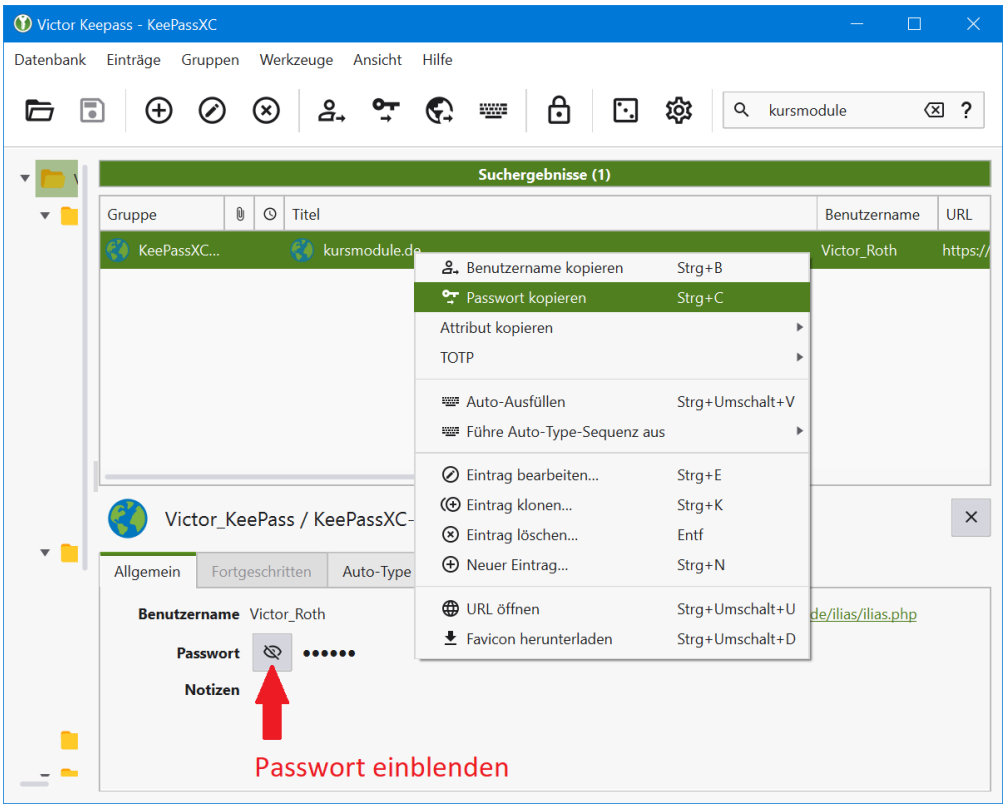
Der zuverlässigere, jedoch etwas umständlichere Weg erfolgt über das Hauptfenster von KeePassXC. Klicken Sie dazu im KeePassXC-Hauptfenster oben links auf das Plus bzw. drücken Sie [Strg]+[N]. Geben Sie im Feld **Titel** einen für Sie verständlichen Titel und im Feld **URL** die Web-Adresse ein, auf der in Zukunft die Autotype-Funktion funktionieren soll. Die Felder Benutzername, Passwort und Notizen sind selbsterklärend.

Sollte (siehe vorheriger Abschnitt) die automatische Passwortspeicherung aus technischem Grund nicht erfolgt sein, so können Sie das eben kopierte komplexe Passwort in das Passwortfeld eintragen.



Eintrag manuell aufrufen

Im Hauptfenster können Sie einen Passworteintrag in der Passwortdatenbank anklicken und dann unter Windows mit [Strg]+[C] bzw. unter macOS mit [command]+[C] das Passwort und mit [Strg]+[B] bzw. [command]+[B] den Benutzernamen rauskopieren.

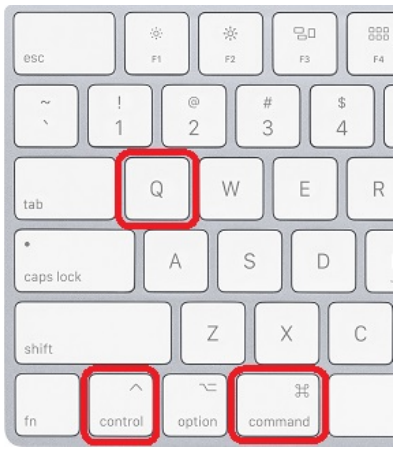


Sie können dann anschließend Benutzername und Passwort im Browser oder an anderer Stelle einfügen. Mit einem Klick auf das stilisierte Auge können Sie das Passwort einblenden lassen.

Datenbank und Arbeitsplatz beim Verlassen sperren

Beim Verlassen des Arbeitsplatzes sollten Sie zumindest die Datenbank, besser noch den gesamten **Arbeitsplatz immer sperren**.

- Das Sperren der Datenbank erfolgt im KeePassXC-Hauptfenster unter Windows mittels [Strg]+[L] und unter macOS mittels [command]+[L].
- Der Arbeitsplatz lässt sich unter Windows mittels [Windows]+[L] und unter macOS mittels [control]+[command]+[Q] sperren.



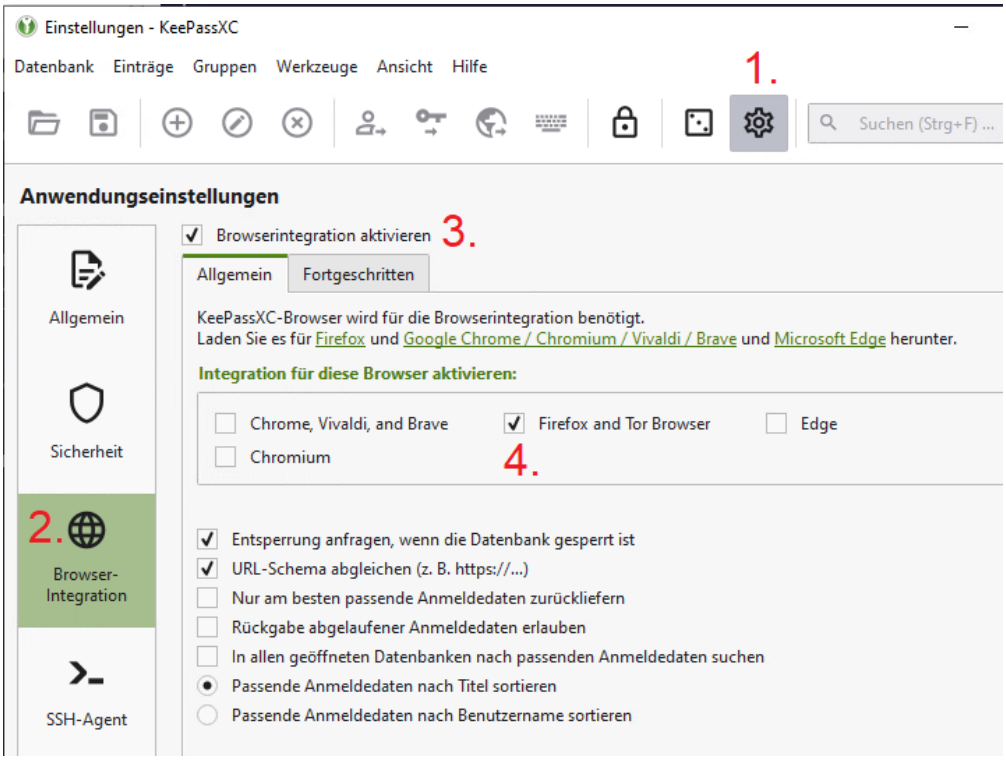
KeePassXC-Browserintegration mit Autotype

Die Funktion "Autotype" ist eine Komfortfunktion, die es erlaubt, Benutzernamen und Passwörter automatisch im Browser einfügen zu lassen (ohne jedes Mal tippen zu müssen), wenn sie vorher richtig in KeePassXC eingetragen wurden. Dafür muss für jeden Browser, mit dem Autotype genutzt werden soll, jeweils das entsprechende Add-on installiert und jeweils eine KeePassXC-Verbindung eingerichtet werden. Im vorliegenden Fall wird die Einrichtung der Browserintegration anhand von Firefox gezeigt.

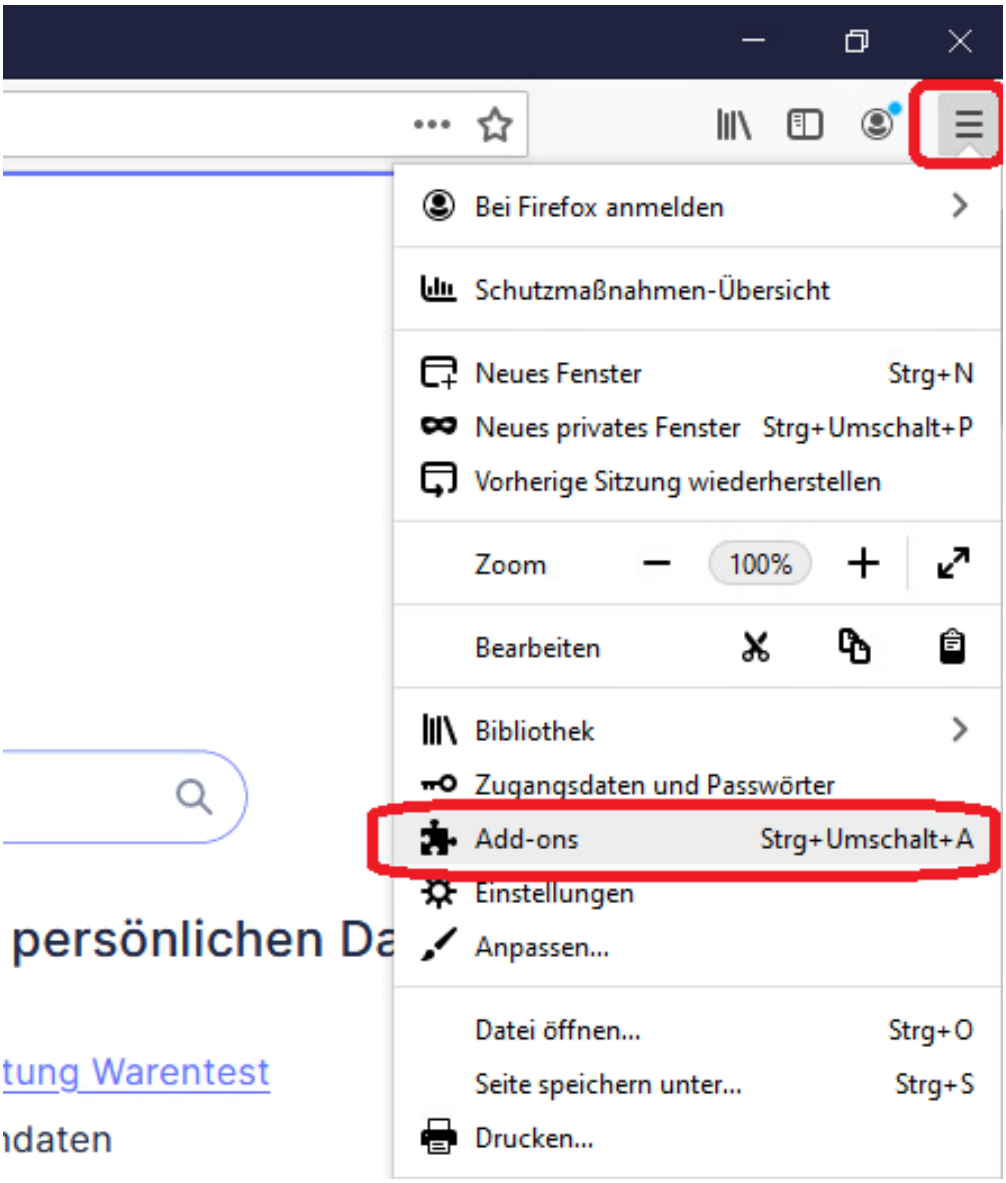
Browserintegration aktivieren

Öffnen Sie zunächst KeePassXC und entsperren Sie ggf. die Datenbank mit Ihrem Master-Passwort (und ggf. einem Zertifikat/Token). Damit KeePassXC im Browser funktioniert, muss die Datenbank auch bei der alltäglichen Verwendung entsperrt sein.

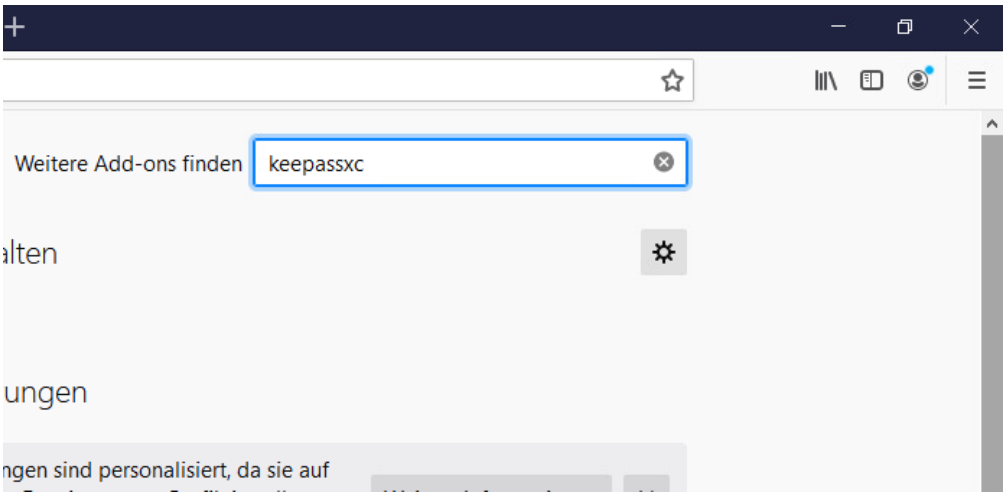
Klicken Sie im KeePassXC-Hauptfenster oben auf 1. das **Zahnrad**, dann links auf 2. **Browser-Integration**, dann oben auf 3. **Browserintegration aktivieren** und dann auf 4. **Firefox,** bestätigen Sie dann mit **OK**:



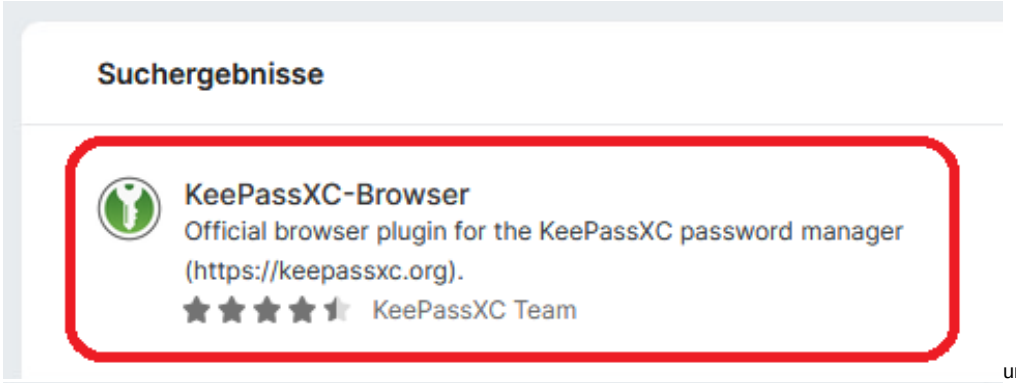
Öffnen Sie Firefox, klicken Sie oben rechts auf das Menü mit den drei Strichen , dann auf Add-ons



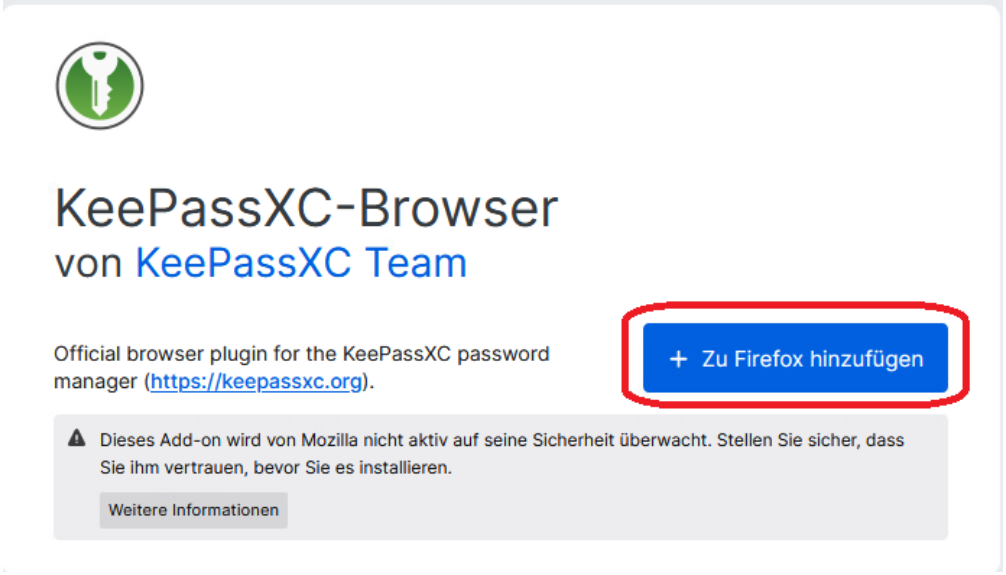
Geben Sie im Suchfeld oben rechts *KeePassXC* ein:



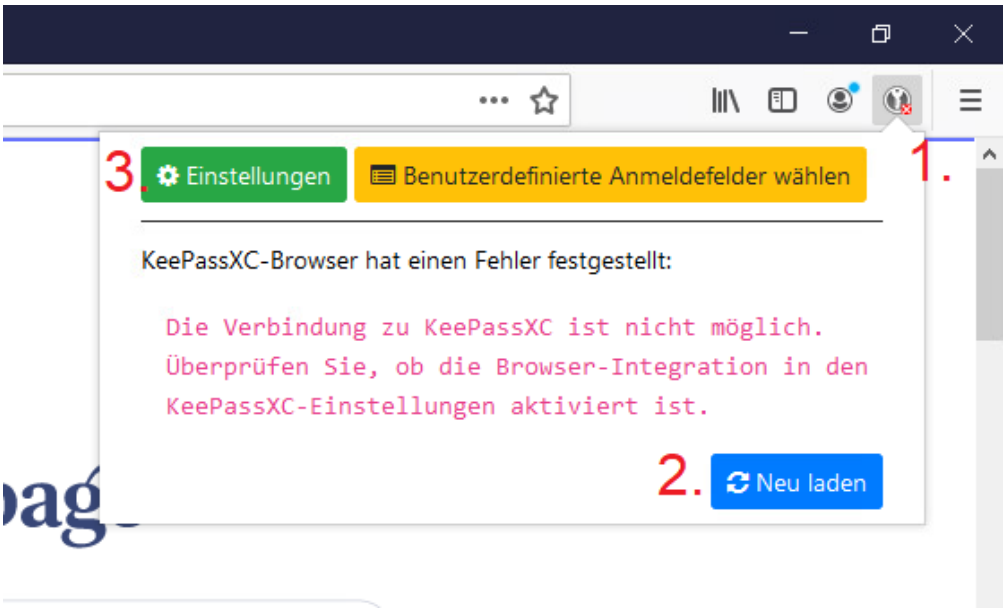
Klicken Sie auf **KeePassXC-Browser** und installieren Sie das Add-on:



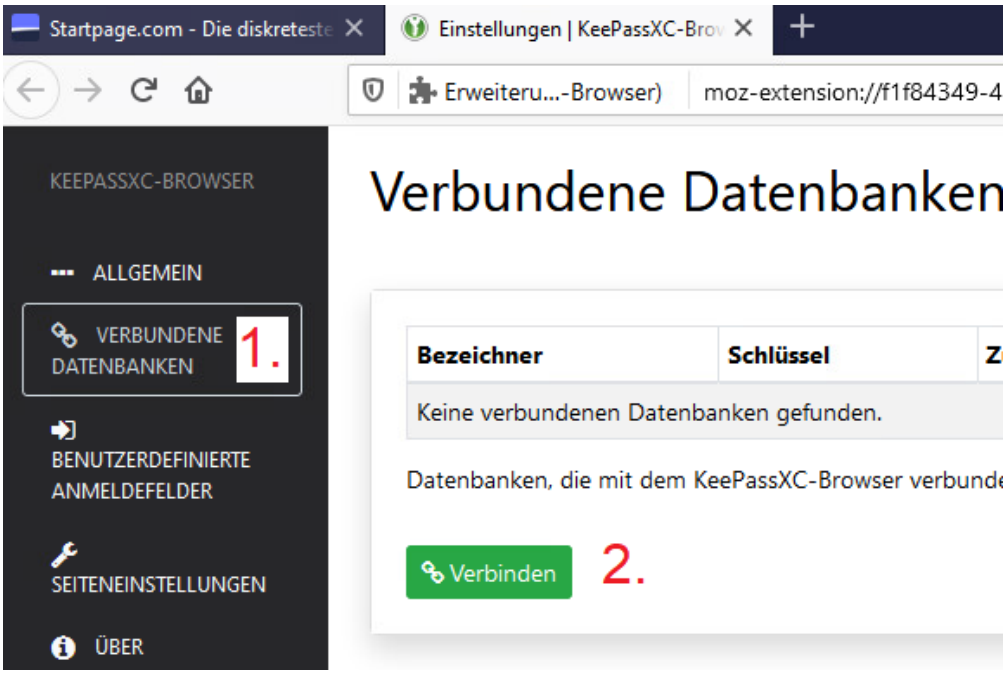
und dann



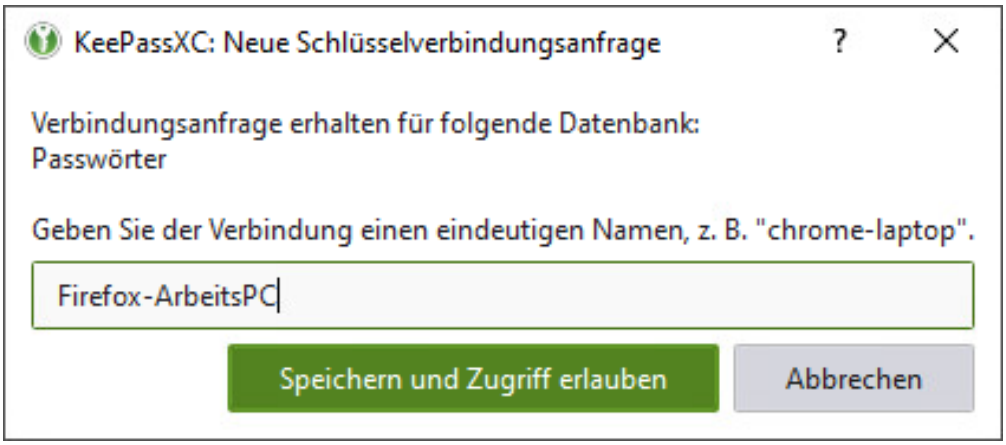
Klicken Sie in Firefox oben rechts auf das 1. neu erschienene **KeePassXC-Symbol**, dann auf 2. **Neu Laden** und dann auf 3. **Einstellungen**:



Klicken Sie in den Einstellungen des Browser Add-ons links auf 1. **Verbundene Datenbanken** und dann 2. auf **Verbinden**:

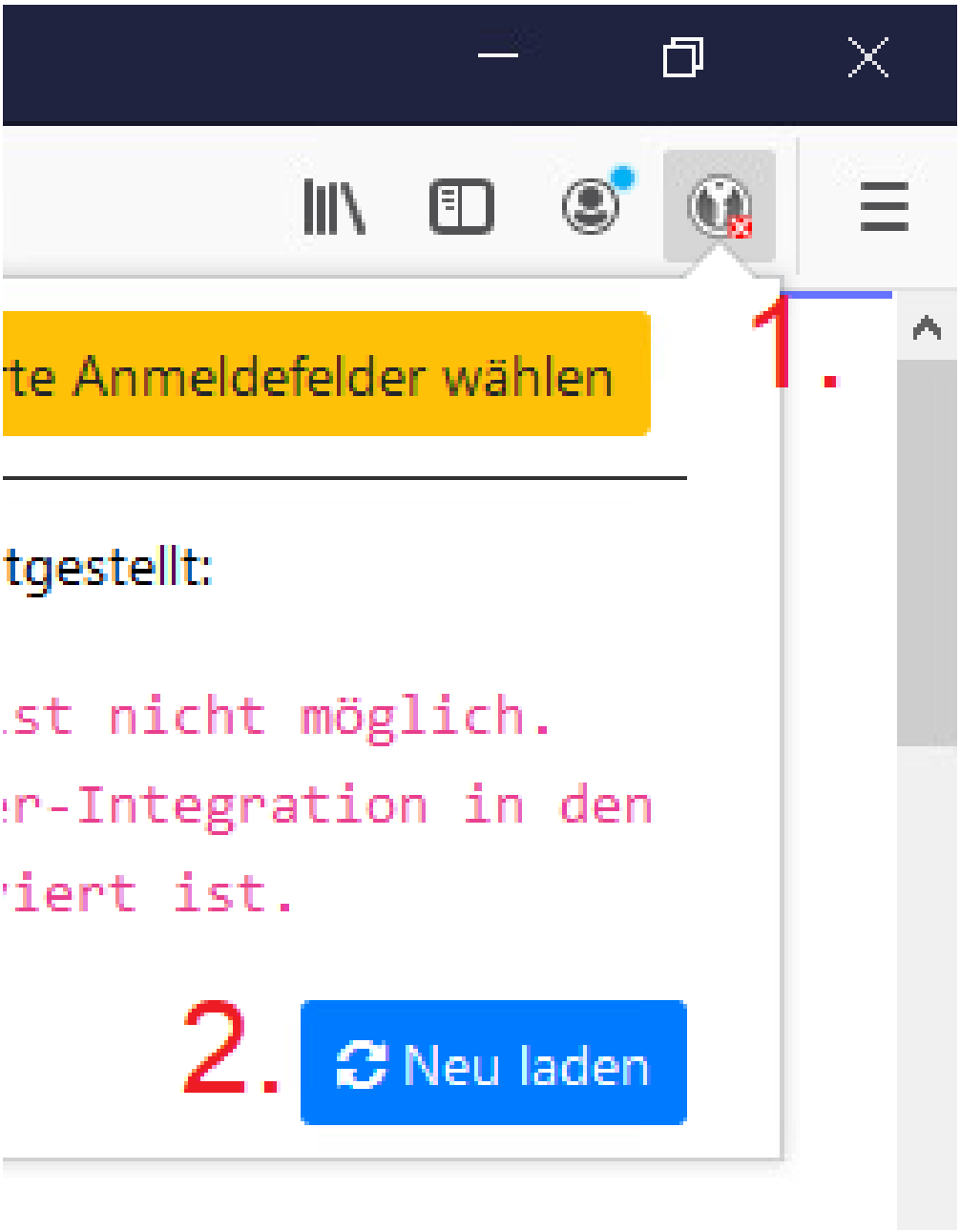


Geben Sie der Verbindung zwischen diesem einen Browser und der KeePass-Datenbank einen für Sie verständlichen Namen:



Dass die Verbindung zwischen Browser und entsperrter Datenbank funktioniert, erkennen Sie im Browser oben rechts am grünen KeePassXC-Symbol.

Sollte das Symbol grau sein und ein rotes Kreuzchen zeigen, dann bedeutet das in der Regel, dass die Datenbank gesperrt ist. In dem Fall **entsperren Sie die Datenbank** über das KeePassXC-Hauptfenster und klicken Sie anschließend (im Browserfenster) in der KeePassXC-Erweiterung auf **Neu Laden:**



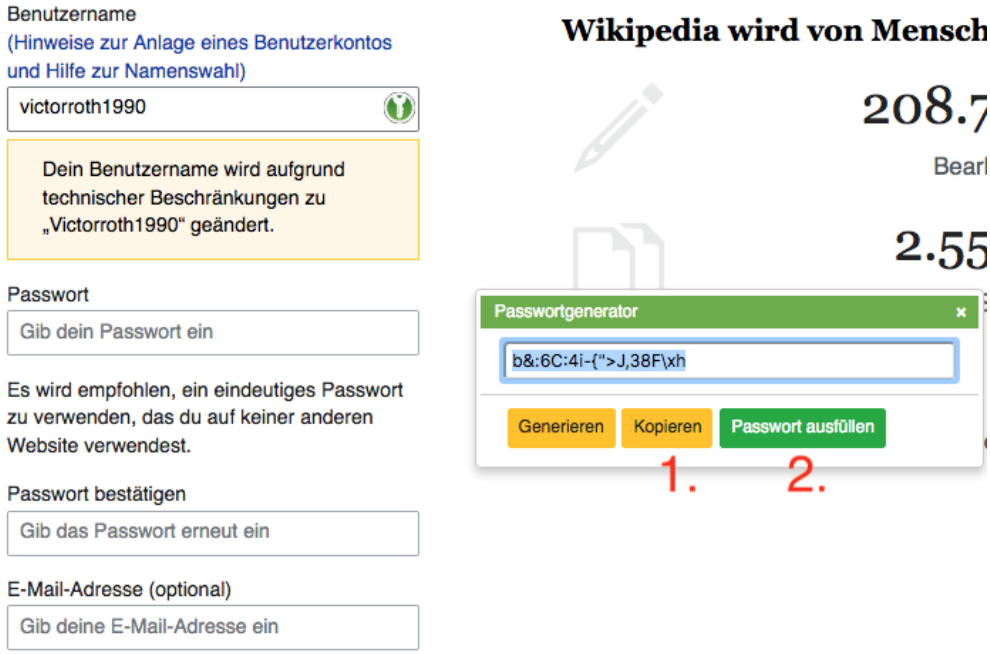
KeePassXC mit Browser-Add-on verwenden

Im folgenden wird angenommen, dass Sie an dieser Stelle die Browserintegration von KeePassXC bereits eingerichtet haben und die Datenbank entsperrt ist. Neben dem oben beschriebenen Weg zur Eintragung von Zugangsdaten zur KeePassXC-Datenbank bietet die KeePassXC-Browsererweiterung Komfortfunktionen. Sollten diese auf einigen Websites versagen, so können Sie stets den oben beschriebenen Weg nutzen.

Eintrag mittels Browsererweiterung automatisch erzeugen

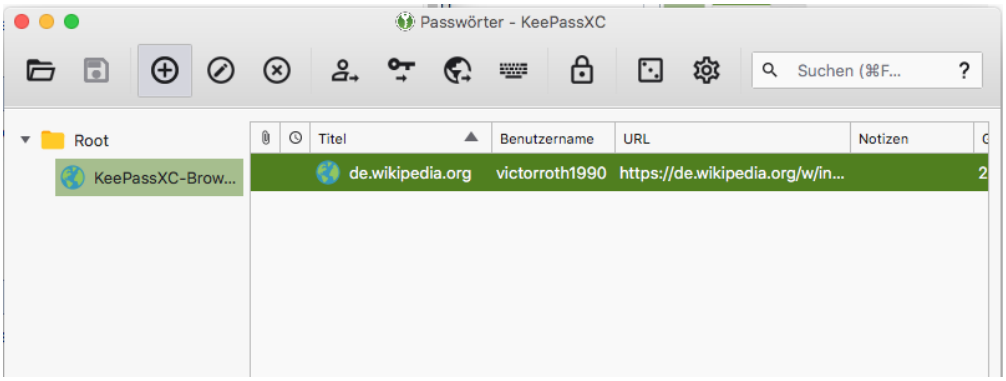
Bei entsperrter Datenbank können Sie sich auf einer Website wie gewohnt einloggen oder neu erzeugen. Füllen Sie Benutzername, Mailadresse und ggf. andere Pflichtfelder bis auf das Passwortfeld aus. Klicken Sie mit der rechten Maustaste ins Passwortfeld, dann auf KeePassXC und dann auf Passwortgenerator.

Das hier generierte Passwort ist einzigartig und sicher. 1. kopieren Sie das Passwort in die Zwischenablage (vgl. nächster Unterabschnitt) und 2. klicken Sie auf **Passwort ausfüllen**:

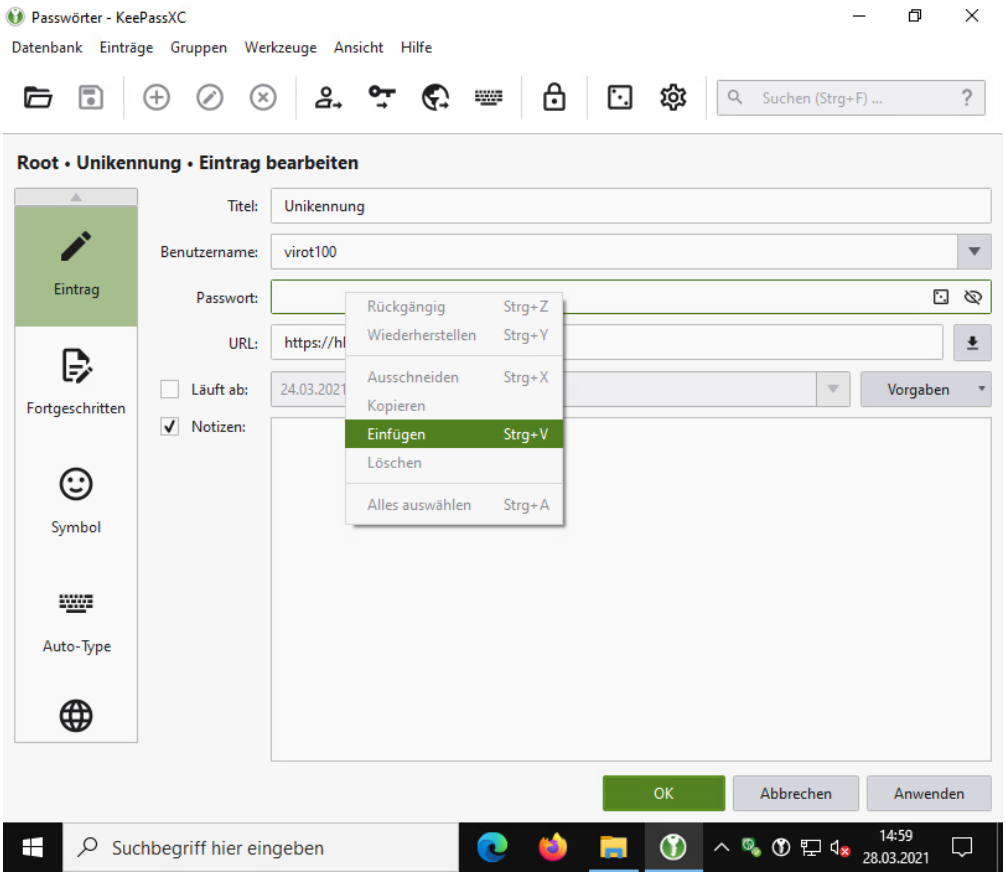


Bestätigen Sie dann die Registrierung auf der Website. Es erscheint dann am oberen Rand des Browsers ein Streifen ("Banner"), der die Speicherung der Zugangsdaten in die Passwortdatenbank über den Button **Neu** anbietet, den Sie für die Speicherung der neu erzeugten Zugangsdaten klicken müssen.

Im KeePassXC-Hauptfenster unter der Rubrik KeePassXC-Browser (mit Weltkugelsymbol) muss nun ein neuer Eintrag mit den neuen Zugangsdaten erscheinen.



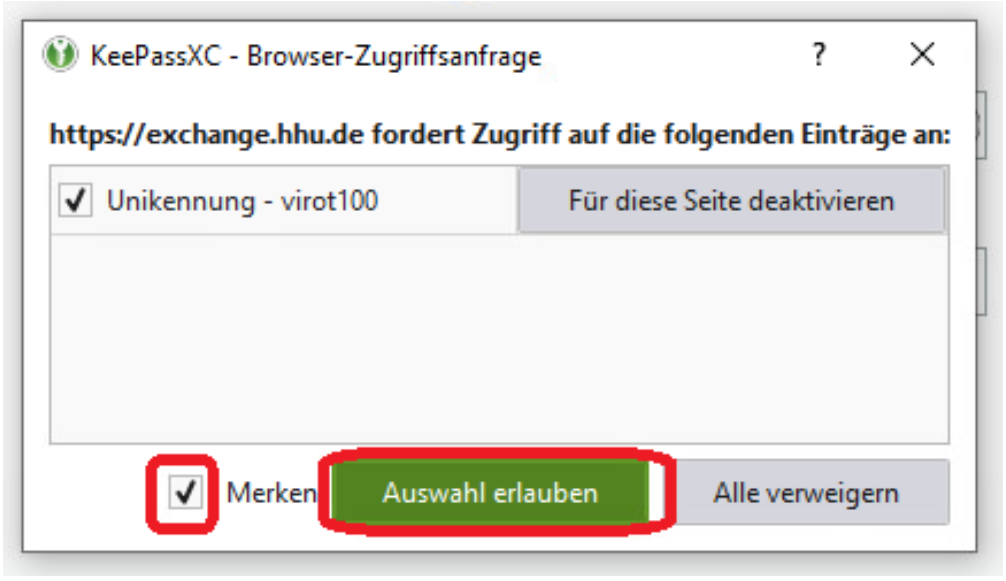
Sollten die Zugangsdaten nicht gespeichert worden sein, so können Sie die Zugangsdaten noch wie oben beschrieben manuell ablegen:



Eintrag aufrufen

Bei entsperrter Datenbank erlaubt die Autotype-Funktion im Browser in der Regel das automatische Einfügen passender Zugangsdaten. KeePassXC erkennt in der Regel auf Websites die Felder, in denen Benutzername bzw. Mailadresse und Passwort eingegeben werden müssen und zeigt im Feld ein grünes Symbol.

Bei der erstmaligen Verwendung von KeePassXC auf einer Website muss die Autotype-Funktion für diese Website genehmigt werden:



Danach können die Zugangsdaten automatisch eingetragen werden, wobei ggf. ein Klick auf das grüne Symbol im Feld für Benutzername/Passwort erforderlich ist:

Sollte dies aus irgendeinem Grund nicht funktionieren oder sollten Sie die Browserintegration nicht eingeschaltet haben, so können Sie KeePassXC, wie oben beschrieben, auch manuell nutzen.

Mobilgeräte

Stand 2021 empfiehlt das Entwicklerteam von KeePassXC für Smartphones und Tablets folgende Apps:

- Für Android: KeePassDX und KeePass2Android
- Für iOS: Strongbox und KeePassium

Der Verfasser hat KeePassium erfolgreich im Einsatz mit der Sciebo-App getestet. Unter iOS ist die Usability aufgrund der Integration in das Betriebssystem etwas schlechter als die von iCloud Keychain, aber auch für den täglichen Gebrauch ausreichend.

Support bei Rückfragen

Bei Fragen bezüglich der Verwendung von KeePassXC wenden Sie sich jederzeit an:

- helpdesk@hhu.de bzw. +49 211 81 10111
- it-support-zuv@hhu.de