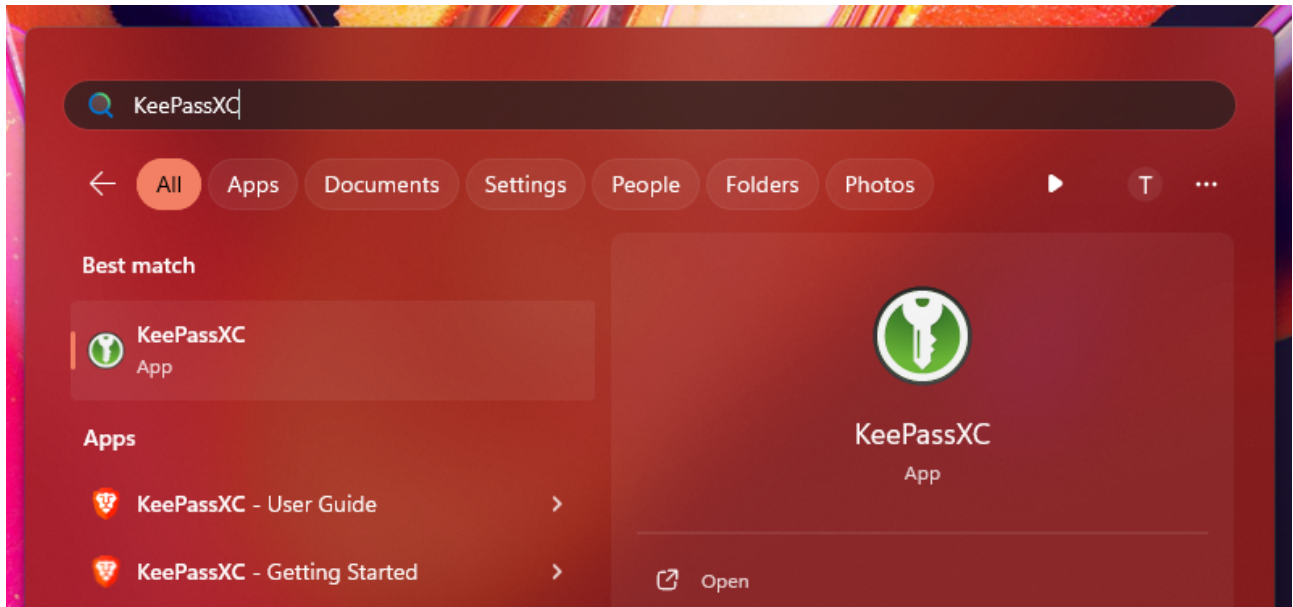
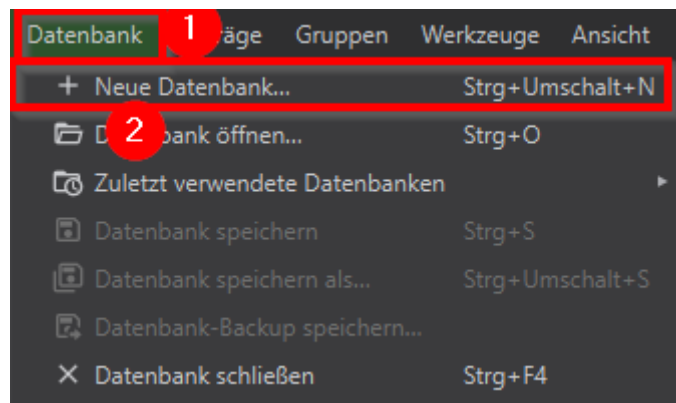


Verwendung & Einrichtung von KeePassXC Passwort-Manager mit Autofill für Browser

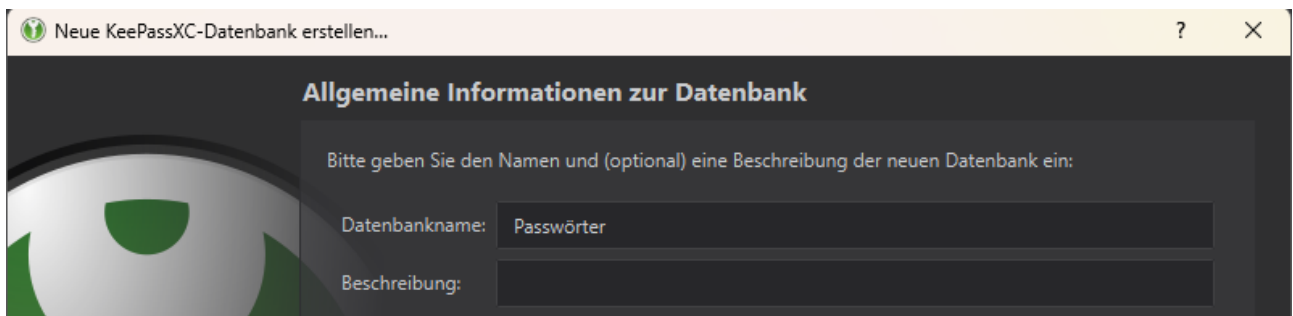
1. KeePassXC über das Windows Startmenü öffnen



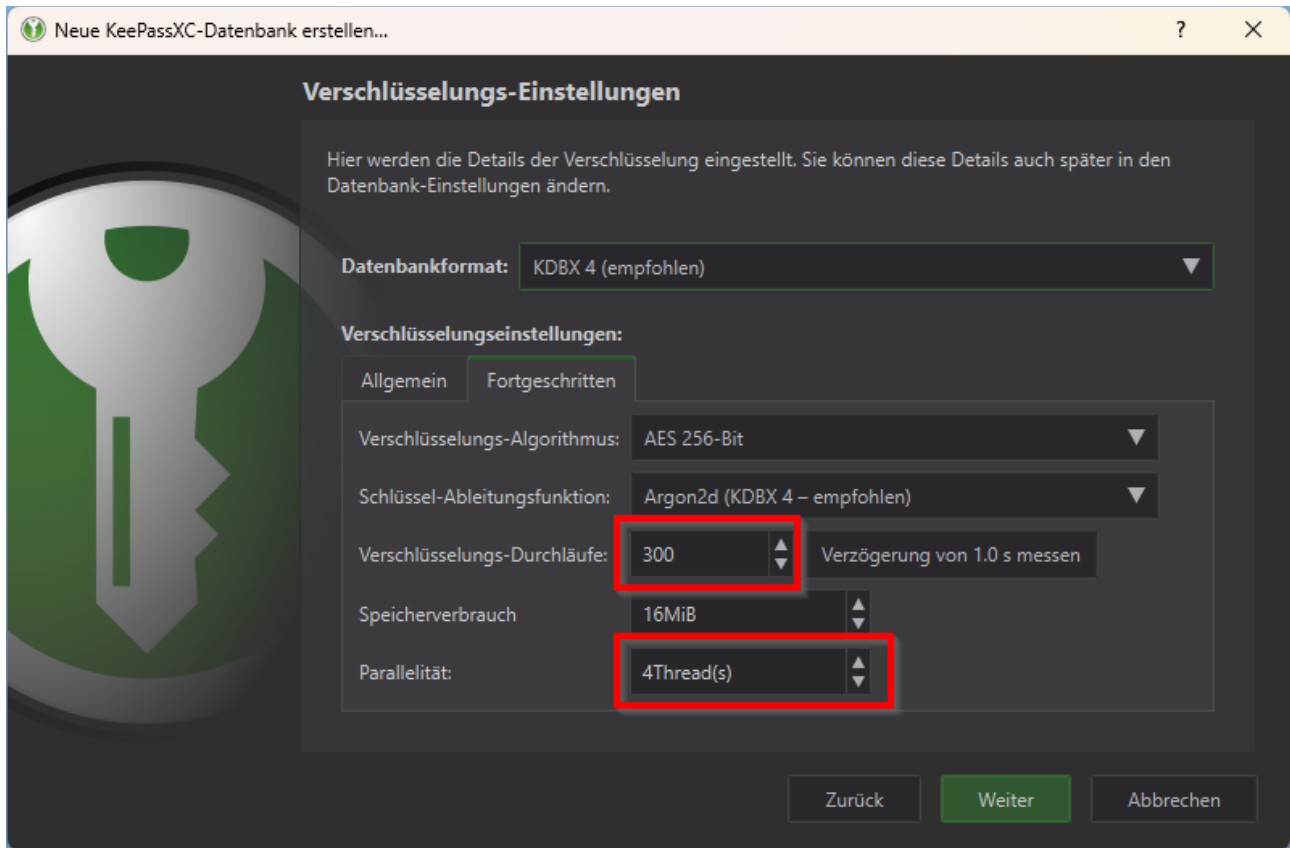
2. Falls noch nicht vorhanden, neue Datenbank anlegen



3. Der Datenbank einen Namen geben



4. Verschlüsselungs-Einstellungen festlegen

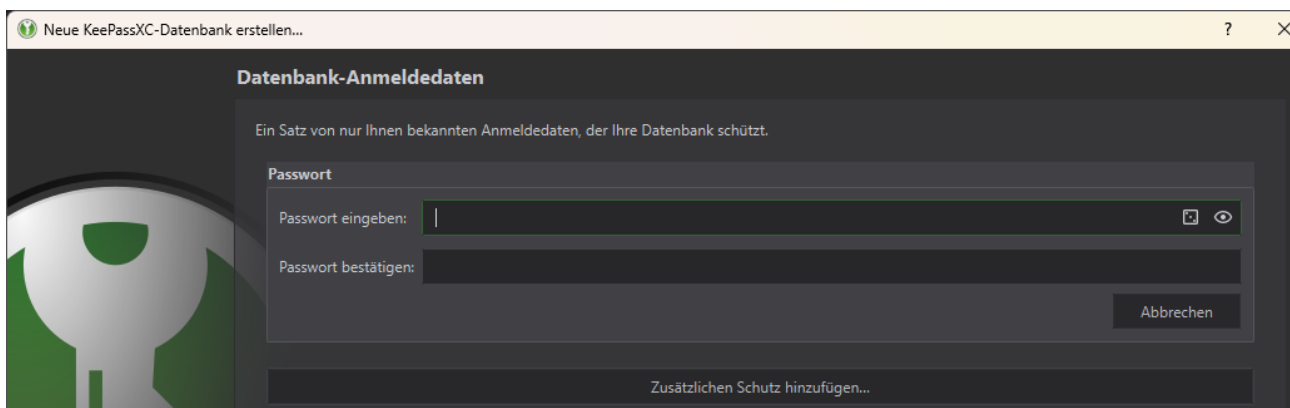


The screenshot shows the 'Verschlüsselungs-Einstellungen' (Encryption Settings) window in KeePassXC. The window title is 'Neue KeePassXC-Datenbank erstellen...'. The main heading is 'Verschlüsselungs-Einstellungen'. Below it, a text box says: 'Hier werden die Details der Verschlüsselung eingestellt. Sie können diese Details auch später in den Datenbank-Einstellungen ändern.' The 'Datenbankformat:' dropdown is set to 'KDBX 4 (empfohlen)'. Under 'Verschlüsselungseinstellungen:', there are two tabs: 'Allgemein' and 'Fortgeschritten'. The 'Fortgeschritten' tab is active, showing several settings: 'Verschlüsselungs-Algorithmus:' is 'AES 256-Bit'; 'Schlüssel-Ableitungsfunktion:' is 'Argon2d (KDBX 4 – empfohlen)'; 'Verschlüsselungs-Durchläufe:' is '300' (highlighted with a red box); 'Speicherverbrauch' is '16MiB'; and 'Parallelität:' is '4Thread(s)' (highlighted with a red box). To the right of the iterations setting is a button 'Verzögerung von 1.0 s messen'. At the bottom are three buttons: 'Zurück', 'Weiter' (highlighted in green), and 'Abbrechen'.

5. Datenbank-Kennwort festlegen

- Kennwortlänge: mindestens 14 Zeichen
- Passwort mit einer Kombination aus:
 - Groß- und Kleinschreibung
 - Zahlen
- Sonderzeichen

→ dieses Passwort UNBEDINGT gut aufbewahren da es keine Möglichkeit gibt, dieses Passwort bei einem Verlust wiederherzustellen!



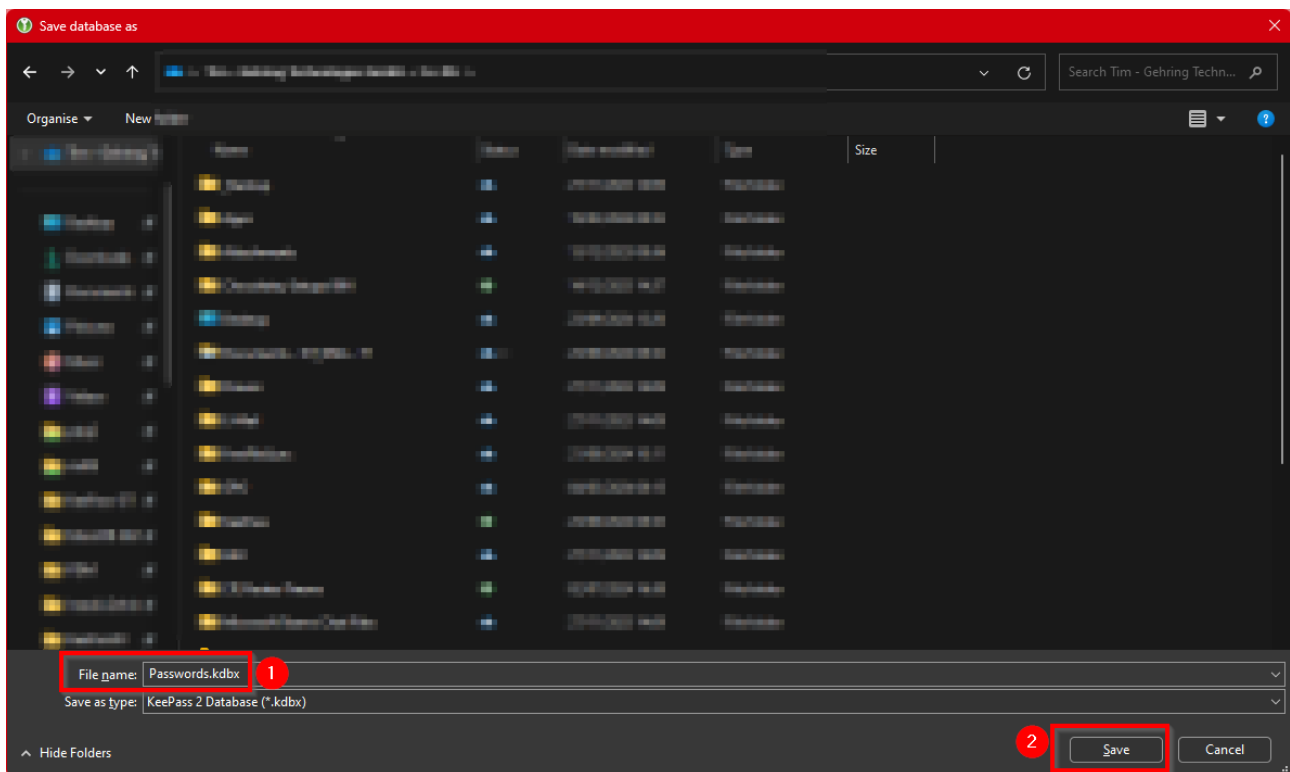
The screenshot shows the 'Datenbank-Anmeldedaten' (Database Credentials) window in KeePassXC. The window title is 'Neue KeePassXC-Datenbank erstellen...'. The main heading is 'Datenbank-Anmeldedaten'. Below it, a text box says: 'Ein Satz von nur Ihnen bekannten Anmeldedaten, der Ihre Datenbank schützt.' Under the heading 'Passwort', there are two input fields: 'Passwort eingeben:' and 'Passwort bestätigen:'. The 'Passwort eingeben:' field has a small icon on the right. At the bottom right is a button 'Abbrechen'. At the very bottom is a link 'Zusätzlichen Schutz hinzufügen...'.

6. Datenbank speichern

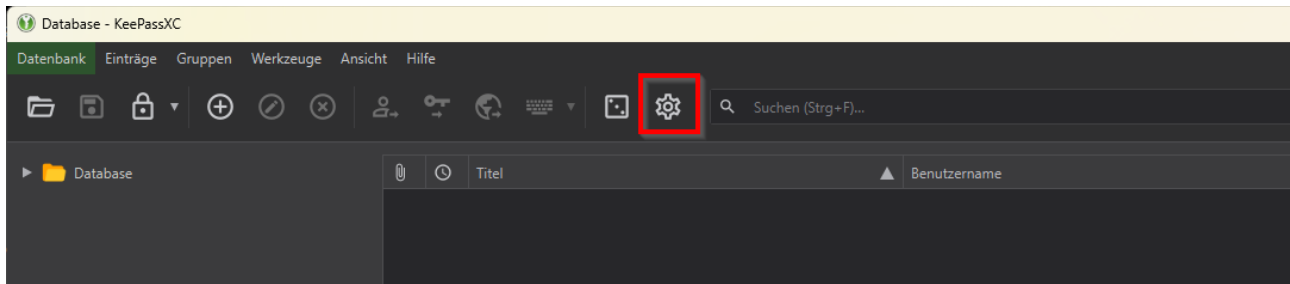
→ Datenbank-Datei **UNBEDINGT** an einen Speicherort ablegen der gesichert wird, damit die Datenbank bei Verlust oder Defekt des Rechners weiterhin verfügbar ist!

gesicherte Speicherorte sind z.B.:

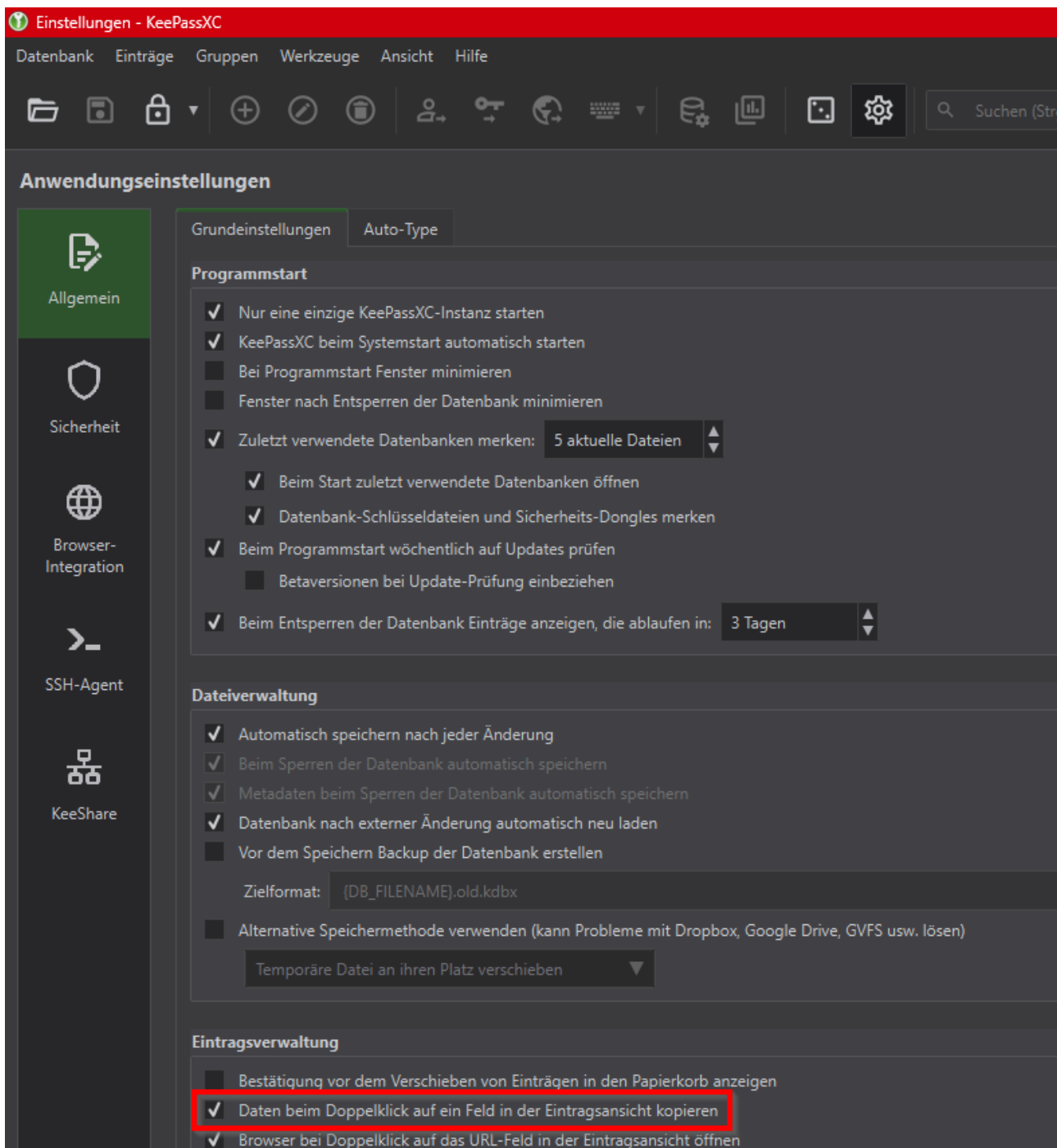
- Cloud (z.B. OneDrive)
 - Zugang zur Cloud muss unabhängig von dieser Passwort-Datei möglich sein!
 - z.B. geschäftliches OneDrive = Zugang kann über die IT erfolgen & zurück gesetzt werden
- Netzlaufwerke



7. Einstellungen öffnen



8. Einstellungen setzen





Anwendungseinstellungen



Allgemein



Sicherheit



Browser-
Integration



SSH-Agent



KeeShare

Timeouts

- ☒ Zwischenablage leeren nach 10 sek
- ☐ Datenbanken sperren nach Inaktivität von 240 sek
- ☐ Suchabfrage löschen nach 5 min

Optionen sperren

- ☒ Schnelle Datenbank-Entsperrung aktivieren (Touch ID/Windows Hello)
- ☒ Datenbanken sperren, wenn Sitzung gesperrt oder Deckel zugeklappt wird
- ☐ Datenbanken sperren beim Minimieren des Fensters

Komfort

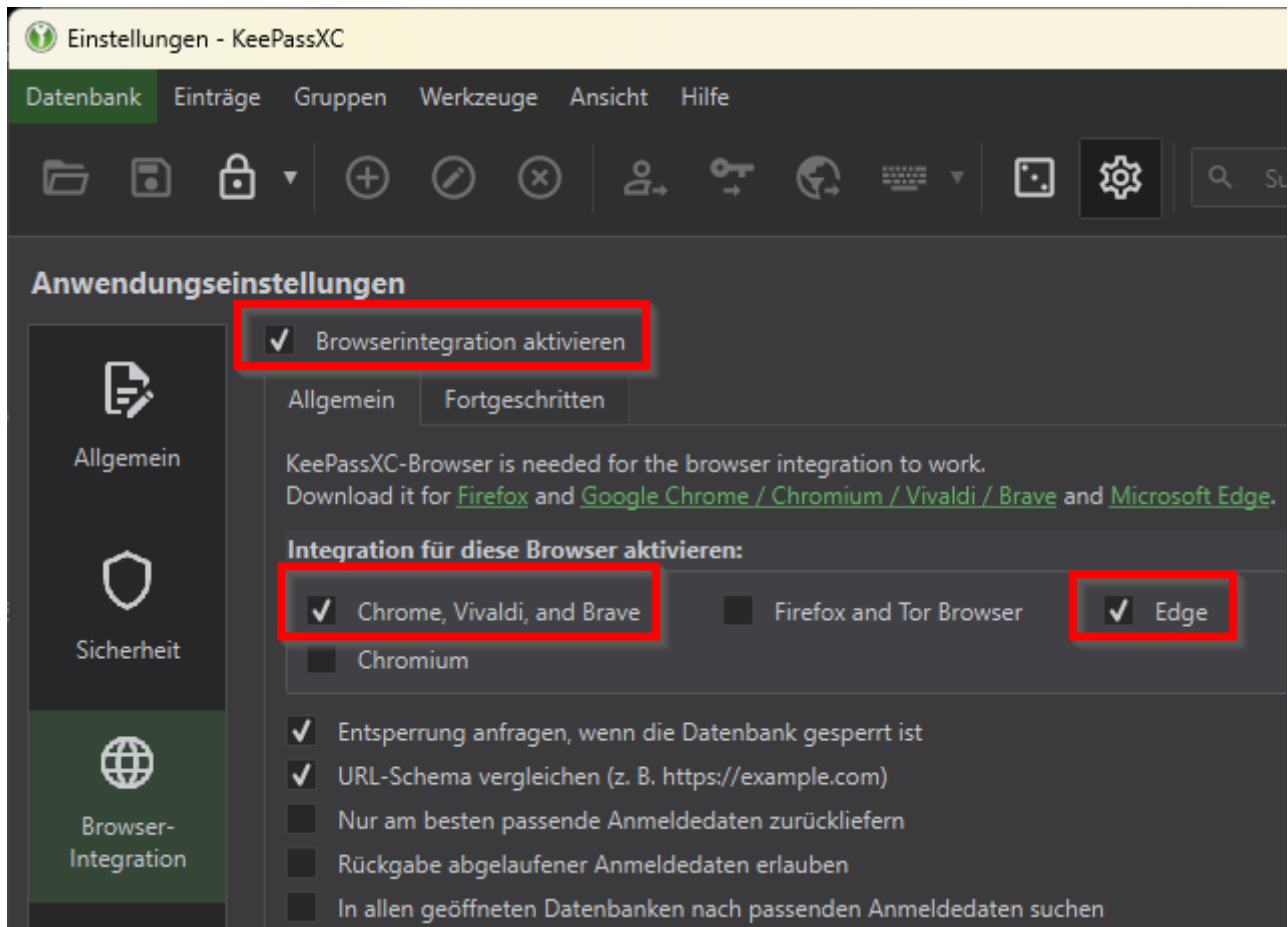
- ☐ Platzhalter für leere Passwortfelder verwenden
- ☒ Passwörter beim Bearbeiten verstecken
- ☒ Passwörter im Eintrags-Vorschau-Panel verstecken
- ☒ TOTP in der Eintragsvorschau verstecken
- ☐ Notizen in der Eintragsvorschau verstecken

Datenschutz

- ☒ DuckDuckGo zum Herunterladen von Webseitensymbolen verwenden

9. Browser Erweiterung aktivieren

→ Je nach verwendetem Browser "Edge", "Chrome[...]" oder beides auswählen



10. Browser Erweiterung installieren

→ Je nach verwendetem Browser im oberen Screenshot klicken auf:

"Download it for [...]"

damit sich die Webseite der Browser-Erweiterung öffnet:

- Microsoft Edge
- Google Chrome[...]

Im Browser dann die Erweiterung installieren.

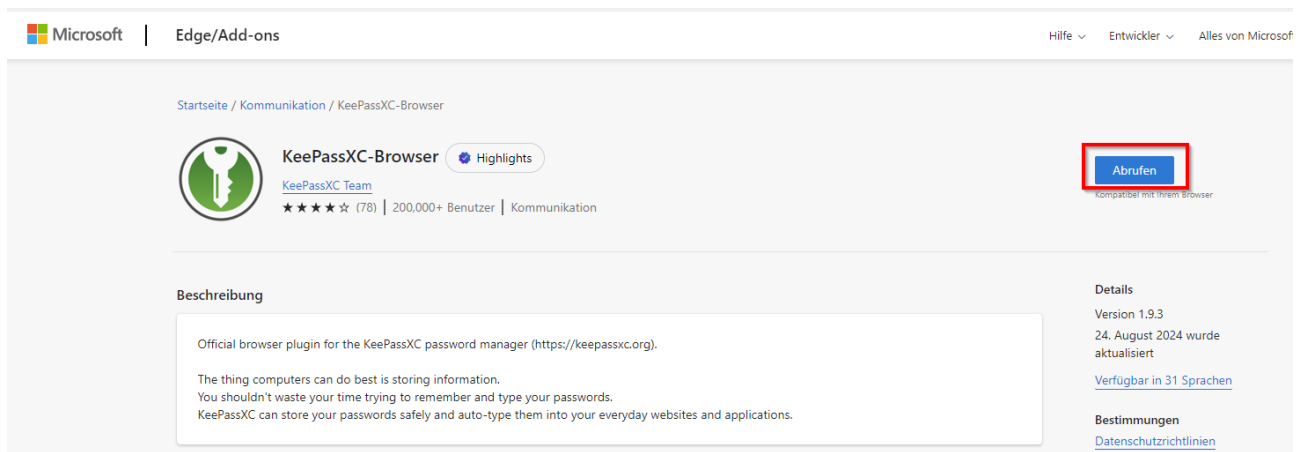
Alternativ hier die Links zu den Erweiterungen:

Edge:

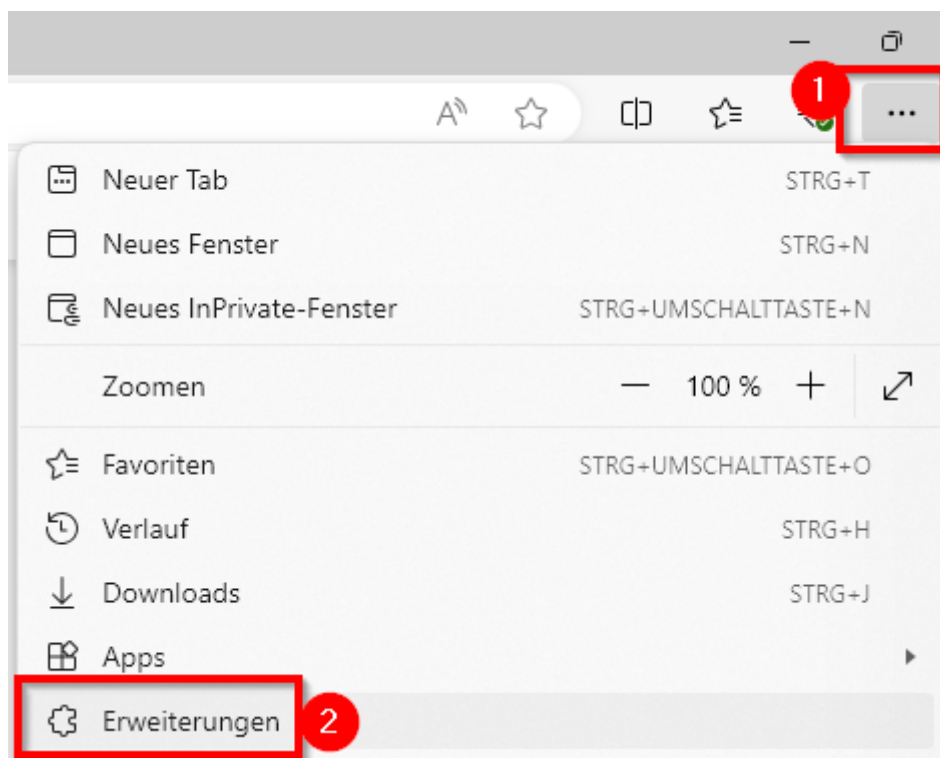
<https://microsoftedge.microsoft.com/addons/detail/keepassxcbrowser/pdfhmdngciaglkoonimfcmckehcpafo>

Chrome:

<https://chromewebstore.google.com/detail/keepassxc-browser/oboonakemofpalcgghocfoadofidjkkk>

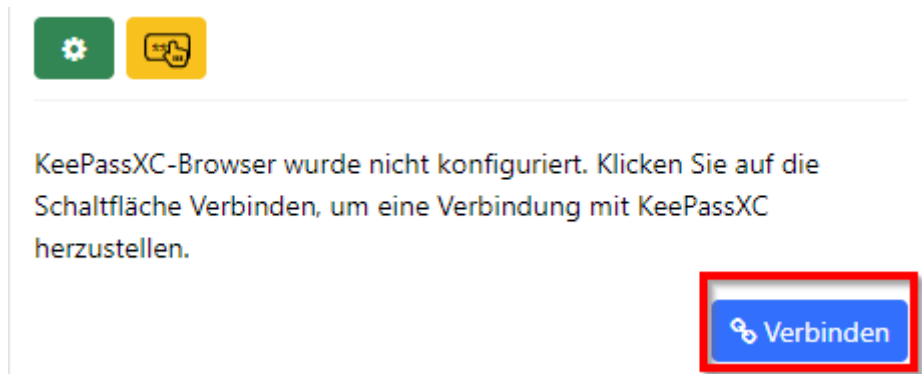


11. KeePassXC Erweiterung im Browser öffnen



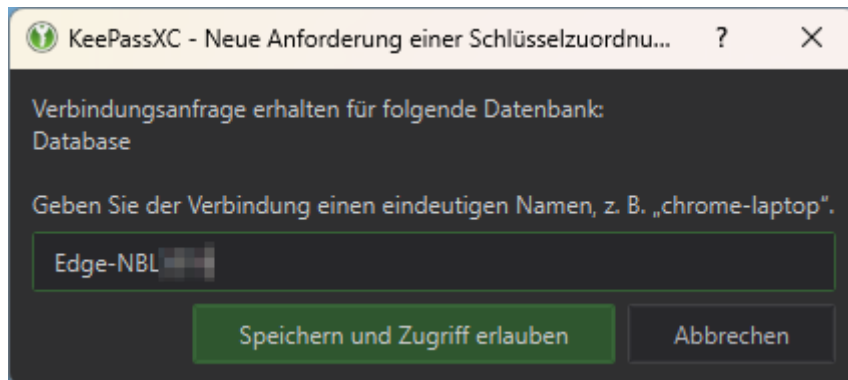
12. KeePassXC Browser Erweiterung mit der KeePassXC Datenbank verbinden

→ Datenbank muss dazu geöffnet und entsperrt sein

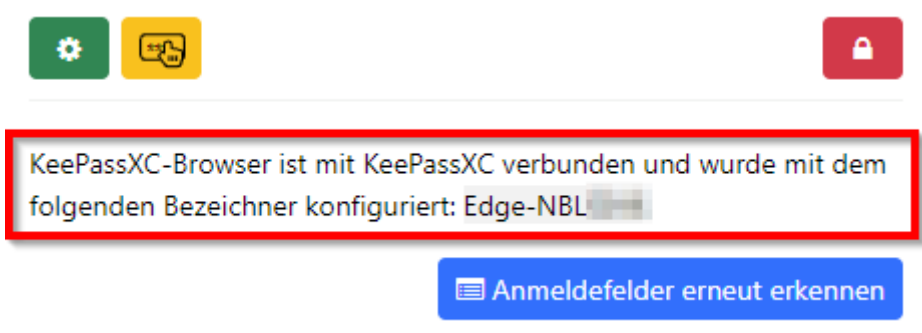


13. Verbindung zwischen Datenbank und Browser einen Namen geben

→ z.B.: [Browser]-[Rechnername], Bsp.: Edge-OFL5320



14. Verbindung zwischen Datenbank und Browser überprüfen



Verwendung von KeePassXC:

Bsp.: KeePassXC Eintrag mit MFA Code anlegen

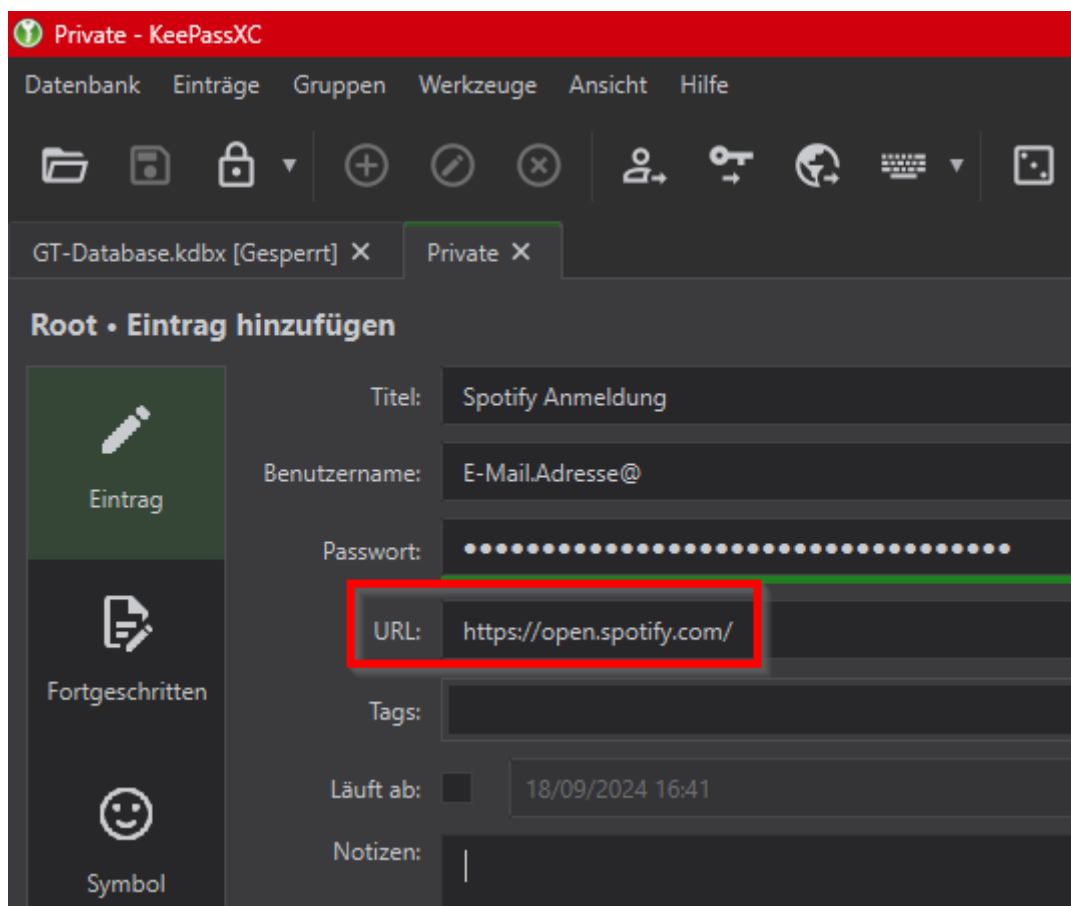
15. KeePass Eintrag anlegen (mit URL für Autofill im Browser)

→ wenn der KeePassXC Eintrag Anmeldedaten für eine Webseite enthält, muss im Feld URL die Webseite stehen, damit die Daten dort per Autofill ausgefüllt werden können

→ am besten die Startseite der Webseite verwenden (erste Seite die beim Aufruf einer Webseite erscheint)

Beispiel: Spotify

Startseite: <https://open.spotify.com/>



Zur Info:

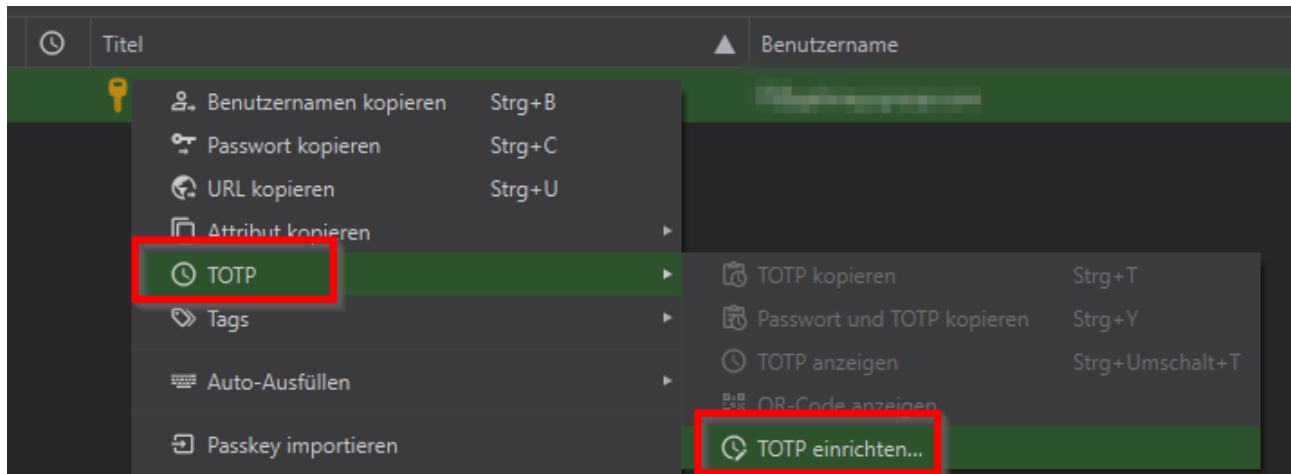
KeePassXC speichert die Datenbank nach jeder Änderung eines Eintrags beim Klicken auf "OK". Durch die Verschlüsselung der Datenbank benötigt das kurz Zeit (ca. 1-2s), währenddessen KeePass kurz "einfriert".

16. MFA Code in KeePass Eintrag hinterlegen

Für Webseiten, die eine MFA / 2FA* über eine Authenticator App verwenden (z.B. Microsoft Authenticator, Google Authenticator, WinAuth), kann KeePassXC auch die Erzeugung des MFA Codes übernehmen.

*MFA: Multifaktorauthentifizierung

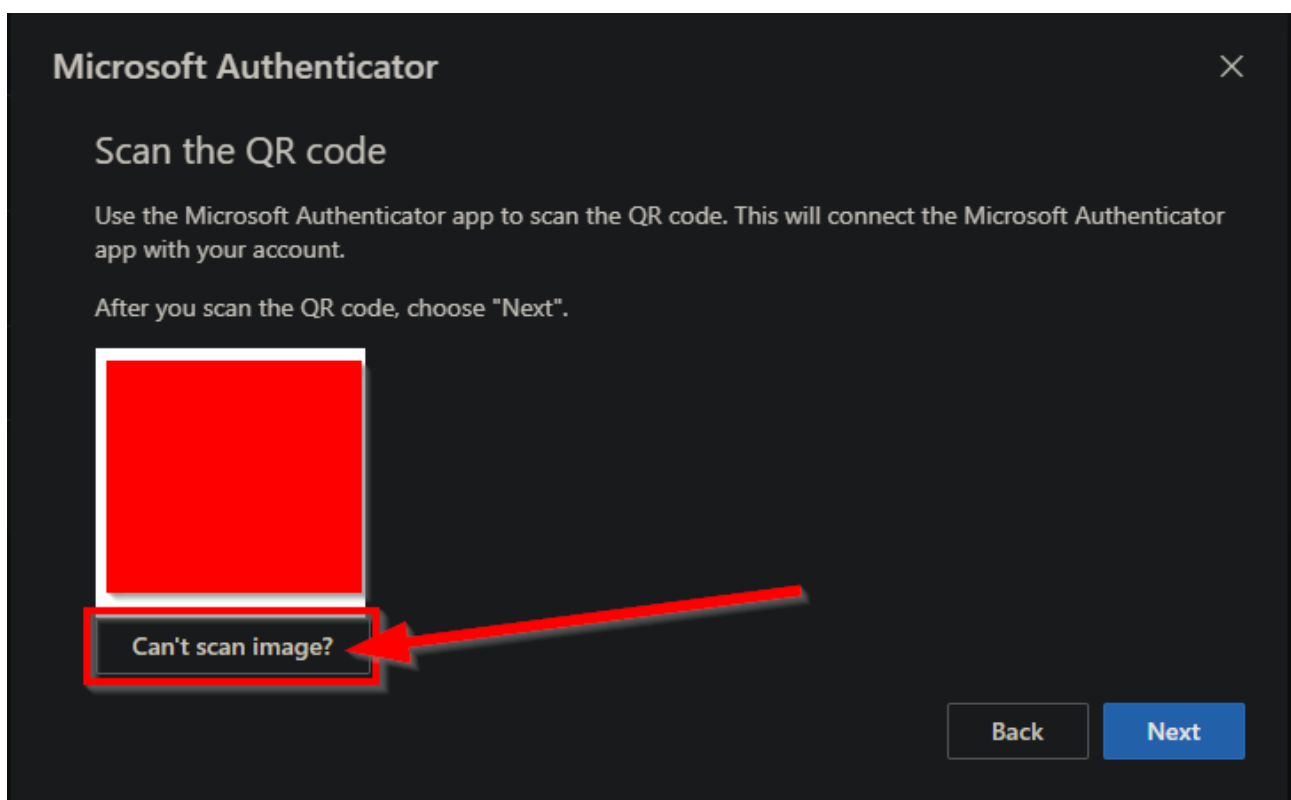
2FA: 2-Faktor-Authentifizierung



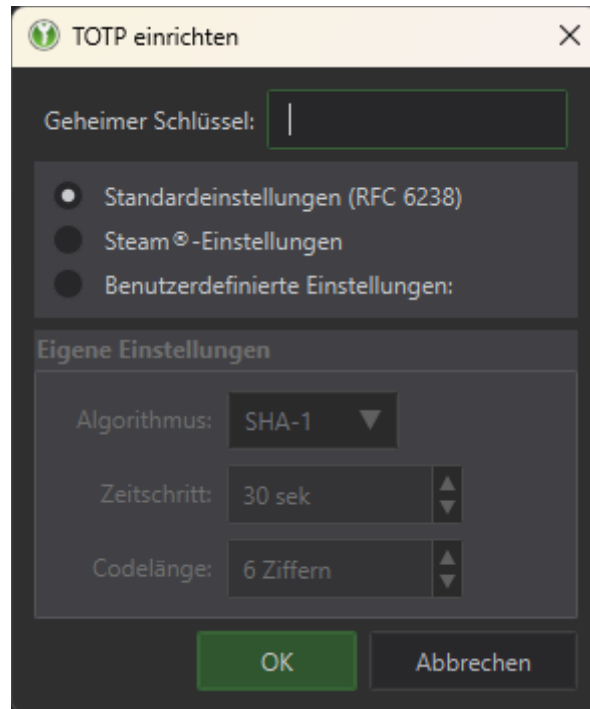
Bei Einrichtung einer MFA / 2FA auf einer Webseite wird meistens ein QR Code zum Abscannen mit einer Authenticator Smartphone App angezeigt.

Es gibt dann im Normalfall die Möglichkeit, sich den "Secret Key" über einen Button daneben anzeigen zu lassen. Der QR Code und der Secret Key enthalten die gleiche Information nur in anderer Form. KeePassXC benötigt zur Hinterlegung des MFA Codes allerdings den Secret Key.

Bei der Einrichtung der MFA im Microsoft Account (<https://aka.ms/MFASetup>) kann sich der Code z.B. so angezeigt werden:

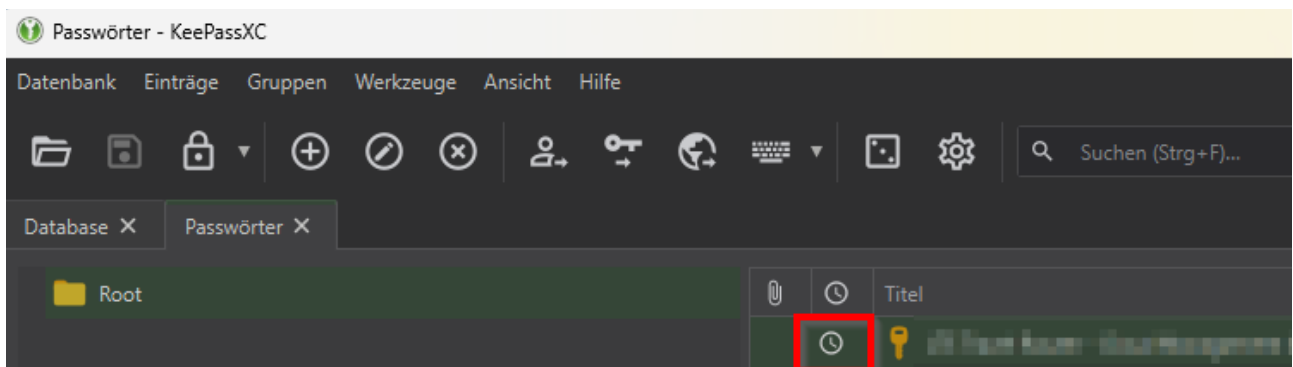


17. Secret Key für MFA in KeePassXC hinterlegen



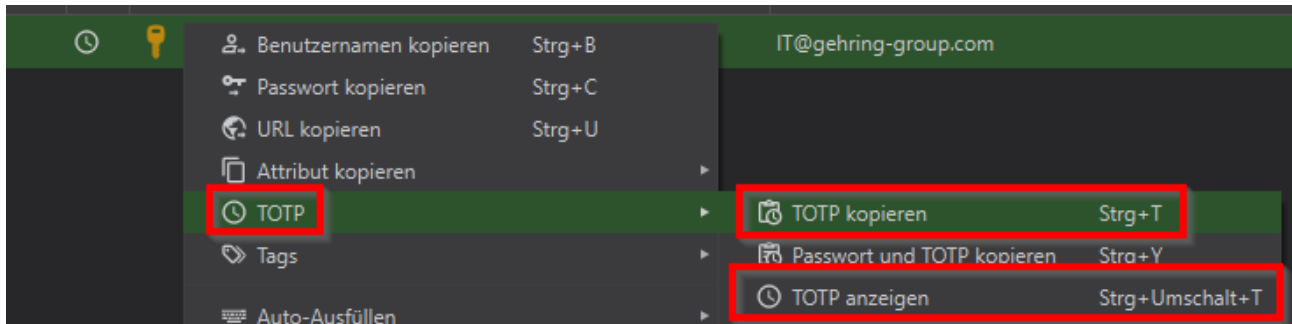
18. KeePassXC Eintrag mit MFA Key

→ wenn der Secret Key im KeePassXC Eintrag hinterlegt und gespeichert wurde, sieht man dann an diesem Symbol (Vgl. Screenshot) in der Liste der KeePassXC Einträge, dass dort zusätzlich ein MFA Code hinterlegt ist:



19. MFA Code anzeigen oder kopieren

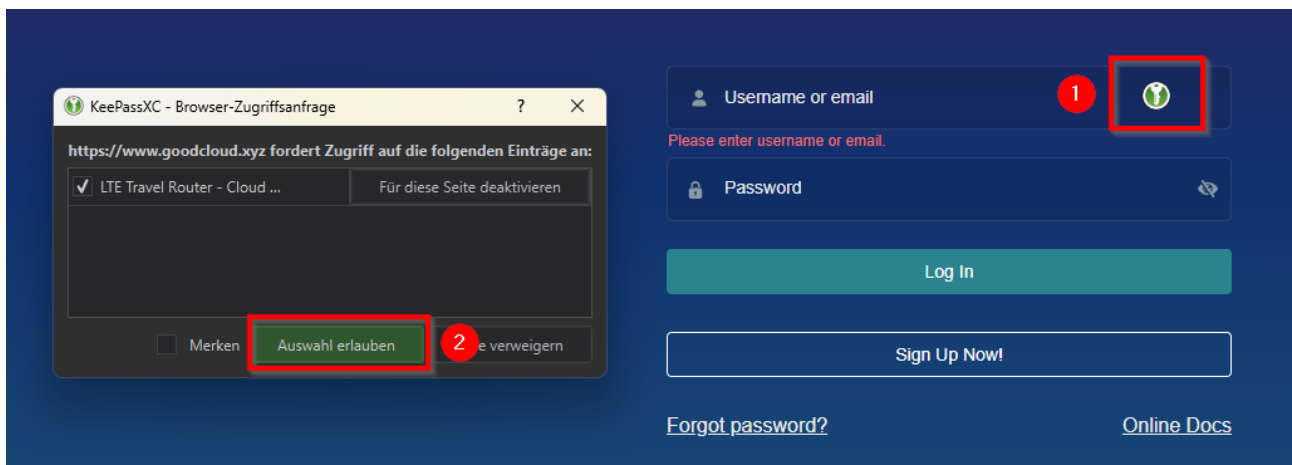
→ der aktuelle MFA Code kann einfach mit einem Doppelklick auf das Uhr-Symbol neben dem Eintrag (siehe Screenshot bei "KeePassXC Eintrag mit MFA Key") kopiert werden
Alternativ kann der Code auch so kopiert oder angezeigt werden:



20. Autofill (automatisches Ausfüllen der Anmeldedaten im Browser)

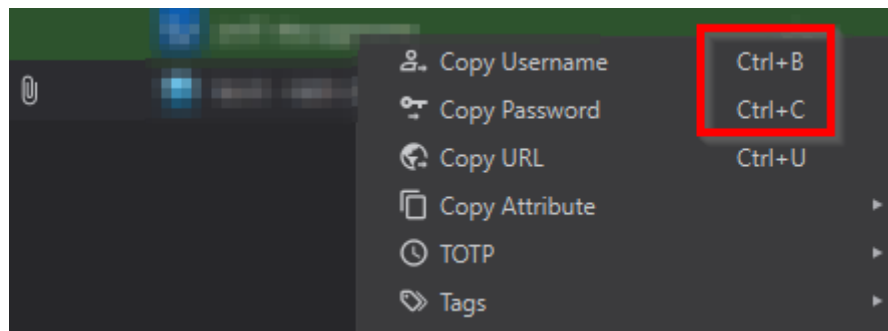
→ nach dem Klick auf (1) (Vgl. Screenshot) kommt zuerst eine Sicherheits-Abfrage von KeePassXC, damit der Zugriff auf den entsprechenden KeePassXC Eintrag für den Browser erlaubt wird

→ bei dieser Abfrage kann optional der Haken bei "Merken" gesetzt werden, damit diese Abfrage für diesen Eintrag in Zukunft nicht nochmal kommt:



→ alternativ können die Anmeldedaten auch über Hotkeys kopiert werden:
diese Daten werden dann kopiert und automatisch nach 10 Sekunden wieder aus der Zwischenablage gelöscht

- Username: Strg+B
- Passwort: Strg+C
- URL: Strg+U
- URL im Browser öffnen: Doppelklick auf das URL Feld



21. Automatisches Ausfüllen des MFA Codes

→ auch der MFA Code kann über die Autofill-Methode automatisch eingefügt werden:

