

MyLastKey

Ausführliche & praktische Anleitung

Inhalt

1) Was ist MyLastKey? (Überblick)	2
2) Lieferumfang & Systemvoraussetzungen	2
3) Sicherheitsgrundsätze	2
4) Start & Ersteinrichtung	2
5) Bedienkonzept (typische Bereiche)	3
6) Einträge anlegen/ändern/löschen.....	3
7) Dokumente einscannen/abfotografieren	3
8) Import aus gängigen Passwortmanagern	4
9) Backup & Wiederherstellung.....	4
10) MyLastKey-Pass (Erbfall/Notfall/geordnete Übergabe).....	5
11) Datenschutz & Sicherheit (Technischer Überblick)	5
12) Updates & Wartung.....	5
13) Fehlerbehebung (Troubleshooting).....	6
14) FAQ (Auszug)	6
15) Empfohlene Anfangs-Einträge (Checkliste)	7
16) Best Practices (Kurzfassung).....	7
 Schlusswort	7

1) Was ist MyLastKey? (Überblick)

- **Digitaler Tresor auf einem USB-Stick**, ausgeliefert in einer MyLastKey-Box zur sicheren Aufbewahrung (z. B. im Tresor).
- **Komplett offline**: Es wird **nichts** in einer Cloud gespeichert.
- **Verschlüsselt (AES-256)**: Alle Inhalte liegen nur verschlüsselt vor.
- **Zweck**: Passwörter, PINs, Bankdaten, Abos, Versicherungen, wichtige Adressen, Notizen, **Geldverstecke** & Dokumente sicher verwalten und aufbewahren – und bei Bedarf **geordnet an Erben übergeben**.
- **Plattform**: Microsoft Windows.

2) Lieferumfang & Systemvoraussetzungen

Lieferumfang

- 1× MyLastKey-USB-Stick (mit integrierter **MyLastKey-Software**)
- 1× MyLastKey-Box zur Aufbewahrung

Voraussetzungen

- Windows 7/10/11
- Arbeitsspeicher: mind. 2 GB
- 1 freier USB-Port
- Optional: Scanner/Kamera für Dokumente (zum Einscannen/Abfotografieren)

3) Sicherheitsgrundsätze

- **Master-Passwort**: Wählen Sie ein starkes, nur Ihnen bekanntes Hauptkennwort.
- **Physische Sicherheit**: Bewahren Sie den Stick **nicht** am PC, sondern getrennt (z. B. im Safe) auf.
- **Backup**: Erstellen Sie regelmäßig **mindestens eine Backupsicherung** auf separaten USB-Stick (siehe Abschnitt 9).
- **Erbfall**: Geregelt über MyLastKey-Pass (Notfallumschlag/Anweisungen/Abschnitt 10).

4) Start & Ersteinrichtung

1. **USB einstecken → MyLastKey.exe starten.**
 - Bei Windows-Hinweisen (SmartScreen/Antivirus) Anwendung **zulassen** (vertrauenswürdige Quelle).
2. **Neuen Tresor erstellen.** Der Name ist frei wählbar.
3. **Master-Passwort festlegen:**

- Das Passwort ist frei wählbar. Ein starkes Passwort sollte haben:
mind. 12 Zeichen, Groß + klein, Zahlen, Sonderzeichen
- 4. **Testeintrag anlegen** und schließen – zur Kontrolle, dass Änderungen gespeichert werden (die Software speichert **automatisch**).
- 5. **Sollten die Testeinträge nicht gespeichert werden:**
Mögliche Ursachen können blockierende Antivirenprogramme aufgrund der starken Verschlüsselungsalgorithmen, ein kurzzeitiger Kontaktverlust des USB-Sticks oder ein defekter USB-Port sein. Versuchen Sie, den Stick an einem anderen USB-Port direkt am PC zu verwenden, das Antivirenprogramm testweise zu deaktivieren und den Speichervorgang erneut durchzuführen.

5) 🗄️ Bedienkonzept (typische Bereiche)

Die genauen Bezeichnungen können je Version variieren – die Struktur ist erprobt und verständlich.

- **Zugangsdaten** (Passwörter & Logins, Dienste/Apps/Webseiten, 2FA-Hinweise, URL, Versicherungen, Streaming, Mitgliedschaften, SIM-PIN/PUK)
- **Bankkonten** (EC/Kreditkarte, Geräte-PINs, IBAN/BIC, Kreditkarten, Depot, Schließfach)
- **Kryptowährungen** (Seeds, Private Keys, Passwörter, PINs)
- **Wichtige Adressen & Kontakte** (Anwälte, Steuerberater, Ärzte, Betreuung)
- **Freitext** (Wünsche, Anweisungen, Geldverstecke, Art/Ort/Anleitung für den Erbfall)
- **Dateitresor** (Passwortlisten, Ausweise, Karten, Verträge, Notfallvollmachten, Testament, Versorgungsvollmachten). Max. 50MB je Datei.

6) 📝 Einträge anlegen/ändern/löschen

1. **Bereich wählen** (z. B. Zugangsdaten).
2. **Felder** ausfüllen: Titel, Benutzername, Passwort, URL, Notizen, Fälligkeiten (z. B. Kündigungsdatum).
3. **Speichern:** Erfolgt **automatisch** – es gibt keinen „Speichern“-Button.
4. **Ändern/Löschen:** Eintrag öffnen → speichern, bearbeiten oder löschen.

Gute Praxis

- **Ein Eintrag je Konto oder Seed** (übersichtlich).
- **Kündigungsfristen/Ablaufdaten** als Feld (Notizen) pflegen.

7) 📄 Dokumente einscannen/abfotografieren

- Scannen Sie wichtige Unterlagen: Personalausweis, Versicherungspolicen, Vollmachten, Karten-Vorder-/Rückseite.

- Verwenden Sie gut lesbare Fotos (keine Reflexionen, flach auflegen).
- Bei mehrseitigen Dokumenten PDFs erzeugen (Scanner-App).

8) Import aus gängigen Passwortmanagern

Empfohlen als „Schnellbefüllung“ des Tresors.

Allgemeines Vorgehen

1. In Ihrem Passwortmanager **Export** durchführen (CSV/JSON je nach Anbieter).
2. In MyLastKey: **Datei-Tresor** → Datei auswählen.
3. Nach erfolgreichem Import die Passwortmanager-Exportdatei **löschen** (Papierkorb leeren).

Hinweise

- Exportdateien sind **sensibel** (unverschlüsselt) – niemals per E-Mail/Cloud teilen.

9) Backup & Wiederherstellung

Warum? Hardware kann ausfallen oder verloren gehen.

Mindestens **ein getrenntes Backup** ist Pflicht.

Backup anlegen (empfohlen)

1. **Zweiten USB-Stick** vorbereiten (neu, zuverlässig, beschriften).
2. **Backup erstellen:** Die MyLastKey-Ordner (**Vaults, FileVaults, Backups**) manuell kopieren.
Aus Sicherheitsgründen wurde auf eine automatische Backup-Funktion verzichtet.
3. **Aufbewahren:** Getrennt vom Haupt-Stick (anderer Ort/Safe).
4. **Protokollieren** (Datum der Sicherung).

Wiederherstellung

1. **Backup-Stick** einstecken.
2. Dateien aus dem Ordner „Backups“ des Backup-Sticks → in den Ordner „Vaults“ des Haupt-Sticks kopieren.
3. **MyLastKey** starten.
4. **Tresor öffnen** → **Master-Passwort** eingeben.

Best Practices

- **Kein Cloud-Backup.**
- Backups **regelmäßig** erneuern (z. B. nach größeren Änderungen).
- **Beschriftung ohne sensible Details** („MLK-Backup 1“, Datum).

10) 📄 MyLastKey-Pass (Erbfall/Notfall/geordnete Übergabe)

Ziel: Ihre Erben/Bevollmächtigten können **ohne Rätselraten** handeln und haben umfangreichen Zugriff auf Ihre digitalen Daten.

Empfohlenes Setup

- **Haupt-Stick** im Safe + **Backup-Stick** an zweitem sicherem Ort.
 - **Notfallumschlag mit MyLastKey-Pass** (versiegelt)
 - **Erbfall-Checkliste für Bevollmächtigte**
1. MyLastKey-Stick finden (Ort lt. Notiz).
 2. Windows-PC nutzen, Stick einstecken, MyLastKey.exe starten.
 3. Master-Passwort gemäß Anweisung verwenden.
 4. **Einzelne Register** öffnen:
 - Vertragsübersicht → Kündigungen
 - Bankverbindungen → Zahlungen/Abschlüsse
 - Dokumente (Vollmachten/Testament/Kontoauflistung)
 - Freitext (Wünsche/Hinweise/Geldverstecke)
 5. **Vorgaben befolgen**, nichts unverschlüsselt kopieren/versenden.

11) 🛡️ Datenschutz & Sicherheit (Technischer Überblick)

- **Verschlüsselung:** Inhalte werden via **AES-256** verschlüsselt.
- **Offline-Prinzip:** Kein Server, keine Cloud, keine Telemetrie – **Angriffsfläche minimal**.
- **Bedrohungsmodell:**
 - **Stark** gegen: Online-Angriffe, Phishing von Tresorinhalten.
 - **Achten Sie auf:** Verlust/Diebstahl + schwaches Master-Passwort.
- **Empfehlungen:**
 - Master-Passwort als **Passphrase** (z. B. 4–5 zufällige Wörter).
 - Windows mit **aktuellen Updates** betreiben.
 - Stick **nicht** dauerhaft eingesteckt lassen.

12) 🔧 Updates & Wartung

- MyLastKey ist **portable**.
- Updates könnten potenziell ein **Sicherheitsrisiko** darstellen, daher verzichten wir bewusst darauf.

- Unsere Software wurde umfassend getestet und ist so konzipiert, dass sie vollständig **offline und autark** arbeitet.
- **Antivirus/SmartScreen:** MyLastKey ggf. **als vertrauenswürdig** eintragen.

13) Fehlerbehebung (Troubleshooting)

A) „Eingegebene Daten wurden nicht gespeichert“

- MyLastKey speichert **automatisch**. Häufige Ursachen:
 - **Antivirus blockiert** Schreibzugriffe → **Ausnahme/Whitelist** für MyLastKey.exe und den Stick setzen.
 - **Schreibschutz** am Stick aktiviert → Schreibschutz lösen.
 - **Kein freier Speicherplatz** auf dem Stick → Platz schaffen.
 - **Stick zu früh entfernt** → Software schließen, dann erst „Hardware sicher entfernen“.

B) Stick wird nicht erkannt

- Anderen USB-Port/PC testen, Kabel/Adapter prüfen.
- In „Datenträgerverwaltung“ nachsehen (Laufwerksbuchstabe belegt?).
- Wenn Windows Reparatur anbietet: **Abbrechen** (Daten nicht riskieren), zuerst **Backup versuchen**.

C) SmartScreen/Antivirensoftware warnt

- Quelle prüfen (Original-Stick).
- Als **vertrauenswürdige App** zulassen.

14) FAQ (Auszug)

Speichert MyLastKey etwas online?

Nein, alles bleibt **offline** auf Ihrem Stick/Tresor.

Gibt es einen Speichern-Button?

Nein – **Änderungen werden automatisch** gespeichert.

Wie schütze ich mein Master-Passwort?

Starke **Passphrase** wählen, getrennt deponieren (Notar/Bankfach). Kein Wiederverwenden.

Kann ich mehrere Tresore nutzen?

Ja, z. B. getrennte Tresore für privat/geschäftlich.

Was passiert bei Verlust des Sticks?

Ohne Master-Passwort sind die Daten **verschlüsselt**. Nutzen Sie Ihr **Backup**.

15) ➡ Empfohlene Anfangs-Einträge (Checkliste)

- Primäre E-Mail-Konten + Passwörter
- Smartphone-PIN/PUK, Geräte-Passcodes
- Router/WLAN (SSID/Passwort)
- Wichtigste Online-Banking/Zahlungsdienste
- Versicherungen & Policen (mit Kündigungsfristen)
- Miet-/Strom-/Telefonverträge (Kundennummern)
- Arbeitgeber/Steuer/Behörden-Zugänge
- Social-Media (optional)
- **Geldverstecke** (klar dokumentiert für Erben)

16) ★ Best Practices (Kurzfassung)

- **Trenne Daten und Orte:** Haupt-Stick, Backup-Sticks, Notfall-Infos getrennt verwahren.
- **Regelmäßig pflegen:** Neue Konten sofort eintragen; Änderungen zeitnah übernehmen.
- **Mind. halbjährlich prüfen:** Backup-Routine + Erbfall-Unterlagen.
- **Keine Kopien streuen:** Je weniger Kopien, desto besser – aber **mind. 1-2** Backups.

📌 Schlusswort

MyLastKey setzt bewusst auf **Offline-Sicherheit** und **einfache Bedienung**. Mit einem starken Master-Passwort, solider Backup-Routine und klaren Erbfall-Anweisungen sind Ihre digitalen Zugänge und Dokumente langfristig geschützt – und im Notfall schnell auffindbar.

Stand: 05/2025