

OBSKURA

UNSICHTBARE SICHERHEIT FÜR DEINE DATEN

BENUTZERHANDBUCH

VERSION 0.3.0

MACOS · WINDOWS · LINUX

OKTOBER 2026

BENUTZERHANDBUCH

INHALT

01	Willkommen bei Obskura	Was es tut, Datenbanken und Tresore	03
02	Installation und erster Start	macOS, Windows, Linux · der Zugangsschlüssel · die Oberfläche	04
03	Passwörter und Schlüsseldateien	Zugangsdaten, Argon2id, Wahl der Chiffre	05
04	Passwort-Datenbanken	Erstellen, entsperren, Einträge ordnen	07
05	Einträge verwalten	Generator, Felder, Anhänge, Verlauf	08
06	Datenbankwerkzeuge	Suche, sicheres Kopieren, Datenbankmenü	09
07	Dateitresore	Einen Tresor erstellen und Dateien verschlüsseln	10
08	Mit Dateien arbeiten	Öffnen, bearbeiten, exportieren	11
09	Entfernte Server	SFTP, WebDAV, SMB, FTP/FTPS	12
10	Mehrere Geräte in Echtzeit	Echtzeit-Synchronisierung, Benachrichtigungen	14
11	Zugangsschlüssel und Geräte	Begleitdateien, Kennungen und Pfade jedes Geräts	15
12	Automatische Sicherung	Zweites Ziel, datierte Kopien, pro Gerät	17
13	Import und Export	Online-Manager, CSV aus KeePass und anderen	18
14	Sprachen	Automatische Sprache, XML-Dateien, neue Übersetzungen	20
15	Sperren und Einstellungen	Automatische Sperre, Zwischenablage, Design, Gerätename	23
16	Tastenkürzel und Kryptografie	Tastenkürzel und technische Details	24
17	Bewährte Praxis und Probleme	Sicherungen, häufige Fragen	25

KONVENTIONEN

Namen von Schaltflächen und Menüs sind **fett**. Tastenkombinationen werden so geschrieben: `Strg/⌘` + `L`, wobei `Strg` für Windows und Linux und `⌘` für macOS gilt. Dateinamen und Endungen stehen in `Festbreitenschrift`. Die Bildschirmfotos zeigen die Oberfläche in der Sprache dieses Handbuchs.

EINFÜHRUNG

01 WILLKOMMEN BEI OBSKURA

Obskura schützt Passwörter und Dateien mit Verschlüsselung auf militärischem Niveau. Kein Konto und kein Drittanbieterdienst: Deine Daten bleiben dort, wo du es entscheidest – auf dem Computer oder auf deinem Server.

Jede Datenbank und jeder Tresor ist eine gewöhnliche Datei bzw. ein gewöhnlicher Ordner. Du kannst sie auf der Festplatte, auf einem USB-Stick, in einem synchronisierten Ordner wie Dropbox, OneDrive oder iCloud Drive oder direkt auf deinem eigenen SFTP-, WebDAV-, SMB- oder FTP-Server ablegen und beliebig viele davon haben: eine private, eine für die Arbeit, eine gemeinsame für die Familie. Mehrere Computer können sie gleichzeitig nutzen und sehen die Änderungen der anderen in Echtzeit – auch wenn sie über unterschiedliche Pfade darauf zugreifen.

PASSWORT-DATENBANK

Eine einzelne `.obk`-Datei nach dem Vorbild von KeePass. Sie enthält Einträge mit Benutzername, Passwort, Adresse, Notizen, eigenen Feldern, Anhängen und Änderungsverlauf, geordnet in Gruppen.

DATEITRESOR

Ein Ordner nach dem Vorbild von Cryptomator. Du ziehst Dokumente, Fotos und Archive hinein: Jede Datei wird einzeln verschlüsselt, einschließlich Namen und Ordnerstruktur.

SO FUNKTIONIERT DER SCHUTZ

Beim Erstellen einer Datenbank oder eines Tresors wählst du ein **Hauptpasswort**, eine **Schlüsseldatei** oder beides. Aus diesen Zugangsdaten leitet Obskura mit Argon2id den Schlüssel ab – einem Algorithmus, der eigens dafür entwickelt wurde, das Erraten von Passwörtern extrem zu verlangsamen. Die Daten werden dann mit AES-256 verschlüsselt, dem Standard, der für als **TOP SECRET** eingestufte Informationen zugelassen ist.

Die Zugangsdaten werden nirgends gespeichert. Ohne sie ist der Inhalt für jeden unlesbar, auch für die Entwickler.

WICHTIG

Ein vergessenes Passwort oder eine verlorene Schlüsseldatei lässt sich auf keine Weise wiederherstellen. Wähle ein Passwort, das du dir merken kannst, und bewahre eine Kopie der Schlüsseldatei an einem sicheren, getrennten Ort auf.

AUF EINEN BLICK

AES-256-GCM · XChaCha20-Poly1305 · Serpent · Twofish · Camellia · Verschlüsselungskaskaden · Argon2id bis 2 GiB · HKDF-SHA256 · AES-SIV für Dateinamen · Speicher beim Schließen gelöscht · Kein Konto · SFTP · WebDAV · SMB · FTPS · Echtzeit · Automatische Sicherung · Pfade pro Gerät · 8 Sprachen · macOS · Windows · Linux

ERSTE SCHRITTE

02 INSTALLATION UND ERSTER START

macOS

Öffne die `.dmg`-Datei und ziehe Obskura in **Programme**. Blockiert macOS die App beim ersten Start, gehe zu **Systemeinstellungen → Datenschutz & Sicherheit** und wähle **Dennoch öffnen**.

Windows

Führe das Installationsprogramm `.exe` aus, das automatisch die Sprache von Windows verwendet, oder starte die portable Version ohne Installation. Erscheint die SmartScreen-Warnung, klicke auf **Weitere Informationen → Trotzdem ausführen**.

Linux

Verwende das Paket `.deb` (Debian, Ubuntu), `.rpm` (Fedora, openSUSE) oder das `.AppImage`, das keine Installation braucht: ausführbar machen und starten.

ERSTER START: SPRACHE UND ZUGANGSSCHLÜSSEL

Obskura öffnet sich in der Systemsprache (Italienisch, Englisch, Deutsch, Spanisch, Russisch, Chinesisch, Japanisch oder Arabisch; für andere Sprachen Englisch). Beim ersten Start fordert es dich auf, den **Obskura-Zugangsschlüssel** zu erzeugen oder – wenn du Obskura schon auf einem anderen Computer nutzt – den dort erzeugten einzugeben. Kapitel 11 erklärt, wozu er dient.

DER STARTBILDSCHIRM

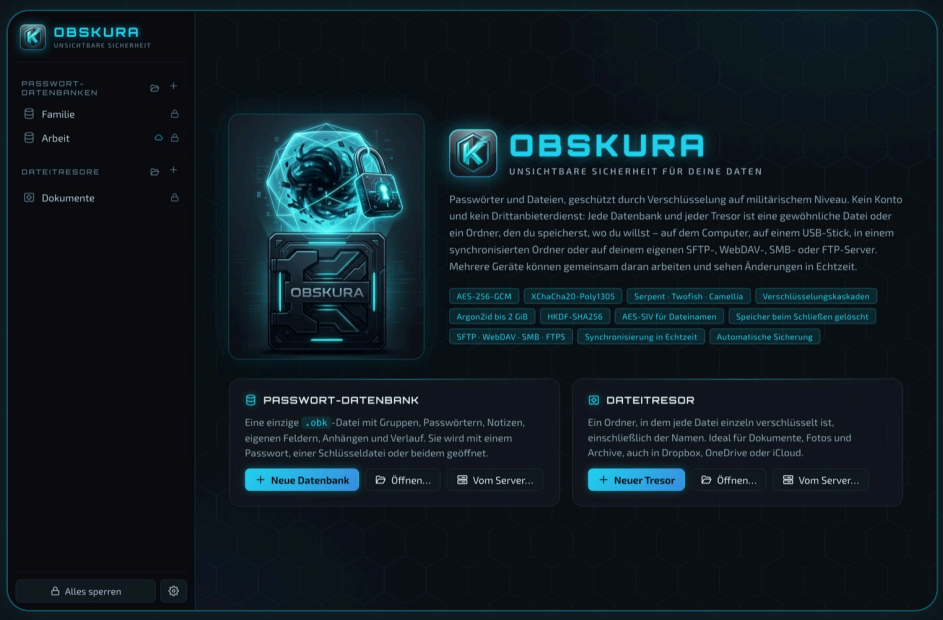


ABB. 1 Der Willkommensbildschirm mit der Seitenleiste.

Die **Seitenleiste** enthält die Bereiche **Passwort-Datenbanken** und **Dateitresore**. Neben jeder Überschrift gibt es zwei Schaltflächen: den Ordner zum **Öffnen** eines vorhandenen Elements und das **+** zum Erstellen eines neuen.

- Jedes zuletzt geöffnete Element bleibt in der Liste, nur mit seinem Namen: Pfade erscheinen nie. Das Schloss zeigt den Zustand: **geschlossen**, wenn gesperrt, **offen**, wenn entsperrt.
- Fährst du über ein Element, erscheint ein **×**, um es aus der Liste zu entfernen (die Datei wird nicht gelöscht), oder ein Schloss, um es sofort zu sperren.
- Unten: **Alles sperren** und das Zahnrad der **Einstellungen**.

DATEN SCHÜTZEN

03 PASSWÖRTER UND SCHLÜSSELDATEIEN

Datenbanken und Tresore öffnen sich mit einem **Hauptpasswort**, einer **Schlüsseldatei** oder beidem zusammen. Die Kombination ist der stärkste Schutz: Man braucht etwas, das man *weiß*, und etwas, das man *besitzt*.

HAUPTPASSWORT

Ein langer Satz ist sicherer als ein komplexes Wort: Vier oder fünf zufällige Wörter sind leicht zu merken und sehr schwer zu erraten. Die Anzeige unter dem Feld schätzt die Stärke in Bit.

Die Würfel-Schaltfläche öffnet den **Generator**, wenn du ein zufälliges Passwort möchtest.

SCHLÜSSELDATEI

Wie bei KeePass kann **jede Datei** als Schlüssel dienen. Du kannst **Vorhandene Datei verwenden** oder **Neue erzeugen** wählen: Obskura erstellt dann eine zufällige Schlüsseldatei am angegebenen Ort.

Bewahre sie zum Beispiel auf einem USB-Stick auf, getrennt von der Datenbank. Obskura merkt sich auf jedem Gerät, wo sie liegt, und sucht sie bei jedem Öffnen selbst (Kapitel 11).

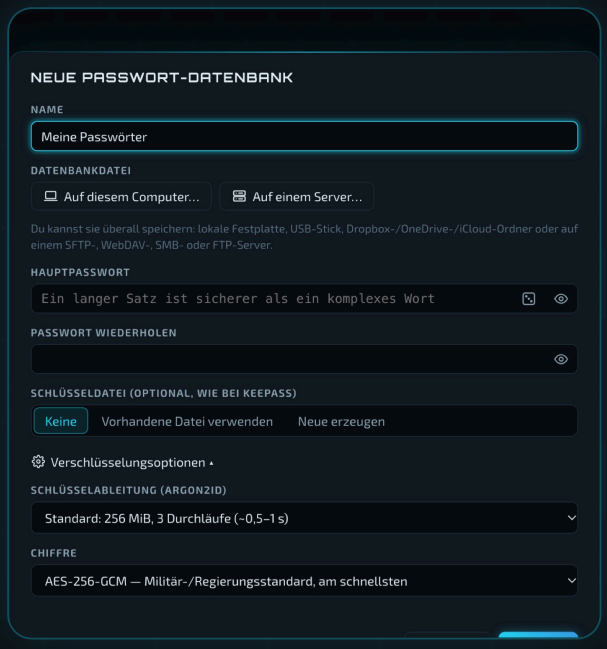


ABB. 2 Erstellen einer Datenbank mit geöffneten Verschlüsselungsoptionen.

VERSCHLÜSSELUNGSOPTIONEN

Unter **Verschlüsselungsoptionen** legst du fest, wie aufwendig die Schlüsselableitung sein soll und welche Chiffre verwendet wird. Die Voreinstellungen Standard und AES-256-GCM sind für jeden Zweck sicher; alle Alternativen werden auf der nächsten Seite beschrieben.

DIE SCHLÜSSELDATEI NIE VERÄNDERN

Verwendest du eine beliebige Datei (ein Foto, ein Dokument) als Schlüssel, macht schon die kleinste Änderung sie unbrauchbar. Von Obskura erzeugte Dateien haben ein erkanntes Textformat, das auch bei geänderten Zeilenumbrüchen gültig bleibt. Bewahre in jedem Fall eine Sicherungskopie auf.

DATEN SCHÜTZEN

03 DIE CHIFFRE WÄHLEN

SCHLÜSSELABLEITUNG (ARGON2ID)

Argon2id verwandelt deine Zugangsdaten in den Schlüssel: Je mehr Speicher und Durchläufe, desto teurer ist es für einen Angreifer, Millionen von Passwörtern auszuprobieren.

STUFE	PARAMETER	ÖFFNUNGSZEIT
Standard	256 MiB Speicher, 3 Durchläufe	etwa 0,5–1 Sekunden
Hoch	1 GiB, 4 Durchläufe	etwa 2–4 Sekunden
Extrem	2 GiB, 6 Durchläufe	etwa 5–12 Sekunden

STUFE EXTREM

Jedes Öffnen erfordert **2 GiB freien Speicher**. Auf einem Computer mit wenig RAM lassen sich Datenbank oder Tresor möglicherweise nicht öffnen: Wähle diese Stufe nur, wenn du deine Dateien auf geeigneten Computern nutzt.

CHIFFREN

Alle Chiffren verwenden 256-Bit-Schlüssel und sind **authentifiziert**: Jede Veränderung der Daten wird erkannt.

CHIFFRE	EIGENSCHAFTEN
AES-256-GCM	**Voreinstellung.** US-Standard, zugelassen für TOP-SECRET-Informationen, dank Hardwarebeschleunigung am schnellsten.
XChaCha20-Poly1305	Stromchiffre, schnell auf jedem Prozessor, auch ohne AES-Befehle.
Serpent-256-GCM	AES-Finalist mit der größten Sicherheitsreserve (32 Runden). Langsamer.
Twofish-256-GCM	AES-Finalist, entwickelt von Bruce Schneier und Kollegen.
Camellia-256-GCM	Internationaler ISO/IEC-Standard, empfohlen in Europa (NESSIE) und Japan (CRYPTREC).
Kaskade AES · Twofish · Serpent	**Die stärkste Wahl.** Drei Verschlüsselungen hintereinander mit unabhängigen Schlüsseln: Die Daten bleiben geschützt, selbst wenn zwei der drei Algorithmen eines Tages gebrochen würden.
Kaskade AES · XChaCha20	Kombiniert eine Block- und eine Stromchiffre aus völlig verschiedenen Familien.

TRESORE

In Tresoren schützt die gewählte Chiffre sowohl die Schlüssel als auch den Inhalt jeder Datei. Änderst du sie mit **Passwort / Schlüsseldatei ändern**, bleiben vorhandene Dateien mit der bisherigen verschlüsselt, und ab dann hinzugefügte nutzen die neue. Die aktive Chiffre steht unten rechts im Tresor.

PASSWORT-MANAGER

04 PASSWORT-DATENBANKEN

EINE DATENBANK ERSTELLEN

1. Klicke auf dem Startbildschirm auf **Neue Datenbank** oder auf das **+** neben **Passwort-Datenbanken**.
2. Gib einen **Namen** ein und wähle, wo die `.obk`-Datei gespeichert wird: **Auf diesem Computer…** oder **Auf einem Server…**.
3. Lege Passwort und/oder Schlüsseldatei fest (Kapitel 03).
4. Drücke **Erstellen**. Die Datenbank öffnet sich bereits entsperrt.

ÖFFNEN UND ENTSPERREN

1. Wähle die Datenbank in der Seitenleiste oder öffne mit dem Ordnersymbol eine vorhandene `.obk`-Datei.
2. Gib das Passwort ein. Schlüsseldatei und Sicherungskopie werden automatisch gesucht; wird die Schlüsseldatei nicht gefunden, wähle sie mit **Wählen…**.
3. Drücke **Entsperren** oder `Eingabe`.

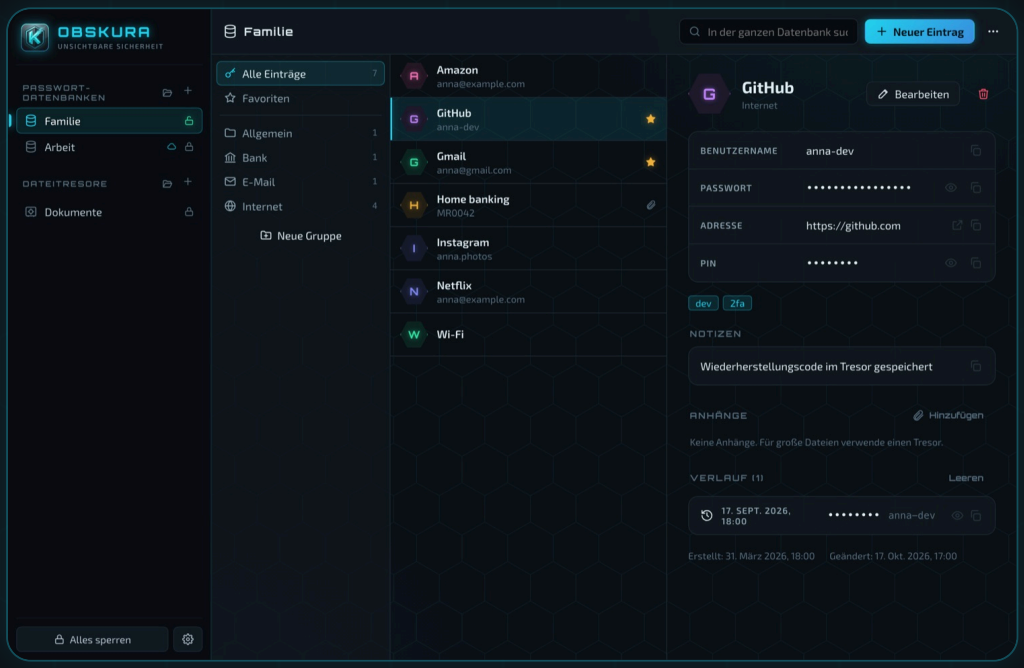


ABB. 3 Eine entsperrte Datenbank: Gruppen, Liste der Einträge und Details des gewählten Eintrags.

DIE DREI SPALTEN

- **Gruppen**: **Alle Einträge**, **Favoriten** und deine Ordner. Beim Überfahren einer Gruppe erscheinen Befehle zum Erstellen einer Untergruppe, Bearbeiten oder Löschen; **Neue Gruppe** steht am Ende der Liste.
- **Einträge**: Titel und Benutzername jedes Eintrags. Der Stern markiert Favoriten, die Büroklammer Anhänge. Ein **Doppelklick** kopiert direkt das Passwort.
- **Details**: alle Felder des Eintrags, mit Schaltflächen zum Anzeigen, Kopieren oder Öffnen der Adresse im Browser.

PASSWORT-DATENBANKEN

05 EINTRÄGE VERWALTEN

Um einen Eintrag hinzuzufügen, drücke **Neuer Eintrag** (oder `Strg/⌘` + `N`); um ihn zu ändern, wähle ihn aus und drücke **Bearbeiten**. Speichere mit der Schaltfläche unten oder mit `Strg/⌘` + `S`. Jede Änderung wird sofort in die Datenbankdatei geschrieben.



ABB. 4 Der Eintragseditor mit geöffnetem Generator.

FELDER EINES EINTRAGS

Titel und Gruppe	Name des Eintrags und Ordner, in dem er liegt.
Benutzername	Konto, E-Mail oder Kundennummer.
Passwort	Mit Stärkeanzeige und Generator.
Adresse	Öffnet sich aus den Details im Browser.
Notizen	Freier Text, verschlüsselt wie alles andere.
Schlagwörter	Durch Kommas getrennte Stichwörter.
Ablaufdatum	Datum, ab dem das Passwort geändert werden sollte.

Der **Stern** oben fügt den Eintrag den **Favoriten** hinzu.

PASSWORTGENERATOR

Klicke auf den Würfel im Passwortfeld. Wähle die **Länge** (8 bis 64 Zeichen) und die Zeichengruppen (`a–z`, `A–Z`, `0–9`, `!@#$`); **Mehrdeutige ausschließen** vermeidet leicht verwechselbare Zeichen wie l, 1, O und 0. Dann **Neu erzeugen**, **Kopieren** oder **Dieses Passwort verwenden**. Die Passwörter stammen aus dem kryptografischen Zufallsgenerator des Systems.

EIGENE FELDER

Füge zusätzliche Angaben wie PINs, Wiederherstellungscodes oder Sicherheitsfragen hinzu. Aktiviere **Geschützt**, um sie verborgen anzuzeigen, wie ein Passwort.

ANHÄNGE UND VERLAUF

Hänge Dateien bis **64 MB** an (für größere Dateien verwende einen Tresor). Jede Änderung bewahrt die vorherige Version: Der **Verlauf** behält die letzten **20** und erlaubt das Kopieren eines alten Passworts.

PASSWORT-DATENBANKEN

06 DATENBANKWERKZEUGE

SUCHEN

Das Feld **In der ganzen Datenbank suchen** oben (oder `Strg/⌘` + `F`) filtert die Einträge aller Gruppen während der Eingabe. `Esc` leert die Suche.

SICHER KOPIEREN

Die Kopierschaltflächen neben Benutzername, Passwort und geschützten Feldern legen den Wert in die Zwischenablage, die Obskura nach 20 Sekunden **automatisch leert** (in den Einstellungen änderbar). Sie wird nur geleert, wenn sie noch den kopierten Wert enthält: Hast du inzwischen etwas anderes kopiert, bleibt es unangetastet.

DAS DATENBANKMENÜ

Die Schaltfläche ••• oben rechts enthält:

EINTRAG	WOZU ER DIENT
Datenbank-Eigenschaften	Name und Beschreibung der Datenbank ändern.
Passwort / Schlüsseldatei ändern	Neue Zugangsdaten festlegen. Die Datenbank wird mit neuen Schlüsseln neu verschlüsselt.
Sicherungskopie speichern…	Eine verschlüsselte Kopie der Datenbank an einem anderen Ort speichern.
Automatische Sicherung…	Das zweite Ziel für die Kopien einrichten (Kapitel 12).
Geräte und Pfade…	Sehen, welche Geräte die Datenbank nutzen, und ihre Pfade (Kapitel 11).
Import / Export	Aus einem Online-Manager oder aus CSV, und nach CSV (Kapitel 13).
Datenbank sperren	Die Datenbank schließen und ihre Daten aus dem Speicher löschen.

SPEICHERN UND SYNCHRONISIEREN

Jede Änderung wird sofort und **atomar** gespeichert: Die neue Datei wird getrennt geschrieben und ersetzt die alte erst, wenn sie vollständig ist – ein Stromausfall kann sie also nicht beschädigen. Hat ein anderer Computer die Datenbank inzwischen geändert, **führt** Obskura die beiden Versionen vor dem Speichern **zusammen**: Nichts geht verloren (Kapitel 10). Eine Entscheidung ist nur nötig, wenn auf einem anderen Gerät **Passwort oder Schlüsseldatei** geändert wurden: Obskura schlägt vor, die Datenbank zu sperren und mit den neuen Zugangsdaten erneut zu öffnen.

> **TIPP**
>
> Um dieselbe Datenbank auf mehreren Computern zu nutzen, lege sie auf deinen Server (Kapitel 09) oder in einen synchronisierten Ordner: Sie kann überall gleichzeitig geöffnet sein.

VERSCHLÜSSELTE DATEIEN

07 DATEITRESORE

Ein Tresor ist ein Ordner, der deine Dateien in verschlüsselter Form enthält. Von außen ist er nur eine Sammlung von Dateien mit unlesbaren Namen: Man erkennt weder, was sie enthalten, noch wie sie geordnet sind.

EINEN TRESOR ERSTELLEN

1. Klicke auf **Neuer Tresor** oder auf das **+** neben **Dateitresore**.
2. Wähle einen Namen und den Ordner, in dem er entstehen soll, auch in Dropbox, OneDrive, iCloud Drive oder auf einem Server.
3. Lege Passwort und/oder Schlüsseldatei fest und drücke **Erstellen**.

DATEIEN HINZUFÜGEN

- **Ziehe** Dateien und Ordner aus dem Finder / Explorer ins Fenster: Sie werden in den gerade angezeigten Ordner verschlüsselt.
- Oder verwende **Dateien hinzufügen** bzw. **Ordner hinzufügen**.
- Die Originale bleiben unberührt: Nach dem Verschlüsseln kannst du sie selbst löschen.

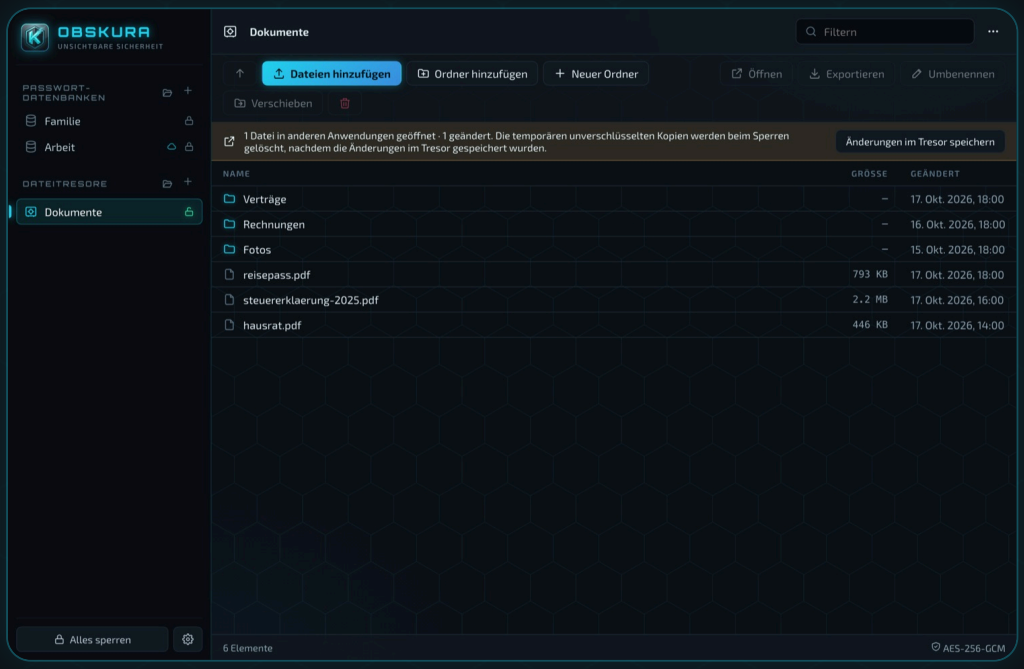


ABB. 5 Ein entsperrter Tresor.

DIE BEFEHLSLEISTE

↑ wechselt in den übergeordneten Ordner · **Neuer Ordner** legt einen Unterordner an · **Öffnen**, **Exportieren**, **Umbenennen**, **Verschieben** und **Löschen** wirken auf die ausgewählten Elemente. Mehrere wählst du mit `Strg/⌘` + Klick oder `Umschalt` + Klick. Unten zeigt die Statusleiste die Anzahl der Elemente und den Fortschritt der Vorgänge.

DATEITRESORE

08 MIT DATEIEN ARBEITEN

EINE DATEI ÖFFNEN UND BEARBEITEN

Doppelklicke auf eine Datei (oder wähle sie aus und drücke **Öffnen**). Obskura entschlüsselt sie in einen geschützten temporären Ordner und öffnet sie mit der Standardanwendung des Systems.

1. Bearbeite und speichere die Datei wie gewohnt in der anderen Anwendung.
2. In Obskura erscheint ein Hinweisband mit den geöffneten und geänderten Dateien.
3. Drücke **Änderungen im Tresor speichern**, um die neue Version zu verschlüsseln.

> **TEMPORÄRE KLARTEXTKOPIEN**
>
> Solange eine Datei geöffnet ist, liegt ihre entschlüsselte Kopie auf dem Datenträger. Beim Sperren des Tresors speichert Obskura zuerst verbliebene Änderungen und **löscht dann die temporären Kopien**. Schließe die Datei in der anderen Anwendung vor dem Sperren.

EXPORTIEREN

Exportieren entschlüsselt die ausgewählten Elemente samt Ordnern in einen Ordner deiner Wahl. Die exportierten Dateien sind **unverschlüsselt**: Nutze die Funktion nur, wenn du sie außerhalb des Tresors brauchst.

ORDNEN

Umbenennen mit **Umbenennen** oder `F2`; verschieben mit **Verschieben** durch Wahl des Zielordners. **Löschen** (oder `Entf`) fragt immer nach. Das Feld **Filtern** zeigt nur Elemente, deren Name den eingegebenen Text enthält.

SYNCHRONISIERUNG MIT DER CLOUD

Jede Datei im Tresor ist einzeln verschlüsselt: Änderst du ein Dokument, lädt der Synchronisierungsdienst nur diese Datei hoch. Deshalb funktionieren Tresore gut in Dropbox, OneDrive, Google Drive oder iCloud Drive.

SO SIEHT EIN TRESOR AUF DEM DATENTRÄGER AUS

ELEMENT	INHALT
`vault.obkv`	Die Schlüssel des Tresors, mit deinen Zugangsdaten verschlüsselt.
`vault.obkv.bak`	Identische Sicherheitskopie, falls die erste Datei beschädigt wird.
`vault.obkx`	Die Begleitdatei, mit dem Zugangsschlüssel verschlüsselt: Schlüsseldatei, Sicherung und Pfade jedes Geräts (Kapitel 11).
`d/`	Alle verschlüsselten Dateien und Ordner nebeneinander: Die echte Struktur ist nicht sichtbar.

Um einen vorhandenen Tresor zu öffnen, verwende das Ordnersymbol neben **Dateitresore** und wähle seinen Hauptordner. Verändere oder verschiebe die Dateien darin nicht von Hand.

WO SPEICHERN

09 ENTFERNTE SERVER

Datenbanken und Tresore müssen nicht auf dem Computer liegen: Obskura öffnet und speichert sie direkt auf deinem Server, ohne Synchronisierungsprogramme dazwischen. Die Daten werden **bereits verschlüsselt** übertragen und bleiben so auf dem Server: Der Serveradministrator – oder wer ihn knackt – sieht nur unlesbare Dateien.

PROTOKOLL	WO ES VERWENDET WIRD	HINWEISE
SFTP	NAS (Synology, QNAP, TrueNAS), Linux-Server, VPS	Empfohlen. Passwort oder SSH-Schlüssel.
WebDAV	Nextcloud, ownCloud, Synology, QNAP, Box, Koofr	Über HTTPS. Für Nextcloud lautet der Pfad `/remote.php/dav/files/<benutzer>`.
SMB	Windows-Freigaben, NAS, Samba	SMB 2 und 3; gib den Namen der Freigabe an.
FTPS	Hosting und FTP-Server mit TLS	FTP verschlüsselt mit `AUTH TLS`.
FTP	Klassische FTP-Server	Die Serverzugangsdaten werden im Klartext übertragen: besser FTPS oder SFTP.

EINE VERBINDUNG EINRICHTEN

1. Öffne **Einstellungen → Serververbindungen** und drücke **Neue Verbindung**.
2. Wähle das Protokoll und gib Adresse, Port (falls nicht Standard), Benutzer und Passwort ein.
3. Drücke **Verbindung testen**, dann **Speichern**.

Das Serverpasswort landet im **Schlüsselbund des Systems** (macOS-Schlüsselbund, Windows-Anmeldeinformationsverwaltung, Secret Service unter Linux), nie in der Einstellungsdatei. Es wird zudem verschlüsselt in die Begleitdatei kopiert: Deine anderen Computer stellen die Verbindung selbst wieder her.

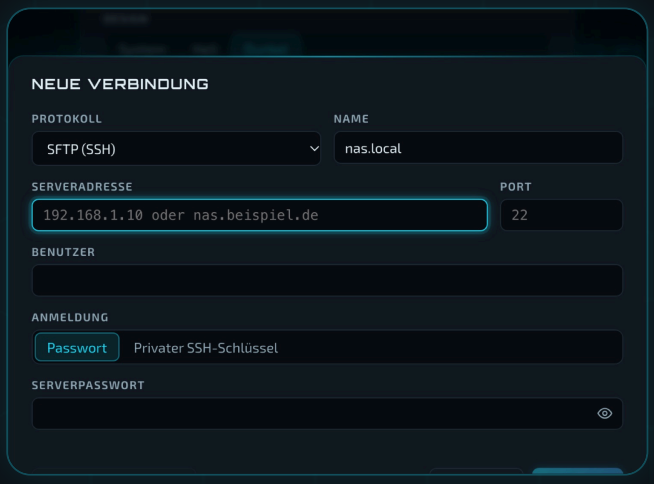


ABB. 6 Eine neue SFTP-Verbindung.

SERVERSCHLÜSSEL (SFTP)

Bei der ersten Verbindung zeigt Obskura den **Fingerabdruck** des Serverschlüssels und bittet dich, ihn zu akzeptieren – wie `ssh`. Ändert er sich später, wird die Verbindung abgelehnt, bis du erneut bestätigst: Es könnte sich jemand als dein Server ausgeben. Hat sich am Server nichts geändert, akzeptiere nicht.

AUF EINEM SERVER ÖFFNEN UND SPEICHERN

- **Öffnen:** Das Ordnersymbol neben **Passwort-Datenbanken** oder **Dateitresore** bietet **Von diesem Computer…** und **Von einem Server…**. Ebenso auf dem Startbildschirm mit **Vom Server…**.
- **Erstellen:** Wähle im Fenster **Neue Datenbank** oder **Neuer Tresor Auf einem Server…** statt **Auf diesem Computer…**.
- Elemente auf einem Server erscheinen in der Liste mit dem **Wolkensymbol**; geöffnet zeigen sie die Markierung `SERVER` oben.



ABB. 7 Der Serverbrowser: Verbindung und Ordner wählen.

Wähle im Browser oben links die Verbindung und bewege dich durch die Ordner. Für eine Datenbank klicke auf die `.obk`-Datei; für einen Tresor öffne seinen Ordner (den mit `vault.obkv`) und drücke **Diesen Tresor öffnen**. Mit dem Ordner+-Symbol legst du einen neuen Ordner auf dem Server an.

> **LEISTUNG**
>
> Datenbanken sind klein und öffnen sich auch entfernt im Nu. Tresore übertragen jeweils eine Datei, wenn du sie öffnest oder exportierst: Bei sehr großen Dateien zählt die Verbindungsgeschwindigkeit.

ZUSAMMENARBEIT

10 MEHRERE GERÄTE IN ECHTZEIT

Dieselbe Datenbank oder derselbe Tresor kann gleichzeitig auf mehreren Computern geöffnet sein: Änderungen auf einem erscheinen auf den anderen in wenigen Sekunden.

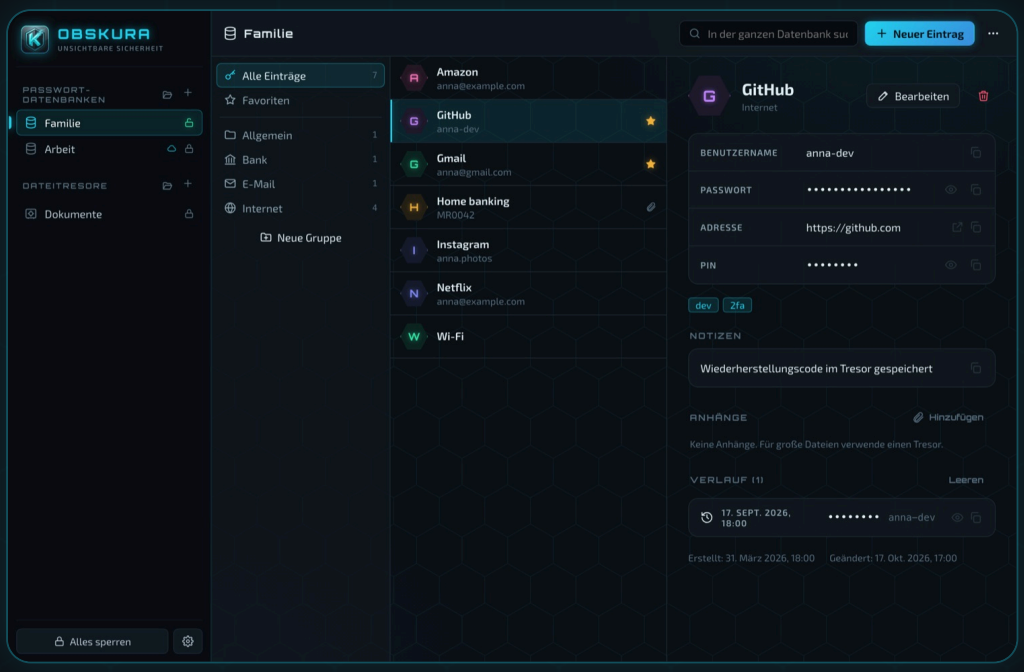


ABB. 8 Eine Benachrichtigung: Ein anderes Gerät hat Einträge hinzugefügt und geändert.

SO FUNKTIONIERT ES

- Obskura prüft die Datei alle **2 Sekunden** auf einem lokalen Datenträger oder in einem synchronisierten Ordner, alle **5 Sekunden** auf einem Server. Dabei werden nur die ersten 88 Byte gelesen.
- Findet es eine neue Version, **führt** es sie Eintrag für Eintrag mit deiner **zusammen**, zeigt eine Benachrichtigung mit den hinzugefügten, geänderten oder gelöschten Einträgen und aktualisiert die Liste sofort.
- Ändern zwei Personen **denselben Eintrag**, gewinnt die neueste Änderung; die andere geht nicht verloren, sondern landet im **Verlauf** des Eintrags.
- Ein Löschvorgang erreicht alle, es sei denn, jemand hat den Eintrag inzwischen geändert: Dann hat die Änderung Vorrang und der Eintrag bleibt.
- Fügt in Tresoren jemand Dateien im angezeigten Ordner hinzu, benennt sie um oder löscht sie, aktualisiert sich die Liste von selbst.

UHREN DER COMPUTER

Um zu entscheiden, welche Änderung neuer ist, nutzt Obskura die Uhrzeit der Computer: Halte sie synchron (automatische Zeiteinstellung, auf allen Systemen meist aktiv).

ALLES WIEDERFINDEN, ÜBERALL

11 ZUGANGSSCHLÜSSEL UND GERÄTE

Neben jeder Datenbank und jedem Tresor liegt eine kleine verschlüsselte Datei, die sich merkt, wo Schlüsseldatei, Sicherungen und Server sind und wie jedes deiner Geräte sie erreicht. Sie ist durch den Obskura-Zugangsschlüssel geschützt.

DER OBSKURA-ZUGANGSSCHLÜSSEL

Ein 55-stelliger Code, der beim ersten Start erzeugt (oder eingegeben, wenn du ihn auf einem anderen Computer erzeugt hast) wird. Er bleibt im Schlüsselbund des Systems; unter **Einstellungen → Obskura-Zugangsschlüssel** kannst du:

- **Anzeigen**: ihn ansehen und kopieren, um ihn auf einem anderen Computer einzugeben.
- **Schlüssel ändern…**: einen neuen erzeugen. Obskura verschlüsselt erreichbare Begleitdateien sofort neu; die übrigen werden beim nächsten Öffnen aktualisiert (frühere Schlüssel bleiben zum Lesen gültig).
- **Schlüssel eingeben…**: den aktuellen Schlüssel verwenden, wenn er auf einem anderen Computer geändert wurde.

DIE BEGLEITDATEIEN

Sie sind mit AES-256-GCM verschlüsselt und ohne den Zugangsschlüssel unlesbar:

DATEI	ENTHÄLT
`.obk.obkx`	Neben jeder Datenbank: Ort der Schlüsseldatei, Sicherungskonfiguration, Serververbindungen und die Gerätedatensätze.
`vault.obkx`	In jedem Tresor: dieselben Angaben.
`recenti.obkx`	Im Datenordner der App: die Liste der zuletzt verwendeten. Auf dem Datenträger bleiben keine Klartextpfade.

VON EINEM ANDEREN COMPUTER ÖFFNEN

Ist der Zugangsschlüssel auf dem neuen Computer eingegeben, genügt es, die Datenbank zu wählen: Obskura liest die Begleitdatei, stellt fehlende Serververbindungen wieder her, findet die Schlüsseldatei (am für dieses Gerät bekannten Ort, neben der Datenbank, unter den Pfaden der anderen Geräte oder in der Sicherungskopie) und bietet die Sicherungskopie an, wenn das Original nicht erreichbar ist.

WICHTIG

Der Zugangsschlüssel ersetzt nicht das Passwort der Datenbank: Ohne Passwort (und Schlüsseldatei) bleiben die Daten unlesbar. Bewahre ihn dennoch sicher auf: Ohne ihn musst du Schlüsseldatei und Sicherungen von Hand wählen.

GERÄTE UND PFADE

Jeder Computer, der Obskura nutzt, hat eine **eindeutige Kennung**, die beim ersten Start erzeugt wird, und einen **Namen** (den des Computers, änderbar unter **Einstellungen → Name dieses Geräts**). Bei jedem Öffnen einer Datenbank oder eines Tresors schreibt er seinen eigenen Datensatz in die verschlüsselte Begleitdatei:

ANGABE	BEISPIEL
Kennung und Name	`3f2a9c1e-…` · „MacBook zu Hause“
System und Version	macOS · Obskura 0.3.0 · letzter Zugriff
Pfad der Datenbank	`/Users/anna/Dropbox/konten.obk` auf dem Mac, `D:\Dropbox\konten.obk` auf dem PC
Pfad der Schlüsseldatei	`/Volumes/USB/schluessel.obkey` oder `E:\schluessel.obkey`
Eigene Sicherung	ein Ordner dieses Geräts oder die gemeinsame Konfiguration (Kapitel 12)

DAS FENSTER „GERÄTE UND PFADE“

Wähle im Menü ⋯ einer Datenbank oder eines Tresors **Geräte und Pfade…**:

- Du siehst alle registrierten Geräte mit System, Version, letztem Zugriff, Nutzung der Schlüsseldatei und Sicherungsziel;
- das Augensymbol zeigt die Pfade jedes Geräts; der Stift benennt dieses Gerät um;
- der Papierkorb **vergisst** ein Gerät, das du nicht mehr nutzt: Seine Pfade und seine Sicherung werden aus der Datei entfernt (öffnet es sie erneut, wird es wieder registriert).

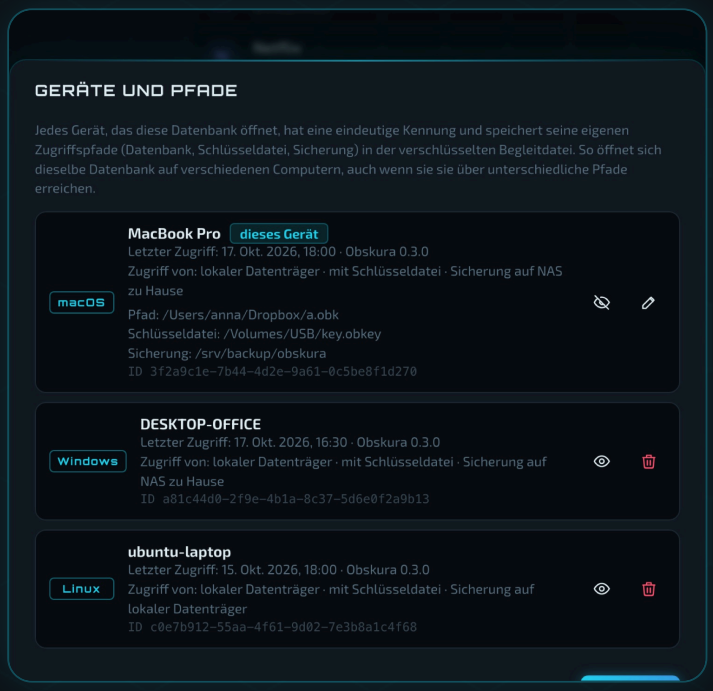


ABB. 9 Die Geräte, die eine Datenbank nutzen.

WARUM DAS WICHTIG IST

Dieselbe Datenbank in Dropbox hat auf Mac, Windows und Linux unterschiedliche Pfade, und der USB-Stick mit der Schlüsseldatei wechselt Laufwerksbuchstaben oder Namen. Dank der Datensätze pro Gerät findet jedes seine eigenen Pfade, ohne die der anderen zu überschreiben.

DATENSICHERHEIT

12 AUTOMATISCHE SICHERUNG

Jede Datenbank und jeder Tresor kann ein **zweites Ziel** haben, auf diesem Computer (zum Beispiel eine externe Festplatte) oder auf einem eingerichteten Server. Bei jeder Änderung kopiert Obskura die neue Version im Hintergrund dorthin, ohne dich zu bremsen.

1. Wähle im Menü ⋯ der Datenbank oder des Tresors **Automatische Sicherung…**
2. Aktiviere **Automatische Sicherung aktiv** und wähle den Ordner: **Auf diesem Computer…** oder **Auf einem Server…**.
3. Ist das Ziel ein Server, kannst du **Diese Konfiguration auf allen Geräten verwenden** aktivieren.
4. Wähle bei Datenbanken, wie viele **datierte Kopien** aufbewahrt werden.
5. Drücke **Speichern**. **Jetzt ausführen** erzwingt eine vollständige Kopie.

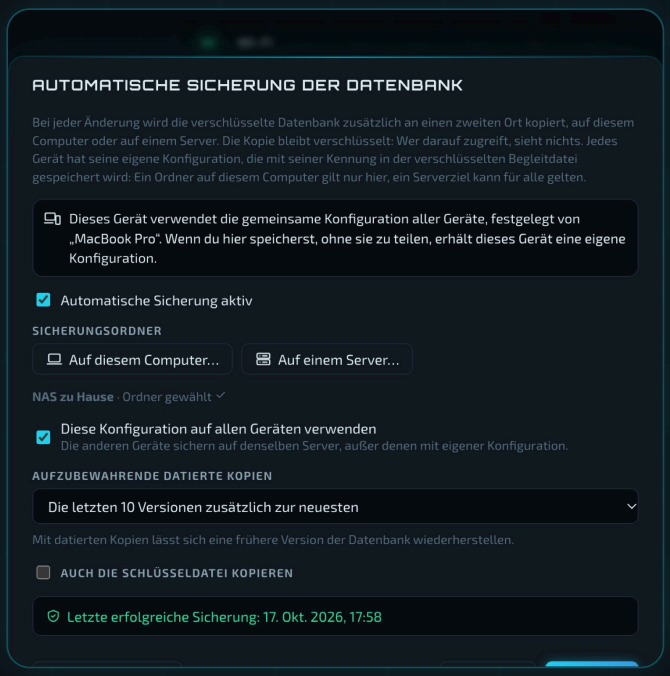


ABB. 10 Sicherung auf ein NAS, gemeinsam für alle Geräte.

WAS	WIE ES KOPIERT WIRD
Datenbank	Die `.obk`-Datei im Sicherungsordner, dazu die datierten Kopien `name.JJJJMMTT-hhmmss.obk`; die ältesten über dem Limit werden gelöscht.
Tresor	Ein Abbild des verschlüsselten Ordners: Bei jeder Änderung werden nur die betroffenen Dateien erneut kopiert. Die Kopie öffnet sich wie ein normaler Tresor.
Schlüsseldatei	Optional: einmal beim Speichern der Einstellung in den angegebenen Ordner kopiert.

EINE SICHERUNG FÜR JEDES GERÄT

- Jedes Gerät hat seine **eigene Konfiguration**, mit seiner Kennung in der Begleitdatei gespeichert: Ein lokaler Ordner (etwa die externe Festplatte des Mac) gilt nur auf diesem Gerät.
- Ein Serverziel kann **gemeinsam** werden: Die anderen Geräte nutzen es, außer denen mit eigener Konfiguration. Das Fenster zeigt, wer es festgelegt hat.
- Die Kopien bleiben **verschlüsselt**: Dem Sicherungsziel muss man nicht vertrauen.
- Schlägt eine Sicherung fehl, erscheint ein Hinweis; Obskura versucht es bei der nächsten Änderung erneut.

SCHLÜSSELDATEI UND SICHERUNG

Lege die Schlüsseldatei nicht in denselben Ordner wie die Sicherung: Wer auf diesen Ordner zugreift, hätte sowohl die Datenbank als auch die Hälfte der Zugangsdaten.

VON UND ZU ANDEREN PROGRAMMEN

13 IMPORT UND EXPORT

AUS EINEM ONLINE-MANAGER IMPORTIEREN

Obskura meldet sich direkt bei deinem alten Dienst an, lädt den verschlüsselten Tresor herunter und entschlüsselt ihn auf deinem Computer, ohne Umweg über eine im Klartext exportierte Datei. Die Zugangsdaten dienen nur dieser Anmeldung und werden nicht gespeichert.

1. Öffne die Zieldatenbank und wähle ⋯ → **Aus einem Online-Manager importieren…**
2. Wähle den Dienst und melde dich an; bei Zwei-Schritt-Bestätigung fragt Obskura nach dem Code.
3. Prüfe die Vorschau: Anzahl der Einträge, Ordner, Beispiele.
4. Entscheide, ob die Ordner als Gruppen übernommen und vorhandene Einträge übersprungen werden, und drücke **Importieren**.

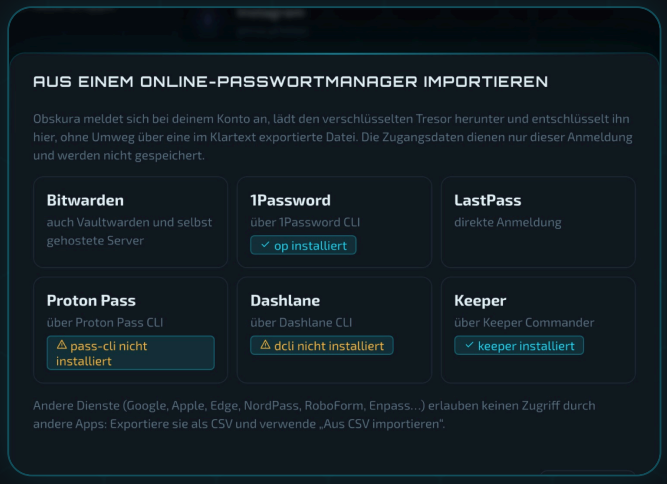


ABB. 11 Die Wahl des Dienstes für den Import.

DIENST	ZUGANG
Bitwarden / Vaultwarden	Direkt, auch bitwarden.eu und selbst gehostete Server; alternativ mit dem persönlichen API-Schlüssel.
LastPass	Direkt, mit Zwei-Schritt-Bestätigung (Code oder Bestätigung auf dem Telefon).
1Password	Über 1Password CLI (`op`), freigegeben durch die 1Password-App oder mit E-Mail, Passwort und Secret Key.
Proton Pass	Über Proton Pass CLI (`pass-cli`), mit Anmeldung im Browser.
Dashlane	Über Dashlane CLI (`dcli`), nach einem ersten `dcli sync` im Terminal.
Keeper	Über Keeper Commander (`keeper`).

Ordner, eigene Felder, TOTP-Codes, Karten und Notizen bleiben erhalten. Andere Dienste (Google, Apple, Edge, NordPass…) erlauben keinen Zugriff durch andere Apps: Exportiere sie als CSV.

AUS CSV IMPORTIEREN (KEEPASS UND ANDERE)

1. Exportiere im Ursprungsprogramm als CSV: KeePass 2 **Datei → Exportieren → KeePass CSV (1.x)**, KeePassXC **Datenbank → Exportieren → CSV-Datei**, Bitwarden, 1Password, Chrome, Edge und Firefox über ihre Einstellungen.
2. Öffne in Obskura die Datenbank und wähle ⋯ **→ Aus CSV importieren (KeePass, …)…**
3. Wähle die Datei: Obskura erkennt Format und Spalten und zeigt eine Vorschau.
4. Entscheide, ob die Gruppen der Datei übernommen und vorhandene Einträge übersprungen werden, und drücke **Importieren**.

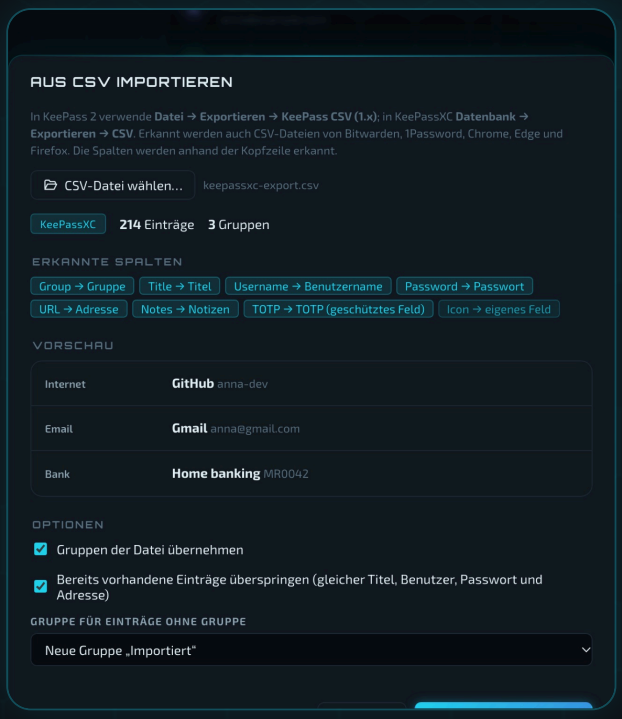


ABB. 12 Vorschau eines KeePassXC-Exports.

Gruppen, Schlagwörter, TOTP-Codes (als geschütztes Feld gespeichert), Erstellungs- und Ablaufdaten bleiben erhalten; nicht erkannte Spalten werden zu eigenen Feldern. Ein erneuter Import derselben Datei erzeugt keine Duplikate.

ALS CSV EXPORTIEREN

⋯ **→ Als CSV exportieren…** erzeugt eine Datei mit den Spalten von KeePassXC, dazu Schlagwörter, Ablaufdatum, Favoriten und eigene Felder: Sie lässt sich in Obskura, KeePassXC und die meisten Passwort-Manager wieder importieren.

CSV IST NICHT VERSCHLÜSSELT

Die Datei enthält alle Passwörter im Klartext. Verwende sie nur zum Übertragen der Daten und lösche sie danach. Lösche nach dem Import auch die vom alten Programm exportierte CSV. Für Sicherungen verwende die automatische Sicherung, die verschlüsselt bleibt.

ANPASSEN

14 SPRACHEN

Obskura spricht acht Sprachen, weitere lassen sich hinzufügen: Alle Texte der App stehen in XML-Dateien, eine pro Sprache.

DIE SPRACHE WÄHLEN

Beim Start verwendet Obskura die Systemsprache; ist sie nicht enthalten, Englisch. Unter **Einstellungen → Sprache** kannst du **Automatisch** lassen oder eine Sprache wählen: Der Wechsel erfolgt sofort, auch für Fehlermeldungen. Arabisch wird von rechts nach links gelesen, und die Oberfläche wird entsprechend gespiegelt.

Italiano	it
English	en
Deutsch	de
Español	es
Русский	ru
中文（简体）	zh
日本語	ja
العربية	ar

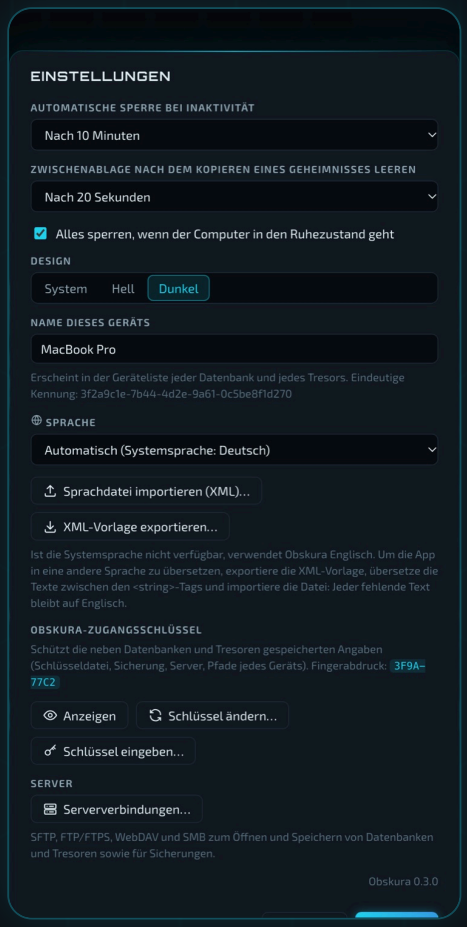


ABB. 13 Der Bereich Sprache in den Einstellungen.

EINE SPRACHE HINZUFÜGEN

1. Drücke unter **Einstellungen → Sprache** auf **XML-Vorlage exportieren…**: Du erhältst die vollständige Datei der aktuellen Sprache (oder lade von der Website das Zip mit den XML-Dateien aller Sprachen).
2. Ändere in der Kopfzeile `code` (den Sprachcode, etwa `fr` oder `pt-BR`), `name` und bei Sprachen, die von rechts nach links laufen, `dir="rtl"`.
3. Übersetze den Text jedes `<string>`-Elements mit einem beliebigen Texteditor und speichere in UTF-8.
4. Drücke **Sprachdatei importieren (XML)…**: Die Sprache erscheint sofort in der Liste und wird auf Systemen in dieser Sprache automatisch verwendet.

DAS DATEIFORMAT

Eine Sprachdatei ist eine XML-Datei mit einem `<language>`-Element und einem `<string>` pro Text:

```
<?xml version="1.0" encoding="UTF-8"?>
<language code="fr" name="Français" english-name="French" dir="ltr">
  <string key="common.cancel">Annuler</string>
  <string key="db.syncFailed">Échec de la synchronisation : {message}</string>
  <string key="vault.itemsN.one">{count} élément</string>
  <string key="vault.itemsN.other">{count} éléments</string>
</language>
```

- Das Attribut `key` wird weder übersetzt noch geändert;
- Platzhalter in geschweiften Klammern wie `{count}` oder `{name}` bleiben unverändert: Die App ersetzt sie durch Zahlen und Namen;
- die Tags `<b>` und `<code>` im Text müssen erhalten bleiben;
- Schlüssel, die auf `.one`, `.two`, `.few`, `.many` und `.other` enden, sind Pluralformen: Verwende die deiner Sprache, `.other` ist Pflicht;
- ein fehlender Text wird auf Englisch angezeigt, eine Teilübersetzung funktioniert also bereits.

EINE ENTHALTENE SPRACHE KORRIGIEREN

Eine XML-Datei mit demselben `code` wie eine enthaltene Sprache (etwa `de`) ersetzt diese nicht: Sie korrigiert nur die enthaltenen Einträge. In den Einstellungen erscheint sie mit dem Hinweis **Korrekturen** und lässt sich mit dem × entfernen, womit die Originaltexte zurückkehren.

TIPP

Importierte Dateien bleiben im Datenordner der App und gelten nur auf diesem Computer: Importiere sie auch auf den anderen.

ÜBERSETZEN MIT DER LEEREN XML-VORLAGE

Für eine neue Sprache kannst du mit der leeren Vorlage `obskura-translation-template.xml` beginnen, die du auf der Website herunterlädst (`obskura.bytenooks.com`, Bereich Download). Sie enthält eine Zeile pro Text der App: Der Text wird zwischen `<string …>` und `</string>` geschrieben; das Attribut `en` enthält den englischen Referenztext und kann bleiben (die App ignoriert es).

```
<language code="fr" name="Français" english-name="French" dir="ltr">
  <string key="common.lock" en="Lock">Verrouiller</string>
  <string key="common.settings" en="Settings">Paramètres</string>
  <string key="common.cancel" en="Cancel">Annuler</string>
</language>
```

1. Lade die Vorlage herunter und speichere sie mit dem Code deiner Sprache, zum Beispiel `fr.xml`.
2. Fülle in der ersten Zeile `<language>` die Attribute `code`, `name`, `english-name` und bei Bedarf `dir="rtl"` aus.
3. Schreib die Übersetzungen mit einem Texteditor, der in UTF-8 speichert, und halte dich an die Regeln oben.
4. **Lösche die Zeilen, die du nicht übersetzt**: Ein leer gelassener Text erschiene in der App leer, eine fehlende Zeile dagegen auf Englisch.
5. Importiere die Datei unter **Einstellungen → Sprache** und prüfe die Texte in der App.

TEILE DEINE ÜBERSETZUNG

Schick sie über die Kontaktseite der Website an den Entwickler: Wähle das Thema „Übersetzung“ und hänge die XML-Datei an (bis 3 MB; eine vollständige Sprachdatei hat etwa 100–150 KB). Eingesandte Übersetzungen können in künftige Versionen aufgenommen werden.

SICHERHEIT

15 SPERREN UND EINSTELLUNGEN

Beim Sperren einer Datenbank oder eines Tresors beendet Obskura die Sitzung und **löscht** Schlüssel und entschlüsselte Daten **aus dem Speicher**. Zum erneuten Öffnen braucht es wieder die Zugangsdaten.

MÖGLICHKEITEN ZUM SPERREN

- **Alles sperren** unten in der Seitenleiste oder `Strg/⌘` + `L`.
- Das Schloss neben einem entsperrten Element der Seitenleiste oder der Eintrag **Sperren** im Menü ⋯.
- **Automatisch**, nach einer Zeit der Inaktivität oder wenn der Computer in den Ruhezustand geht.

EINSTELLUNGEN

EINSTELLUNG	WIRKUNG	STANDARD
Automatische Sperre bei Inaktivität	Sperrt alles nach 1–60 Minuten ohne Maus- oder Tastaturnutzung, oder nie.	10 Minuten
Zwischenablage leeren	Leert die Zwischenablage 10–120 Sekunden nach dem Kopieren eines Geheimnisses, oder nie.	20 Sekunden
Sperre im Ruhezustand	Sperrt alles, wenn der Computer in den Ruhezustand geht.	Aktiv
Design	System, Hell oder Dunkel.	Dunkel
Name dieses Geräts	Erscheint in der Geräteliste jeder Datenbank und jedes Tresors; darunter steht die eindeutige Kennung.	Computername
Sprache	Automatisch oder eine der verfügbaren Sprachen; Import und Export der XML-Dateien (Kapitel 14).	Automatisch
Obskura-Zugangsschlüssel	Den Schlüssel anzeigen, ändern oder eingeben (Kapitel 11).	—
Server	Die Verbindungen SFTP, FTP/FTPS, WebDAV und SMB (Kapitel 09).	—

Die Einstellungen enthalten keine Geheimnisse: Serverpasswörter liegen im Schlüsselbund des Systems, und die Liste der zuletzt verwendeten ist mit dem Zugangsschlüssel verschlüsselt.

REFERENZ

16 TASTENKÜRZEL UND KRYPTOGRAFIE

TASTENKÜRZEL

TASTEN	WO	AKTION
`Ctrl/⌘` + `L`	Überall	Alles sperren
`Esc`	Dialogfenster	Schließt das Fenster
`Ctrl/⌘` + `F`	Datenbank	Suchen
`Ctrl/⌘` + `N`	Datenbank	Neuer Eintrag
`Ctrl/⌘` + `S`	Eintragseditor	Eintrag speichern
Doppelklick	Eintragsliste	Passwort kopieren
`Ctrl/⌘` + `A`	Tresor	Alles auswählen
`Enter`	Tresor	Öffnet Datei oder Ordner
`F2`	Tresor	Umbenennen
`Del` · `⌘` + `⌫`	Tresor	Ausgewählte Elemente löschen
`⌫`	Tresor	Zum übergeordneten Ordner

KRYPTOGRAFISCHE DETAILS

KOMPONENTE	ALGORITHMUS
Schlüsselableitung	Argon2id: 256 MiB / 3 Durchläufe, 1 GiB / 4 Durchläufe oder 2 GiB / 6 Durchläufe, zufälliges 256-Bit-Salt.
Zusammengesetzter Schlüssel	SHA-256 aus Passwort (NFC-normalisiert) und Schlüsseldatei, wie KeePass KDBX4.
Verschlüsselung	AES-256, XChaCha20, Serpent, Twofish, Camellia oder Kaskaden, stets authentifiziert (GCM oder Poly1305); in Kaskaden hat jede Schicht einen eigenen, per HKDF abgeleiteten Schlüssel.
Unterschlüssel	HKDF-SHA256 mit neuem Seed bei jedem Speichern.
Integrität	Authentifizierter Kopf: Jede Veränderung verhindert das Öffnen.
Namen in Tresoren	AES-SIV, an den enthaltenden Ordner gebunden.
Dateiinhalt	Blöcke zu 64 KiB, zufälliger Schlüssel pro Datei, Schutz vor Umordnung und Abschneiden.
Begleitdateien	AES-256-GCM mit einem per HKDF aus dem Obskura-Zugangsschlüssel (256 Zufallsbits) abgeleiteten Schlüssel.
Speicher	Schlüssel und Klartextdaten bleiben im nativen Prozess und werden beim Schließen gelöscht.

HILFE

17 BEWÄHRTE PRAXIS UND PROBLEME

BEWÄHRTE PRAXIS

- **Aktiviere die automatische Sicherung** oder kopiere regelmäßig die `.obk`-Dateien und Tresorordner auf eine externe Festplatte. Sie sind bereits verschlüsselt, die Sicherung ist also überall sicher.
- **Bewahre die Schlüsseldatei getrennt** von der Datenbank auf und halte mindestens eine Ersatzkopie bereit.
- **Bewahre den Obskura-Zugangsschlüssel** auf Papier oder an einem anderen Ort als dem Computer auf.
- **Verwende für jeden Dienst ein anderes Passwort**, mit dem Generator erzeugt: Merken musst du dir nur eines.
- **Sperre, wenn du dich entfernst**: `Strg/⌘` + `L` geht am schnellsten.
- **Vergiss Geräte**, die du nicht mehr nutzt, im Fenster **Geräte und Pfade**.

HÄUFIGE FRAGEN

ICH HABE DAS HAUPTPASSWORT VERGESSEN. KANN ICH ES WIEDERHERSTELLEN?

Nein. Genau das macht Obskura sicher: Niemand, auch nicht die Entwickler, kann eine Datenbank oder einen Tresor ohne die richtigen Zugangsdaten öffnen.

„FALSCHES PASSWORT ODER FALSCHE SCHLÜSSELDATEI“, OBWOHL ICH SICHER BIN, DASS SIE STIMMEN.

Prüfe, ob du dieselbe Schlüsseldatei wie beim Erstellen gewählt hast und ob sie verändert wurde. Hast du Passwort *und* Schlüsseldatei verwendet, braucht es beide. Prüfe auch die Feststelltaste.

DAS ÖFFNEN DAUERT EINIGE SEKUNDEN. IST DAS NORMAL?

Ja: Das ist die Zeit von Argon2id, gewollt, um das Erraten des Passworts zu bremsen. Die Stufe Hoch braucht einige Sekunden und 1 GiB freien Speicher, Extrem bis zu 12 Sekunden und 2 GiB.

AUF EINEM ANDEREN COMPUTER WIRD DIE SCHLÜSSELDATEI NICHT GEFUNDEN.

Schließe das Laufwerk an, auf dem sie liegt: Obskura sucht sie unter dem Pfad, den dieser Computer zuletzt verwendet hat, neben der Datenbank, unter den Pfaden der anderen Geräte und in der Sicherungskopie. Findet es sie nicht, wähle sie mit **Wählen…**: Beim nächsten Mal wird der Pfad für dieses Gerät gespeichert.

ES ERSCHEINT „MIT EINEM ANDEREN ZUGANGSSCHLÜSSEL GESCHÜTZT“.

Der Zugangsschlüssel wurde auf einem anderen Computer geändert. Klicke auf **Aktuellen Schlüssel eingeben** und verwende den neuen; entsperren kannst du trotzdem mit dem Passwort und der von Hand gewählten Schlüsseldatei.

„ZUGANGSDATEN ANDERSWO GEÄNDERT“ IST ERSCHIENEN.

Jemand hat auf einem anderen Gerät Passwort oder Schlüsseldatei der Datenbank geändert. Wähle **Sperren** und öffne sie mit den neuen Zugangsdaten erneut; **Überschreiben** würde die anderswo vorgenommene Änderung rückgängig machen.

ICH KANN MICH NICHT MIT DEM SERVER VERBINDEN.

Prüfe Adresse, Port und Zugangsdaten mit **Verbindung testen**. Bei WebDAV prüfe den Basispfad (für Nextcloud `/remote.php/dav/files/<benutzer>`), bei SMB den Namen der Freigabe. Bei einem selbstsignierten Zertifikat aktiviere **Selbstsignierte Zertifikate akzeptieren** nur in einem vertrauenswürdigen Netz.

ÄNDERUNGEN AN EINER DATEI IM TRESOR SCHEINEN NICHT GESPEICHERT.

Stelle sicher, dass du die Datei in der anderen Anwendung gespeichert hast, und drücke dann **Änderungen im Tresor speichern**. Sperrst du den Tresor bei noch geöffneter Datei, versucht Obskura trotzdem, sie vor dem Löschen der temporären Kopie zu speichern.

DIE APP ÖFFNET SICH IN EINER SPRACHE, DIE NICHT MEINE IST.

Obskura folgt der Systemsprache; ist deine nicht enthalten, wird Englisch verwendet. Wähle die Sprache unter **Einstellungen → Sprache** oder importiere eine XML-Datei (Kapitel 14).

MACOS ODER WINDOWS MELDEN, DIE APP SEI NICHT VERIFIZIERT.

Die App ist nicht mit einem kommerziellen Zertifikat signiert. Folge den Anweisungen in Kapitel 02, um sie beim ersten Mal zu öffnen.



OBSKURA

UNSICHTBARE SICHERHEIT FÜR DEINE DATEN

Passwort-Manager und verschlüsselte Dateitresore · auf deinem Computer oder deinem Server

macOS · Windows · Linux · Version **0.3.0**

https://obskura.bytenooks.com