INFORMAZIONI:

GESTORE DI PASSWORD - KEYCRYPTA VERSIONE 1.0 ULTIMO AGGIORNAMENTO: Marzo 2026 Autore: Roberto Stocchetti Email: info@keycrypta.com Web: www.keycrypta.com

DESCRIZIONE KeyCrypta è un gestore di password offline ad altissima sicurezza, progettato per proteggere i tuoi dati sensibili da ogni minaccia: attacchi informatici, furti fisici, intercettazioni, keylogger e tecniche di forzatura avanzate. Il Software opera offline. Le uniche comunicazioni verso l'esterno possono avvenire: (i) per l'attivazione/ri-attivazione della licenza se l'utente invia volontariamente l'UUID; (ii) per la funzione opzionale "Verifica Violazione Password" (vedi sotto). Nessun dato viene trasmesso o archiviato al di fuori del dispositivo, salvo quanto sopra indicato. Non invia automaticamente dati a nessuno: è progettata per rimanere offline. Tutti i dati sono cifrati, firmati, verificati e auto-protetti direttamente sul dispositivo dell'utente dove viene installata e lanciata l'applicazione. L'intera architettura è stata aggiornata per supportare anche algoritmi post-quantum, assicurando protezione contro minacce future legate all'informatica quantistica.

COMPATIBILITÀ KeyCrypta è supportata esclusivamente su Microsoft Windows 10 e Microsoft Windows 11. L'uso su altri sistemi operativi (Linux in tutte le distribuzioni, macOS, FreeBSD, Android, iOS, ChromeOS) non è consentito né supportato e può causare malfunzionamenti per i quali non è prevista alcuna responsabilità né assistenza.

PUNTI DI FORZA UNICI

- Progettata per mantenere la cassaforte inaccessibile con architettura pronta a integrare algoritmi post-quantum per aumentare la resilienza a minacce future
- Cifratura autenticata e derivazione robusta: XChaCha20-Poly1305 + Argon2id
- Firma e integrità: firme digitali Ed25519 e controlli anti-manomissione
- Formato blindato (.kc.cloud): cassaforte esportabile ovunque, anche su cloud, ma completamente inaccessibile
- Derivazione memory-hard: derivazione di chiavi ultra-sicure con protezione contro attacchi a dizionario e forza bruta
- Autenticazione a quattro livelli: login, password crittografica, risposta segreta obbligatori e

verifica MFA TOTP a due fattori facolativa

- Modalità amministratore per gestire e limitare le autorizzazioni (es. sola lettura) in ambienti aziendali, con una procedura di recupero di emergenza che consente,
ove abilitata, il recupero delle credenziali utilizzate di un utente solo in casi di necessità, tramite una chiave privata dedicata e una funzione di attivazione specifica
- Protezione anti-forza bruta: lockout progressivo, binding UUID e tracciamento cifrato degli accessi/login errati visualizzabile da menu
- Verifica integrità automatica: protezione contro manomissioni invisibili e file alterati
- Backup automatici antifalsificazione: backup cifrati generati automaticamente con protezione anti-manomissione e controllo hardware
(cartella backups)
- Blocco screenshot attivabile
- Export come sequenza parole: possibilità di salvare la cassaforte come lista di parole in lingua naturale
- Clipboard sicura: copia autodistruttiva, timeout sessione e blocco istanza singola regolabile da menu
- Modalità panico: distruzione volontaria e irreversibile della cassaforte in caso di emergenza
- Cancellazione sicura: sovrascrittura RAM e file temporanei anche su dischi SSD, con fallback automatico
- Protezione file sensibili: ACL di sistema attivi contro accessi e cancellazioni non autorizzate
- Rilevamento ambienti ostili: blocco/limitazioni in caso di sandbox, VM, emulatori o strumenti di analisi non autorizzati
- Autodistruzione da tentativi falliti: cassaforte eliminata automaticamente dopo vari login errati secondo requisiti di sicurezza elevati

MODALITÀ PORTABILE SU CHIAVETTA USB CRITTOGRAFATA (PUNTO DI FORZA DISTINTIVO) KeyCrypta è progettato per funzionare anche in modalità completamente portabile, senza installazione su Windows. L'intera applicazione (programma, cassaforte, backup) può risiedere su una chiavetta USB crittografata, consentendo di mantenere tutti i dati sensibili su un unico supporto fisico sicuro. Questa modalità permette di utilizzare KeyCrypta su più computer

autorizzati dalla licenza (UUID multipli), senza lasciare tracce operative permanenti sui PC utilizzati. In ambito aziendale, la modalità portabile consente una gestione sicura delle credenziali anche in scenari di mobilità, postazioni condivise o distribuzione controllata ai dipendenti. In caso di uscita di un utente dall'azienda, se è stato predisposto il Recupero di Emergenza Amministratore, l'amministratore può accedere alla cassaforte su PC autorizzato da licenza, recuperare le credenziali aziendali e procedere alla bonifica del supporto, garantendo continuità operativa e controllo totale 100%.

In ambito aziendale, KeyCrypta adotta un modello offline di segregazione per utente/progetto: ogni dipendente può operare su una cassaforte cifrata dedicata (anche su USB), con policy applicabili dall'amministratore (es. limitazione export/import/backup) e tracciabilità tramite audit cifrato. In caso di offboarding, se è predisposto il Recupero di Emergenza Amministratore, l'IT può recuperare le credenziali aziendali e dismettere/bonificare il supporto secondo le procedure interne.

VANTAGGI TECNICI AVANZATI

- Cassaforte kc.cloud salvabile anche in remoto o in cloud/via mail, ma sempre cifrata e inutilizzabile senza password
- Algoritmi certificati: usa algoritmi crittografici moderni e ampiamente adottati
- Nessuna trasmissione dati: 100% offline, 0% tracciamento
- Nessuna dipendenza da cloud, server o librerie esterne remote
- Import/export autenticati: Ogni operazione di import/export è protetta da controlli di integrità e autenticità invisibili all'utente
- Allegati cifrati (.kc.attachments) protetti in modo trasparente, cancellati automaticamente al termine della visualizzazione, salvabili anche in remoto o in cloud/via mail, ma sempre cifrata e inutilizzabile senza password
- Funzione anti-intrusione: distruzione dati dopo vari login errati secondo requisiti di sicurezza elevati
- Dashboard integrata, cassaforte, backup ZIP, sequenza parole, allegati, log, report
- Supporto nativo a firma digitale modulare: struttura pronta per integrazione di algoritmi

post-quantum (es. Dilithium3) non appena disponibili

INFORMATIVA PRIVACY KeyCrypta non raccoglie né invia automaticamente dati personali. Le uniche comunicazioni verso l'esterno possono avvenire: (i) per attivazione/ri-attivazione licenza se l'utente invia volontariamente l'UUID; (ii) per la funzione facoltativa "Verifica Violazione Password" se attivata, che invia solo i primi 5 caratteri dell'hash SHA1 della password al servizio HaveIBeenPwned per il confronto. Nessuna password viene mai trasmessa o salvata; nessun dato è trasmesso automaticamente. L'UUID può essere inviato dall'utente solo per attivazione/ri-attivazione licenza. L'unico dato tecnico raccolto e usato è l'UUID del dispositivo, necessario per vincolare la licenza al PC dell'utente. Nessuna trasmissione o trattamento remoto è previsto: ogni dato resta salvato cifrato in locale. L'UUID (Universally Unique Identifier) è un identificatore hardware-level, fornito direttamente dal BIOS o UEFI del computer. Non viene generato dal sistema operativo, ma solo letto da esso (es. tramite Windows). L'UUID, di per sé, non include nome/cognome né contenuti della cassaforte. Questo codice è intrinseco all'hardware di ogni computer, stabile nel tempo e non contiene dati personali né informazioni sensibili. Viene usato esclusivamente per vincolare la cassaforte crittografata di KeyCrypta a uno specifico dispositivo fisico, il computer. KeyCrypta utilizza l'UUID come chiave univoca locale per impedire che la cassaforte venga aperta su computer diversi, anche in caso di copia, duplicazione o furto del file. L'UUID non viene trasmesso automaticamente: può essere inviato dall'utente all'autore per l'attivazione/ri-attivazione della licenza. L'utente sceglie di inviarlo all'autore per l'attivazione della licenza.

CONTRATTO DI LICENZA Questo software è concesso in licenza personale e non trasferibile. L'uso è autorizzato solo sui dispositivi associati agli UUID previsti dalla licenza acquistata. La copia, distribuzione, decodifica o alterazione non autorizzata del software è espressamente vietata.

LIMITAZIONE DI RESPONSABILITÀ Il software è fornito "così com'è", senza alcuna garanzia, esplicita o implicita. L'autore non è responsabile per perdita di dati, danni diretti o indiretti o usi impropri. L'uso avviene interamente a rischio dell'utente, che deve adottare misure di backup e protezione dei dati.

MODIFICHE L'autore si riserva il diritto di aggiornare il software e i presenti termini senza preavviso. La prosecuzione dell'uso dopo tali modifiche costituisce accettazione implicita delle stesse.