Nutzung von TOTP in KeePassXC

1. Übersicht

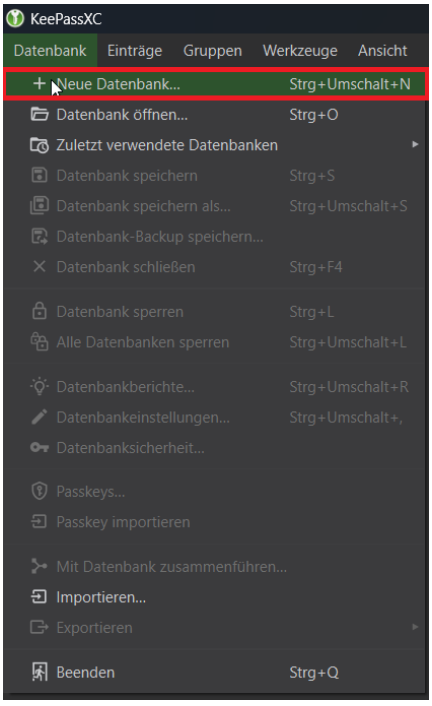
TOTP („Time-based One-Time Password“) ist eine Variante der Zwei-Faktor Authentifizierung welche auf Grundlage eines gemeinsamen Geheimnisses zwischen Dienst und Nutzer innerhalb fester Zeitfenster Einmalkennwörter generiert. Die Berechnung der Codes aus dem Geheimnis erfolgt auf Nutzerseite über einen „Authenticator“.

Um die TOTP „Authenticator“ Funktion von KeePassXC nutzen zu können, muss eine verschlüsselte und durch das Programm verwaltete Datenbank zum Eintragen der Geheimnisse genutzt werden.

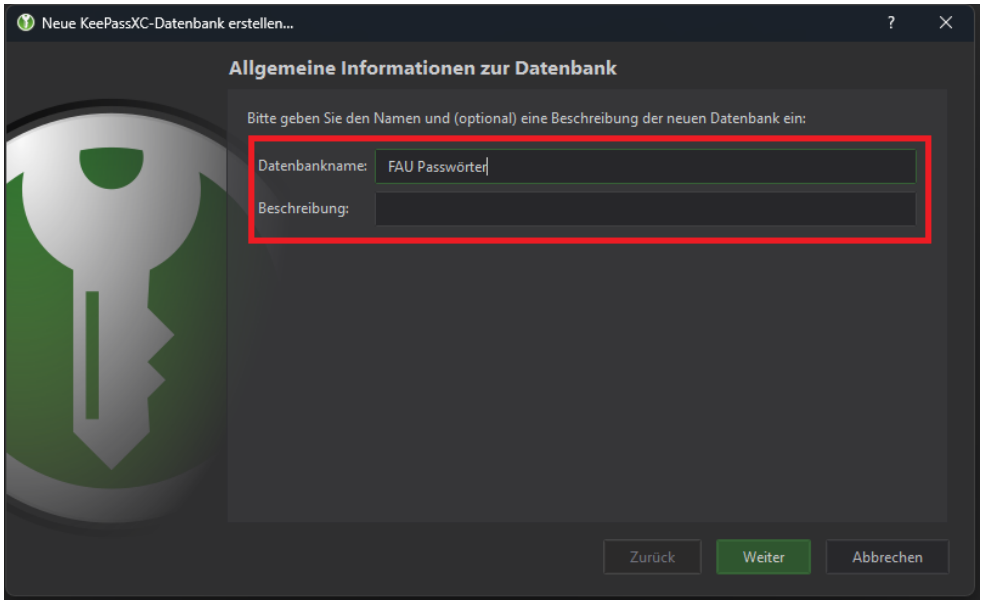
Wie das funktioniert, wird im anschließenden Kapitel erklärt.
Falls Sie KeePass schon mit einer Datenbank nutzen, können Sie dieses Kapitel überspringen.

2. Erstellen einer Datenbank

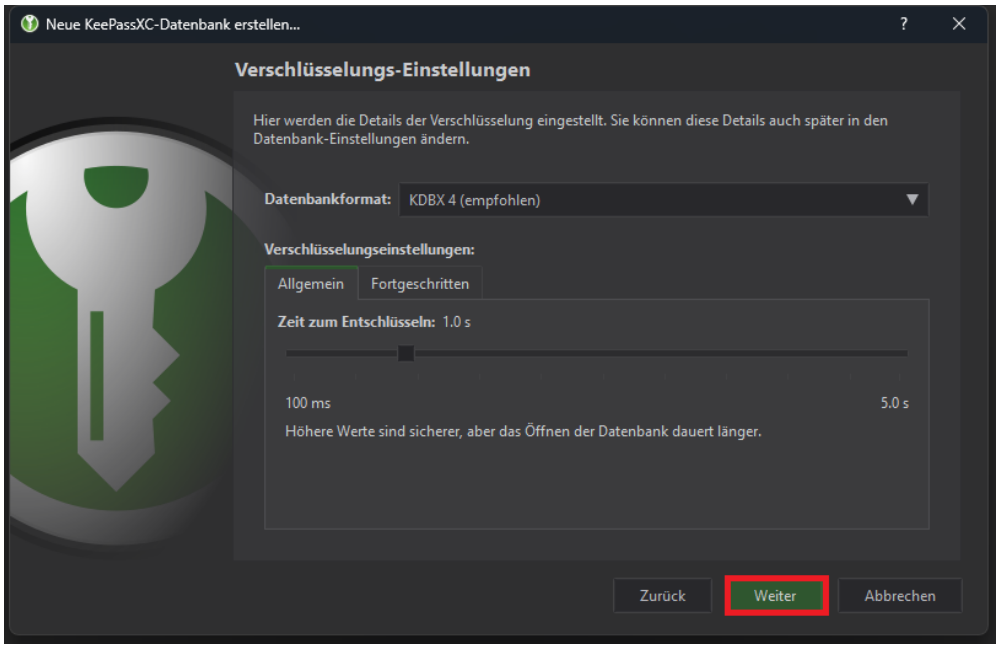
Um sich eine neue Datenbank zu erstellen, wählen Sie in der oberen Menüleiste im Karteireiter ***„Datenbank“*** den Eintrag ***„Neue Datenbank“.***



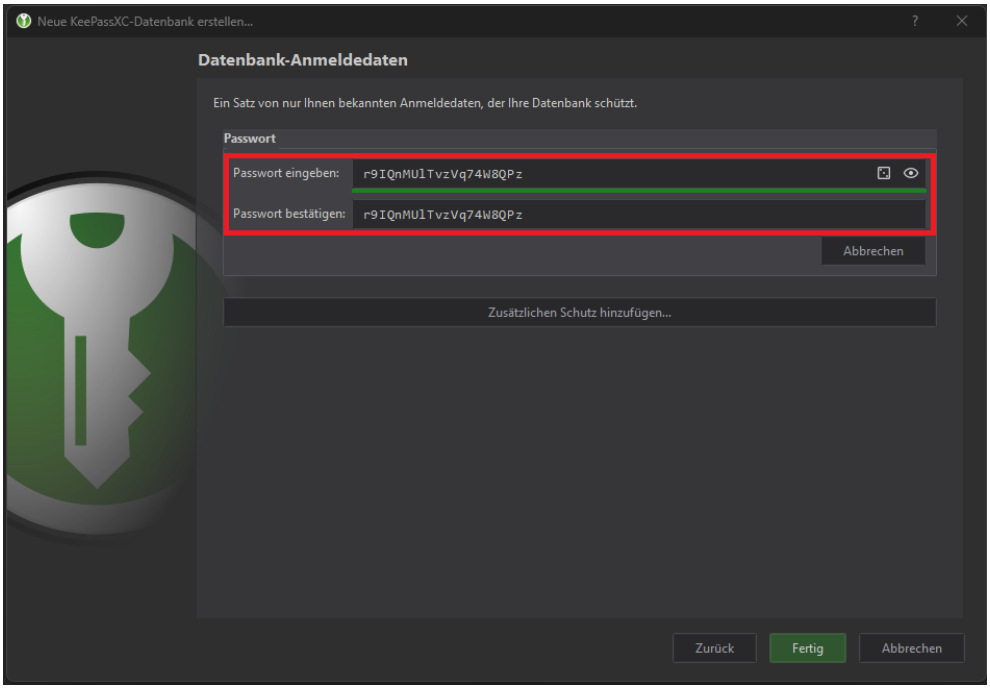
Im Anschluss kann ein Datenbankname sowie eine optionale Kurzbeschreibung festgelegt werden. Es empfiehlt sich, zumindest den Datenbanknamen aussagekräftig zu wählen. (*hier*: *„FAU Passwörter“*)



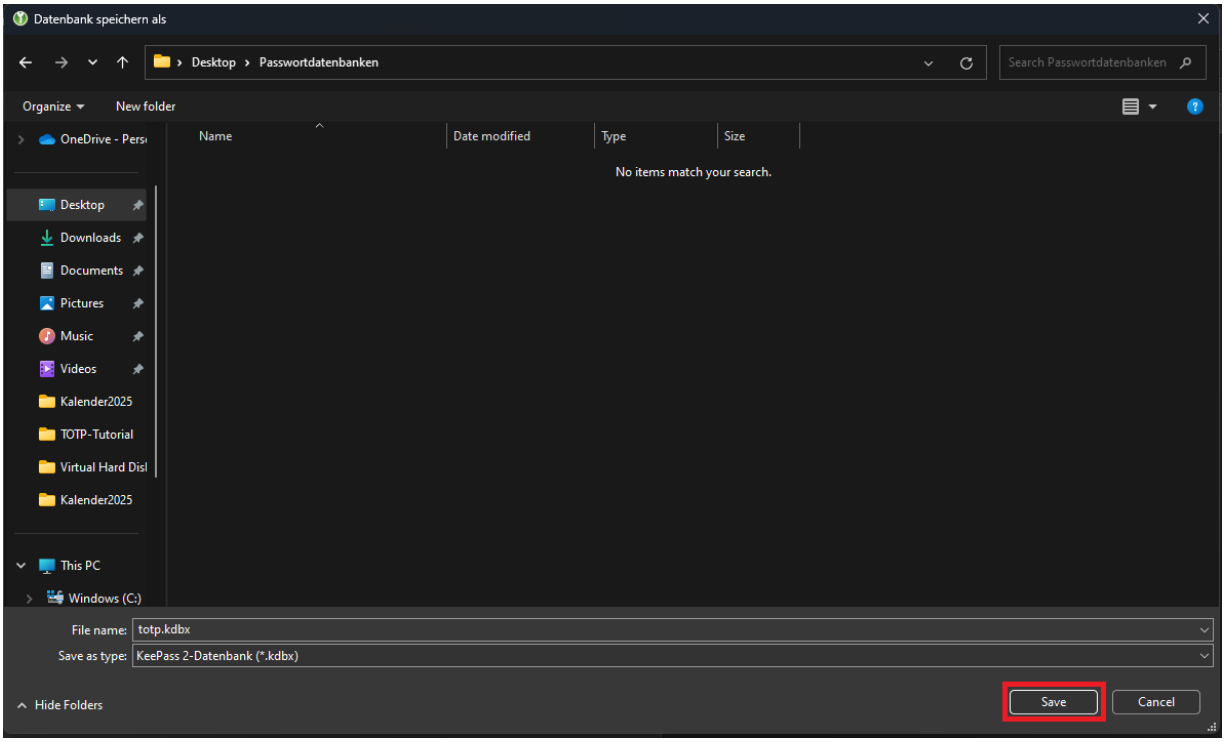
Die Voreinstellungen von KeePassXC zur Datenbankverschlüsselung können wie vorgeschlagen übernommen werden.



Das im Anschluss zu wählende Passwort sollte als Hauptschlüssel zum Entsperren der Datenbank möglichst sicher sein.

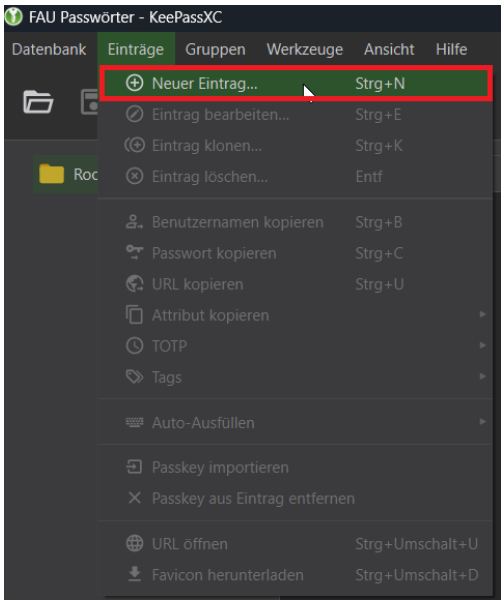


Danach kann die Datenbank an einem geeigneten Ort gespeichert werden.

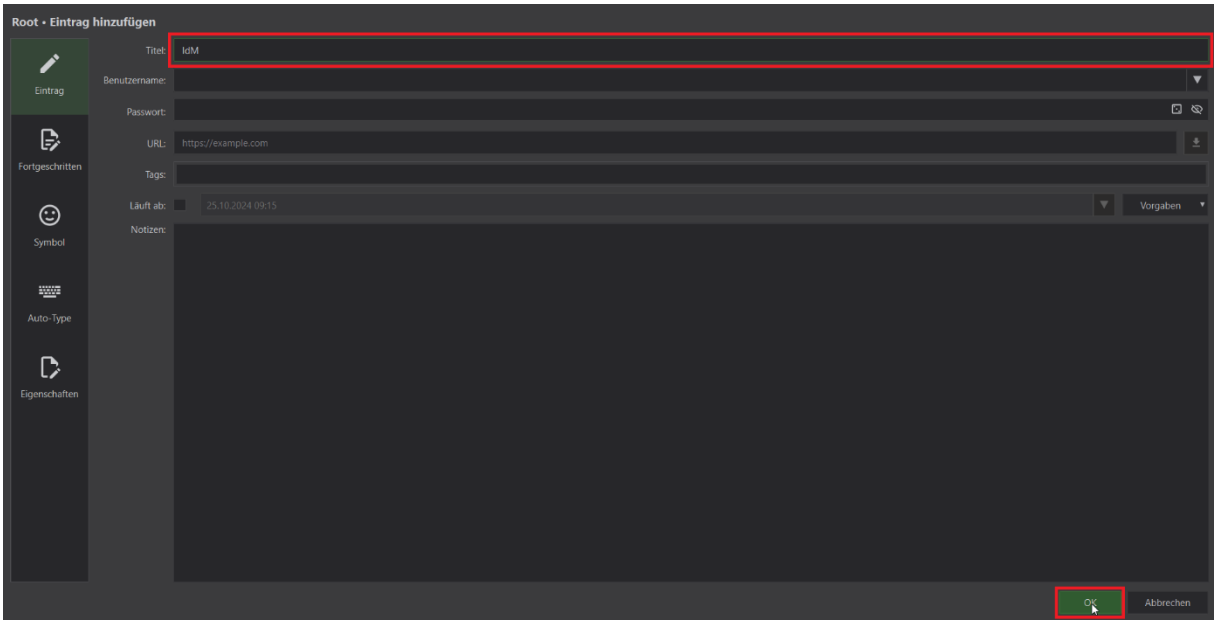


3. Konfiguration eines Datenbankeintrags mit einem TOTP-Secret

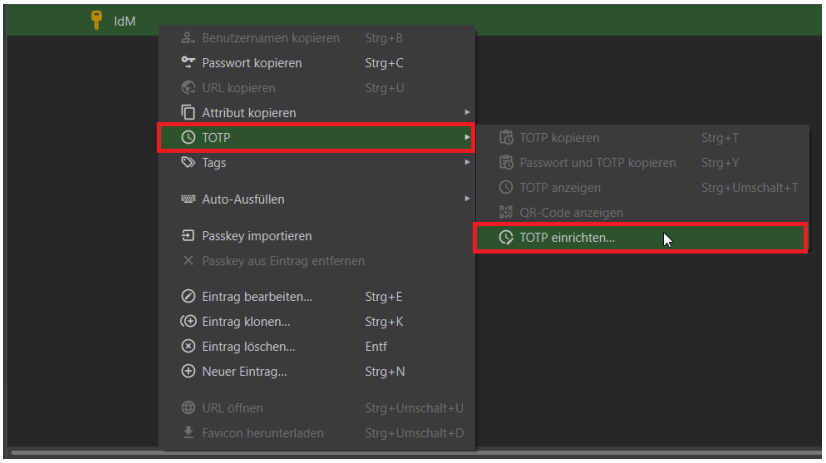
Um die TOTP-Funktion zu nutzen, muss zuerst ein Datenbankeintrag erstellt werden. Entsperren Sie hierzu die Datenbank mit ihrem Hauptschlüssel und klicken Sie im Karteireiter unter ***„Einträge“*** auf ***„Neuer Eintrag“***.



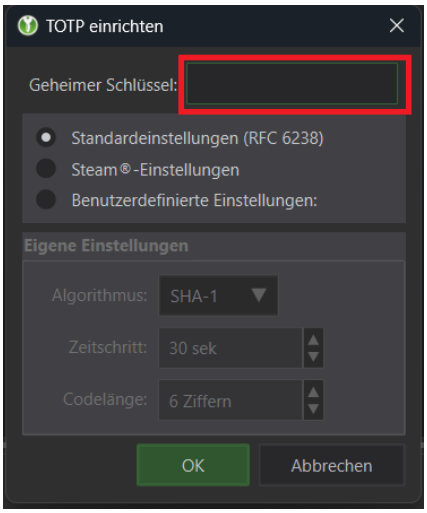
Im Editor können verschiedenste Informationen für einen Datenbankeintrag gespeichert werden. Mindestens sollte jedoch ein aussagekräftiger ***„Titel“*** für den Eintrag (*hier: „IdM“*) vergeben werden. Die Eingaben werden mit dem Button ***„OK“*** unten rechts abgeschlossen.



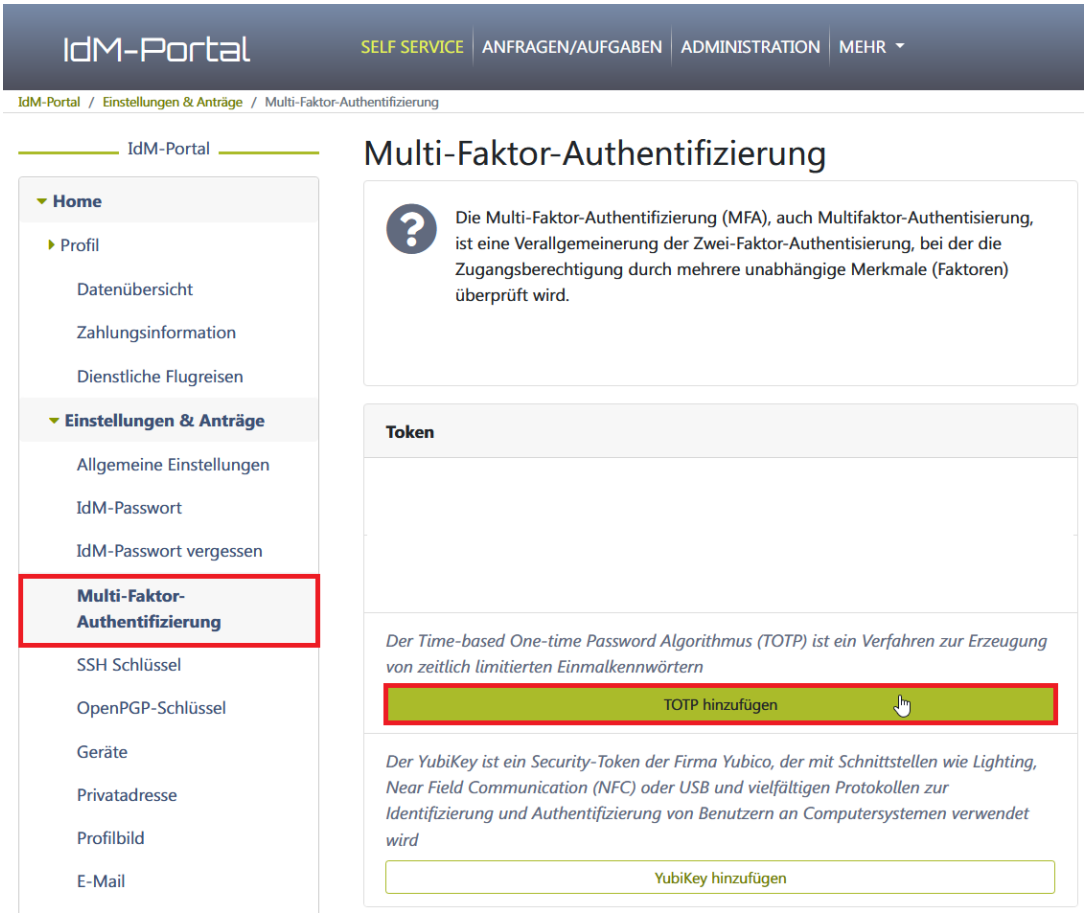
Im Anschluss lässt sich, nach einem Rechtsklick auf den markierten Eintrag, über das Kontextmenü des (neu angelegten) Eintrages unter dem Punkt ***„TOTP“*** der Untermenüpunkt ***„TOTP-Einrichten“*** auswählen.



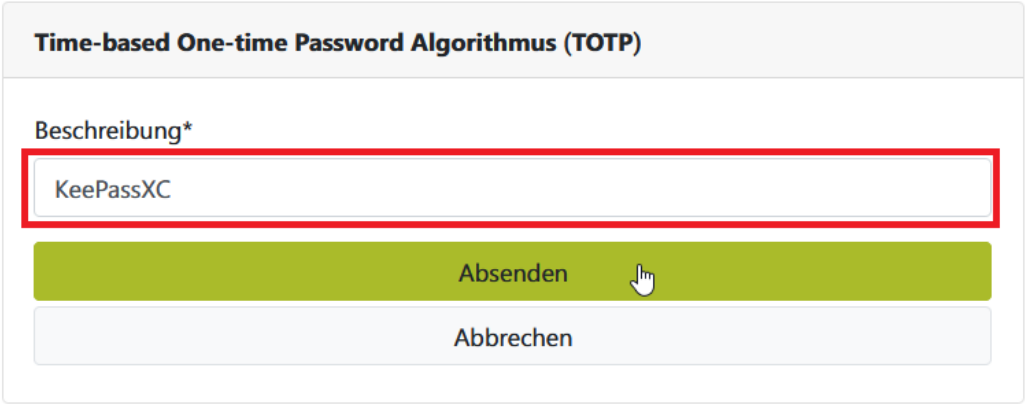
Im Kontextfenster lässt sich das TOTP-Geheimnis im Feld ***„Geheimer Schlüssel“*** eintragen. Diesen finden Sie in der IdM-Oberfläche.



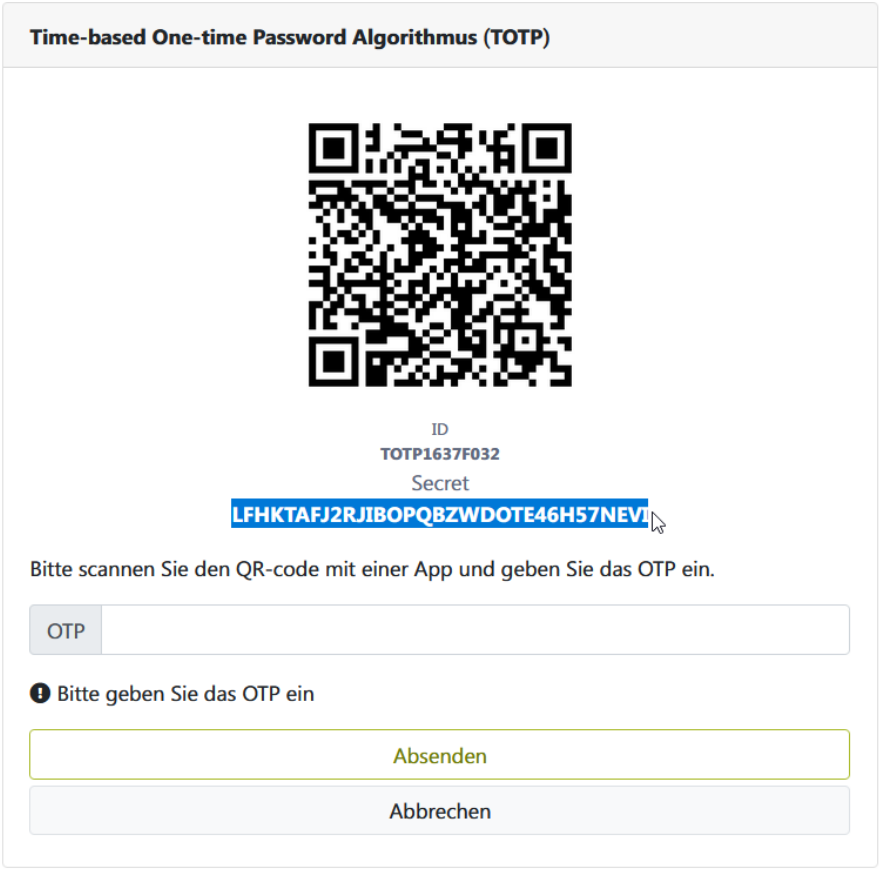
Melden Sie sich dazu im RRZE Identity Management (https://idm.fau.de) an und begeben Sie sich zur Funktion ***„Self Service“***. Unter der Menügruppierung ***„Einstellungen & Anträge“*** ist der Menüpunkt ***„Multi-Faktor-Authentifizierung“*** zu finden. Wählen Sie dort nun ***„TOTP hinzufügen“***, um einen individuellen „geheimen Schlüssel“ zu erhalten.



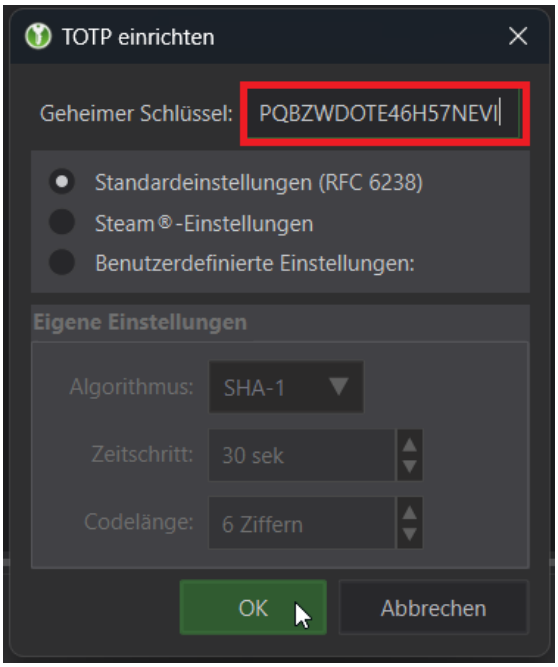
Im Anschluss muss das „Token“ noch benannt werden. Der Name sollte möglichst eindeutig sein, um zum Beispiel das genutzte Programm zu beschreiben.



Im folgenden Dialog kann das eigentliche Secret kopiert werden. Markieren Sie die Zeichenfolge unter der Bezeichung „Secret“ und kopieren sie diese, um sie dann in den Datenbankeintrag in KeePassXC einfügen zu können.Die ***Webseite*** muss für die Bestätigung des Codes und den Abschluss des Vorgangs noch ***geöffnet bleiben!***

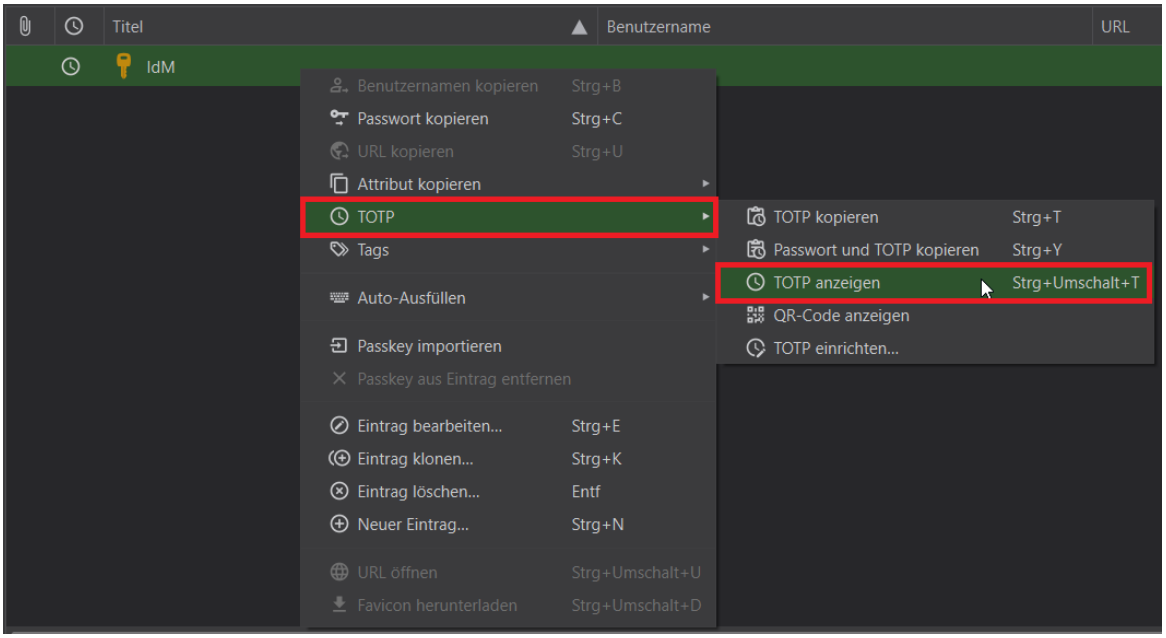


Tragen Sie das Secret nun im Feld ***„Geheimer Schlüssel“*** ein und bestätigen Sie den Dialog.



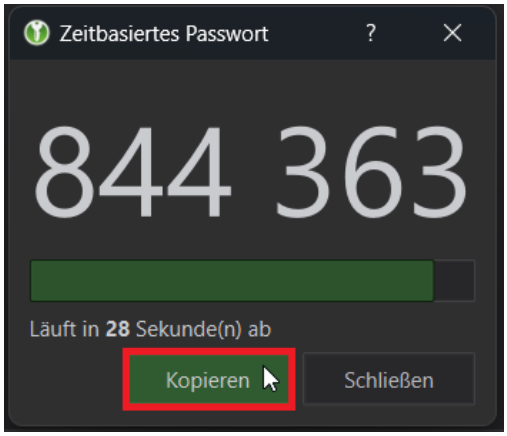
Nach erfolgreicher Einrichtung erscheint neben dem Datenbankeintrag ein Uhrensymbol, das den TOTP-Eintrag graphisch hervorhebt.

Um die Konfiguration im IdM abzuschließen, muss das Geheimnis und die korrekte Interpretation durch KeePassXC durch erstmalige Eingabe eines neu generierten Einmalcodes verifiziert werden. Markieren Sie dafür den Datenbankeintrag und rufen Sie das Kontextmenü durch „Rechtsklick“ auf. Wählen sie im Menüpunkt ***„TOTP“***, den Untermenüeintrag ***„TOTP anzeigen“***. Alternativ kann auch nach Markieren des Eintrags die Tastenkombination ***„STRG-UMSCHALT-T“*** verwendet werden.

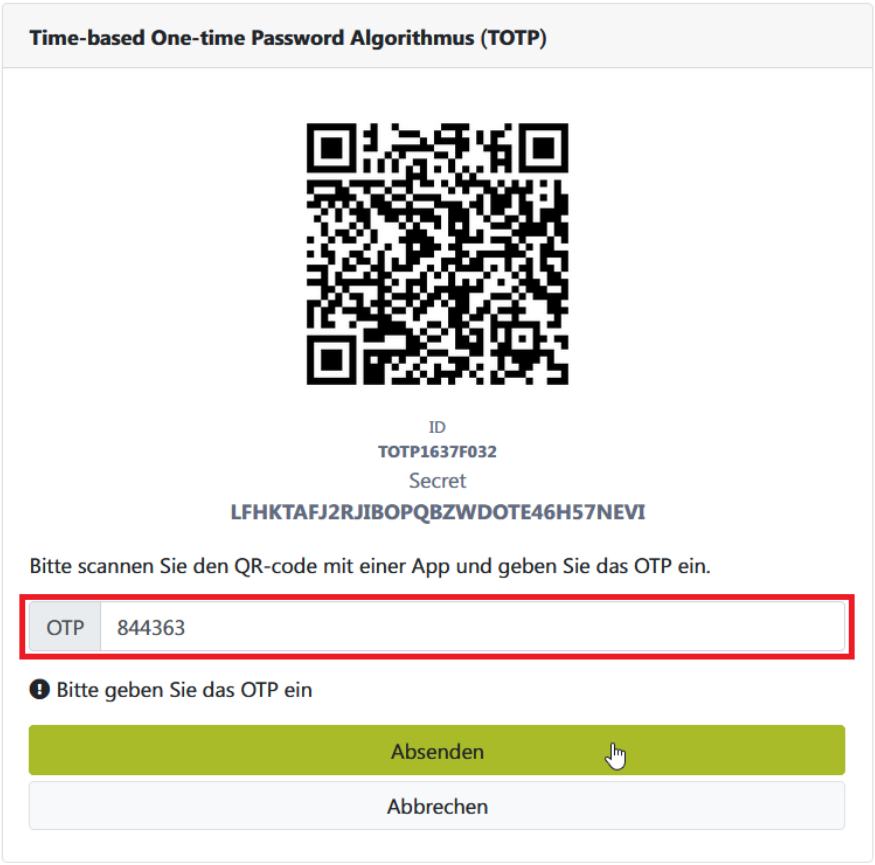


Im nun erscheinenden Dialog ist das zeitbasierte Password für das aktuelle 30 Sekundenfenster zu sehen. Im unteren Bereich ist die restliche Gültigkeit des Codes visualisiert als sich leerender Balken, als auch mit genauer Zeitangabe erkennbar. Über den Button ***„Kopieren“*** kann der Code in die Zwischenablage gelegt werden.

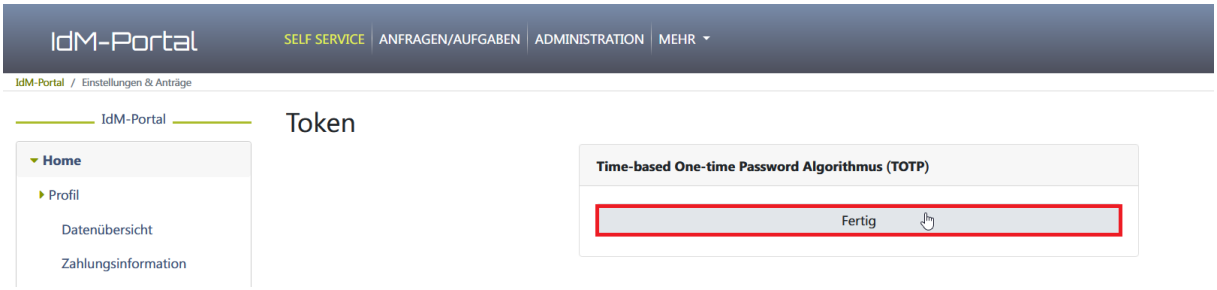
Aufgrund der zeitlichen Beschränkung ist es vorteilhaft für das Einfügen in die IdM-Maske einen Code mit möglichst langer Gültigkeit zu nutzen und so gegebenenfalls auf das Ablaufen eines nur noch wenige Sekunden gültigen Codes zu warten.



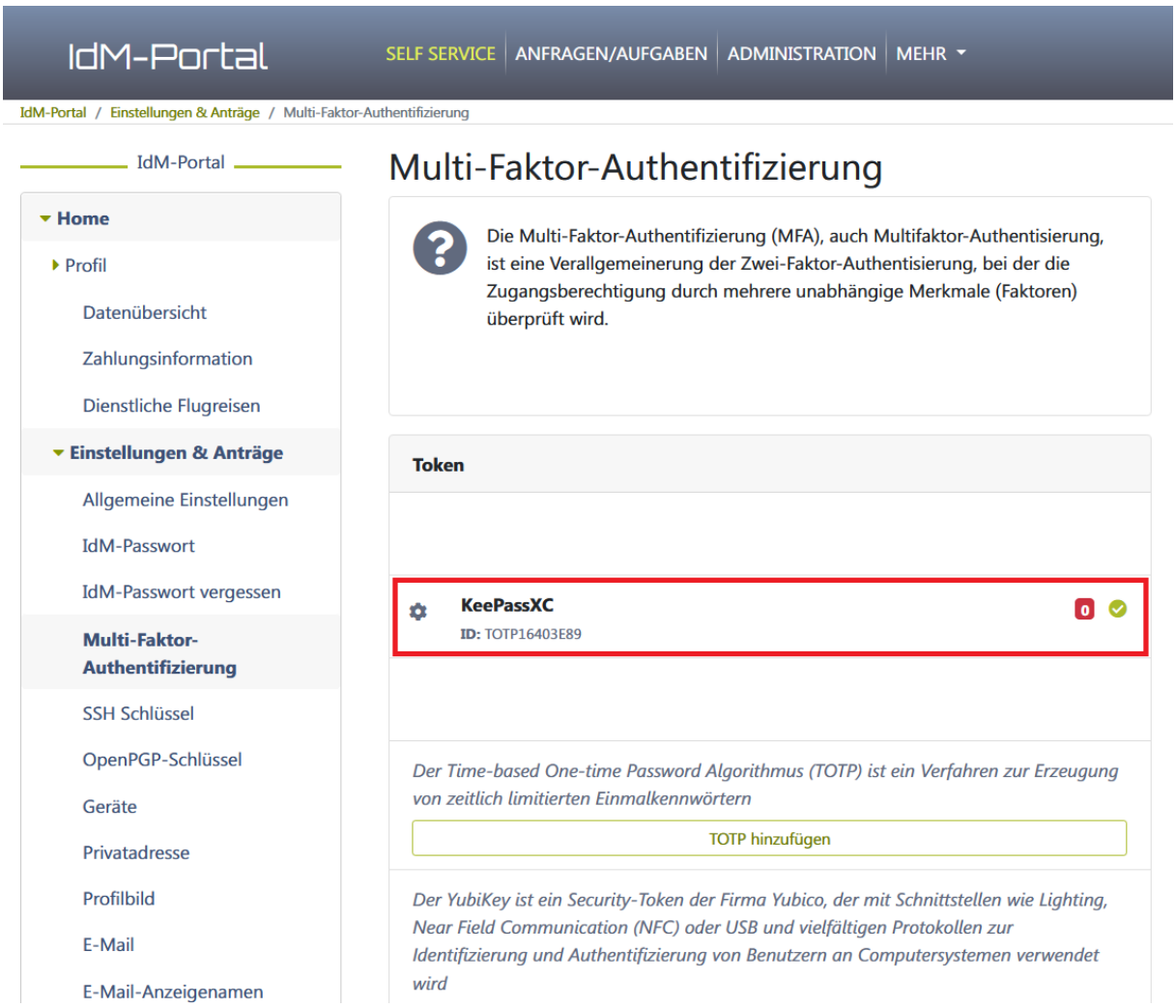
Der aus obigem Schritt kopierte Code wird nun zur Verifikation in das Feld ***„TOTP“*** eingefügt und mit ***„Absenden“*** bestätigt.



War der Vorgang erfolgreich, kann die Einrichtung mit ***„Fertig“*** abgeschlossen werden.

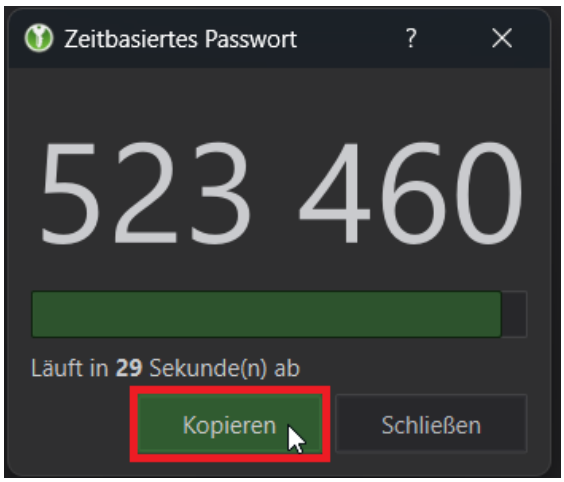


Auf der Übersichtseite ist nun auch die gerade eingerichtete Konfiguration für den zweiten Faktor sichtbar und kann verwaltet werden.

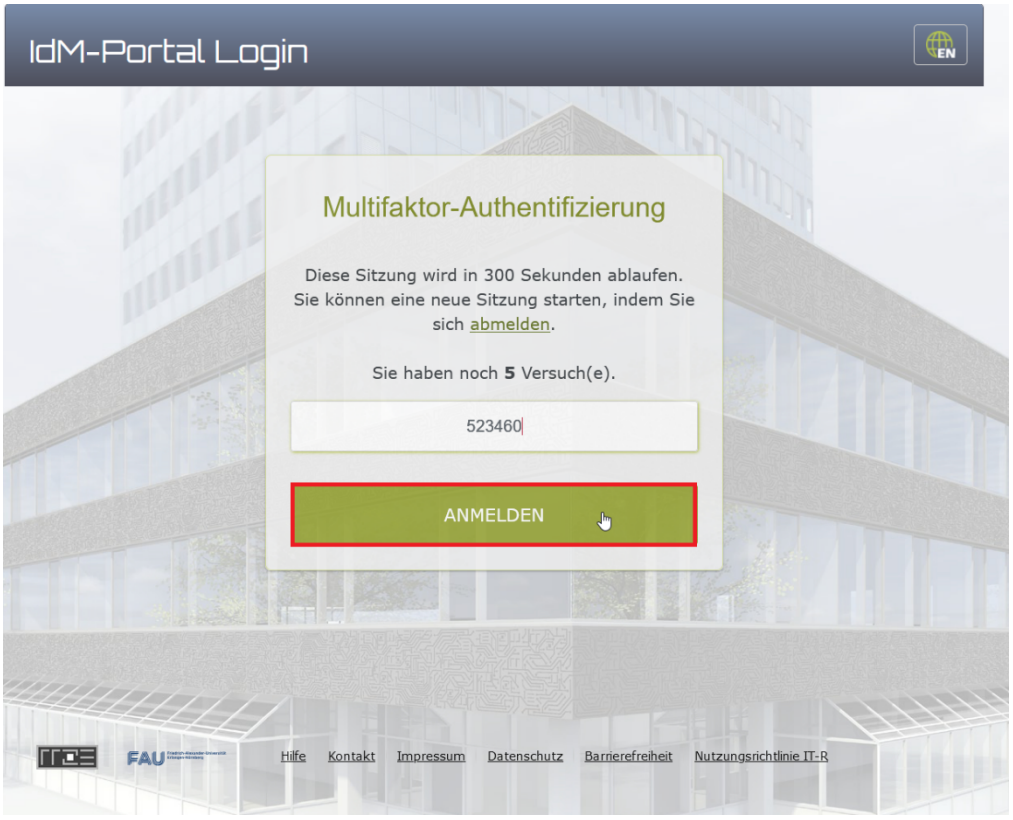


4. Anmeldung mit zweitem Faktor

Falls ein zweiter Faktor für Ihr IdM-Konto eingerichtet ist, lassen Sie sich den Code wie in Kapitel 2 beschrieben anzeigen und kopieren Sie diesen durch einen Klick auf ***„Kopieren“***.



Tragen Sie diesen Code anschließend in dafür vorgesehen Maske ein und bestätigen Sie die Eingabe durch einen Klick auf ***„Anmelden“***.



5. Überprüfen der TOTP-Einstellungen

Unter ***„Einstellungen & Anträge“***, ***„Multi-Faktor-Authentifizierung“*** lässt sich auf der rechten Menüfläche mit der Bezeichnung ***„Einstellungen“*** die Anmeldung mit zweitem Faktor durch die Schaltfläche „***Multi-Faktor-Authentifizierung für die Webseiten des IdM-Portals (Self Service, Anfragen/Aufgaben, Administration, ...) aktivieren“*** aktivieren und deaktivieren.