Verschlüsselung

So lassen sich Daten vor unbefugtem Zugriff schützen

Image by Peter Lomas: https://pixabay.com/de/illustrations/internet-sicherheit-verschl%C3%BCsselung-2537786/

Ein Vertiefungsworkshop des Service-Teams Forschungsdaten in Kooperation mit dem Chaos Computer Club Hannover e.V. und dem LUIS-Sicherheitsteam

24. Oktober 2024

Kennenlernen

Bitte stellt euch kurz vor:

- Wie heißt ihr?
- Was ist euer Fachgebiet?
- Was motiviert euch, heute hier zu sein?

Image by Freepik: https://www.freepik.com/free-photo/low-angle-friends-chairs-with-chat-bubbles_5965457.htm

Was euch heute erwartet

14:00	Kennenlernen
14:20	Einführung: Was ist Verschlüsselung und wie funktioniert sie?
14:40	Verschlüsseltes Kommunizieren über den Messenger-Dienst Matrix
	kurze Pause
15:40	Verschlüsseln von Datei-Containern mit Veracrypt und Cryptomator
	kurze Pause
16:40	Verschlüsseln von E-Mails mit S/MIME und PGP
17:40	Feedbackrunde

Image by Menno de Jong: https://pixabay.com/de/photos/lemur-neugierig-halfaap-guck-guck-329589

Gast-WLAN (für alle, die kein Eduroam haben)**:**

Netzwerkname(SSID): UHEvent
WPA2-Schlüssel: Y3bGK8tV

Aufgaben Matrix Messenger

- Anleitungen:
https://www.luis.uni-hannover.de/de/services/kommunikation/matrix-messenger

1) Führen Sie die Ersteinrichtung im Element-Client (oder alternativ im Browser) durch

2) Erstellen Sie einen privaten Raum und laden Sie andere Personen aus dem Workshop ein

3) Erstellen Sie eine Umfrage

4) Versenden Sie eine Datei

5) Erstellen Sie einen Space, fügen Sie Räume und Personen hinzu und testen Sie die Einstellungen

Dateiverschlüsselung mit Veracrypt

Was ist und kann Veracrypt?

Neue Container-Datei verschlüsseln 1

Neue Container-Datei verschlüsseln 2

Container-Datei erstellen oder auswählen

Containergröße festlegen und Passwort wählen

Dateisystem wählen und „Zufälligkeit“ generieren

Geschafft!

Verschlüsselten Container und Laufwerksbuchstaben auswählen

Passwort eingeben

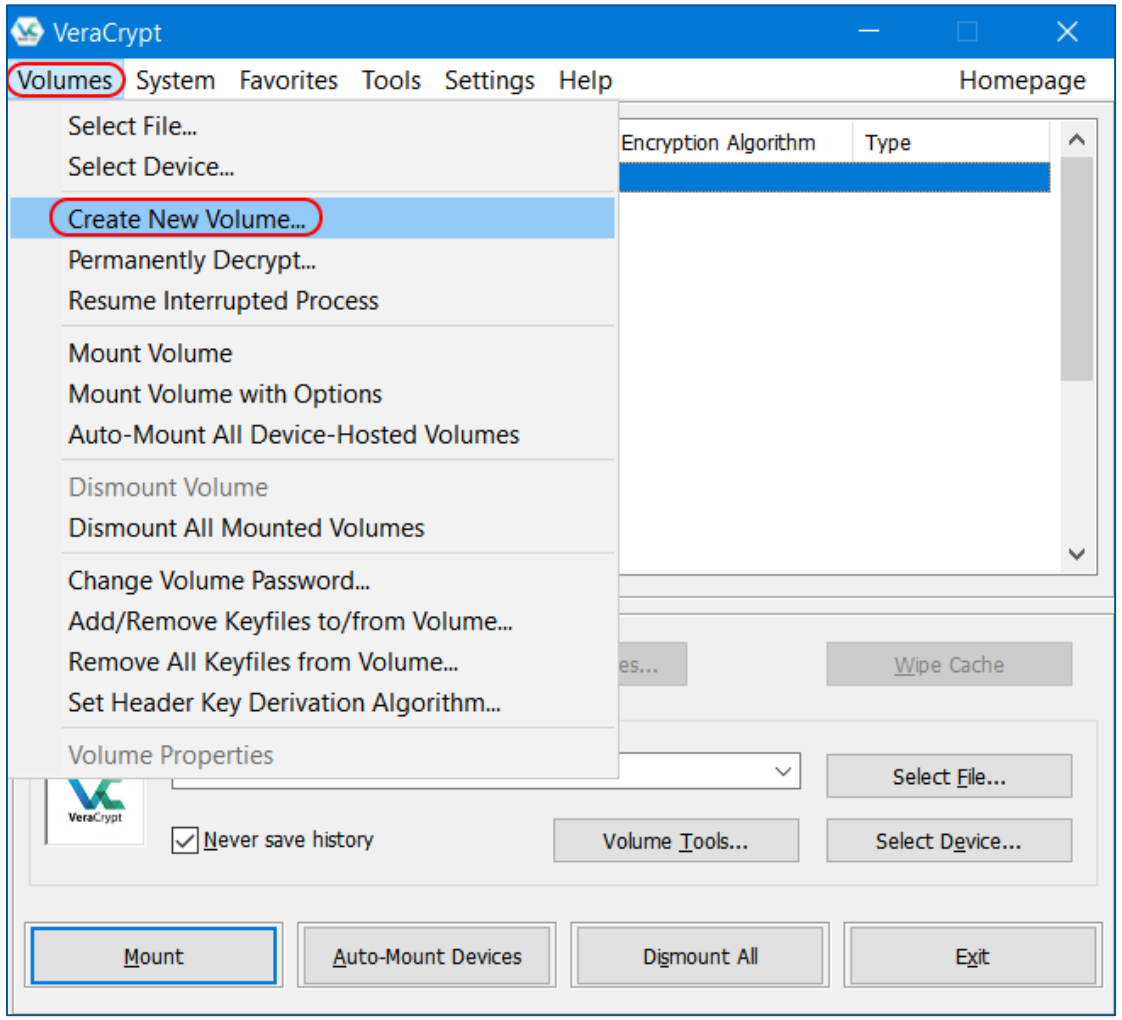
Was ist und kann Veracrypt?

- Verschlüsselt Container-Dateien und ganze Laufwerke (auch Systemlaufwerke)
- Nutzt symmetrische Verschlüsselung: alle Zugriffsberechtigten nutzen dasselbe Passwort
- Kann Container-Dateien verstecken
- Kann mehrere Verschlüsselungsalgorithmen verschachteln
- Container/Laufwerke werden stets komplett entschlüsselt
  → große Angriffsfläche für Hacker

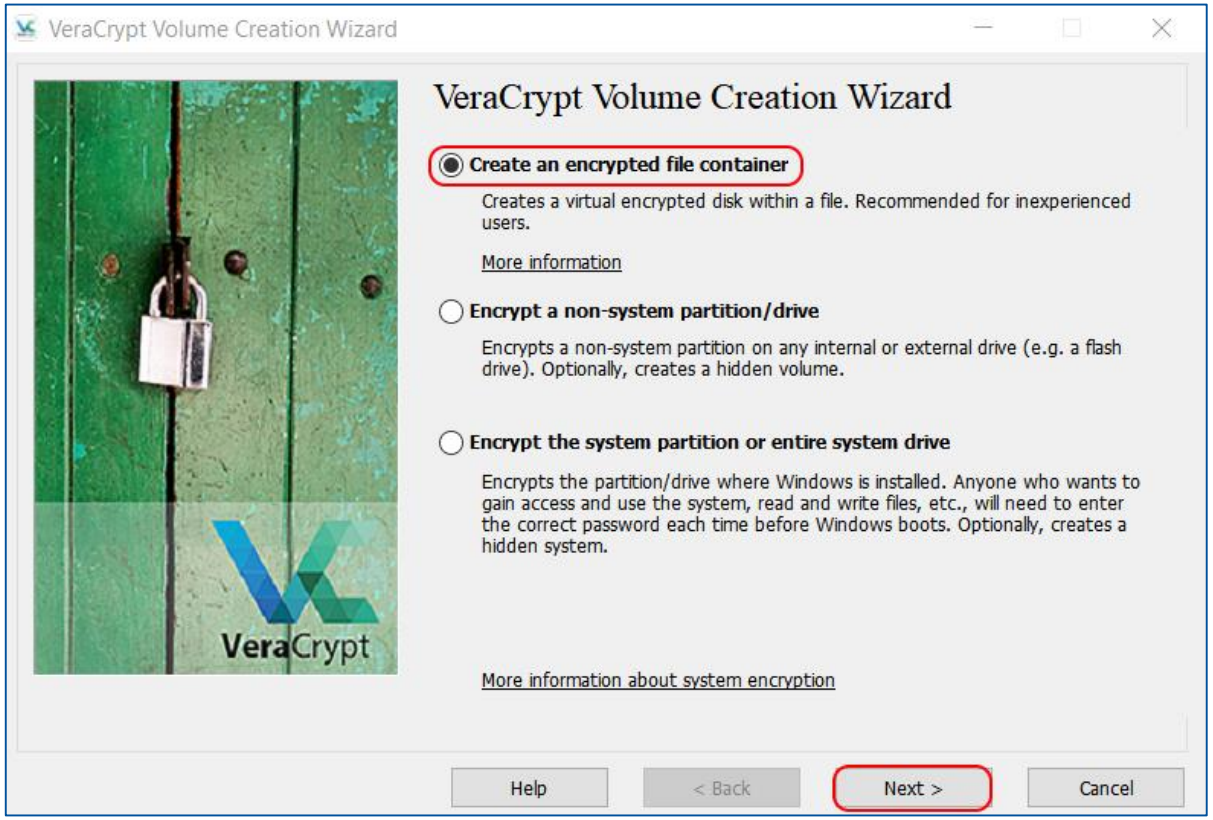
Offizielle Dokumentation

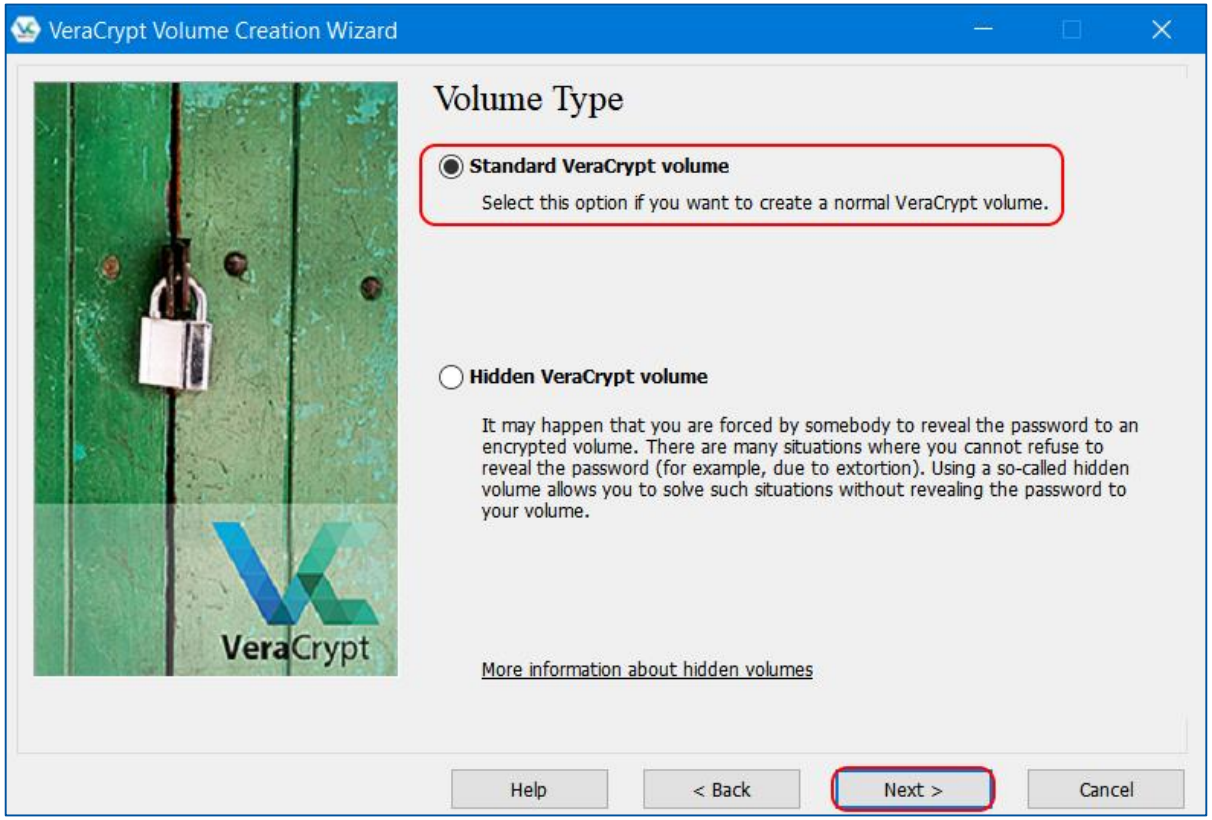
Tutorial-Videos (YouTube)

Neue Container-Datei verschlüsseln 1

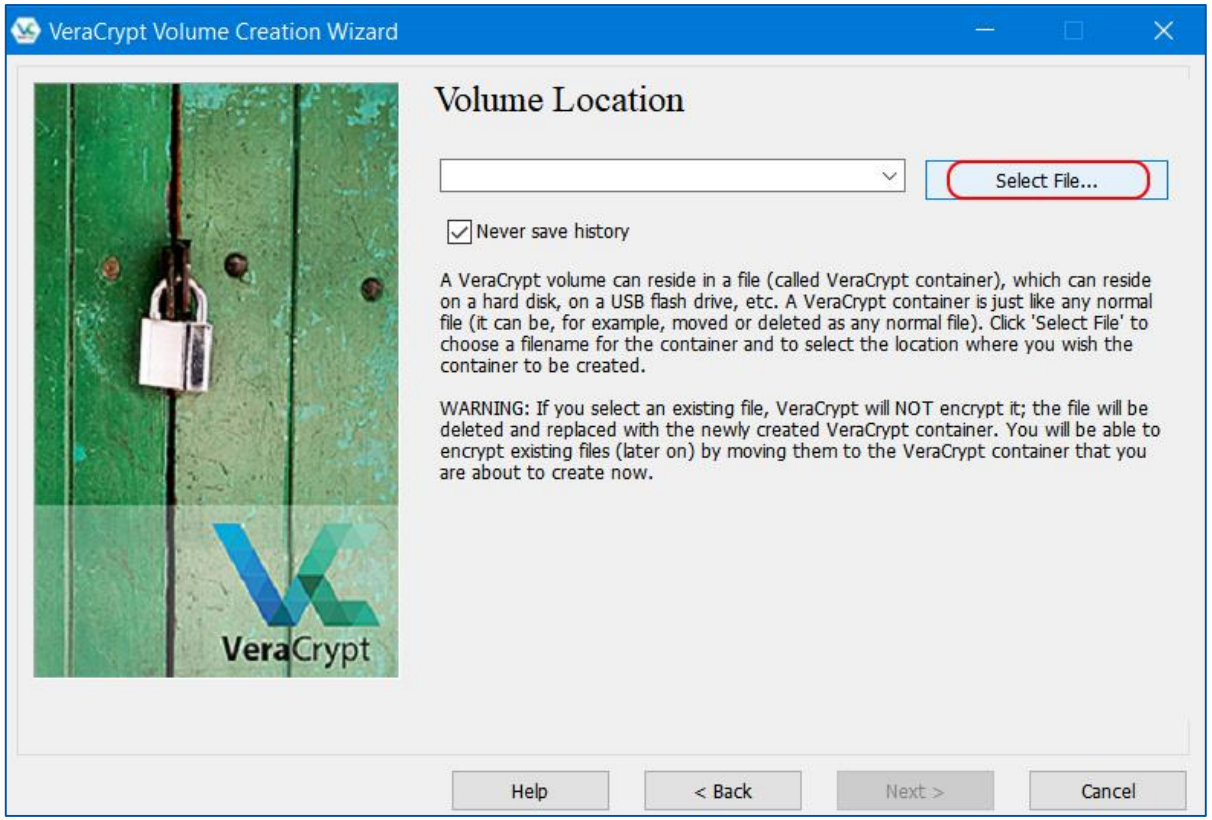


Neue Container-Datei verschlüsseln 2

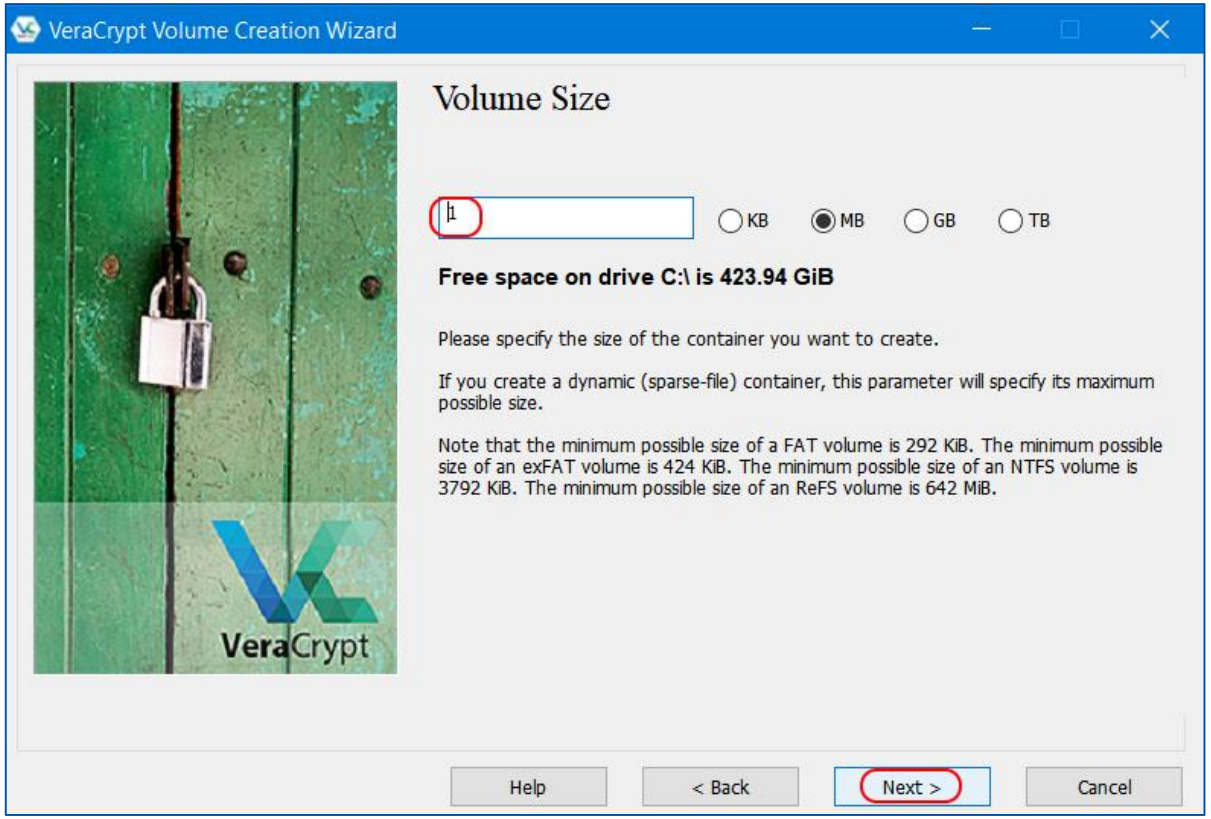


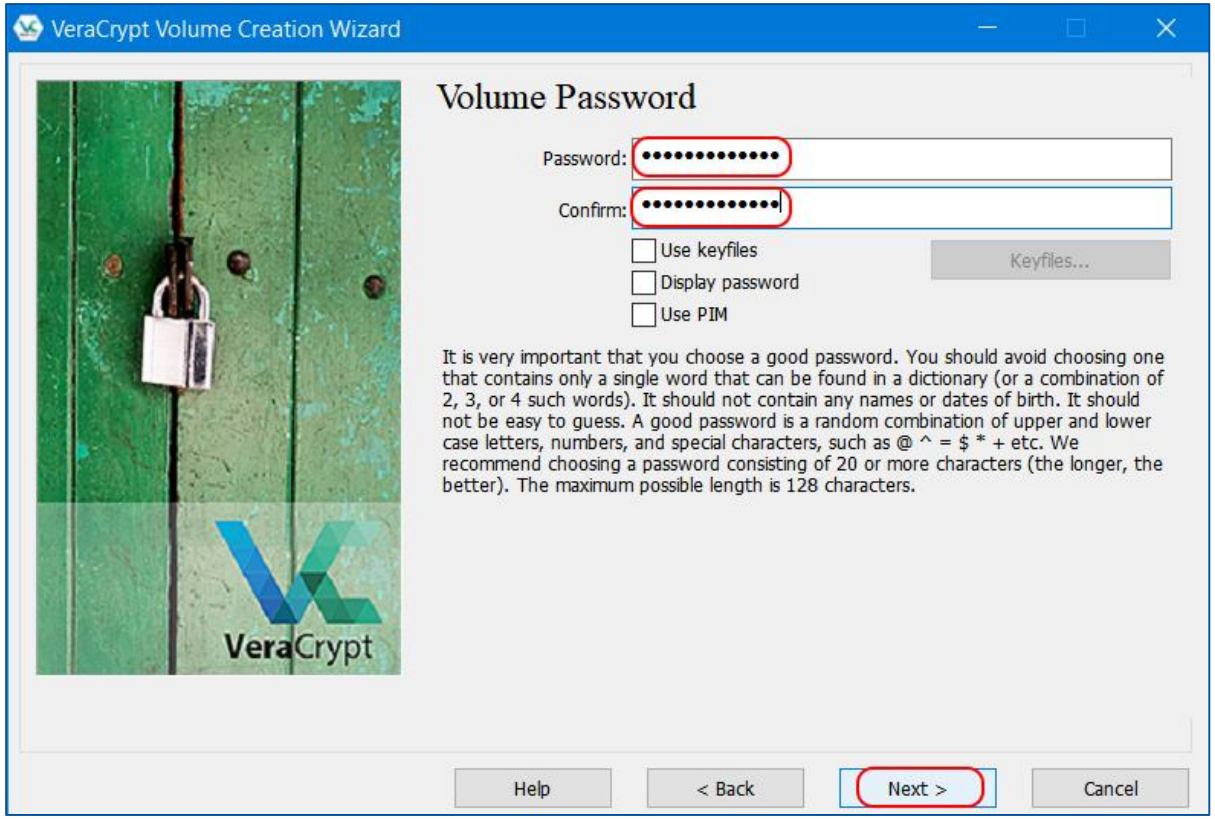


Container-Datei erstellen oder auswählen

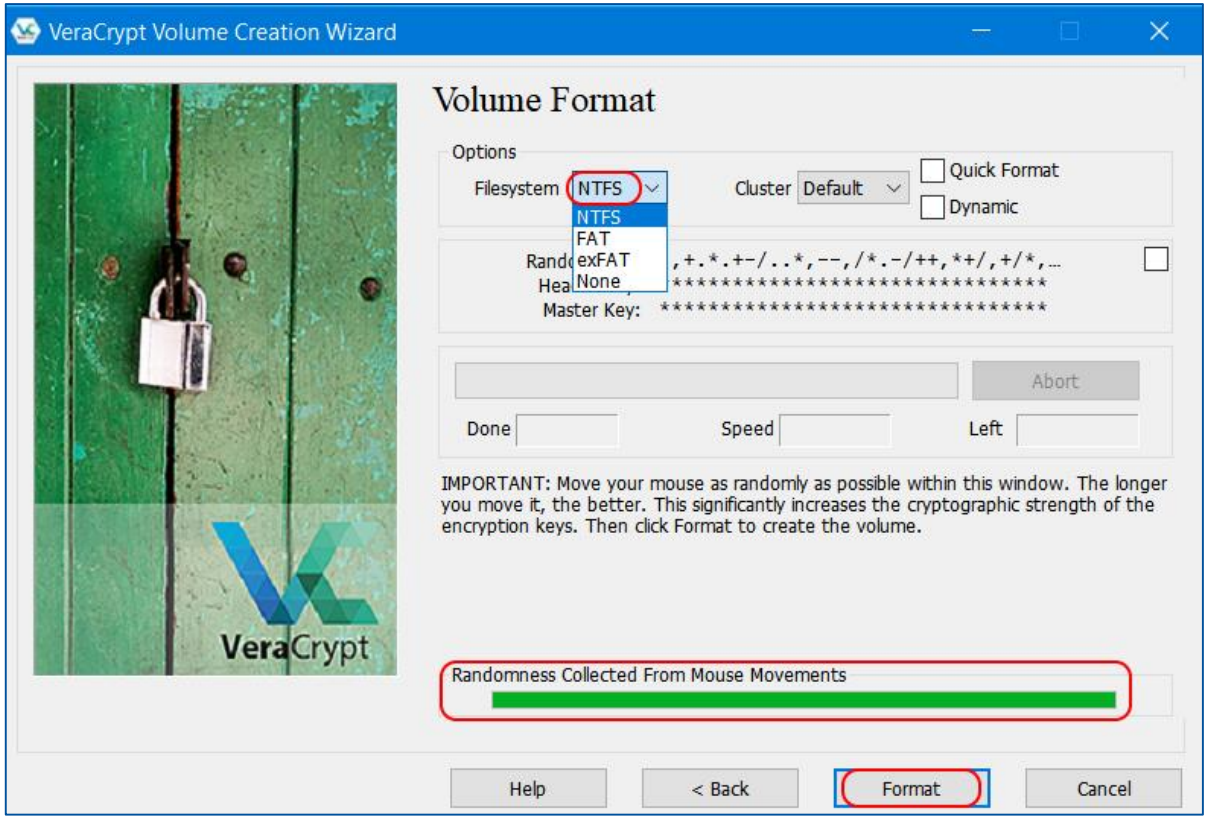


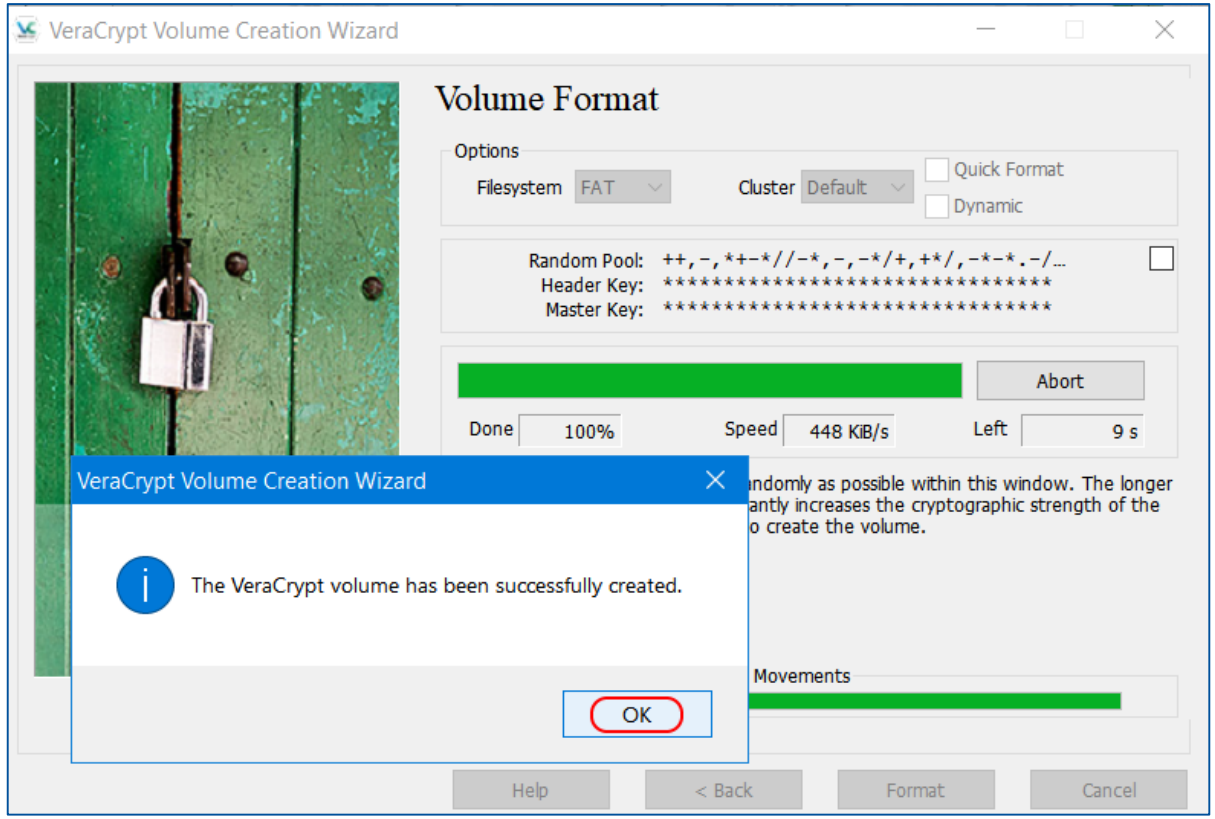
Containergröße festlegen und Passwort wählen



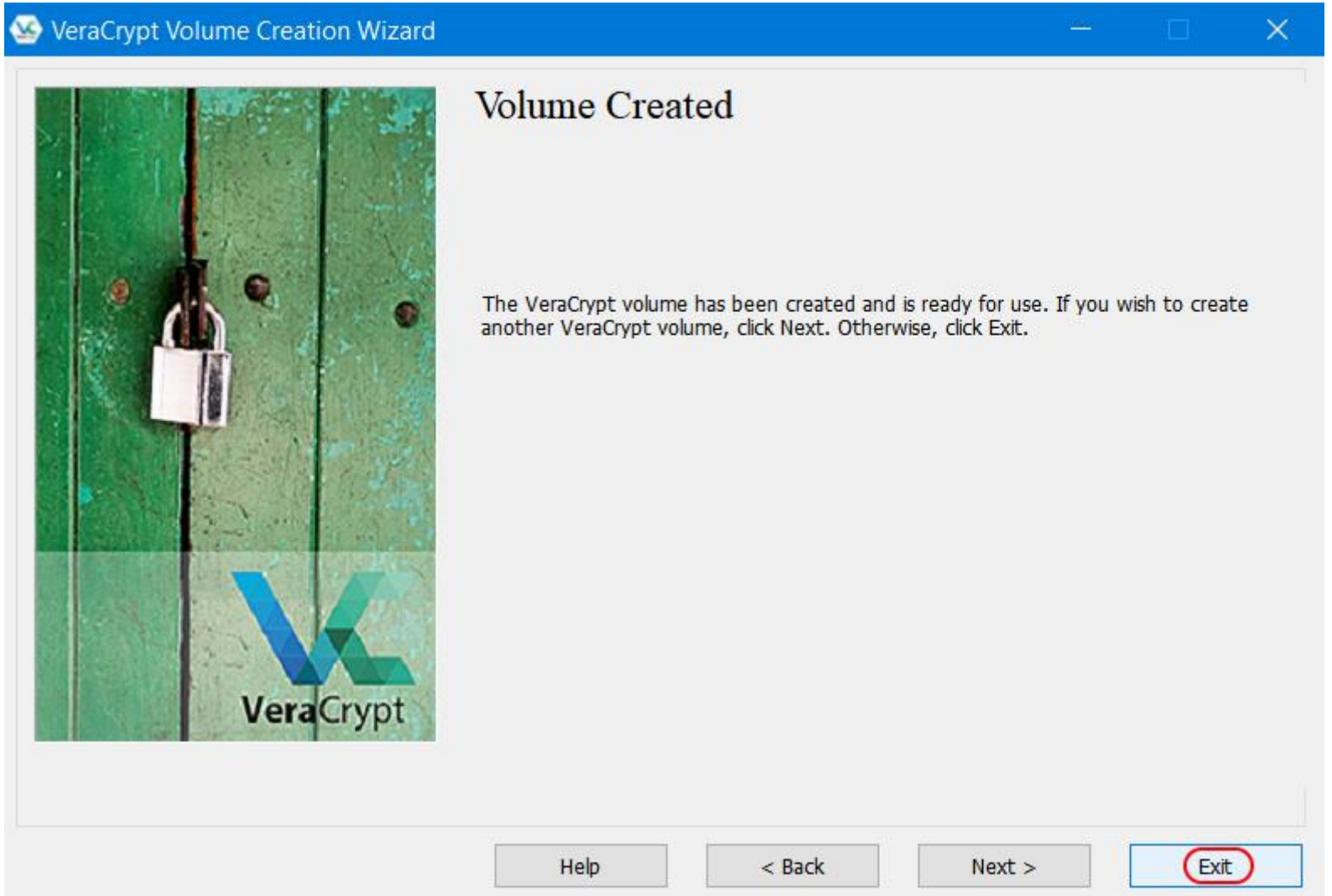


Dateisystem wählen und „Zufälligkeit“ generieren

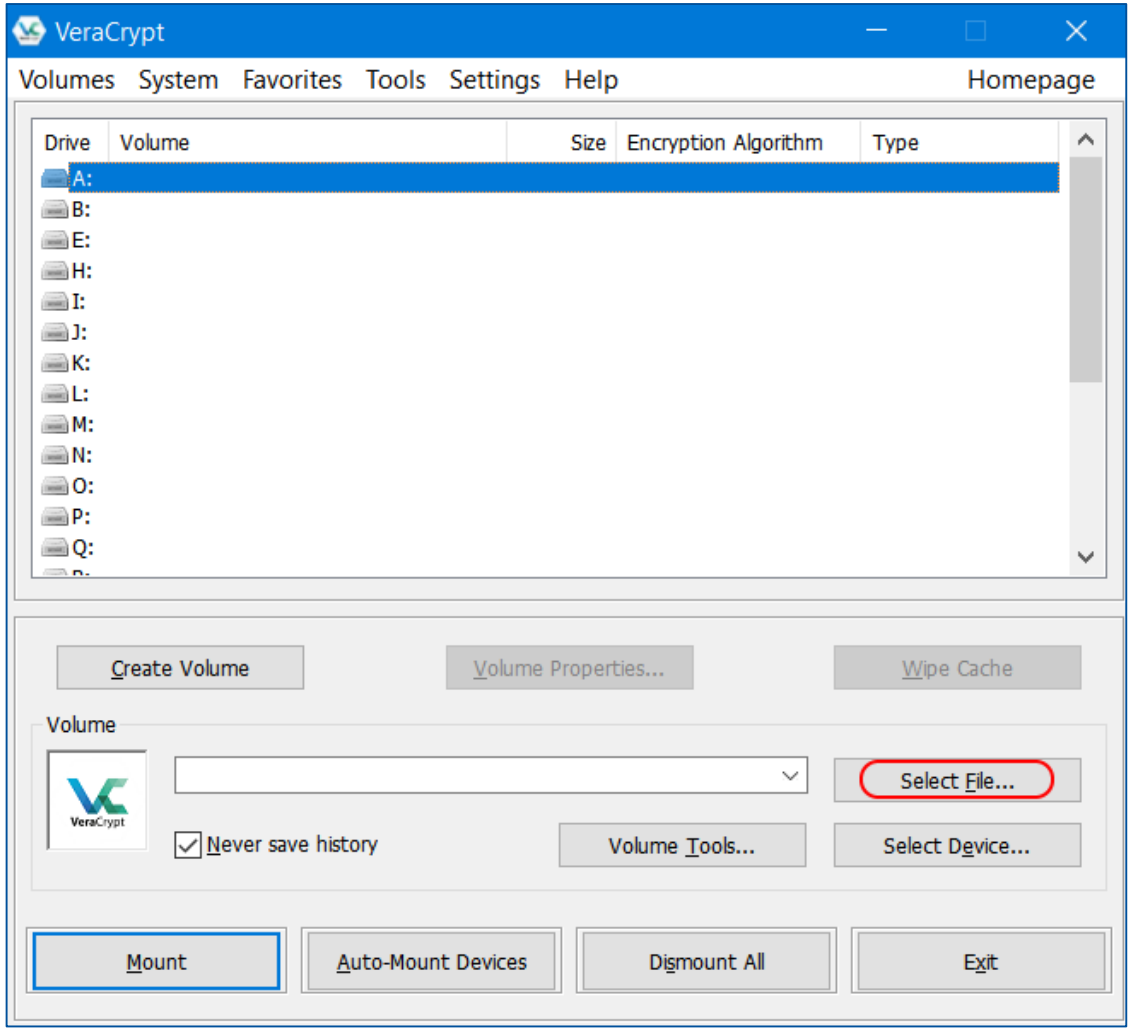


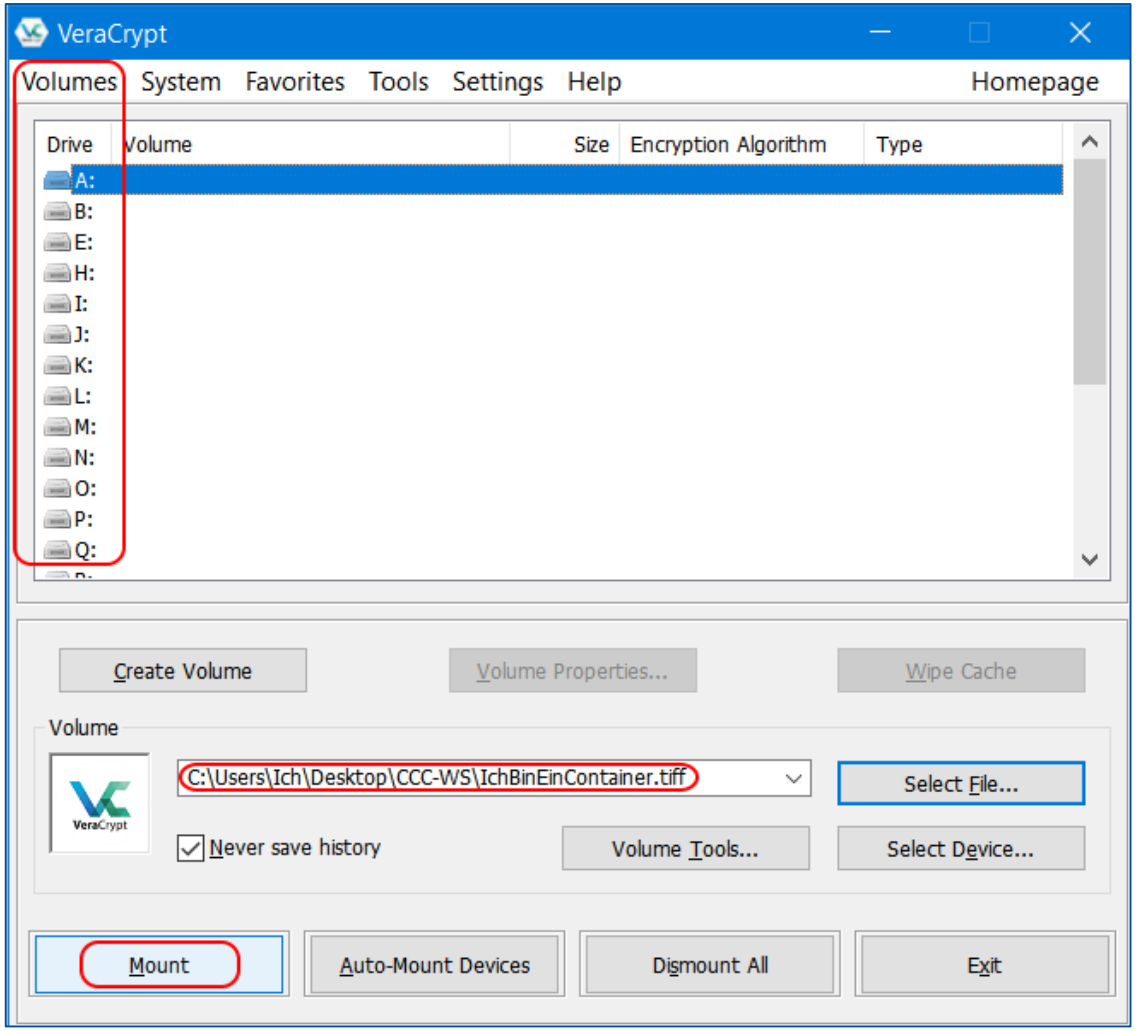


Geschafft!

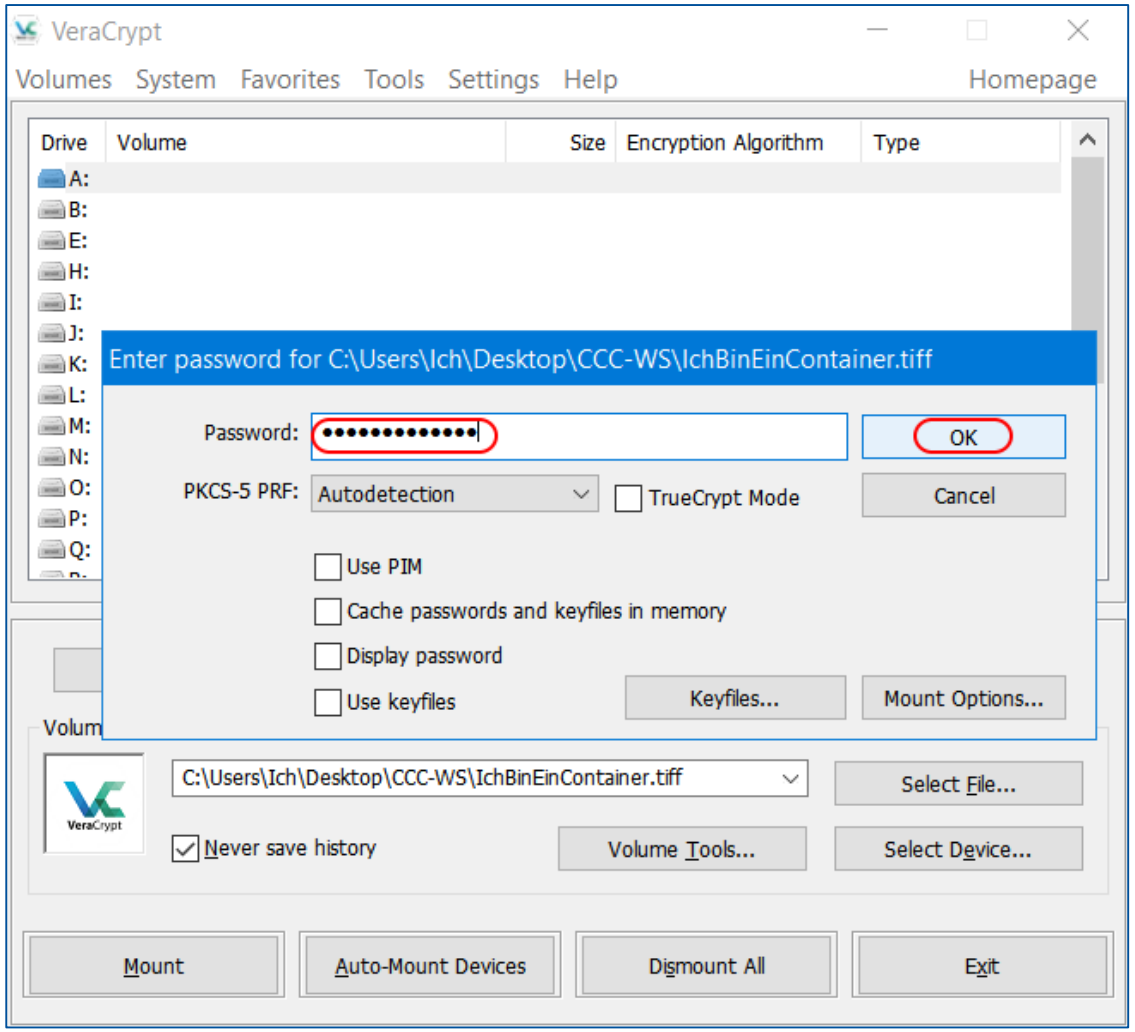

VeraCrypt Volume Creation Wizard
Volume Created
The VeraCrypt volume has been created and is ready for use. If you wish to create another VeraCrypt volume, click Next. Otherwise, click Exit.
VeraCrypt
Help
< Back
Next >
Exit

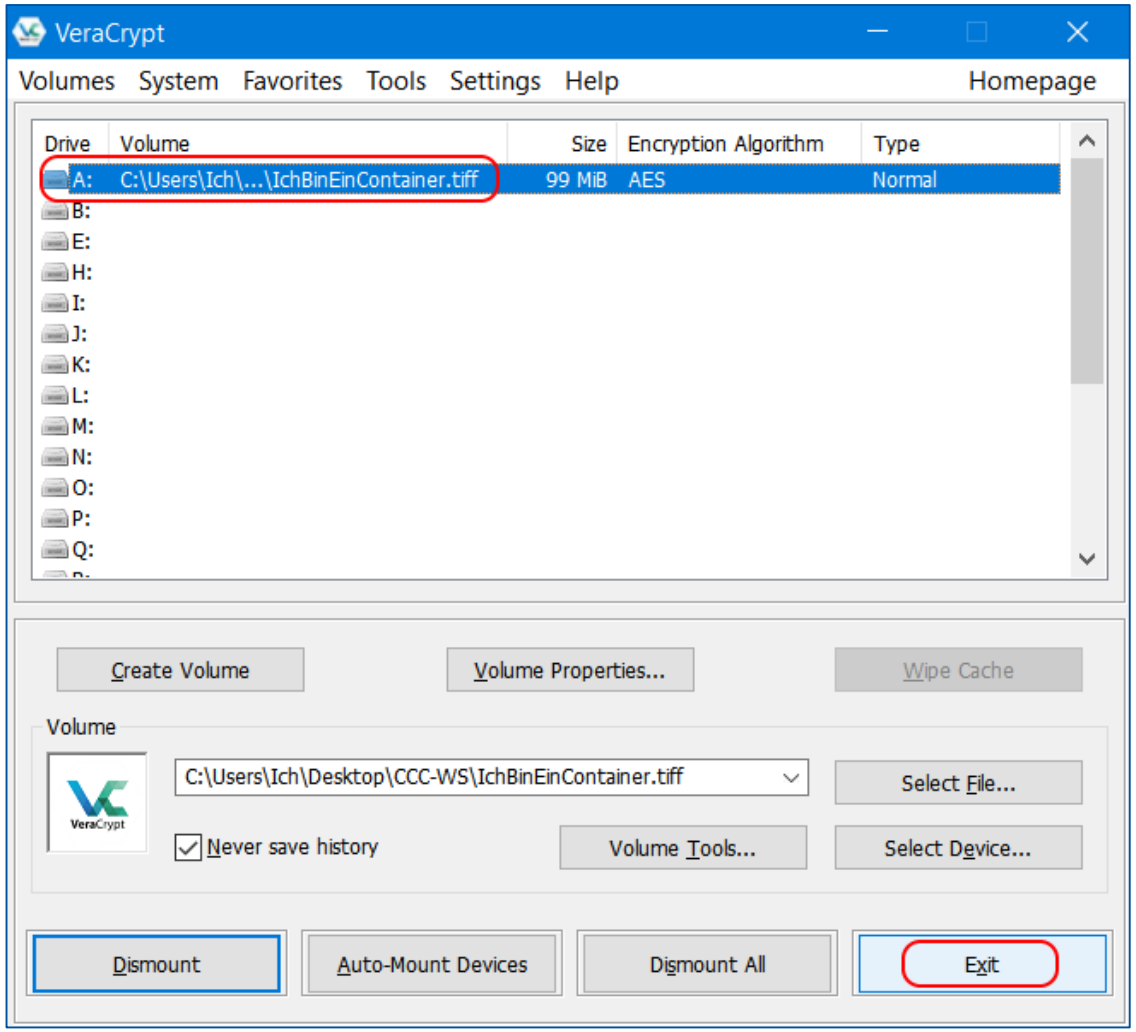
Verschlüsselten Container und Laufwerksbuchstaben auswählen





Passwort eingeben





Dateiverschlüsselung mit Cryptomator

Was ist und kann Cryptomator?

Neuen „Tresor“ anlegen

Namen und Speicherort wählen

Passwort wählen und Recovery Key generieren

„Tresor“ öffnen

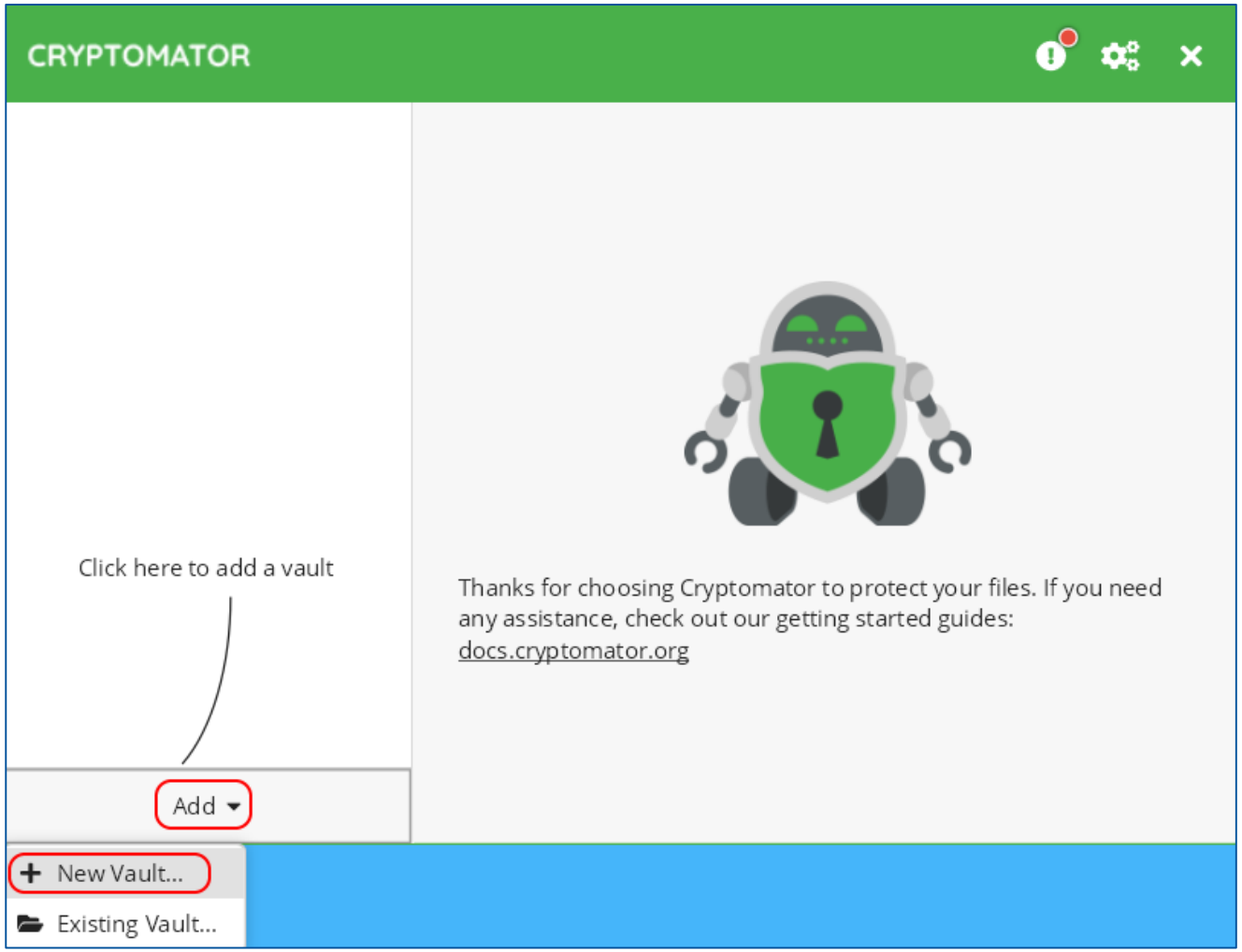
Was ist und kann Cryptomator?

- Verschlüsselt Container-Dateien („Tresore“)
- Nutzt symmetrische Verschlüsselung: alle Zugriffsberechtigten nutzen dasselbe Passwort
- Optimiert für die Nutzung in Cloudspeichern
- Nicht geöffnete Dateien im Container bleiben auch dann verschlüsselt, wenn der Container geöffnet ist → wenig Angriffsfläche für Hacker

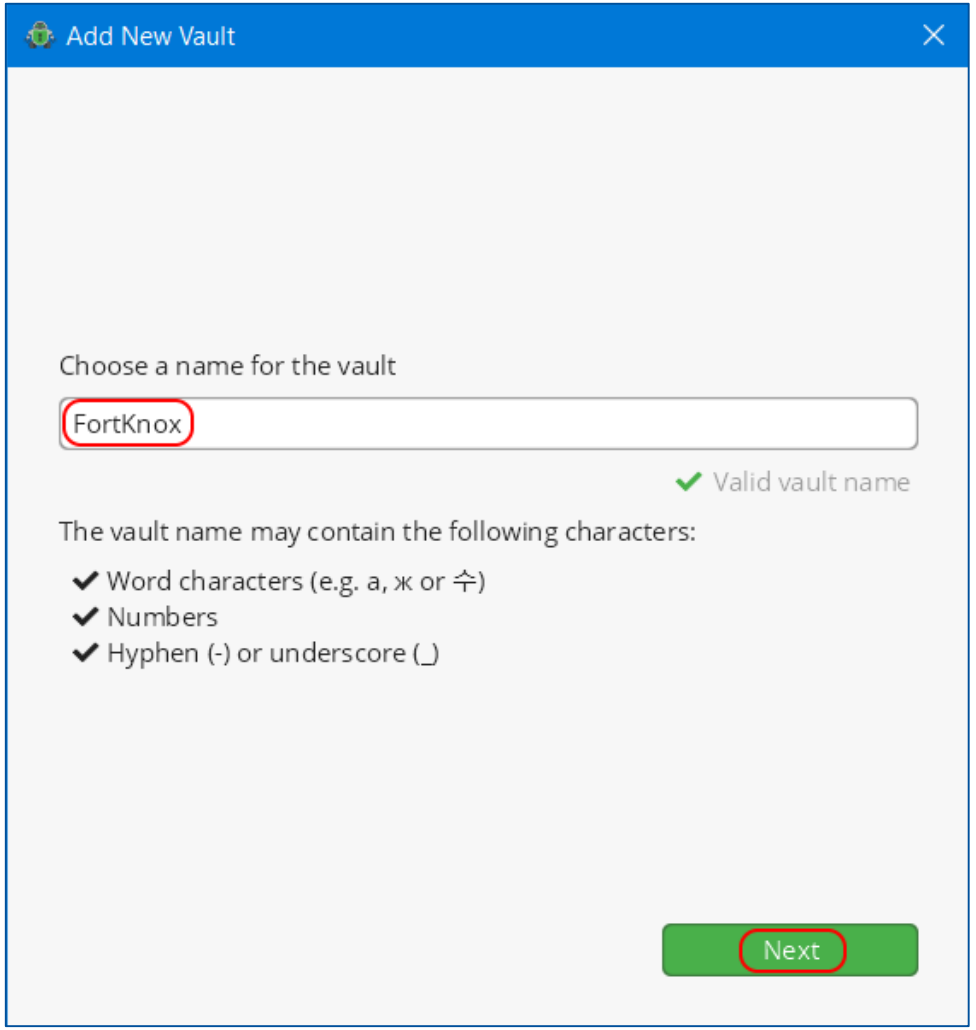
Offizielle Dokumentation

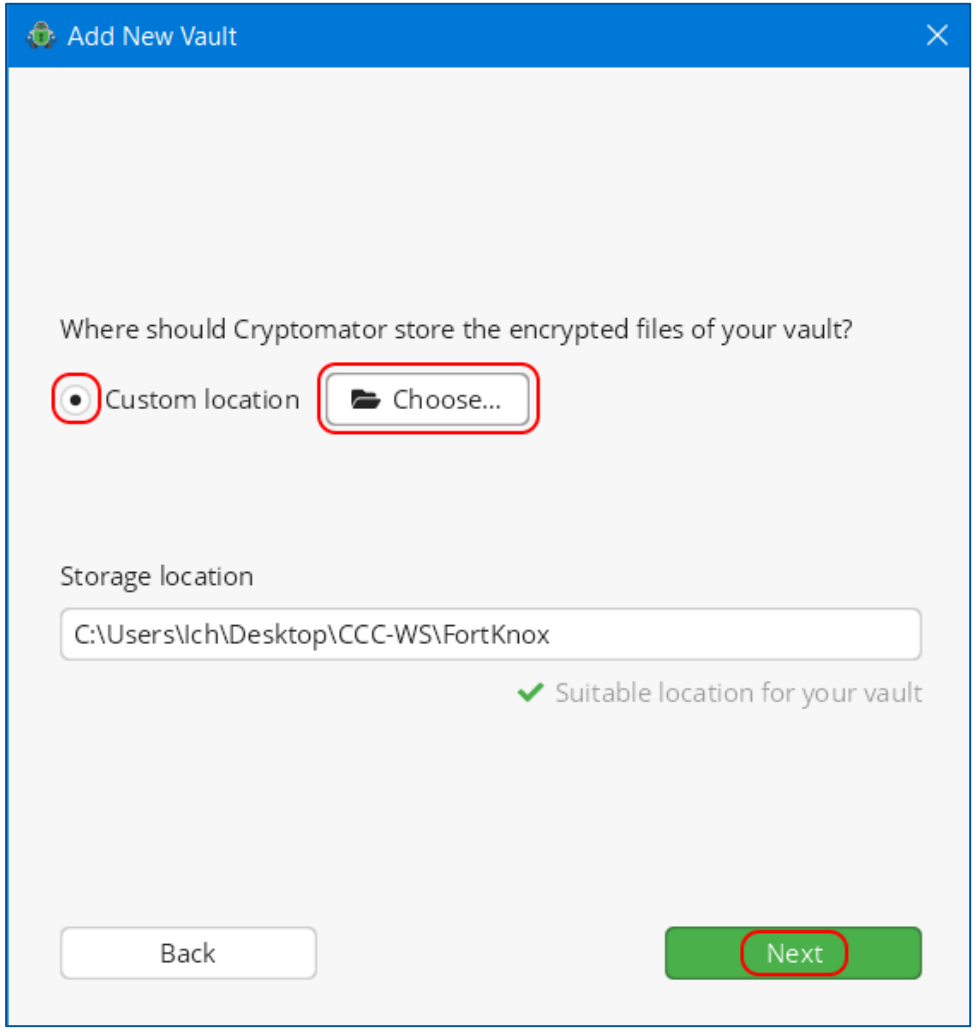
Tutorial-Videos (YouTube)

Neuen „Tresor“ anlegen

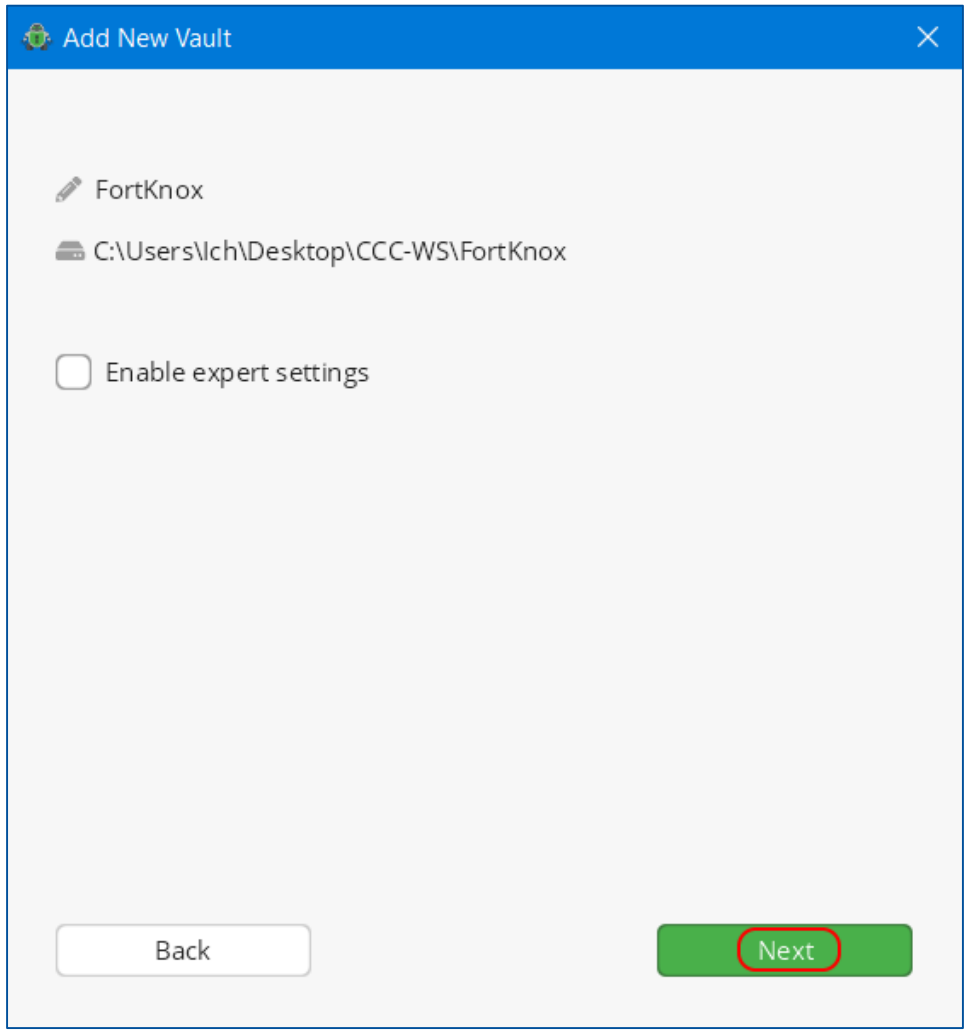


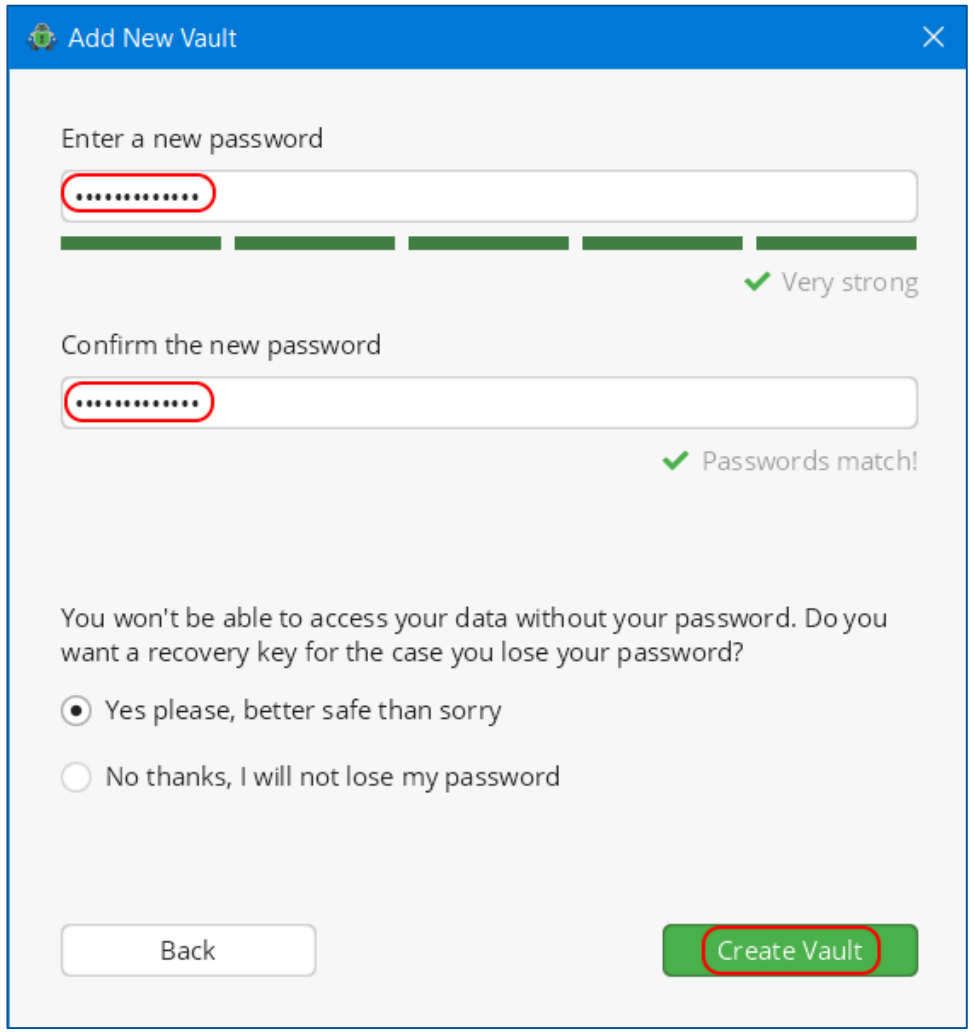
Namen und Speicherort wählen



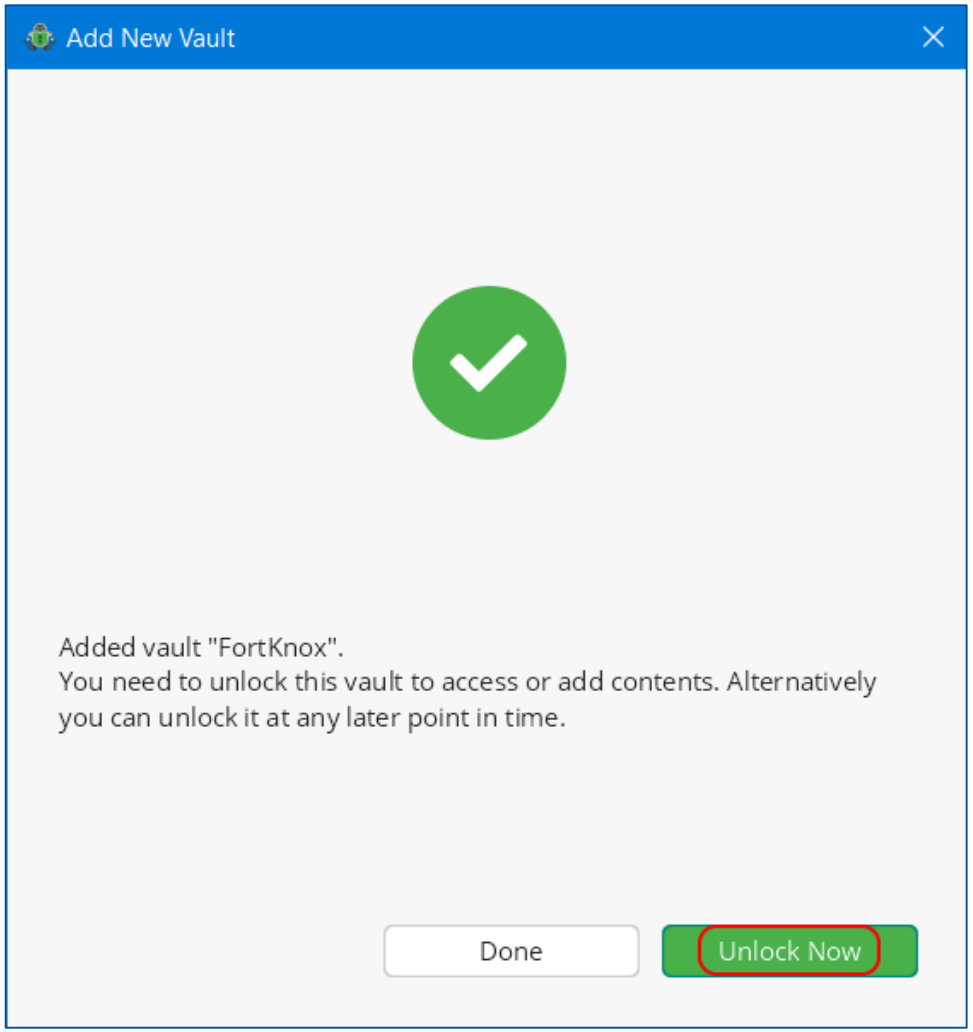


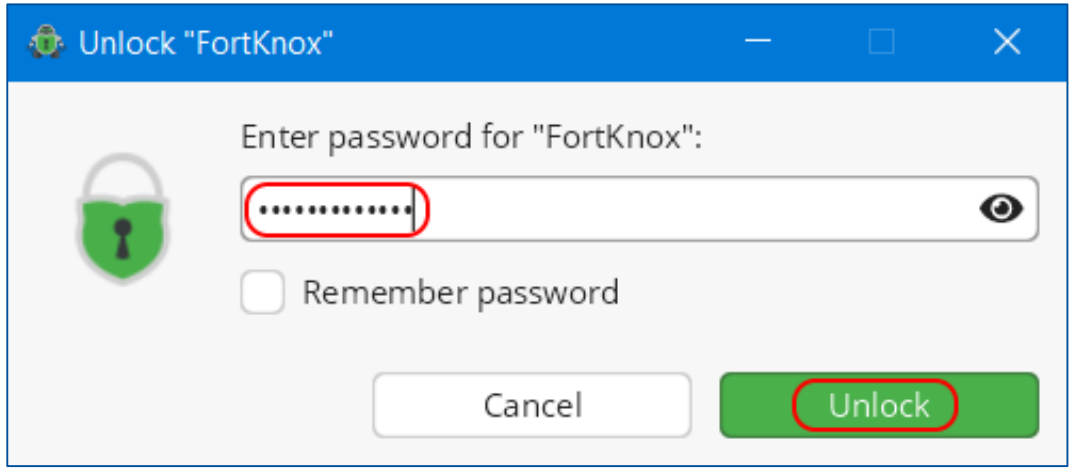
Passwort wählen und Recovery Key generieren

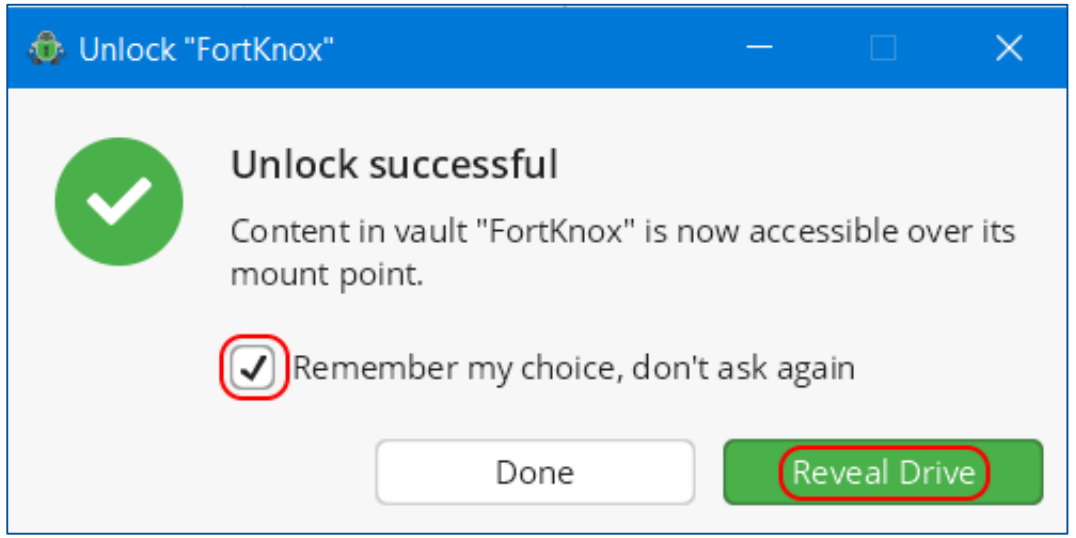




„Tresor“ öffnen





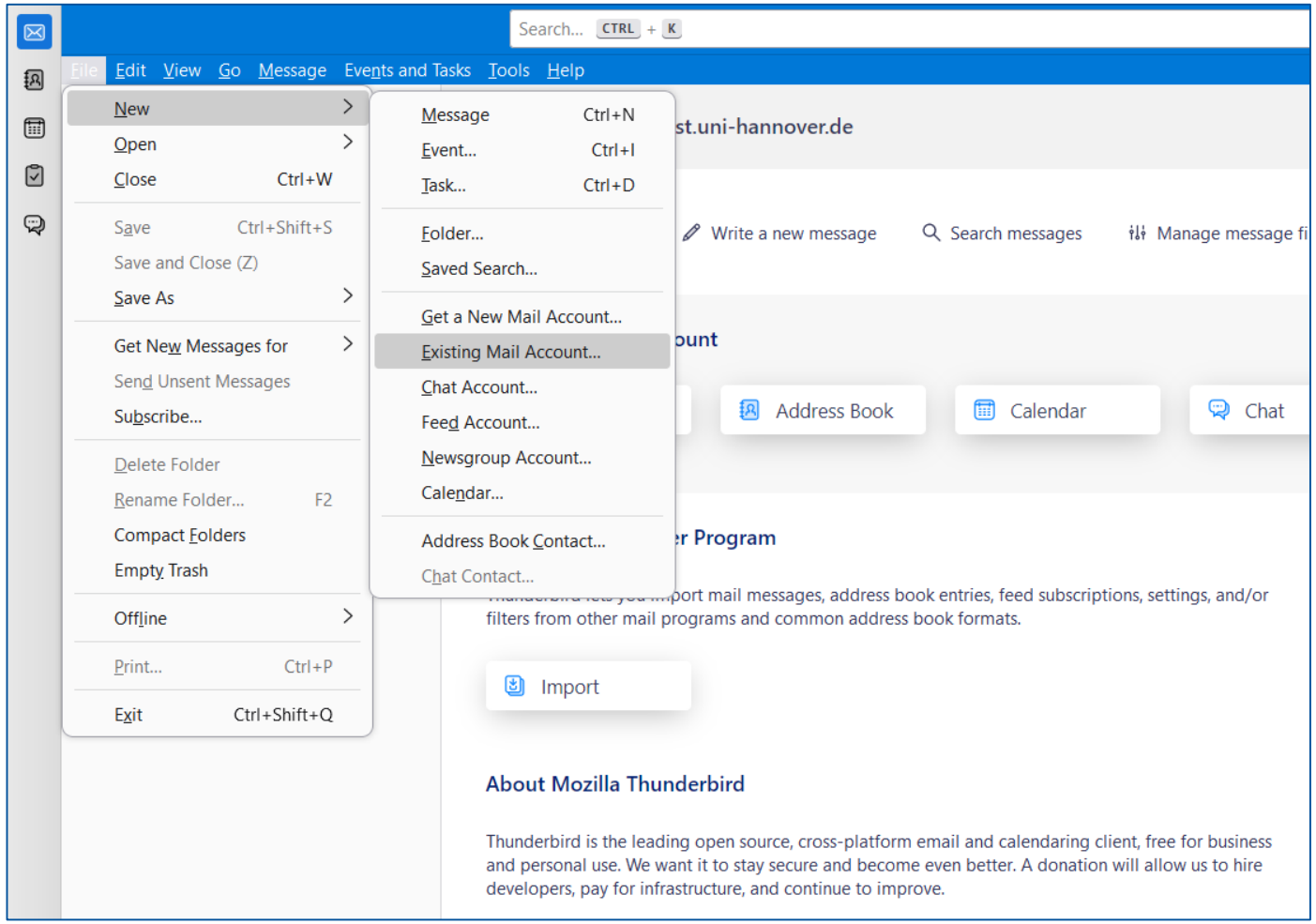


E-Mail-Konto in Thunderbird einbinden

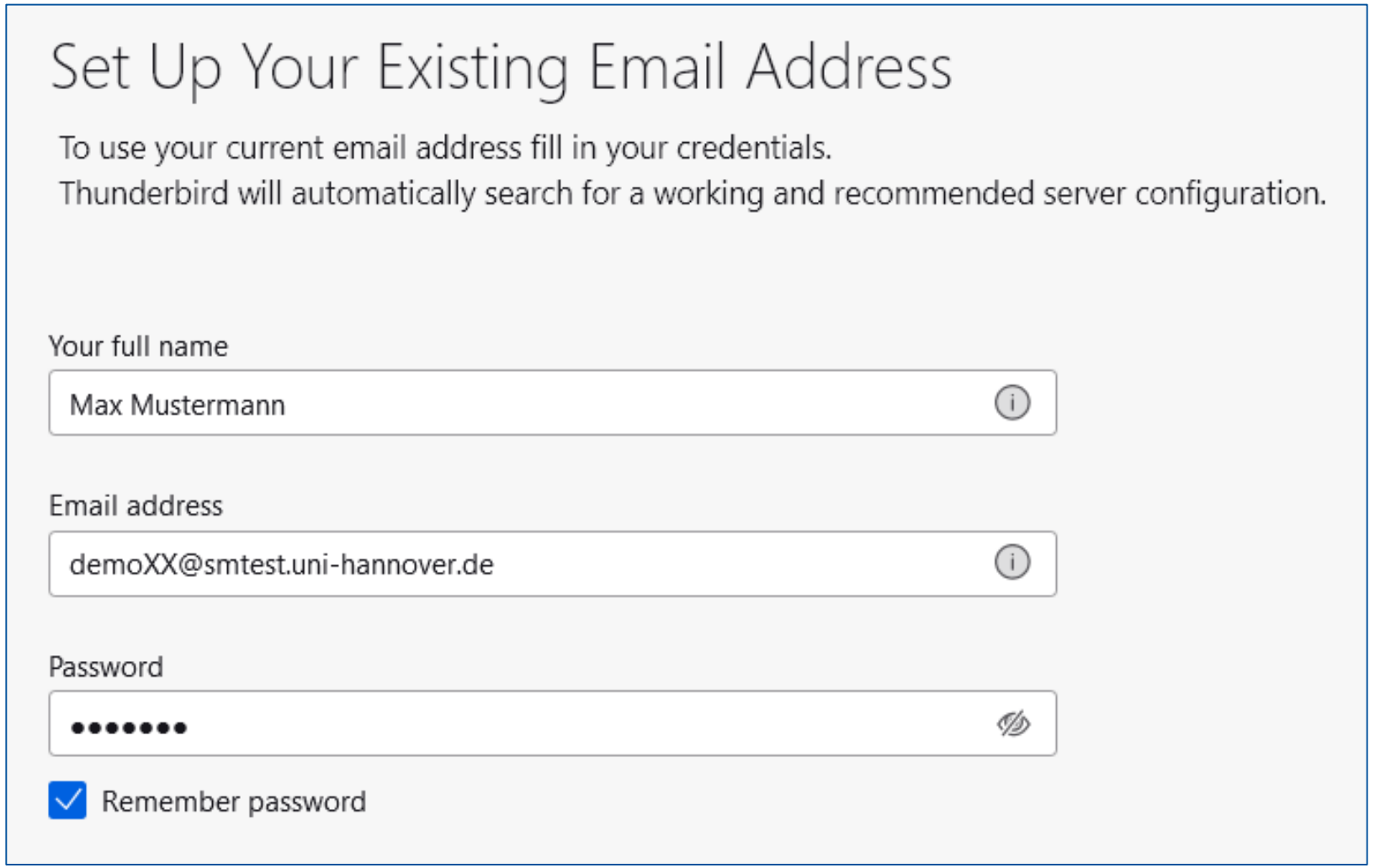
Neues Profil für einen existierenden Account anlegen

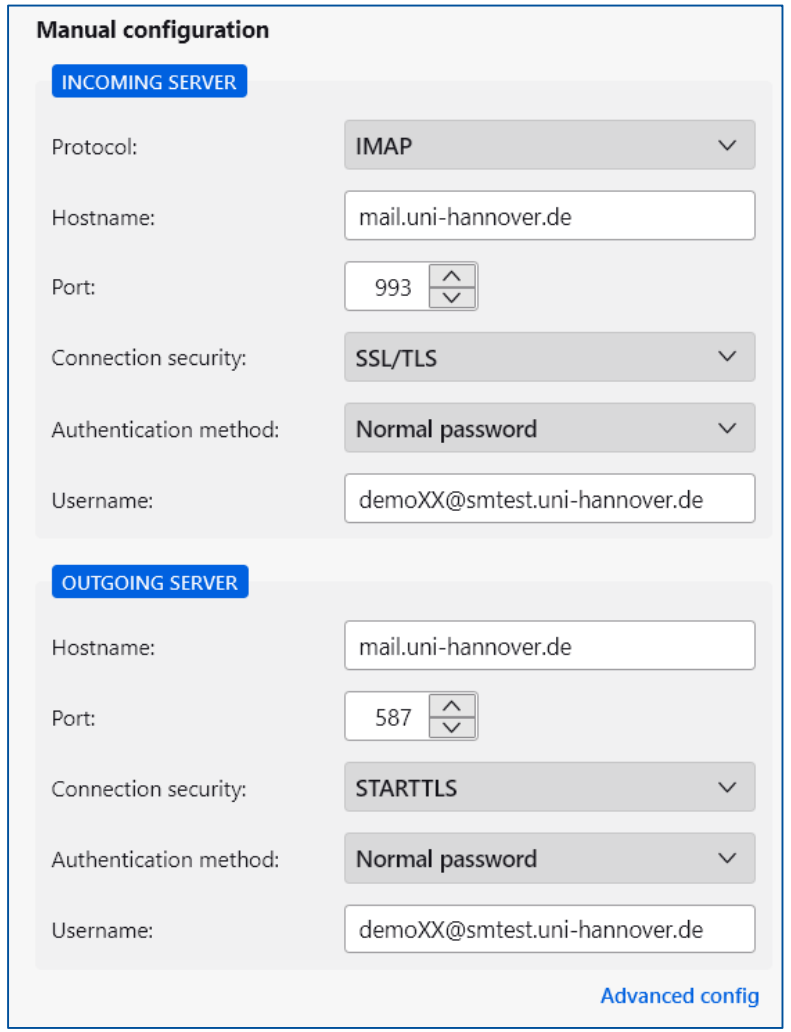
Account- und Mailserver-Daten angeben

Neues Profil für einen existierenden Account anlegen



Account- und Mailserver-Daten angeben





Leibniz Universität IT Services

Leibniz Universität Hannover

Nutzerzertifikate (S/MIME) an der LUH

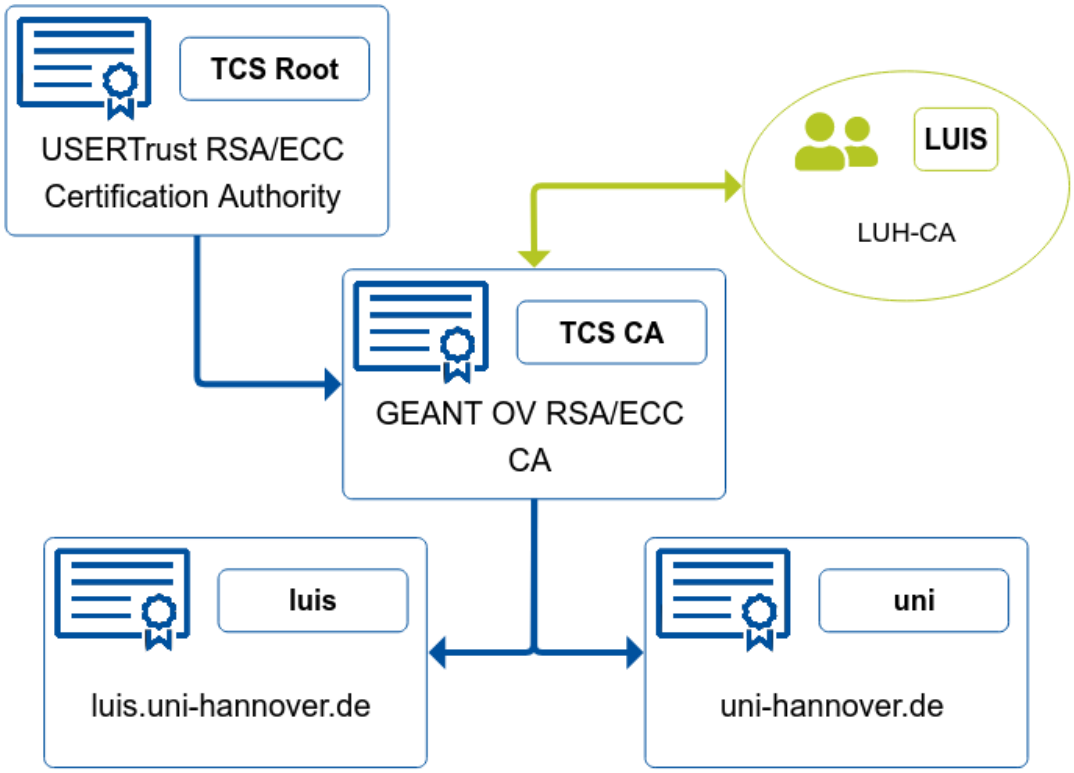
S/MIME

- **S**ecure / **M**ultipurpose **I**nternet **M**ail **E**xtensions
- Standard für Signierung & Verschlüsselung
- S/MIME-Zertifikat verbindet
  - privatem und öffentlichem Schlüssel mit
  - Name, E-Mail-Adresse,…

- **PKI**-Hierarchie (Public-Key-Infrastructure)
  - Vertrauensanker: **Wurzelzertifikat** (ggf. browserverankert)
  - Zertifizierungsstelle (**CA**) stellt Zertifikate aus
- **Identifizierung**snachweis bei Beantragung notwendig

- Nutzbar für E-Mail oder auch Dokumente (z.B. PDFs)

Beispiel: Zertifikatshierarchie bei GEANT TCS



S/MIME im Vergleich zu PGP

S/MIME	PGP
PKI-Hierarchie	Web of Trust
CA stellt Zertifikate aus	Nutzer generiert Schlüssel
Verwendung in Unternehmen / Organisationen	Verwendung „für jeden“. Gute Alternative, um „mit extern“ zu kommunizieren.

Links

- Anleitungen:
https://www.luis.uni-hannover.de/de/services/it-sicherheit/zertifikate-der-luh-ca/anleitungen

- Beantragung Nutzerzertifikate:
https://www.luis.uni-hannover.de/de/services/it-sicherheit/zertifikate-der-luh-ca/nutzerzertifikate

- Rund um Zertifikate:
https://www.luis.uni-hannover.de/de/services/it-sicherheit/zertifikate-der-luh-ca

- Rund um E-Mail-Sicherheit:
https://www.luis.uni-hannover.de/de/services/it-sicherheit/praevention/e-mail