

Workshop

Wie verwalte ich
sicher, nachhaltig und bequem
meine Passwörter?



Agenda



1. Passwörter
2. Was ist ein Passwortsafe?
3. Warum macht er mein Online-Leben sicherer, nachhaltiger und bequemer?
4. Los geht's 😊
5. Weitere Hinweise



Passwörter

Wurde mein Passwort schon mal gestohlen?



Betroffener Dienst	Datum	Verifiziert	Betroffene Nutzer	Passwort	Vor- und Zuname	Geburtsdatum	Anschrift	Telefonnummer	Kreditkarte	Bankkontodaten	Sozialversicherungs-nr.
verifications.io	Feb. 2019	✓	763.002.527	–	–	–	–	–	–	–	–
Unknown (Collection #1-#5)	Jan. 2019		2.191.498.885	Betroffen	–	–	–	–	–	–	–
Dieser Datensatz wurde im Januar 2019 veröffentlicht und enthält riesige Listen von Zugangsdaten unbekannter Herkunft, ältere Leaks und kleinere Datenbankabzüge.											
Onliner Spambot (Spamlist)	Aug. 2017		128.471.704	–	–	–	–	–	–	–	–
Unknown (Anti-Public Combolist)	Dez. 2016		541.567.187	Betroffen	–	–	–	–	–	–	–
nexusmods.com	Dez. 2015	✓	5.918.307	Betroffen	–	–	–	–	–	–	–
kickstarter.com	Feb. 2014	✓	5.174.845	–	–	–	–	–	–	–	–
adobe.com	Okt. 2013	✓	152.375.851	–	–	–	–	–	–	–	–
dropbox.com	Sep. 2012	✓	68.658.165	Betroffen	–	–	–	–	–	–	–
last.fm	Jun. 2012	✓	39.329.766	Betroffen	–	–	–	–	–	–	–

Quelle: HPI Identify Leak Checker

Passwörter

Gegen wen schützen wir uns eigentlich?



- Neugierige Nachbar*innen von nebenan?
- Experimentierfreudige Studierende?
- Professionelle Cracker*innen?
- Geheimdienste?

→ Für die meisten ist das realistischste Szenario ein **Daten-Leak** bei einem verwendeten Online-Dienst

Hauptproblem: Offline Brute-Force-Attacken (dictionary attack)

Passwörter

Empfehlungen vom Hasso-Plattner-Institut



- Lange Passwörter (> 15 Zeichen)
- Alle Zeichenklassen verwenden (Groß-, Kleinbuchstaben, Zahlen, Sonderzeichen)
- Keine Wörter aus dem Wörterbuch
- Keine Wiederverwendung von gleichen oder ähnlichen Passwörtern bei unterschiedlichen Diensten
- Verwendung von Passwortmanagern
- Passwortwechsel bei Sicherheitsvorfällen und bei Passwörtern, die die obigen Regeln nicht erfüllen
- Zwei-Faktor-Authentifizierung aktivieren, wenn möglich

Passwörter

Merkhilfe 1: Akronymtechnik



Konzept:

Einen vergleichsweise einfach zu merkenden Satz ausdenken und aus den Anfangsbuchstaben und den Satzzeichen ein Passwort zusammensetzen

Beispiele

- „Das ist 1 Passwort, das ich mir garantiert merken kann! 😊“
→ Di1PW,dimgmk!:)
- „Jeden Morgen trinke ich einen Schwarztee mit Hafermilch und ohne Zucker ♥“
→ JMtieStmHm&oZ<3



Passwörter

Merkhilfe 2: Diceware-Verfahren

Konzept: Erzeugung einer Passphrase anhand zufällig ausgewählter Wörter aus einer Wortliste mit 7.776 Wörtern: http://world.std.com/~reinhold/diceware_german.txt

Vorgehen:

- Für jedes Wort werden fünf Würfelwürfe gebraucht, deren Augen als Ziffern einer fünfstelligen Zahl dienen, beispielsweise 26215
- Anhand dieser Zahl wird das zugehörige Wort aus der Wortliste ausgewählt, beispielsweise 26215 = „gepard“
- Dieser Vorgang wird mind. fünf Mal wiederholt, so dass sich daraus eine sichere Passphrase zusammensetzt

26215: gepard
26124: gelder
61211: tast
34542: kehlilig
15213: bezirk
51134: prinz

Beispiel: gepard-gelder-tast-kehlilig-bezirk-prinz

Passwortsafe

Sicher, nachhaltig, bequem?



- ✓ Überall verschiedene, sehr sichere Passwörter



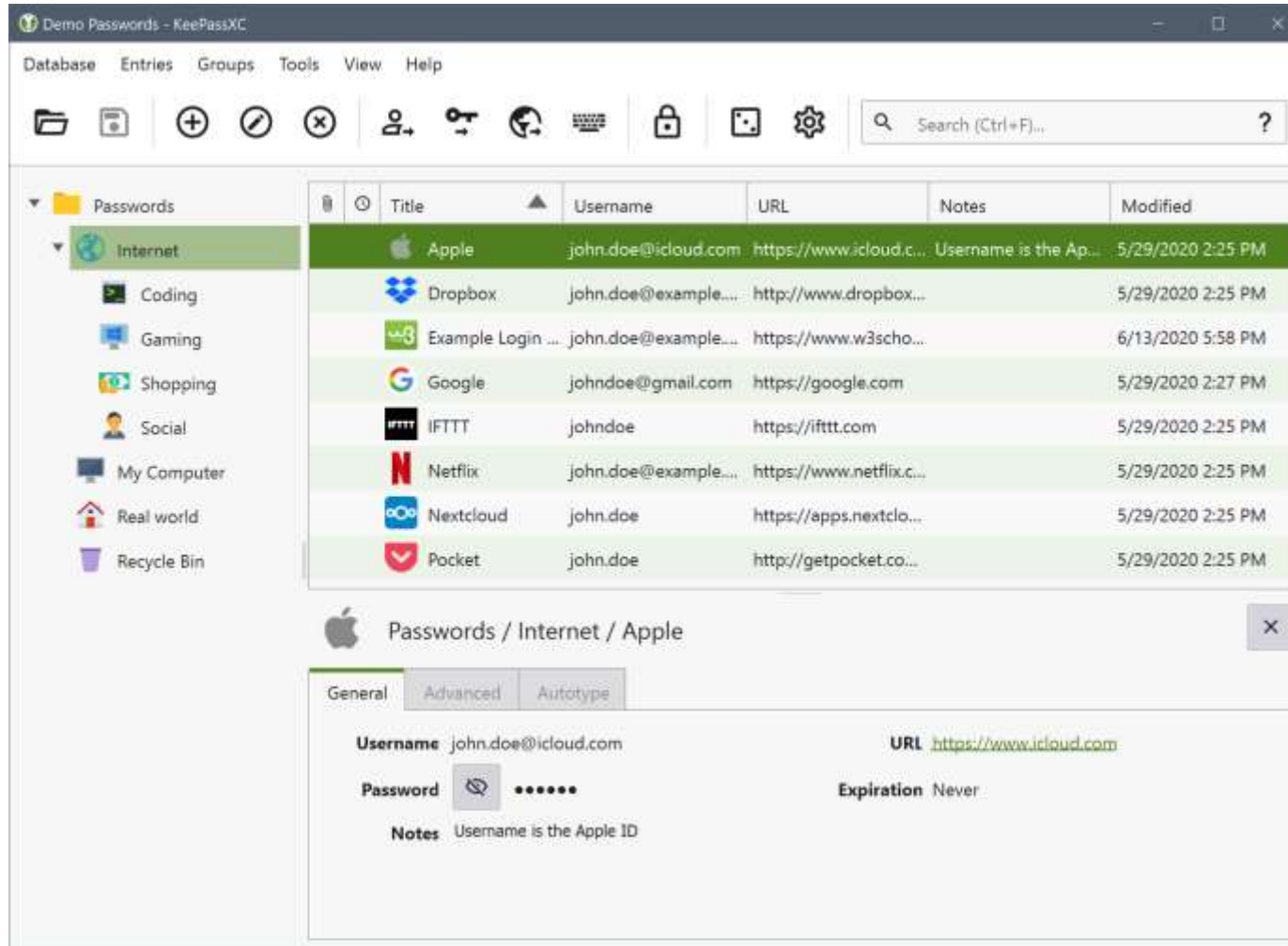
- ✓ „Passwort vergessen“ gibt es nicht mehr (du musst dir nur noch 2-3 Passwörter merken)
- ✓ Überblick über alle Accounts



- ✓ Automatisches Einfügen von Zugangsdaten
- ✓ Verfügbar auf allen Geräten

Passwortsafe

Was ist das überhaupt?



Passwortsafe

Nur für Passwörter?



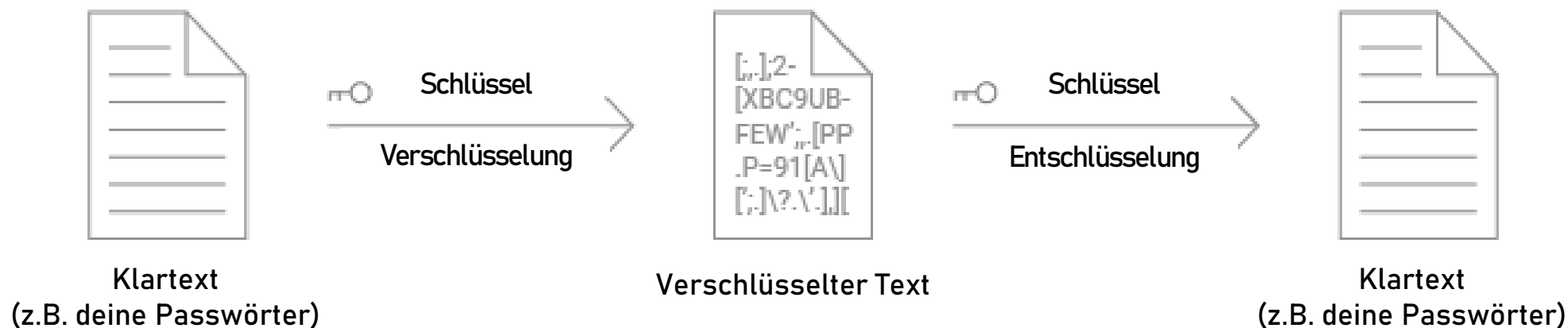
- Passwörter
- WLAN-Schlüssel
- Nummern (z.B. Sozialversicherungsnummer, Mitgliedsnummern, etc.)
- Lizenzschlüssel
- Private Informationen
- ...

Passwortsafe

Wie funktioniert ein Passwortsafe?

Symmetrische Verschlüsselung

Gleicher Schlüssel für
Verschlüsselung und Entschlüsselung



Passwortsafe

Varianten



Offline / Lokal

Verschlüsselte Datei

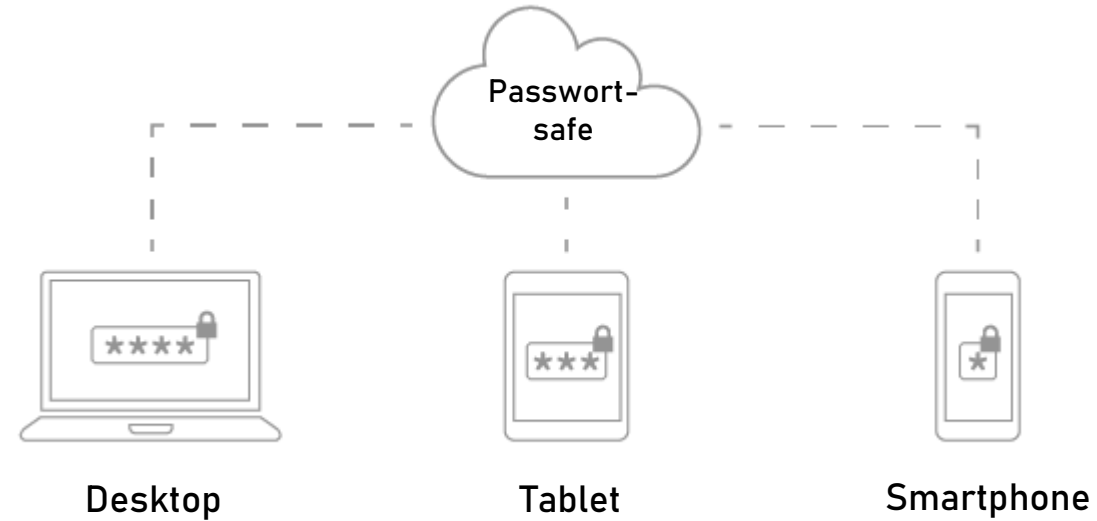


Dein Gerät



Online / Cloud

Passwort-
safe



Passwortsafe

Große Auswahl...



Open Source &
Lokale Speicherung



KeePass
Password
Safe



Open Source &
Self-Hosting möglich



Closed Source & Cloud-Service

LastPass...



1Password



NordPass



Passwortsafe

KeePass



- ✓ Offener Standard + große Community + viele Open Source Implementierungen
- ✓ Lokale Speicherung → kein automatisches Hochladen zu irgendwelchen Servern
- ✓ KISS-Prinzip → einzelne Datei (Synchronisation wird anderen Tools überlassen)
- ✓ Es existieren Programme für Linux, MacOS und Windows, Apps für Android & iOS sowie Browser-Erweiterungen
- ✓ Viele Funktionalitäten & Anpassungsmöglichkeiten

KeePass

Kleine Auswahl an KeePass-kompatiblen Programmen / Apps



	Name	Kosten	Open Source	Browser-Integration	Anmerkungen
Windows	KeePassXC	-	ja	<i>KeePassXC-Browser*</i>	
Linux	KeePassXC	-	ja	<i>KeePassXC-Browser*</i>	
macOS	KeePassXC	-	ja	<i>KeePassXC-Browser*</i>	
Android	KeePassDX / Keepass2Android	-	ja	-	
iOS	KeePassium (Free)	Free: 0 € Pro: 14,99 € p.a.	ja	-	• Mit TouchID • nur eine Datenbank
	Strongbox (Free)	Free: 0 € Pro: 13,49 \$ p.a.	ja	-	• Ohne TouchID • mehr als eine Datenbank

*Erweiterung verfügbar für Google Chrome, Vivaldi, Brave, Mozilla Firefox, Microsoft Edge, Chromium

Demo



Los geht's!

Einrichtung von KeePass



To-dos:

1. Passwortsafe installieren
2. Datenbank erstellen
3. Datenbank synchronisieren
4. Neue Einträge erstellen (Passwortgenerator verwenden)
5. Browser-Integration einrichten
6. App auf Smartphone / Tablet einrichten

Einrichtung von KeePassXC

KeePassXC: Getting Started Guide:

https://keepassxc.org/docs/KeePassXC_GettingStarted.html





Einrichtung von KeePassXC

Download & Installation

 KeePassXC

[The Project](#) [Screenshots](#) [Download](#) [Blog](#) [Docs / FAQ](#) [The Team](#)

Download

 Linux

 macOS

 Windows

 Source Code

Official Packages:

 **Installer (64-bit)**



 MSI installer

 PGP signature  SHA-256 digest

 **Portable (64-bit)**



 Portable ZIP archive

 PGP signature  SHA-256 digest

 **Installer (32-bit)**



 MSI installer

 PGP signature  SHA-256 digest

 **Portable (32-bit)**



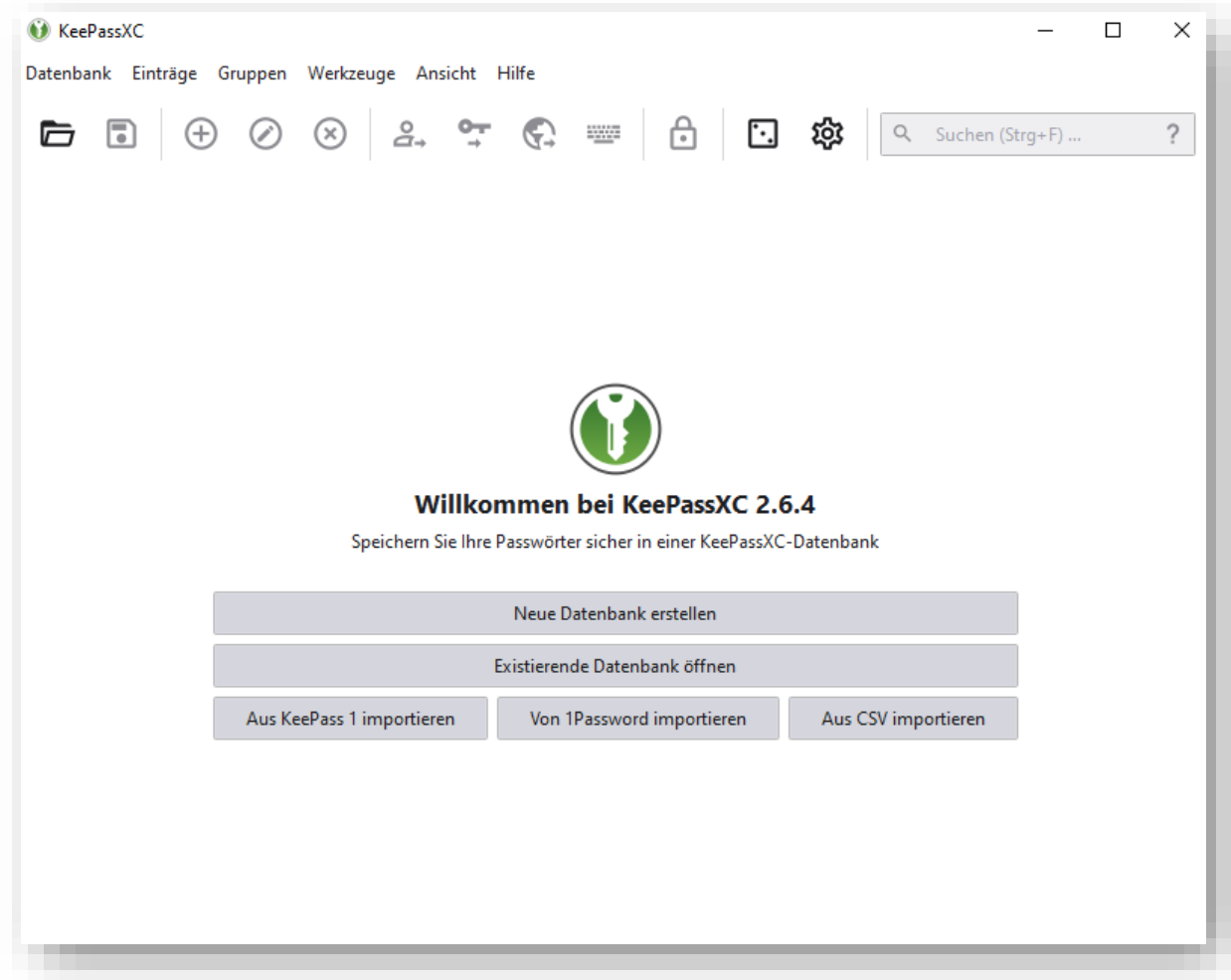
 Portable ZIP archive

 PGP signature  SHA-256 digest

<https://keepassxc.org/download/>

Einrichtung von KeePassXC

Startseite



Einrichtung von KeePassXC

Datenbank erstellen



Neue KeePassXC-Datenbank erstellen ...

Allgemeine Informationen zur Datenbank

Bitte geben Sie den Namen und (optional) eine Beschreibung der neuen Datenbank ein:

Datenbankname:

Beschreibung:

Zurück Weiter Abbrechen

Einrichtung von KeePassXC

Einstellungen zur Verschlüsselung

Neue KeePassXC-Datenbank erstellen ...

Verschlüsselungs-Einstellungen

Hier werden die Details der Verschlüsselung eingestellt. Sie können diese Details auch später in den Datenbank-Einstellungen ändern.

Zeit zum Entschlüsseln: 1.0 s

100 ms 5.0 s

Höhere Werte sind sicherer, aber das Öffnen der Datenbank dauert länger.

Datenbankformat: KDBX 4.0 (empfohlen)

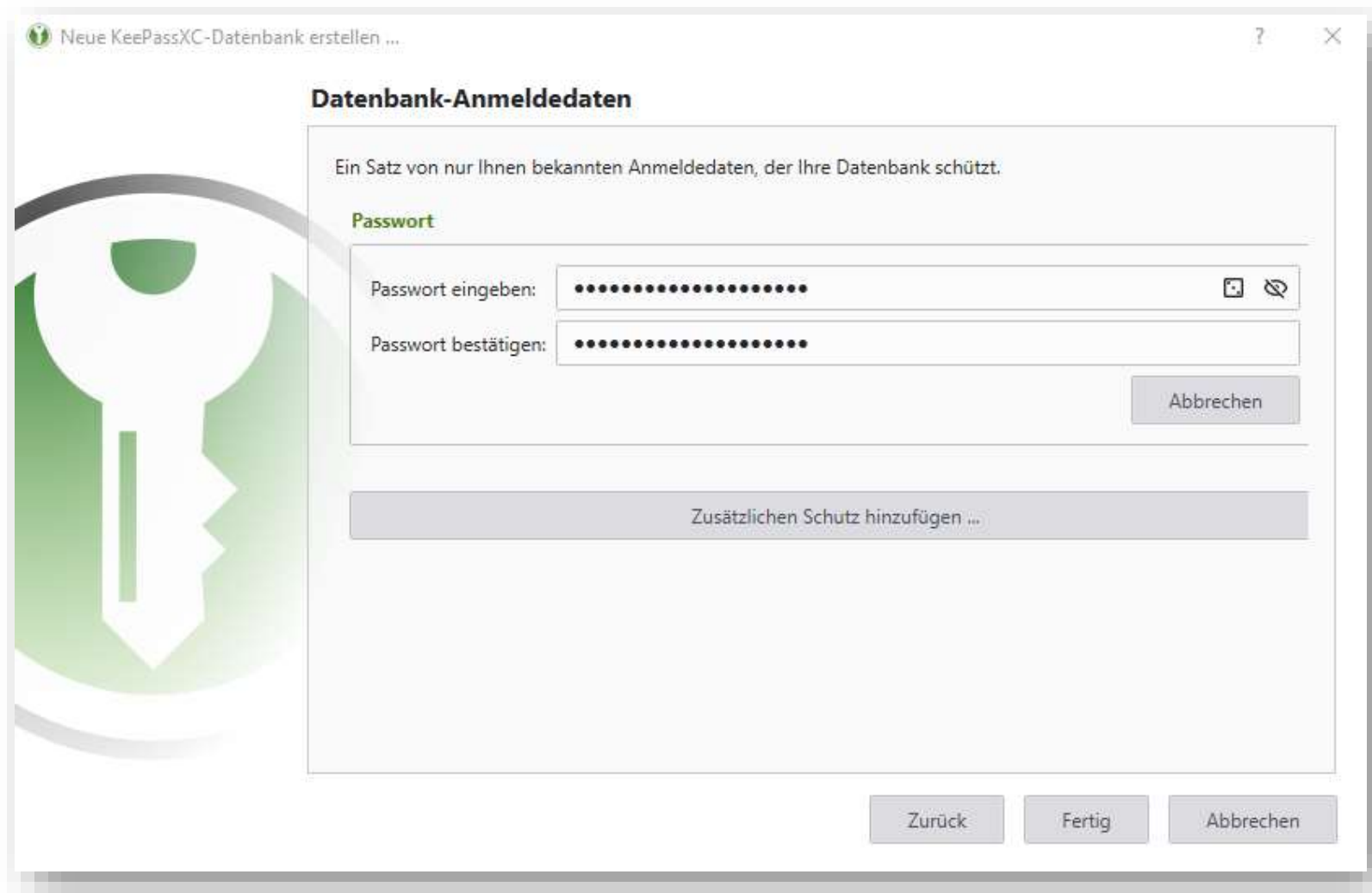
Nur wichtig, wenn Sie die Datenbank mit anderen Programmen verwenden müssen.

Fortgeschrittene Einstellungen

Zurück Weiter Abbrechen

Einrichtung von KeePassXC

Passwort für Datenbank festlegen



Neue KeePassXC-Datenbank erstellen ...

Datenbank-Anmeldedaten

Ein Satz von nur Ihnen bekannten Anmeldedaten, der Ihre Datenbank schützt.

Passwort

Passwort eingeben:

Passwort bestätigen:

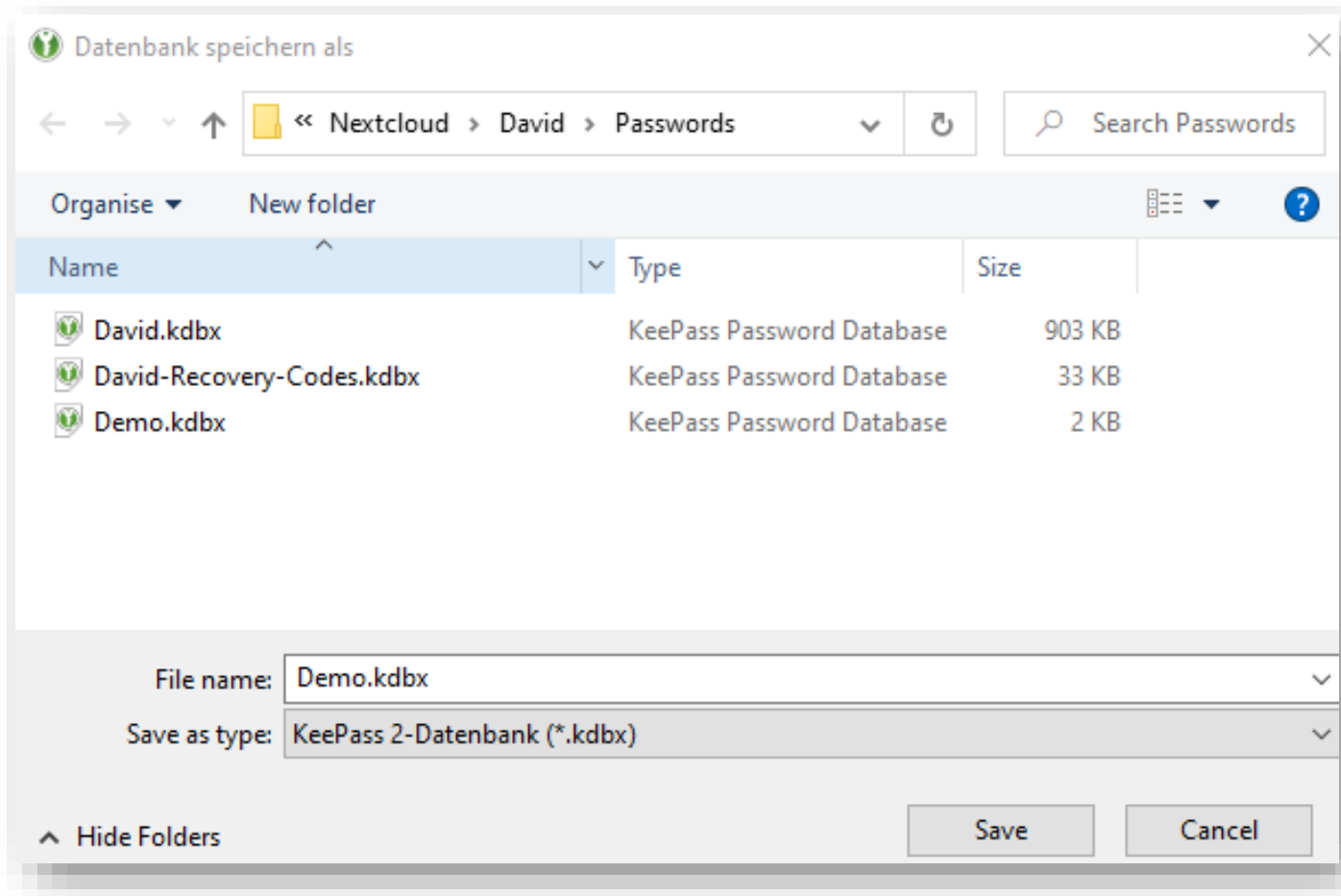
Abbrechen

Zusätzlichen Schutz hinzufügen ...

Zurück Fertig Abbrechen

Einrichtung von KeePassXC

Speicherort festlegen



Einrichtung von KeePassXC

Ersten Eintrag anlegen

Demo - KeePassXC

Datenbank Einträge Gruppen Werkzeuge Ansicht Hilfe

Suchen (Strg+F) ...

Demo • Eintrag hinzufügen

Eintrag

Fortgeschritten

Symbol

Auto-Type

Titel: Nextcloud

Benutzername: david

Passwort:

URL: https://cloud.davidkopp.de/

☐ Läuft ab: 09.03.2021 10:21

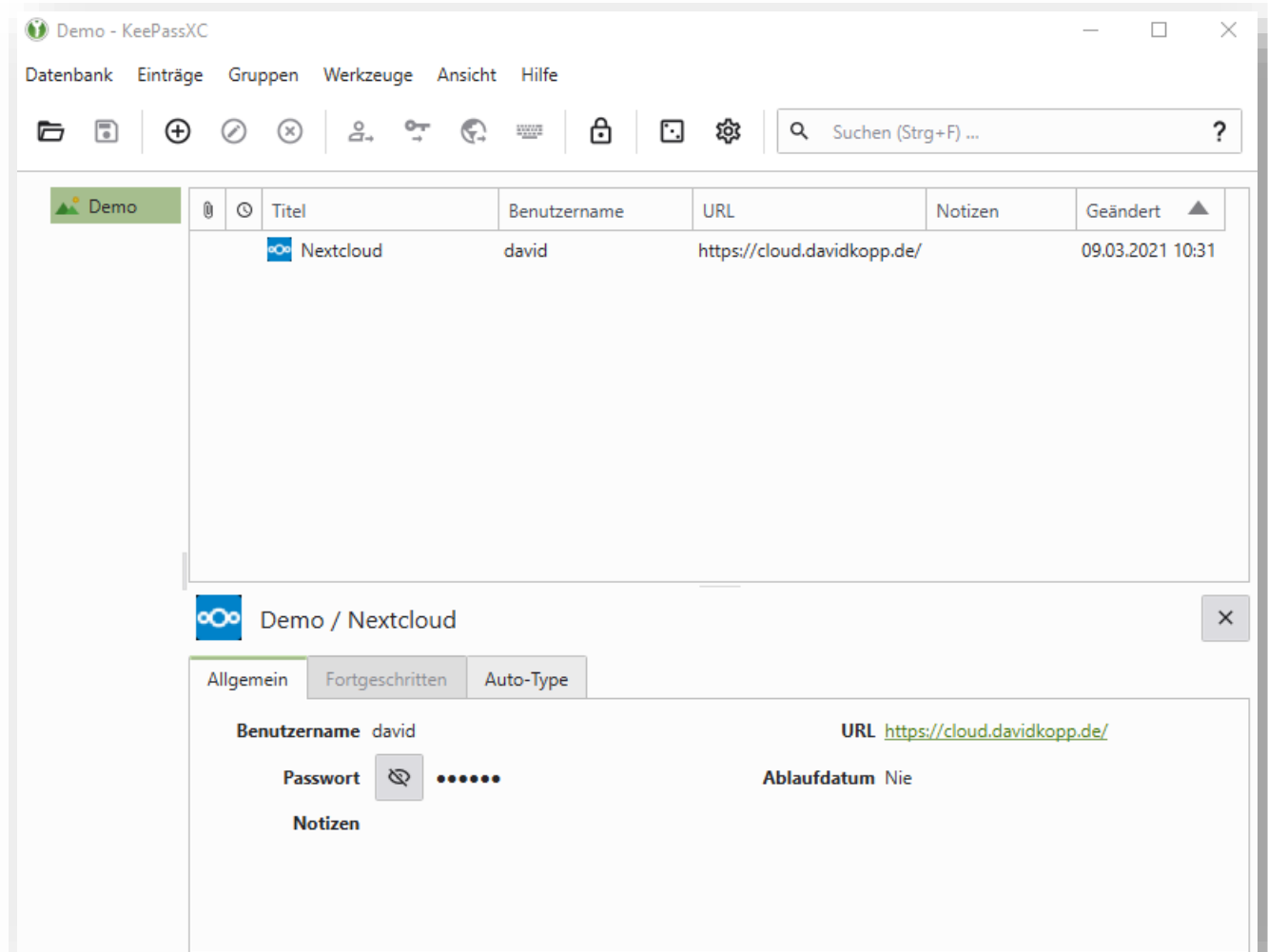
☐ Notizen: Setzen Sie das Häkchen, um die Notizen anzuzeigen.

Vorgaben

OK Abbrechen

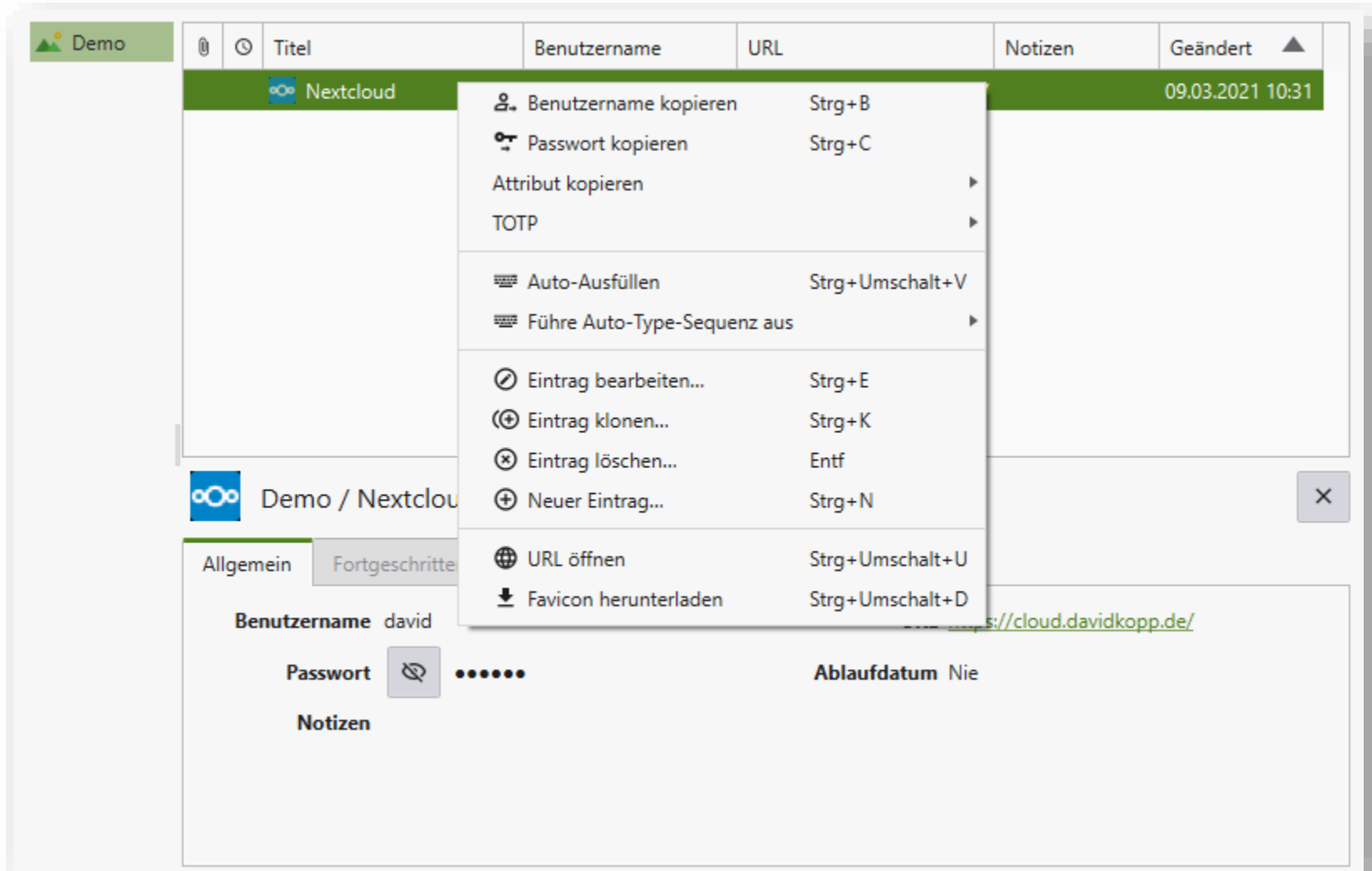
Einrichtung von KeePassXC

Übersicht



Einrichtung von KeePassXC

Kontextmenü



Einrichtung des KeePassXC-Browser Add-ons

Browserintegration aktivieren



Einstellungen - KeePassXC

Datenbank Einträge Gruppen Werkzeuge Ansicht Hilfe

Suchen (Strg+F) ...

Anwendungseinstellungen

☒ Browserintegration aktivieren

Allgemein Fortgeschritten

KeePassXC-Browser wird für die Browserintegration benötigt.
Laden Sie es für [Firefox](#) und [Google Chrome / Chromium / Vivaldi / Brave](#) und [Microsoft Edge](#) herunter.

Integration für diese Browser aktivieren:

☐ Chrome, Vivaldi, and Brave ☒ Firefox and Tor Browser ☐ Edge
☐ Chromium

☒ Entsperrung anfragen, wenn die Datenbank gesperrt ist
☒ URL-Schema abgleichen (z. B. https://...)
☒ Nur am besten passende Anmeldedaten zurückliefern
☐ Rückgabe abgelaufener Anmeldedaten erlauben
☐ In allen geöffneten Datenbanken nach passenden Anmeldedaten suchen
☒ Passende Anmeldedaten nach Titel sortieren
☐ Passende Anmeldedaten nach Benutzername sortieren

OK Abbrechen

Einrichtung des KeePassXC-Browser Add-ons

Add-on für deinen Browser installieren



The screenshot shows the Firefox Browser Add-ons page for the KeePassXC-Browser extension. The page has a dark purple header with the Firefox logo and 'ADD-ONS' text. Navigation links include 'Entdecken', 'Erweiterungen' (highlighted), 'Themes', and 'Mehr...'. A search bar on the right says 'Add-ons suchen'. The main content area features the KeePassXC logo (a green key in a circle) and the title 'KeePassXC-Browser von KeePassXC Team'. Below this, it states 'Official browser plugin for the KeePassXC password manager' with a link to <https://keepassxc.org>. A blue button labeled '+ Zu Firefox hinzufügen' is positioned to the right. On the right side of the page, there is a statistics section showing '43.484 Nutzer' and '347 Bewertungen' with a 4.3-star rating. Below this is a breakdown of star ratings: 5 stars (233), 4 stars (55), 3 stars (20), 2 stars (9), and 1 star (30).

Rating	Count
5 stars	233
4 stars	55
3 stars	20
2 stars	9
1 star	30

Einrichtung des KeePassXC-Browser Add-ons

Verbindung aufbauen



Browser window showing the KeePassXC-Browser Add-on settings page. The page title is "Verbundene Datenbanken". The left sidebar contains navigation links: "ALLGEMEIN", "VERBUNDENE DATENBANKEN", "BENUTZERDEFINIERT ANMELDEFELDER", "SEITENEINSTELLUNGEN", and "ÜBER". The main content area displays a table with columns "Bezeichner", "Schlüssel", and "Zuletzt verwendet". Below the table, it states "Keine verbundenen Datenbanken gefunden." and "Datenbanken, die mit dem KeePassXC-Browser verbunden sind." A green button labeled "Verbinden" is visible. A modal dialog box is open, displaying an error message: "KeePassXC-Browser hat einen Fehler festgestellt: Die Verbindung zu KeePassXC ist nicht möglich. Überprüfen Sie, ob die Browser-Integration in den KeePassXC-Einstellungen aktiviert ist." The dialog includes buttons for "Einstellungen", "Benutzerdefinierte Anmeldefelder wählen", and "Neu laden".

Bezeichner	Schlüssel	Zuletzt verwendet
Keine verbundenen Datenbanken gefunden.		

Datenbanken, die mit dem KeePassXC-Browser verbunden sind.

[Verbinden](#)

Einstellungen **Benutzerdefinierte Anmeldefelder wählen**

KeePassXC-Browser hat einen Fehler festgestellt:

Die Verbindung zu KeePassXC ist nicht möglich.
Überprüfen Sie, ob die Browser-Integration in den
KeePassXC-Einstellungen aktiviert ist.

[Neu laden](#)

Einrichtung des KeePassXC-Browser Add-ons

Verbindung aufbauen



KEEPASSXC-BROWSER

- ALLGEMEIN
- VERBUNDENE DATENBANKEN**
- BENUTZERDEFINIERT ANMELDEFELDER
- SEITENEINSTELLUNGEN
- ÜBER

Verbundene Datenbanken

Bezeichner	Schlüssel	Zuletzt verwendet
Keine verbundenen Datenbanken gefunden.		

Datenbanken, die mit dem KeePassXC-Browser verbunden sind.

[Verbinden](#)

KeePassXC: Neue Schlüsselverbindungsanfrage

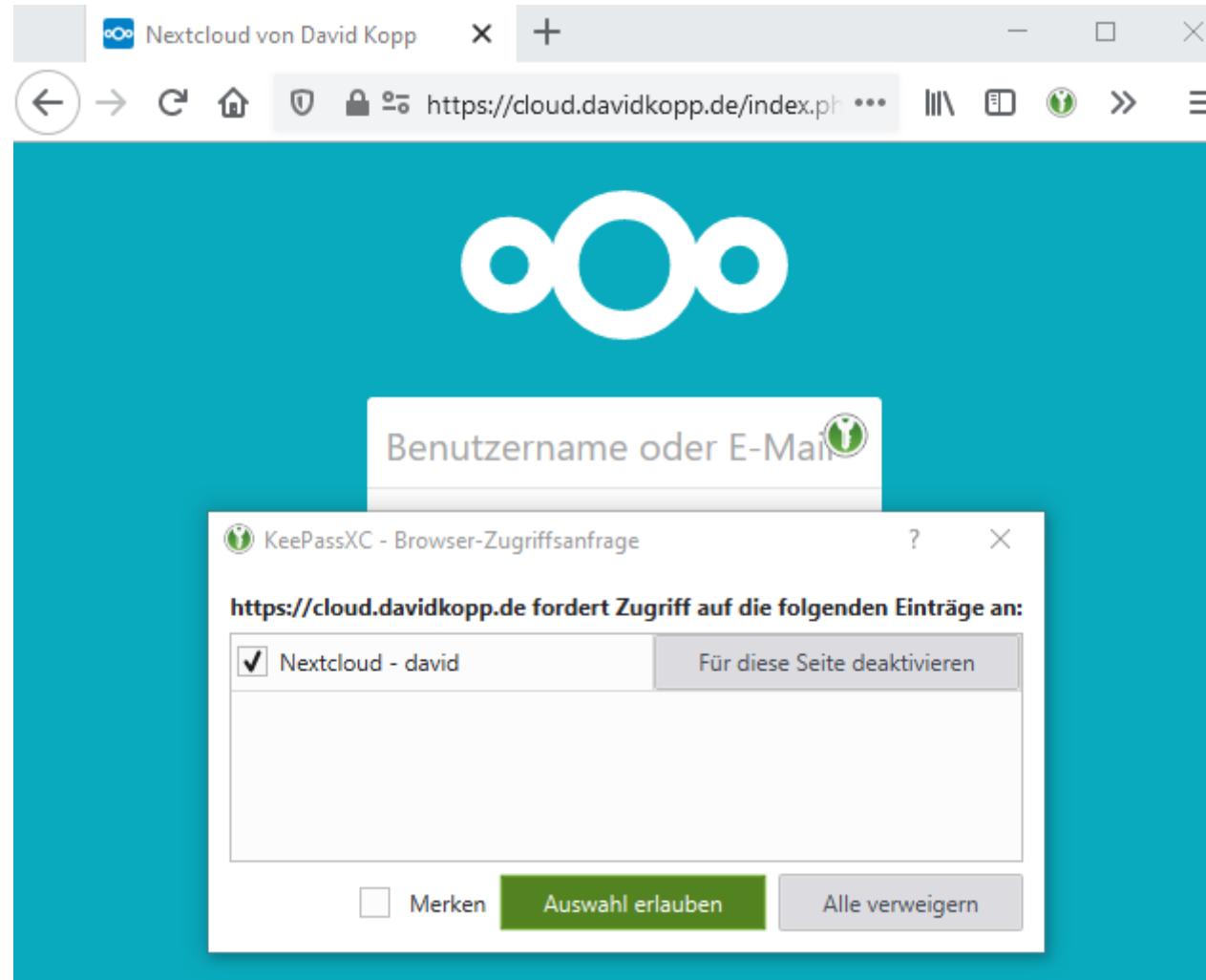
Verbindungsanfrage erhalten für folgende Datenbank:
Passwörter

Geben Sie der Verbindung einen eindeutigen Namen, z. B. "chrome-laptop".

[Speichern und Zugriff erlauben](#) [Abbrechen](#)

Einrichtung des KeePassXC-Browser Add-ons

Zugriff auf Eintrag erlauben



Einrichtung des KeePassXC-Browser Add-ons

Login-Felder werden automatisch ausgefüllt



The screenshot shows a web browser window with the address bar displaying 'https://cloud.davidkopp.de/index.php'. The page has a teal background and features the Nextcloud logo at the top. Below the logo is a login form with a text input field containing 'david' and a password field represented by a series of dots. To the right of the password field is an eye icon for toggling visibility. Below the password field is a large, rounded button labeled 'Anmelden' with a right-pointing arrow. Underneath the button are two links: 'Passwort vergessen?' and 'Mit einem Gerät anmelden'. At the bottom of the page, it says 'Nextcloud von David Kopp – Honeypot'.

Passwortgenerator

Integriert in KeePassXC



Neue KeePassXC-Datenbank erstellen ...

Passwort erzeugen

dbY~<h;t b;Q(s^GIL!2

Passwort-Qualität: Ausgezeichnet Entropie: 115.48 bit

Passwort Passphrase

Länge: 20 Fortgeschritten

Zeichentypen

A-Z a-z 0-9 /* + & ... Erweitertes ASCII

Schließen Passwort anwenden

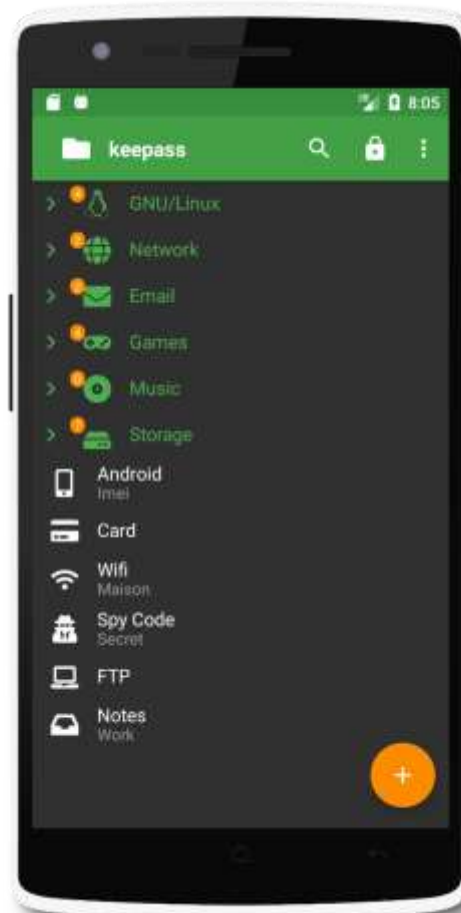
Zurück Fertig Abbrechen

Einrichtung am mobilen Endgerät

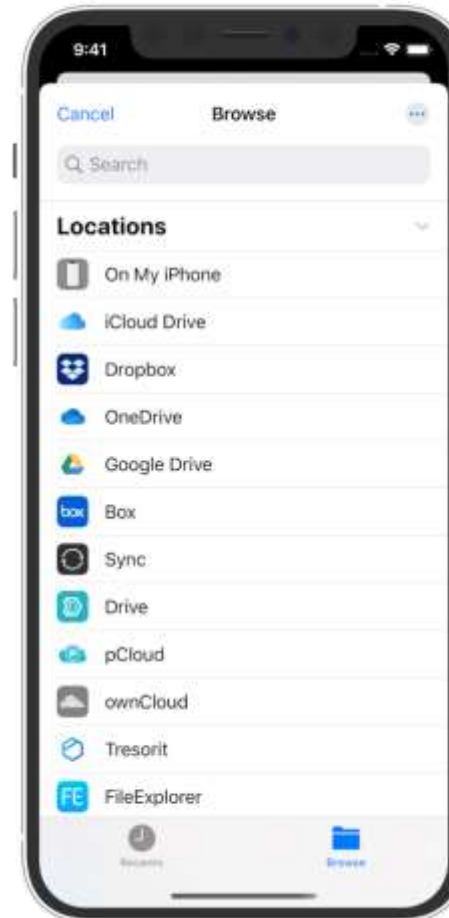
Android / iOS



KeePassDX



Keepassium



Einrichtung am mobilen Endgerät

Voraussetzung: Synchronisation



Lokal



Cloud



Nextcloud



Wie richte ich meine eigene (Next)Cloud ein?

Google Drive, Dropbox oder iCloud – warum nicht einfach selbst die ganz eigene Cloud hosten? Und wofür brauche ich überhaupt eine Cloud?

In diesem Workshop wird anhand der Open-Source-Software Nextcloud gezeigt, wie leicht es möglich ist, die Souveränität über die eigenen Daten wiederzuerlangen. Wie sich während des interaktiven Workshops zeigen wird, lassen sich mit Nextcloud nicht nur meine Dateien plattformübergreifend verwalten, sondern auch meine Termine, Kontakte, Passwörter und vieles mehr. Begleitet von kleinen live Demonstrationen, werden einzelne Funktionalitäten vorgestellt.

 **DATUM**
20. Mai 2021

 **UHRZEIT**
10:00 - 12:00

 **LABELS**
Anmeldung erforderlich.
Sustainable ME

 **KATEGORIE**
 Online
 Workshop



Einrichtung am mobilen Endgerät

Anleitungen



- Teil 1: [KeePassXC: Auto-Type und Browser-Add-on im Alltag nutzen](#)
- Teil 2: [KeePassDX: Magikeyboard und AutoFill im Android-Alltag nutzen](#)
- Teil 3: [Syncthing: KeePass-Datenbank zwischen PC und Android synchronisieren](#)

Weitere Hinweise

Backup

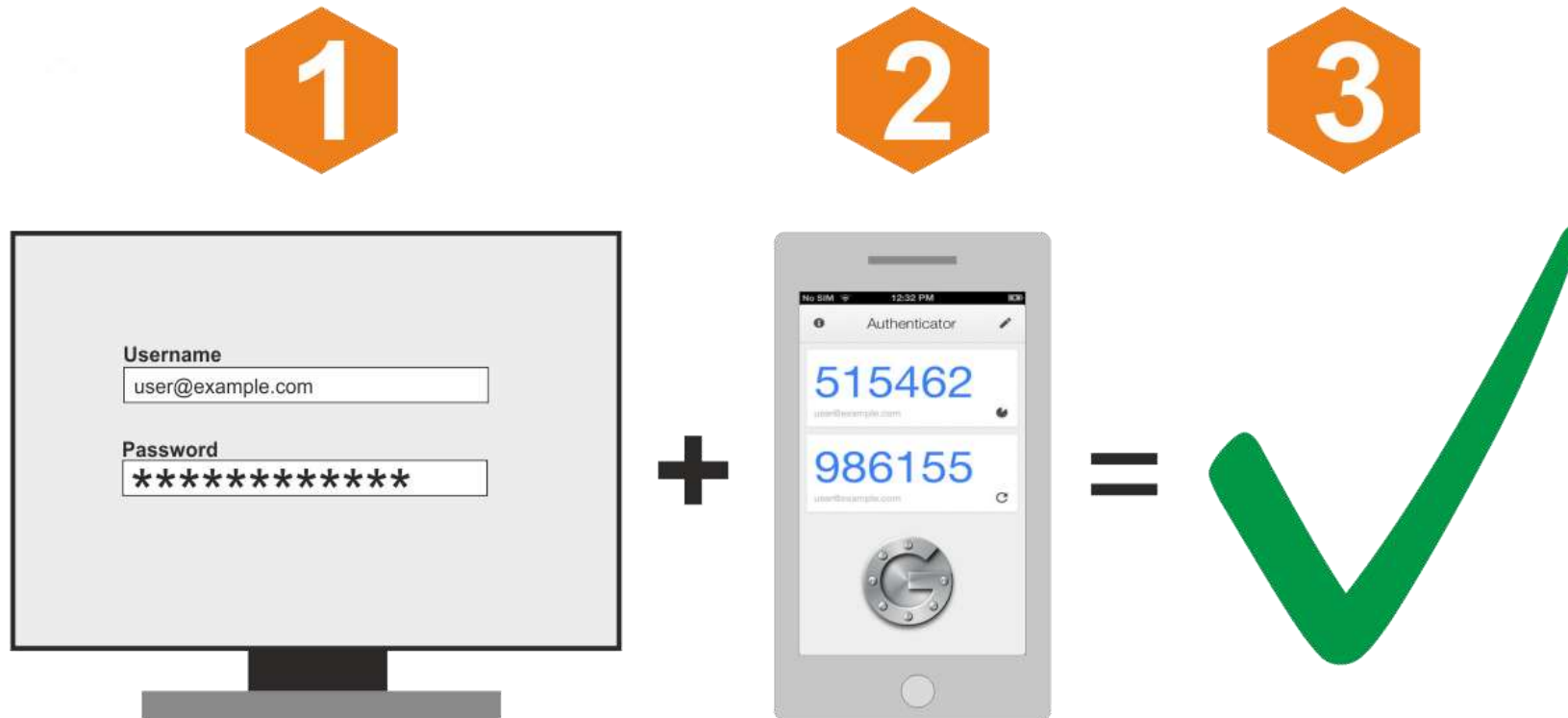


- Datenbank-Datei an verschiedenen physikalisch getrennten Orten speichern
- Ausdruck auf Papier (nur dann, wenn du einen sehr sicheren Ort hast)
→ [Paper Backup](#)



Weitere Hinweise

2FA-Authentifizierung



Du hast es geschafft!



18.05.2021

Fragen / Probleme



David Kopp



Telegram: @davidkopp

Matrix: @dkopp:stuvus.de

E-Mail-Adresse: david.kopp@campusforfuture.de

Links



Ist meine E-Mail-Adresse Teil eines Datendiebstahls? → <https://haveibeenpwned.com/>

Wurden meine Identitätsdaten ausspioniert? → <https://sec.hpi.de/ilc/search>

Diceware-Wortliste DE: http://world.std.com/~reinhold/diceware_german.txt

Diceware-Generator: <https://www.starkes-passwort.de/diceware-generator/>

Getting Started Guide: https://keepassxc.org/docs/KeePassXC_GettingStarted.html

Präsentation: <https://hochschule-n-bw.de/mediathek/>