Fimberger Digitales Erbe
Digitales Nachlass-, Vorsorge- und Erbschaftsmanagement
Kathreinweg 33 | 81827 München
+ 49 89 56 82 10 70 | www.digitaleserbe.net

SICHERHEITSKONZEPT DLH STICK

Ab Version 2.x für Windows und MacOS

Digitales Erbe Fimberger

Kathreinweg 33
81827 München
Germany

Telefon +498956821070
E-Mail info@digitaleserbe.net

Fimberger Digitales Erbe
Digitales Nachlass-, Vorsorge- und Erbschaftsmanagement
www.digitaleserbe.net

DLH Stick Sicherheitskonzept

Historie und Sicherheitsphilosophie des DLH Sticks

Die Entwicklung des DLH Sticks begann am Ende des Jahr 2016 mit dem Ziel, eine sichere und langlebige Lösung zur Verwaltung sensibler Zugangsdaten bereitzustellen. Der ursprüngliche Fokus lag auf der Speicherung von:

- Zugangsdaten zu Internetkonten
- Gerätepasswörtern und sicherheitsrelevanten Informationen
- Sicherheit von persönlichen Daten

Mit dem Hintergrund:

- Kein Vertrauen in Cloudlösungen
- Kein Abo-Modell oder versteckte Kosten
- Einmalige transparente Kosten
- Maximaler Kundensupport

Bereits in der initialen Entwicklungsphase wurde konsequent auf einen maximalen Sicherheitsansatz gesetzt.
Der erste DLH Stick wurde Anfang 2018 final fertiggestellt und zum Verkauf angeboten.

Grundprinzip: Maximale Verschlüsselung

Ein zentrales Leitprinzip der Entwicklung war von Anfang an:
Kein Schutz unterhalb des aktuellen Industriestandards
Konkret bedeutet dies:

- Einsatz von AES-256-Bit-Verschlüsselung oder gleichwertigen Verfahren
- durchgängige Verschlüsselung sensibler Datenbereiche
- keine Speicherung kritischer Informationen im Klartext
- Dieses Prinzip gilt sowohl für:
- gespeicherte Zugangsdaten
- interne Sicherheitsmechanismen
- Kennwortgestützte Backup-Prozesse

Erweiterte Passwortsicherheit (Patentlösung)

Zur Absicherung benutzerschwacher Passwörter wurde ein patentierter Mechanismus integriert:

- EP 3 057 029 B1 (Europa)
- US 10,263,780 B2 (USA)

Dieser Ansatz erweitert klassische Passwortmechanismen und ermöglicht:

- Schutz auch bei schwachen Benutzerpasswörtern
- sichere Darstellung sensibler Inhalte (z. B. Passwortanzeige)
- zusätzliche Schutzschicht unabhängig von der Passwortqualität

Hardware-Sicherheitskonzept

Der DLH Stick basiert bewusst nicht auf Standard-USB-Medien, sondern auf speziell ausgewählten Komponenten mit erhöhtem Sicherheits- und Qualitätsanspruch:
Eigenschaften der eingesetzten Hardware:

- Hardwarebasierte Verschlüsselung (keine reine Softwarelösung)
- Einsatz hochwertiger, langlebiger Bauteile
- physischer Schutz:
- wasserfest
- stoßfest / trittfest
- ausgelegt auf langfristige Nutzung (digitale Nachlassplanung)

Abgrenzung:
Der DLH Stick ist ausdrücklich kein Standard-USB-Stick, sondern ein sicherheitsoptimiertes Speichersystem.

Mehrschichtige Sicherheitsarchitektur

Im Laufe der Weiterentwicklung wurde das Sicherheitskonzept konsequent erweitert:

- Zusätzliche Schutzmechanismen
- softwareseitige Feldverschlüsselung sensibler Daten
- optionale Master-Passwort-Absicherung
- kontrollierte Anzeige sensibler Inhalte

- strukturierte Zugriffskontrolle innerhalb der Anwendung
- Backup-Sicherheit
- Backups werden grundsätzlich mit AES-256-Bit verschlüsselt
- keine unverschlüsselten Sicherungskopien sensibler Daten
- Sicherstellung der Wiederherstellbarkeit bei gleichzeitigem Datenschutz

Konsolidierung der Plattformen (2025)

Mit wachsender Funktionalität entwickelten sich die Windows- und macOS-Versionen zunehmend auseinander, was zu erhöhtem Pflegeaufwand führte.
Daher wurde im Jahr 2025 eine strategische Neuausrichtung umgesetzt:
Ziel:
Plattformübergreifende Konsistenz bei maximaler Sicherheit
Maßnahmen**:**
Einführung einer einheitlichen Datenbankstruktur
Sicherstellung der vollständigen Kompatibilität zwischen:

- Windows
- macOS
- Zugriff auf identische Daten unabhängig vom eingesetzten System

Funktionale Weiterentwicklung

Der DLH Stick hat sich von einem reinen Passwortmanager zu einer umfassenden Sicherheitslösung entwickelt.

Heutige Funktionsbereiche:

- Passwort- und Geräteverwaltung
- Dokumentenarchiv
- Finanzplaner
- Vorsorgeplaner (digitale Nachlassplanung)
- Passkey- und 2FA-Verwaltung
- Adressmanagement
- persönliche Datenverwaltung (z. B. für Behördenprozesse)
- Speicherung persönlicher Botschaften

Dabei gilt weiterhin:

Alle Erweiterungen erfolgen unter Beibehaltung des maximalen Sicherheitsniveaus.

Leitprinzip bis heute

Unverändert seit 2018 gilt für den DLH Stick:
Fokus auf Offline-Sicherheit
Kombination aus:

- Hardwareverschlüsselung
- Softwarebasierter Zusatzsicherheit
- Brute Force Attacken verhindern, **da sich der DLH Stick nach 10 fehlerhaften Eingaben automatisch und konsequent löscht.**

konsequente Ausrichtung auf:

- Vertraulichkeit
- Langlebigkeit
- Benutzerkontrolle
- Der Stick darf nur eine Verbindung zum Internet aufbauen, wenn der Benutzer es ausdrücklich wünscht (z.B. Update).

Technologische Grundlage

Die Anwendungen wurden von Beginn an plattformübergreifend entwickelt:

Windows: auf Basis von .NET (anfänglich .NET 4.x, heute moderne .NET-Versionen)
macOS: native Entwicklung mit Swift (ab macOS 13)

Durch kontinuierliche Weiterentwicklung wurde die Software an neue Betriebssystemversionen und Sicherheitsanforderungen angepasst, insbesondere im Hinblick auf:

- sich verändernde Sicherheitsmechanismen (Apple / Microsoft)
- neue UI-/UX-Anforderungen
- steigende Bedrohungslagen

Zielsetzung und Schutzbedarf

Die Neuentwicklung der Software basiert auf einer fundierten Sicherheitsanalyse, bei der mögliche Angriffsvektoren systematisch identifiziert und durch gezielte Maßnahmen adressiert wurden.

Host-System kompromittiert

Der kritischste Punkt bleibt der Rechner selbst.
Beispiele:

- Keylogger liest Eingaben mit
- Screenshot-/Screenreader-Trojaner sieht angezeigte Passwörter
- Clipboard-Monitor liest kopierte Passwörter
- Malware liest Prozessspeicher
- Malware manipuliert lokale Dateien oder Datenbanken
- Debugger/Dump-Tools greifen auf Speicherabbilder zu

Ein vollständig kompromittiertes Host-System kann softwareseitig nie vollständig ausgeschlossen werden.
Man kann Risiken nur reduzieren und welche Maßnahmen haben wir getroffen.

Clipboard-Angriffe

Wenn ein Passwort kopiert wird:

- bleibt es ggf. in der Zwischenablage
- andere Programme können es auslesen
- Clipboard-History von Windows/macOS kann es speichern
- Cloud-Sync der Zwischenablage kann aktiv sein

Maßnahmen:

- automatische Löschung nach z. B. 20–30 Sekunden
- Warnhinweis bei sensiblen Kopiervorgängen
- keine automatische Kopie ohne Nutzeraktion
- optional: statt Kopieren lieber temporär anzeigen

Shoulder Surfing

Auch ohne Malware kann jemand den Bildschirm sehen:

- Kollege
- Familienmitglied
- Kamera im Raum
- Remote-Support-Tool
- Videokonferenz mit Bildschirmfreigabe

Maßnahmen:

- Passwörter standardmäßig maskiert
- Anzeigen nur zeitbegrenzt
- Inaktivitäts-Sperre

Datenbankmanipulation

Ein Angreifer könnte versuchen:

- SQLite-Dateien zu verändern
- Werte zu ersetzen
- verschlüsselte Felder auszutauschen
- alte Datenbankstände zurückzuspielen
- die App durch kaputte Werte zum Absturz zu bringen

Maßnahmen:

- Integritätsprüfungen
- saubere Fehlerbehandlung
- Eingabevalidierung
- HMAC/Signatur für kritische Datensätze

Backup-Angriffe

Backups sind oft schwächer geschützt als Originaldaten.

Risiken:

- Backup-Datei wird kopiert
- altes Backup enthält alte Passwörter
- Backup wird auf unsicheren Datenträger exportiert
- Backup-Passwort ist schwach
- Backup wird manipuliert

Maßnahmen:

- AES-256-verschlüsseltes Backup
- Backup nie unverschlüsselt erzeugen
- klare Warnung vor Verlust des Backup-Passworts
- Unser Patent zum erhöhten Schutz des Kennwortes

Update-/Supply-Chain-Angriffe

Risiken:

- manipulierte Update-Datei
- falsche Downloadquelle
- kompromittierte Website
- Austausch der EXE/App
- DLL-Sideloading
- manipulierte Abhängigkeiten

Maßnahmen:

- SHA-256-Hash veröffentlichen
- Code Signing – In Zukunft
- Signaturprüfung im Updateprozess
- Updates nur manuell
- keine automatische Ausführung heruntergeladener Dateien

DLL-/Library-Hijacking

Besonders bei Windows relevant:

- Angreifer legt manipulierte DLL neben die EXE
- App lädt falsche Bibliothek
- SQLite-/Crypto-Bibliothek wird ersetzt

Maßnahmen:

- feste Ladepfade
- keine unnötigen DLLs im App-Verzeichnis
- Signaturprüfung kritischer Komponenten
- Publish als Self-contained prüfen
- Schreibrechte auf App-Verzeichnis begrenzen

Rechte- und Pfad-Angriffe

Risiken:

- App greift auf falschen Stick zu
- Laufwerksbuchstabe wird manipuliert
- Symlink/Junction zeigt auf fremden Speicherort
- macOS Bookmark zeigt auf falschen Pfad
- Datenbank liegt nicht auf erwarteter Hardware

Maßnahmen:

- Stick eindeutig identifizieren
- Datenpfade validieren
- Datenbank nur aus erwarteter Struktur laden
- keine blind vertrauten Pfade
- klare Fehlermeldung bei nicht plausibler Umgebung

SQL-Injection und Eingabeangriffe

Auch lokale Apps brauchen Schutz.

Risiken:

- manipulierte Importdateien
- CSV-Injection
- extrem lange Eingaben
- Steuerzeichen
- HTML-/Markdown-Injection in Druck/PDF/Export
- fehlerhafte Sonderzeichen

Maßnahmen:

- parametrisierte SQL-Abfragen
- Längenlimits
- Whitelisting/Sanitizing
- Export-Encoding
- CSV-Formelzeichen entschärfen: =, +, -, @

Import-Angriffe

Gerade bei Browserpasswort- und Adressimport wichtig:

- manipulierte CSV-Dateien
- Duplikate mit bewusst veränderten Feldern
- schädliche URLs
- extrem große Dateien
- Encoding-Tricks
- Formelfelder in CSV

Maßnahmen:

- Import nur in Staging-Tabellen
- Vorschau vor Übernahme
- Dublettenprüfung
- Größenlimit
- keine automatische Ausführung von Links
- klare Trennung zwischen Importdaten und produktiven Daten

Druck- und PDF-Angriffe

Da ihr PDF/Druckfunktionen habt:

- sensible Daten landen im Druckerspooler
- PDF wird unverschlüsselt gespeichert
- temporäre HTML-/PDF-Dateien bleiben liegen
- Druckvorschau zeigt sensible Daten
- Betriebssystem speichert Vorschauen/Thumbnails

Maßnahmen:

- Warnhinweis vor Ausdruck sensibler Daten
- temporäre Dateien löschen
- sensible Druckoptionen bewusst aktivieren
- keine Passwörter standardmäßig drucken
- optional: „sicheren Ausdruck“ ohne Geheimnisse

Logging- und Fehlerdiagnose

Risiken:

- Passwörter/PINs landen in Logs
- Datenbankpfade offenbaren Struktur
- Stacktraces enthalten sensible Inhalte
- Debug-Ausgaben bleiben in Release-Version

Maßnahmen:

- niemals Geheimnisse loggen
- Release-Logging minimieren
- Debug-Ausgaben entfernen
- Fehlertexte benutzerfreundlich, aber nicht zu technisch

Speicher- und Cache-Reste

Risiken:

- entschlüsselte Werte bleiben im RAM
- UI-Bindings halten Klartext länger als nötig
- Undo/Redo-Puffer speichern Eingaben
- Crash-Dumps enthalten sensible Daten
- Swap/Pagefile kann Klartext enthalten

Maßnahmen:

- Klartext nur kurzzeitig halten
- nach Anzeige wieder löschen
- SecureString soweit sinnvoll
- Crash-Dumps deaktivieren bzw. nicht erzeugen
- Auto-Lock leert sensible ViewModels

Berechtigungs- und Rollenproblem

Beim digitalen Nachlass gibt es ein fachliches Risiko:

- Nutzer möchte Daten erfassen
- Angehörige sollen später Zugriff haben
- aber nicht jeder soll alles sofort sehen

Maßnahmen:

- getrennte Sichtbarkeit sensibler Felder

- Masterkennwort für Geheimnisse
- erklärter Notfall-/Nachlassprozess
- klare Benutzerhinweise: Wer das Masterkennwort nicht hat, kann verschlüsselte Felder nicht wiederherstellen

Social Engineering

Risiken:

- Nutzer wird zum Herausgeben des Masterkennworts verleitet
- Fake-Update wird installiert
- falscher Support fordert Daten an
- Phishing über angebliche DLH-Stick-Mails

Maßnahmen:

- klare Update-Regeln
- Wir fragen niemals nach einem Kennwort
- Sicherheitsseite auf Website
- Hash/Signaturhinweise
- Supportprozess definieren

Technologische Weiterentwicklung der Plattform

Im Zuge der Weiterentwicklung des DLH Sticks wurde die zugrunde liegende Technologiearchitektur gezielt modernisiert. Dies betrifft insbesondere die Migration von älteren Plattformversionen auf aktuelle Laufzeitumgebungen:

- macOS: von älteren Versionen (z. B. macOS 13) auf aktuelle Systemversionen
- Windows: von .NET 4.x auf .NET 10

Sicherheitsanforderungen

Ein wesentlicher Treiber für die Migration war die kontinuierliche Weiterentwicklung der Sicherheitsmechanismen moderner Betriebssysteme und Frameworks.
Neue Plattformversionen bieten u. a.:

- verbesserte Speicherverwaltung (Reduktion von Memory-Leaks und Angriffspunkten)
- erweiterte Schutzmechanismen gegen Code-Injection und Manipulation

- aktualisierte Kryptographie-Bibliotheken
- verbesserte Sandbox- und Berechtigungskonzepte (insbesondere unter macOS)

Ältere Frameworks wie .NET 4.x erreichen zunehmend das Ende ihres Sicherheitslebenszyklus und erhalten nur noch eingeschränkte Updates.

Zukunftssicherheit und Wartbarkeit

Die Migration stellt sicher, dass:

- langfristig Security Updates verfügbar bleiben
- neue Betriebssystemversionen vollständig unterstützt werden
- Abhängigkeiten (Libraries, Compiler, Toolchains) aktuell gehalten werden

Ziel war es, eine Plattformbasis zu schaffen, die auch in den kommenden Jahren stabil betrieben und weiterentwickelt werden kann.

Performance und Stabilität

Moderne Laufzeitumgebungen wie .NET 10 bieten:

- deutlich verbesserte Ausführungsgeschwindigkeit
- optimierte Speicherverwaltung
- stabileres Multithreading
- effizientere Datenbankzugriffe (z. B. SQLite-Anbindung)

Dies wirkt sich direkt auf die Zuverlässigkeit und Reaktionsfähigkeit der Anwendung aus.

Plattformkonsolidierung

Ein weiterer zentraler Grund war die Reduzierung des Entwicklungs- und Pflegeaufwands:

- Vereinheitlichung der technischen Basis zwischen Windows und macOS
- Reduktion von divergierenden Codepfaden
- bessere Testbarkeit und Qualitätssicherung

Dies war insbesondere notwendig, da sich die Plattformen im Laufe der Jahre zunehmend auseinanderentwickelt hatten.

Anpassung an Herstelleranforderungen

Sowohl Apple als auch Microsoft entwickeln ihre Plattformen kontinuierlich weiter:

- Änderungen an UI-Frameworks
- neue Sicherheitsrichtlinien
- Einschränkungen für ältere APIs

Durch die Migration wird sichergestellt, dass die Anwendung weiterhin:

- kompatibel bleibt
- alle sicherheitsrelevanten Systemfunktionen nutzen kann
- zukünftige Plattformanforderungen erfüllt

Fazit

Die Migration auf aktuelle Plattformen ist kein rein technisches Upgrade, sondern ein zentraler Bestandteil des Sicherheitskonzepts:
Nur durch den Einsatz moderner, aktiv gepflegter Plattformen kann ein dauerhaft hohes Sicherheitsniveau gewährleistet werden.

Verantwortung des Anwenders und sicherer Umgang mit dem DLH Stick

Die Sicherheit des DLH Sticks basiert auf einer Kombination aus technischer Absicherung und verantwortungsbewusstem Umgang durch den Anwender. Trotz umfangreicher Schutzmechanismen kann ein hohes Sicherheitsniveau nur gewährleistet werden, wenn grundlegende Sicherheitsprinzipien im täglichen Einsatz beachtet werden.

Verantwortung des Anwenders

Der Anwender trägt maßgeblich zur Sicherheit der gespeicherten Daten bei. Dies betrifft insbesondere:

- den sicheren Umgang mit dem DLH Stick
- die Wahl und Geheimhaltung des Master-Passworts
- den Einsatz auf vertrauenswürdigen Systemen

- die regelmäßige Aktualisierung des Betriebssystems

Ein unsicheres Nutzungsverhalten kann die Wirksamkeit technischer Schutzmaßnahmen erheblich einschränken.

Empfehlungen für den sicheren Einsatz

Verwendung vertrauenswürdiger Systeme

Der DLH Stick sollte ausschließlich auf Systemen verwendet werden, die:

- frei von Schadsoftware sind
- regelmäßig aktualisiert werden
- über aktuelle Sicherheitsupdates verfügen

Nicht empfohlen:

- öffentliche Rechner (z. B. Internetcafés)
- fremde oder nicht kontrollierte Geräte

Sicheres Passwort

Das Passwort stellt die zentrale Schutzinstanz für verschlüsselte Inhalte dar.

Empfehlungen:

- ausreichend lang (mindestens 12–16 Zeichen)
- Kombination aus Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen
- keine Wiederverwendung bestehender Passwörter
- keine Weitergabe an Dritte

Wichtiger Hinweis:

Ein Verlust des Passworts führt zum dauerhaften Verlust des Zugriffs auf verschlüsselte Daten.

Schutz vor Einsicht durch Dritte

- sensible Daten nur bei Bedarf anzeigen
- Bildschirm bei Abwesenheit sperren
- Nutzung in öffentlichen oder überwachten Umgebungen vermeiden
- keine Bildschirmfreigabe während sensibler Vorgänge

Umgang mit Zwischenablage (Clipboard)

Beim Kopieren von Passwörtern ist zu beachten:

- Inhalte der Zwischenablage können durch andere Programme ausgelesen werden
- automatische Löschung sensibler Inhalte wird empfohlen
- Zwischenablage nicht unnötig verwenden

Sicherer Umgang mit Backups

- Backups ausschließlich verschlüsselt erstellen
- Backup-Dateien sicher aufbewahren
- Backup-Passwort getrennt vom Backup speichern
- regelmäßige Überprüfung der Wiederherstellbarkeit

Updates und Softwareintegrität

- Updates ausschließlich aus vertrauenswürdigen Quellen beziehen
- bereitgestellte Prüfsummen (z. B. SHA-256) verwenden – Grundsätzlich prüfen wir das automatisch in der Software – Hinweise auf Anomalien sollten beherzigt werden.
- keine Ausführung unbekannter oder veränderter Dateien

Physischer Schutz des DLH Sticks

- vor Verlust oder Diebstahl schützen
- nicht unbeaufsichtigt lassen
- sichere Aufbewahrung (z. B. Tresor) bei besonders sensiblen Daten

Grenzen der technischen Sicherheit

Auch bei Beachtung aller Sicherheitsmaßnahmen bestehen Restrisiken, insbesondere durch:

- kompromittierte oder manipulierte Endgeräte
- Schadsoftware (z. B. Keylogger, Screen-Capture-Tools)
- bislang unbekannte Schwachstellen in Betriebssystemen oder Software
- unzureichenden Update-Stand von Systemkomponenten

Zusammenfassung

Der DLH Stick stellt eine hochsichere Lösung zur Speicherung sensibler Daten dar. Die tatsächliche Sicherheit ergibt sich jedoch aus dem Zusammenspiel von:

- technischer Absicherung
- aktueller Systemumgebung
- verantwortungsbewusstem Nutzerverhalten

Nur durch die konsequente Beachtung dieser Faktoren kann das volle Sicherheitsniveau des DLH Sticks ausgeschöpft werden.

Die wichtigsten Sicherheitsregeln auf einen Blick

Nur auf sicheren Geräten verwenden

Nutzen Sie den DLH Stick ausschließlich auf vertrauenswürdigen, aktuellen Systemen.

Passwort/Passwörter schützen

Verwenden Sie ein starkes, einzigartiges Passwort – und geben Sie es nur eine vertrauenswürdige Person weiter.

Sensible Daten bewusst anzeigen

Passwörter nur bei Bedarf einblenden und nicht unbeaufsichtigt sichtbar lassen.

Updates nur aus vertrauenswürdiger Quelle

Laden Sie Updates ausschließlich mit Hilfe des integrierten Update-Modul und prüfen Sie diese.

Backup nicht vergessen

Erstellen Sie regelmäßig verschlüsselte Backups und bewahren Sie diese sicher auf.