

KluisAPP

AUSFÜHRLICHES BENUTZERHANDBUCH

Version 0.3.1 (functions) / 1.1 (German localization) • Android • Deutsche Ausgabe • October 2026

Jeffrey Haimé | Jeffrey-Apps

Wichtig: Die Bezeichnungen der Bedienelemente sind sinngemäß übersetzt. Prüfe den genauen Wortlaut in deiner installierten App.

Inhalt

1. Hinweise zur Verwendung
2. Was ist KluisAPP?
3. Installation und erste Einrichtung
4. Entsperren und Sperren
5. Dateien hinzufügen und verschieben
6. Fotos, Videos und Dokumente ansehen
7. Exportieren und Löschen
8. Einstellungen und Zugangsmittel
9. Vollständige verschlüsselte Sicherung erstellen
10. Aus einer Sicherung wiederherstellen
11. Interner Speicher und SD-Karte
12. Sicherheit und Datenschutz
13. Probleme beheben
14. Häufig gestellte Fragen
15. Begriffe
16. Checkliste für sichere Nutzung

1. Hinweise zur Verwendung

Dieses Handbuch beschreibt KluisAPP 0.3.1 anhand der stabilen Quellcode-Inventur und praktischer Tests. Bezeichnungen können je nach Gerät und App-Sprache leicht abweichen. Version 1.1 ergänzt die deutsche Übersetzung, ohne die hier beschriebenen Sicherheitsabläufe zu ändern.

WICHTIG: Bewahre Passwort oder PIN und Wiederherstellungscode sicher außerhalb des Tresors auf. Gehen alle gültigen Zugangsmittel verloren, können die verschlüsselten Dateien dauerhaft unzugänglich werden.

2. Was ist KluisAPP?

KluisAPP ist eine Android-App zur verschlüsselten Aufbewahrung von Fotos, Videos und anderen Dateien. Der Tresor liegt entweder im privaten internen App-Speicher oder in einem ausgewählten Ordner auf einer entfernbaren SD-Karte.

Die App kann Dateien importieren, Fotos anzeigen, Videos abspielen, Dokumente extern öffnen, Dateien exportieren und löschen sowie verschlüsselte Sicherungen erstellen und wiederherstellen.

Sie ist kein Cloud-Synchronisierungsdienst. Eine SD-Karte ersetzt keine unabhängige Datensicherung.

3. Installation und erste Einrichtung

Entscheide dich zunächst für internen Speicher oder eine entfernbare SD-Karte und bereite einen sicheren Aufbewahrungsort für den Wiederherstellungscode vor.

1. Öffne KluisAPP und wähle Internen Speicher verwenden oder SD-Karten-Ordner auswählen. Wähle für SD eine geeignete leere Mappe über die Android-Ordnerauswahl.
2. Wähle Passwort (mindestens 10 Zeichen) oder PIN (mindestens 8 Ziffern), gib es zweimal ein und fahre fort. Das Passwort muss mindestens vier verschiedene Zeichen enthalten; einfache PIN-Muster sind nicht zulässig.
3. Der 32-stellige Wiederherstellungscode wird nur einmal angezeigt. Schreibe ihn sorgfältig ab und bewahre ihn außerhalb des Geräts auf. Bestätige die sichere Aufbewahrung.
4. Gib den vollständigen Code zur Prüfung erneut ein und erstelle den Tresor.

Der Code basiert auf 160 zufälligen Bits und kann in Version 0.3.1 später weder erneut angezeigt noch geändert werden.

Zum Wiederherstellen eines vorhandenen Tresors wähle Auf Sicherung wiederherstellen auf dem Einrichtungsbildschirm. Überschreibe niemals einen bestehenden Tresor.

4. Entsperren und Sperren

1. Öffne KluisAPP und kontrolliere den angezeigten aktiven Speicherort.
2. Gib dein Passwort oder deine PIN ein und tippe auf Entsperren.
3. Bei Bedarf wähle Mit Wiederherstellungscode wiederherstellen und gib den vollständigen Code ein.

Mit dem Schloss-Symbol sperrst du den Tresor manuell. Beim Ausschalten des Bildschirms wird sofort gesperrt; beim Verlassen der App gilt die eingestellte automatische Sperrfrist.

Mehrere falsche Eingaben führen zu längeren Wartezeiten bis maximal fünf Minuten. Dadurch werden keine Dateien gelöscht.

5. Dateien hinzufügen und verschieben

In KluisAPP: Entsperre den Tresor, tippe auf In den Tresor verschieben, wähle Dateien über Android aus und warte auf Import, Verschlüsselung und Prüfung.

Anschließend wähle Original löschen oder Original behalten.

Aus Galerie oder Eigene Dateien: Dateien auswählen, Teilen verwenden, KluisAPP auswählen und die Übertragung bestätigen.

Die App verschlüsselt die Daten und prüft Dateigröße sowie SHA-256. Android kann zum Löschen der Originale eine Bestätigung verlangen oder das Löschen verweigern.

Bei der Meldung Kopiert; Original konnte nicht gelöscht werden kann eine lesbare Kopie außerhalb des Tresors verbleiben. Kontrolliere die Quelle selbst.

6. Fotos, Videos und Dokumente ansehen

Die Tresorübersicht zeigt Dateianzahl und Kacheln mit Exportieren und Löschen.

Tippe auf ein Foto für die Vollbildansicht mit Schließen, Exportieren und Löschen.

Bei Videos kannst du In KluisAPP abspielen oder Anderen Videoplayer wählen. Der interne Player bietet Start/Pause, zehn Sekunden vor/zurück und Vollbild.

Ein externer Player erhält nach deiner Bestätigung vorübergehenden Lesezugriff auf eine entschlüsselte temporäre Kopie. Verwende nur vertrauenswürdige Apps.

Dokumente werden nach Bestätigung in einer geeigneten externen App geöffnet und können dadurch außerhalb der direkten Kontrolle von KluisAPP verarbeitet werden.

7. Exportieren und Löschen

Zum Exportieren tippe auf Exportieren, wähle Zielordner und Dateinamen in Android und warte auf die Erfolgsmeldung.

Anschließend wähle Im Tresor behalten (sicherer Standard) oder Aus Tresor entfernen. Bei Abbruch oder Fehler bleibt die Tresordatei erhalten.

ACHTUNG: Exportierte Dateien sind am Ziel lesbar und nicht mehr durch die Tresorverschlüsselung geschützt.

Zum Löschen tippe auf Löschen, lies die Bestätigung und wähle Endgültig löschen nur, wenn du sicher bist. Damit wird das Tresorelement entfernt, nicht irgendeine Datei außerhalb des Tresors.

8. Einstellungen und Zugangsmittel

Öffne Einstellungen in der Tresorübersicht.

Automatische Sperre: sofort beim Verlassen, nach 15 oder 30 Sekunden, 1, 5 oder 15 Minuten. Beim Ausschalten des Bildschirms erfolgt die Sperre sofort.

Speicheroptionen: interner Speicher oder SD-Karten-Ordner; Migration auf SD ist bei internem Tresor möglich.

Weitere Funktionen: Vollständige Sicherung erstellen, Aus Sicherung wiederherstellen, Passwort oder PIN ändern sowie Videoplayer-Präferenz (intern, extern oder jedes Mal fragen).

Je nach aktueller Konfiguration sind PIN festlegen, Passwort ändern und PIN entfernen verfügbar.

Bewahre den Wiederherstellungscode unabhängig vom Passwort oder der PIN auf. Ohne gültige Zugangsdaten kann eine Sicherung möglicherweise nicht entschlüsselt werden.

9. Vollständige verschlüsselte Sicherung erstellen

1. Entsperre den Tresor und öffne Einstellungen.
2. Wähle Vollständige Sicherung erstellen.
3. Wähle einen sicheren Speicherort und einen eindeutigen ZIP-Dateinamen über Android.
4. Warte auf die Erfolgsmeldung und prüfe, ob die ZIP-Datei vorhanden ist.
5. Kopiere die Sicherung auf ein anderes Gerät oder externes Laufwerk.

Die verschlüsselte ZIP enthält kluisapp-backup.properties, kluis.props, index.enc und verschlüsselte Dateien unter data/. Sie enthält keine lesbaren Fotos.

Prüfe Größe und möglichst ZIP-Integrität sowie SHA-256 nach dem Kopieren. Eine fehlerfreie ZIP-Prüfung beweist noch keine erfolgreiche Entschlüsselung und Wiederherstellung.

Eine Sicherung nur auf demselben Tablet schützt nicht vor Verlust, Diebstahl oder Gerätedefekt.

10. Aus einer Sicherung wiederherstellen

Die Wiederherstellung erfordert einen geeigneten leeren Zielort; KluisAPP überschreibt keinen vorhandenen Tresor.

1. Stelle sicher, dass du die ZIP-Sicherung und das richtige Passwort oder den Wiederherstellungscode hast.
2. Wähle einen leeren Speicherort, niemals den aktiven Tresor.
3. Wähle Aus Sicherung wiederherstellen auf dem Einrichtungsbildschirm oder in Einstellungen.
4. Wähle die ZIP-Datei und warte auf Prüfung und Wiederherstellung.
5. Entsperre den wiederhergestellten Tresor und prüfe, ob alle erwarteten Dateien lesbar sind.

Teste eine Wiederherstellung ausschließlich an einem separaten leeren Zielort. Gefährde nicht deinen einzigen funktionierenden Tresor.

11. Interner Speicher und SD-Karte

Der interne Speicher verwendet den privaten App-Ordner filesDir/kluis. Verändere dessen Inhalt nicht manuell.

Für SD-Karten verwendet die App die Android-Ordnerauswahl und überprüft Datenträger- und Tresoridentität. Wenn Karte oder Ordner fehlen oder nicht übereinstimmen, halte an und prüfe das richtige Medium.

Migration: Öffne bei aktivem internem Tresor Einstellungen, wähle Auf SD-Karte migrieren, bestimme einen geeigneten Zielordner, gib bei Aufforderung die Zugangsdaten ein und warte auf Kopie und Prüfung.

Prüfe anschließend, ob der SD-Tresor aktiv und lesbar ist. Nach dokumentierter Implementierung bleibt der interne Tresor erhalten; lösche ihn nicht, bevor du Sicherungen und aktiven Speicherort geprüft hast.

Wähle oder lösche niemals unbekannte Ordner nur aufgrund ihres Namens.

12. Sicherheit und Datenschutz

Schlüsselableitung: Argon2id mit 64 MiB Arbeitsspeicher, 3 Durchläufen und Parallelität 4.

Schutz des Hauptschlüssels: AES-256-GCM. Dateien und Index: authentifizierte Streaming-Verschlüsselung mit AES-256-GCM/HKDF-SHA256.

Wiederherstellungscode: 160 zufällige Bits als 32 Zeichen. Fehlversuche führen zu Wartezeiten von bis zu fünf Minuten.

FLAG_SECURE verhindert gewöhnliche Bildschirmaufnahmen; automatische Android-App-Sicherungen sind deaktiviert und die App fordert keine Netzwerkberechtigung an.

Dateinamen, Typen, Größen und Hashwerte liegen im verschlüsselten Index. Externe Anzeige kann temporäre entschlüsselte Dateien erzeugen.

Der übertragbare Tresorschlüssel ist nicht an den Android Keystore gebunden. Das erleichtert den Transfer mit korrekten Zugangsdaten, verlangt aber deren sichere Aufbewahrung.

13. Probleme beheben

Falsches Passwort oder falsche PIN: Eingabe und Tastatur prüfen; nicht ständig weiterprobieren.

Falscher Wiederherstellungscode: alle 32 Zeichen mit der ursprünglichen Notiz vergleichen.

Zu viele Fehlversuche: angezeigte Wartezeit abwarten.

SD-Karte oder Ordner nicht verfügbar: richtige Karte, Berechtigungen und Zugriff prüfen.

Ordner gehört zu einem anderen Tresor: abbrechen und Tresoridentität prüfen.

Gewählter Ordner nicht leer: einen anderen leeren Ordner wählen; unbekannte Daten nicht löschen.

Zu wenig Speicherplatz: außerhalb des Tresors Platz schaffen, keine unbekannten verschlüsselten Dateien entfernen.

Kopiert, Original nicht gelöscht: Original in Galerie oder Eigene Dateien prüfen.

Export fehlgeschlagen: Ziel, Berechtigungen und freien Platz prüfen; Tresororiginal bleibt erhalten.

Am Ziel besteht bereits ein Tresor: nur an einen leeren Ort wiederherstellen.

Kein externer Videoplayer: internen Player verwenden oder eine vertrauenswürdige kompatible App installieren.

14. Häufig gestellte Fragen

Kann ich den Wiederherstellungscode später ansehen? Nein, in Version 0.3.1 wird er nur bei der Einrichtung angezeigt.

Ist eine PIN möglich? Ja, mindestens acht Ziffern und gemäß Sicherheitsregeln.

Wird das Original beim Import immer gelöscht? Nein, du entscheidest; Android kann das Löschen verhindern.

Kann ich Videos extern abspielen? Ja, nach Warnung mit einer temporären entschlüsselten Kopie.

Sind exportierte Dateien verschlüsselt? Nein, die exportierte Kopie ist lesbar.

Kann eine Sicherung einen vorhandenen Tresor überschreiben? Nein, die dokumentierte Wiederherstellung lehnt dies ab.

Benötige ich Internet? Nein, die App hat keine Netzwerkberechtigung.

Kann ich einen SD-Tresor auf einem anderen Gerät verwenden? Das Konzept unterstützt Übertragbarkeit, aber Kompatibilität, Speicherwahl und Zugangsdaten müssen geprüft werden; zuerst sichern.

15. Begriffe

Tresor: verschlüsselter Speicher mit Dateien und Index.

Wiederherstellungscode: einmalig angezeigter Code zur Wiederherstellung des Schlüsselzugangs.

Sicherung: ZIP mit den notwendigen verschlüsselten Tresordaten.

Exportieren: lesbare Kopie außerhalb des Tresors speichern.

Migration: geprüfter Umzug an einen anderen Speicherort.

SAF: Android Storage Access Framework mit Datei- und Ordnerauswahl.

SHA-256: Prüfsumme für bytengenauen Vergleich.

Argon2id: Algorithmus zur Ableitung kryptografischer Schlüssel.

AES-256-GCM: authentifizierte Verschlüsselung.

Vault ID: eindeutige Kennung eines Tresors.

16. Checkliste für sichere Nutzung

Wiederherstellungscode und Passwort/PIN sicher und getrennt aufbewahren.

Nach dem Import prüfen, ob Dateien im Tresor geöffnet werden können.

Nach dem Verschieben prüfen, ob lesbare Originale außerhalb des Tresors wirklich gelöscht sind.

Regelmäßig vollständige verschlüsselte Sicherungen erstellen und mindestens eine aktuelle Kopie außerhalb des Android-Geräts aufbewahren.

Kopierte Sicherungen möglichst mit SHA-256 prüfen.

Wiederherstellung nur an einem separaten leeren Ziel testen.

Unbekannte Tresorordner, Indexdateien oder alte Sicherungen nicht ungeprüft löschen.

Nur vertrauenswürdige externe Video- und Dokumenten-Apps verwenden.