Browser und Erweiterungen

Wahl des Browsers

Empfohlener Webbrowser: **Mozilla Firefox**

- Für GNU/Linux, Windows und macOS: https://mozilla.org/de/firefox/new/
- Für Android: https://www.mozilla.org/de/firefox/android/
- Für iOS: https://www.mozilla.org/de/firefox/ios/

Einstellungen

≡ **Menübutton** → ***Einstellungen*** → ***Datenschutz***:

- **Chronik**: nach benutzerdefinierten Einstellungen, dort z.B. einstellen:
  - Cookies von Drittanbietern nicht akzeptieren
  - Chronik löschen, wenn Firefox geschlossen wird (insbes. Cookies)
  - ***Do Not Track*** aktivieren (Websites mitteilen, Ihre Aktivitäten nicht zu verfolgen)

≡ **Menübutton** → ***Einstellungen*** → ***Suche***:

- Alternative **Suchmaschinen** hinzufügen, Suchvorschläge deaktivieren und Standardsuchmaschine ändern (z.B. StartPage.com, Ixquick.eu, MetaGer.de, DuckDuckGo.com)

Erweiterungen / Add-ons & Plugins

≡ **Menübutton** → ***Add-ons*** → ***Alle Add-ons durchsuchen***:

- **uBlock Origin** blockiert Werbung und Tracker
- **HTTPS Everywhere** ruft verschlüsselte Verbindung zu Websites auf, wenn verfügbar
- **NoScript** verbessert die Sicherheit des Browsers und blockiert die Ausführung von Programmen – Einstellung: ***Skripte allgemein erlauben*** (auch wenn dies nicht vom Entwickler empfohlen wird)
- **Privacy Settings** konfiguriert diverse Einstellungen des Firefox im Sinne des Datenschutzes – empfohlene Einstellung: ***Privacy (compatible) & Security***

Add-ons für Fortgeschrittene:

- **NoScript** mit der Standardeinstellung ***Skripte allgemein verbieten***, Whitelist löschen
- **uMatrix** unterbindet alle Drittanbieteraufrufe

Adobe Flash Player:

- Deinstallieren oder Deaktivieren (***Shockwave Flash*** unter ***Add-ons*** → ***Plugins***)
- Falls man auf Flash angewiesen ist: Nur auf Nachfrage aktivieren

Wirkung der Einstellungen und Add-ons überprüfen:

- Die Erweiterung **Lightbeam** zeigt von welchen Drittanbietern Inhalte nachgeladen werden (eine dauerhafte Aktivierung des Add-ons ist nicht ratsam, da es langsam ist)
- Ohne Add-on: ≡ **Menübutton** → ***Entwickler-Werkzeuge*** → ***Netzwerk-Analyse*** zeigt beim Laden einer Website alle Anfragen als Liste
- Der Browser-Fingerabdruck testen: https://panopticlick.eff.org/

Passwörter

Passwörter wenn möglich nicht im Firefox speichern. Für alle gängigen Betriebssysteme gibt es den Passwortmanager KeePassX: https://www.keepassx.org/

Tor-Browser

Der Tor-Browser ist ein vorkonfigurierter Firefox, der über das Tor-Netzwerk im Internet surft – Erweiterungen zum Schutz der Privatsphäre sind bereits installiert. Weitere Informationen und Download unter: https://www.torproject.org/

Bitte beachtet die umfangreiche Dokumentation, da eure Anonymität im Tor-Netzwerk vor allen Dingen von eurem Surf-Verhalten abhängt. Installiert keine weiteren Add-ons und lest vor Benutzung die offizielle Dokumentation:
https://www.torproject.org/docs/documentation.html.en (Englisch)

E-Mail-Verschlüsselung

Schritt 1: Software installieren

- **GnuPG** zur Verschlüsselung der E-Mails.
  - Linux: meistens schon installiert
  - Windows: GPG4Win https://www.gpg4win.org/ (Minimale Installation oder Vanilla-Version reichen)
  - Mac: GPGTools https://gpgtools.org/
- E-Mail-Programm **Thunderbird** zur Verwaltung der E-Mails.
  - https://www.mozilla.org/de/thunderbird
  - Beim ersten Aufruf E-Mail-Konto konfigurieren und Feineinstellung durchführen (S. 4)
- Thunderbird-Add-On **Enigmail**, die Schnittstelle zu GnuPG.
  - In Thunderbird unter ***Extras*** → ***Add-Ons*** nach Enigmail suchen und installieren.

Schritt 2: Schlüssel erstellen

Mit dem Assistenten:

- Wähle in der Menüleiste von Thunderbird: ***Enigmail*** → ***Einrichtungs-Assistent.***
  - Tipp: Lies die Texte des Assistenten in Ruhe durch.
- Wähle die **ausführliche Konfiguration** für Fortgeschrittene.
- Wähle das E-Mail-Konto, für das die Schlüssel gelten sollen.
- Gib eine **Passphrase** ein.
  - Diese musst du immer eingeben, wenn du auf den Schlüssel zugreifen willst, um Missbrauch des Schlüssels zu verhindern. Du kannst sie später ändern.
- Schlüssel wird erzeugt, dies kann eine Weile dauern.
- Erzeuge das **Widerrufszertifikat**.
  - Damit kannst du deinen öffentlichen Schlüssel von Key-Servern widerrufen, auch nach Verlust des privaten Schlüssels (oder der Passphrase).

Oder manuell:

- Wähle in der Menüleiste von Thunderbird: ***Enigmail*** → ***Schlüssel verwalten***
- Dann ***Erzeugen*** → ***Neues Schlüsselpaar***
- Wähle das E-Mail-Konto, für das die Schlüssel gelten sollen
- Gib eine **Passphrase** ein
- Ablaufdatum nicht länger als 5 Jahre
- Unter Erweitert: Schlüsselstärke **4096** Bit, Algorithmus RSA
- Schlüssel erzeugen, dies kann eine Weile dauern
- Erzeuge das **Widerrufszertifikat**

Schritt 3: öffentliche Schlüssel importieren/exportieren

Zur Verschlüsselung verwendet man den **öffentlichen Schlüssel der Empfängerin**. Also: damit andere Personen dir verschlüsselte E-Mails schicken können, brauchen sie deinen öffentlichen PGP-Schlüssel.

Den öffentlichen Schlüssel auf Key-Server hochladen:

Key-Server sind die bequemste Möglichkeit. Dort kann dein Schlüssel einfach gefunden werden, allerdings sind die im Schlüssel eingetragenen E-Mail-Adressen dann öffentlich.

- Wähle in der Menüleiste von Thunderbird: ***Enigmail → Schlüssel verwalten***
- Setze einen Haken bei ***Standardmäßig alle Schlüssel anzeigen***
- **Rechtsklick** auf deinen Schlüssel, auf Schlüsselserver hochladen

Oder den öffentlichen Schlüssel direkt an Kommunikationspartner schicken:

- Wähle in der Menüleiste von Thunderbird: ***Enigmail → Schlüssel verwalten***
- **Rechtsklick** auf deinen Schlüssel, ***Öffentliche Schlüssel per E-Mail senden***

Um anderen Personen verschlüsselte Nachrichten schreiben zu können, brauchst du wiederum deren öffentlichen PGP-Schlüssel.

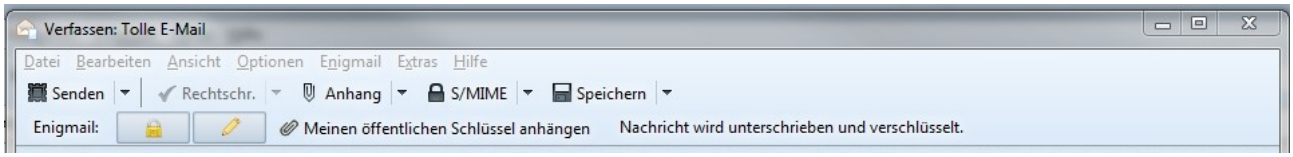
Auf Key-Server suchen:

- Wähle in der Menüleiste von Thunderbird: ***Enigmail → Schlüssel verwalten***
- Dann ***Schlüsselserver → Schlüssel suchen***, um einzelne Schlüssel zu finden
- Oder ***Schlüsselserver → Schlüssel für alle Kontakte suchen*** (damit gibst du allerdings dem Key-Server dein Kontakt-Netzwerk bekannt)

Oder Schlüssel aus E-Mail-Anhang importieren:

- Der PGP-Schlüssel hat die Dateiendung .asc
- Rechtsklick auf die Datei: PGP-Schlüssel importieren.

Schritt 4: E-Mails unterschreiben und verschlüsseln



- Neue E-Mail in Thunderbird verfassen
- Stelle sicher, dass ***unterschreiben*** und ***verschlüsseln*** aktiviert ist
  - Verschlüsseln setzt voraus, dass der Empfänger auch PGP nutzt
  - Unterschreiben geht immer – auch wenn Empfänger nichts damit anfangen können
- Zum Unterschreiben muss du beim Senden deine **Passphrase** eingeben

Bonusmaterial I: Schlüssel unterschreiben (Key-Signing)

Du kannst öffentliche PGP-Schlüssel von anderen Leuten unterschreiben. Damit bestätigst du die Zuordnung des Schlüssel zu dieser Person. So entsteht ein „Vertrauensnetzwerk“ (Web of Trust): Wer die andere Person nicht kennt, aber dich kennt und dir vertraut, kann auch dem Schlüssel der anderen Person vertrauen. Allerdings wird dadurch möglicherweise dein Kontakt-Netzwerk auf einem Key-Server öffentlich einsehbar. Überlege dir also, wessen Keys du signierst.

Überprüfe, ob der besagte Schlüssel zu der Person gehört:

- Wenn ihr Name in der E-Mail-Adresse vorkommt: prüfe z.B. per Personalausweis
- Sonst: lasse dir von ihr eine verschlüsselte und unterschriebene E-Mail schicken mit einem Inhalt, den du dir im direkten Kontakt ausdenkst und mitteilst.

Gleiche den Schlüssel-Fingerabdruck ab:

Als erstes überprüfst du, ob der Schlüssel, den die andere Person besitzt, dem öffentlichen Schlüssel entspricht, den du von ihr hast. Dies geht über den weltweit eindeutigen Fingerabdruck.

- Lasse dir den öffentlichen Schlüssel per Mail schicken oder lade ihn vom Key-Server
- Wähle in der Menüleiste von Thunderbird: **Enigmail** → **Schlüssel verwalten**
- **Rechtsklick** auf den Schlüssel → ***Schlüsseleigenschaften***
- Lasse dir von der anderen Person den Fingerabdruck ihres Schlüssel geben
  - ausgedruckt auf Papier
  - oder diktieren etc.

Schlüssel unterschreiben

- Wähle in der Menüleiste von Thunderbird: ***Enigmail*** → ***Schlüssel verwalten***
- **Rechtsklick** auf den Schlüssel → ***Unterschreiben***
- Zum Signieren musst du deine **Passphrase** eingeben

Den signierten Schlüssel seinem Besitzer schicken:

- Wähle in der Menüleiste von Thunderbird: ***Enigmail*** → ***Schlüssel verwalten***
- **Rechtsklick** auf den Schlüssel → öffentlicher Schlüssel per E-Mail senden

Wenn jemand anderes deinen Schlüssel signiert hat und dir schickt, kannst du ihn auf einen Keyserver hochladen, wenn du möchtest. Falls dein Schlüssel dort schon liegt, wird er aktualisiert.

Unterschriften einsehen:

- Wähle in der Menüleiste von Thunderbird: ***Enigmail*** → ***Schlüssel verwalten***
- **Rechtsklick** auf den Schlüssel → ***Schlüsseleigenschaften*** → Reiter ***Zertifikate***

Bonusmaterial II: Feineinstellung

- Einstellungen in Thunderbird korrigieren: **≡ Menübutton** → ***Einstellungen*** → Icon ***Erweitert*** → Reiter ***Allgemein*** → Knopf ***Konfiguration bearbeiten …*** und
  - JavaScript deaktivieren: **javascript** ins Suchfeld eingeben, Einstellung **javascript.enabled** finden; falls **true**, per Doppelklick auf **false** setzen
  - Falls gewünscht, dafür sorgen, dass neue Mails oben stehen: **sort_order** ins Suchfeld eingeben, die beiden mit **mailnews** beginnenden Einträge doppelklicken, Wert **2** eingeben, Enter (gilt nur für Mail-Ordner, die noch nicht geöffnet wurden)
- Eine Einstellung nach der Installation von Enigmail, ohne die manche Mails nicht entschlüsselt werden:
  - **≡ Menübutton** → ***Add-Ons*** → im Fenster links ***Erweiterungen*** → bei ***Enigmail*** den Knopf ***Einstellungen*** klicken
    → Falls Reiter ***Erweitert*** nicht vorhanden, im Reiter ***Allgemein*** den Knopf ***Experten-Optionen und -Menüpunkte anzeigen*** klicken
    → Reiter ***Erweitert*** → Haken entfernen bei ***Anhänge nur herunterladen, wenn diese geöffnet werden sollen (nur bei IMAP)***
    → falls gewünscht, wieder zurück zum Reiter ***Allgemein*** und Knopf ***Experten-Optionen und -Menüpunkte ausblenden*** klicken
    → Einstellungen mit ***OK*** schließen

Mobilgeräte

Hinweis: Da Betriebssysteme für Mobilgeräte laufend weiterentwickelt und von den Geräteherstellern stark angepasst werden, ist es möglich, dass bestimmte Einstellungen bei dir nicht auffindbar oder unter anderen Menüpunkten zu finden sind.

Datenschutzfreundliche Einstellungen

- Smartphones gehen oft verloren oder werden geklaut. Damit Fremde nicht direkt auf dein Gerät zugreifen können, solltest du **einen Pin oder ein Passwort zum Entsperren** des Geräts wählen. Insbesondere Wischgesten und Sperrmuster bieten oft keinen ausreichenden Schutz vor Fremdzugriff.

- **WLAN, GPS, Bluetooth, etc. nur bei Bedarf aktivieren**. Dann werden auch keine unnötigen Daten versendet und der Akku geschont

- **Synchronisation abschalten** (Kalender, Kontakte, etc.). Diese privaten Daten musst du nicht mit Datenkraken teilen.

- **Browser** (Firefox) **konfigurieren**: Keine Cookies von Drittanbietern zulassen, Adblocker installieren, Do-Not-Track aktivieren, (Standard)Suchmaschine anpassen. Viele Empfehlungen unseres Browser-Handouts lassen sich auch parallel auf dem Smartphone umsetzen.

- Android:
  - **Datenschutzmodus standardmäßig aktivieren** (*Einstellungen → Datenschutz*). Unter *Einstellungen → Apps* unnötige App-Berechtigungen entziehen
  - In der App **Google-Einstellungen** alles Unnötige deaktivieren
- iOS:
  - Unter *Einstellungen → Datenschutz* **Zugriff von Apps beschränken.**

Dateisystem verschlüsseln

Damit die Daten auf dem Gerät bei Diebstahl oder Verlust nicht ausgelesen werden können, solltest du das Dateisystem verschlüsseln.

- **Android:** *Einstellungen → Sicherheit → Smartphone verschlüsseln*
- **iOS:** Ab Version 8 integriert

Verschlüsselt kommunizieren

E-Mail-Verschlüsselung ist auch auf Smartphones möglich. Unter Android geht dies mit **K-9 Mail** und **OpenKeychain**. Allerdings ist die Wahrscheinlichkeit mangels Gerätehoheit größer, dass du die Kontrolle über deinen privaten Schlüssel verlierst.

Als mögliche Alternatve zu WhatsApp & Co ist **Signal** einen Blick wert, das im Gegensatz zu vielen Konkurrenten freie Software ist (Android: https://signal.org/android/apk/). Auch SMS & MMS (via **Signal**, **Silence**) und Chats via Jabber/XMPP (**Conversations** auf Android, **ChatSecure** auf iOS) lassen sich verschlüsseln.

Exkurs zu Android

Schritt 1: Google-Apps deinstallieren/deaktivieren

Unter **Einstellungen → Apps** kannst du Apps deinstallieren oder je nach Android-Version wenigstens deaktivieren, sofern du sie nicht unbedingt nutzen willst. Oft musst du ausprobieren, wie stark das Deaktivieren bzw. Deinstallieren dieser Apps den Betrieb deines Systems einschränkt. Hier ist eine Liste von (meist unfreier) Android-Software, deren Deaktivierung ihr in Erwägung ziehen könnt:
https://github.com/jaredsburrows/android-bloatware/blob/master/disable-list.txt

Schritt 2: Alternative zum Play Store nutzen

F-Droid ist ein alternatives Verzeichnis für Apps („App Store“). Dort findet man ausschließlich freie Software, die häufig größeren Wert auf eure Privatsphäre legt als viele Apps im Play Store. Alternativ können sämtliche Apps auch als APKs direkt von der Website heruntergeladen werden. https://f-droid.org/

Zur Installation von Apps aus F-Droid und APK-Dateien musst du ggf. **die Installation von Apps aus unbekannten Quellen zulassen** (*Einstellungen → Sicherheit → Unbekannte Herkunft*).

Schritt 3: Datenschutzfreundliche Apps & Dienste nutzen

Zu vielen unfreien, kostenpflichtigen Apps und vorinstallierten Diensten von Google gibt es freie Alternativen, bei denen in der Regel deutlich mehr Wert auf die Privatsphäre des Nutzers gelegt wird. Alle gelisteten Apps sind in **F-Droid** zu finden.

- **Amaze**: Ein schneller Dateimanager mit vielen Funktionen.
- **AntennaPod**: Verwaltung und Abspielen von Audiopodcasts.
- **AnySoftKeyboard**: Eine Alternative zur Hersteller/Android-Tastatur.
- **DAVdroid**: Kontakt-, Aufgaben und Kalendersynchronisation via CalDAV/CardDAV.
- **Etar**: Alternative Kalender-App zum Google Kalender.
- **Feeder**: Verwaltet und zeigt RSS/Atom-Feeds an.
- **FFUpdater**: Den Browser **Mozilla Firefox** herunterladen und aktualisieren.
- **Galerie**: Bild-/Medienbetrachter ohne Schnick-Schnack.
- **LibreOffice Viewer**: Betrachter für Office-Dateien, der besonders gut mit offenen Standards umgehen kann.
- **K-9 Mail**: Umfangreicher E-Mail-Client, kann in Verbindung mit OpenKeychain auch
- E-Mails verschlüsseln.
- **KeePassDroid**: Mit KeePassX kompatible Passwortverwaltung.
- **MuPDF**: Betrachter für PDF-Dateien.
- **Net Monitor**: Listet Netzwerkverbindungen aktiver Apps und Dienste auf.
- **NewPipe**: Client für YouTube, der auch Audio- und Videodownloads ermöglicht.
- **Obscr**: Ein flinker QR-Code-Scanner.
- **Offline Calendar**: Kalender ohne Online-Account/Synchronisation erstellen.
- **OpenKeychain**: GnuGPG und Schlüsselverwaltung unter Android
- **OsmAnd+**: Anwendung für Karten und Routenplanung, die auch offline funktioniert.

- **Transportr**: Öffentliche Verkehrsverbindungen und Fahrpläne abrufen.
- **Transistor**: Radio-/Audiostreams sammlen und abspielen.
- **Twidere**: Ein Twitter-/Microblogging-Client.
- **Vanilla Music**: Ein schlanker Musikplayer.
- **VLC**: Vom Desktop bekannter Video- und Audioplayer, der mit vielen Formaten
- umgehen kann. https://www.videolan.org/vlc/download-android.html

Weitere alternative Dienste zu unfreien Apps und Diensten findet ihr z.B. bei Prism-Break und bei der digitalen Selbstverteidigung bei DigitalCourage:

- https://prism-break.org/de/categories/android/
- https://digitalcourage.de/digitale-selbstverteidigung/freie-apps-fuer-das-befreite-smartphone

Schritt 4: Freies Android-Betriebssystem installieren (für Profis)

Vorinstallierte Versionen von Android enthalten oft Anpassungen des Herstellers und schränken die Anpassbarkeit stark ein. Auch die Dienste und Apps von Google sind häufig fest ins System integriert. Wer Google gänzlich entsagen will, sollte eine **alternative Android-Variante** auf seinem Gerät installieren. Das ist zwar meistens mit dem Verlust der Herstellergarantie verbunden, dafür wirst du wieder laufend mit Updates versorgt und hast auf deinem Gerät bei Bedarf Root-Zugriff (Stichwort **Gerätehoheit)**, wodurch du jegliche Softwarekomponenten verändern kannst. Das Wiki von LineageOS (englisch) listet für viele Geräte die Schritte auf, wie man dort ein alternatives Betriebssystem installieren kann: https://wiki.lineageos.org/

WARNUNG: Installation auf eigene Gefahr! Wir können euch im Rahmen dieser Veranstaltung leider nicht bei der Installation unterstützen und haften nicht für Datenverlust, Geräteschäden und ähnliches.

- **LineageOS**: Der Quasi-Nachfolger zum beliebten CyanogenMod, der sich zwar noch in Entwicklung befindet, allerdings schon für über 150 Geräte verfügbar ist und grundsätzlich sehr stabil läuft.
  - https://lineageos.org/

- **Replicant**: Replicant will nicht nur einfach einfach ein freies Betriebssystem sein, sondern setzt für die Hardwareunterstützung freie Gerätetreiber ein, die sonst von den Herstellern selbst oder Google stammen. Daher ist es nur für sehr wenige ältere Geräte verfügbar.
  - https://www.replicant.us/

Mike Kuketz hat in seinem Blog eine empfehlenswerte und äußerst detaillierte Artikelreihe **Your phone – your data: Android ohne Google** veröffentlicht, in der Schritt für Schritt erläutert wird, wie ihr euer Android-Smartphone und eure Daten den neugierigen Blicken von Google und anderen Datenkraken entziehen könnt. Zwar sind die Empfehlungen nicht mehr ganz auf dem aktuellen Stand (März 2016 mit Bezug auf das mittlerweile eingestellte CyanogenMod), allerdings gibt es nirgends einen ähnlich umfangreichen Guide, der sich mit der „Befreiung“ von Android-Smartphones beschäftigt: https://www.kuketz-blog.de/your-phone-your-data-teil1/

Einen aktuelle Artikelreihe zur datenschutzfreundlichen Einrichtung unter Android findet ihr dort ebenfalls: https://www.kuketz-blog.de/your-phone-your-data-light-android-unter-kontrolle/ (**Your Phone Your Data (light) – Android unter Kontrolle**)

Dateiverschlüsselung

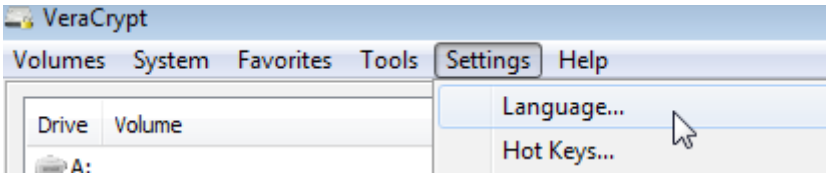
VeraCrypt kann verwendet werden, um ganze Datenträger, einzelne Partitionen oder Container zu verschlüsseln. Container kann man sich praktisch als passwortgeschützte Ordner vorstellen.

Schritt 1: Software installieren

VeraCrypt kann unter https://www.veracrypt.fr/ als Installer für GNU/Linux, Windows und macOS heruntergeladen werden.

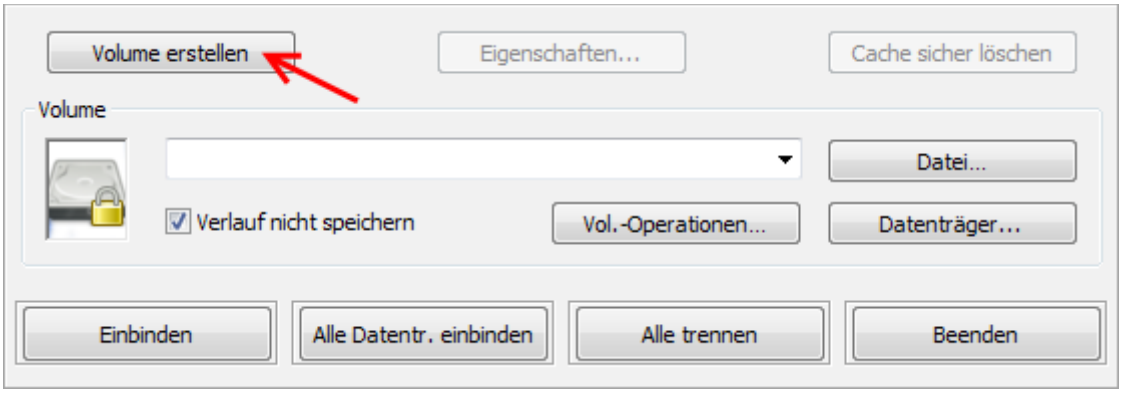
Schritt 2: Sprache ändern

Beim ersten Start ist die Oberfläche von VeraCrypt standardmäßig englischsprachig. Die Sprache könnt ihr oben im Menü auf Deutsch ändern, wenn ihr auf **"Settings"** klickt und dann auf **"Language...":**

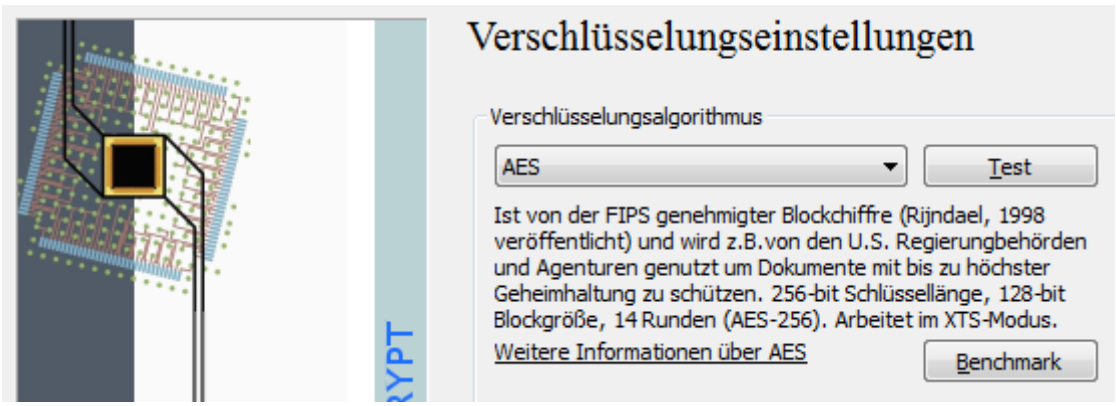


Schritt 3: Container erstellen

- Auf **"Volume erstellen"** klicken:



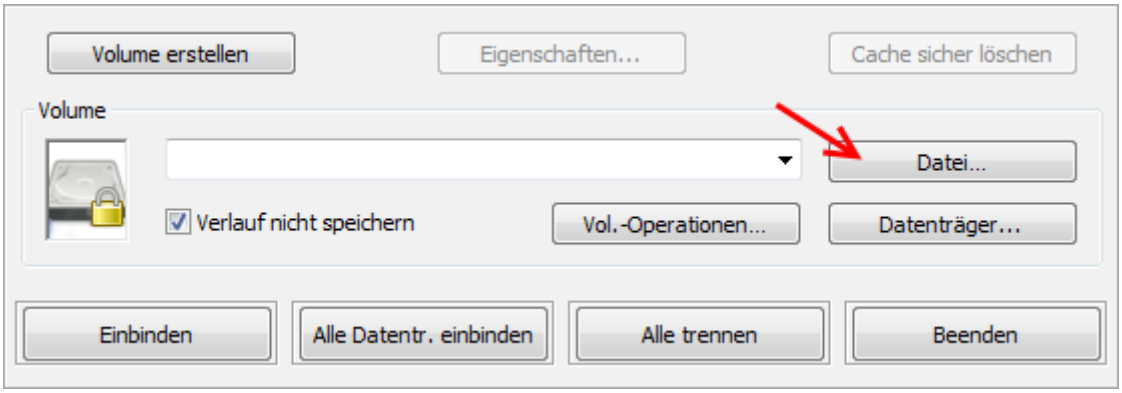
- Unten zweimal auf "**Weiter**" klicken.
- Unter "**Datei...**" legst du fest, wie der Container benannt wird und wo er gespeichert werden soll.
- Hier kann man die Verschlüsselungsart einstellen. Standardmäßig muss man aber nichts ändern:



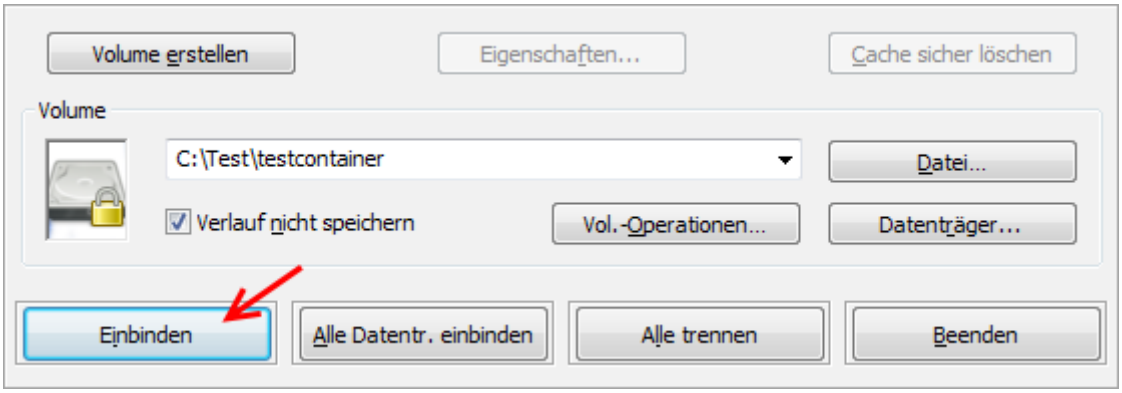
- Dann legst du die Größe des Containers fest.
- Als Nächstes musst du ein Passwort eingeben, mit dem der Container ver/-entschlüsselt wird.
- Dann kannst du das Dateisystem einstellen. Bewege den Mauszeiger für mind. 30 Sekunden zufällig über das VeraCrypt-Fenster. Anschließend auf "**Formatieren**" klicken. Der verschlüsselte Container wird nun erstellt.

Schritt 4: Container öffnen

- Über "**Datei**" wählst du den Container aus:



- Auf "**Einbinden**" klicken:



- Passwort eingeben und bestätigen.
- **Rechtsklick** auf den neuen Eintrag im VeraCrypt-Fenster:
  - Durch "**Öffnen**" greifst du auf den Container zu.
  - Durch "**Trennen**" wird er geschlossen.