ENTERPRISE SECURITY OVERVIEW (PUBLIC)

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

0) SCOPO DEL DOCUMENTO (PUBBLICO)

Questo documento descrive, in modo pubblico e non confidenziale, l'impostazione di sicurezza, i controlli principali e gli scenari d'uso "enterprise" di KeyCrypta. È pensato per IT, security officer, procurement e compliance che devono valutare un password manager OFFLINE e on-premise.

NOTA IMPORTANTE:

- Questo documento NON contiene dettagli operativi sensibili.
- I dettagli "NDA/Confidential" sono disponibili separatamente solo sotto accordo di riservatezza (NDA).

1) DESCRIZIONE (EXECUTIVE SUMMARY)

KeyCrypta è un gestore di password offline ad alta sicurezza progettato per la protezione locale di credenziali e dati sensibili. L'architettura segue il principio "data sovereignty first": la cassaforte e gli artefatti di sicurezza restano sempre sotto il controllo dell'utente o dell'organizzazione.

Operatività:

- Funzionamento locale/offline come impostazione di base.
- Nessuna telemetria, nessun account cloud, nessun server obbligatorio.
- Le funzioni opzionali che richiedono rete possono essere disattivate via policy.

Target enterprise:

- Ambienti che richiedono segregazione per utente/ruolo/progetto.
- Organizzazioni che vogliono evitare la sincronizzazione cloud delle credenziali.
- Contesti con requisiti di controllo locale (on-premise / portable-offline).

1.1 SINTESI DI SICUREZZA (WHITE PAPER - VERSIONE SEMPLICE) KeyCrypta è stata

progettata e validata per resistere a scenari di attacco reali tipici dei contesti enterprise, con approccio "misurabile": Niente claim di marketing, ma test automatici, deterministici e ripetibili in ambiente isolato (sandbox), senza accesso a dati reali.

DESIGN GOALS (obiettivi di progetto)

- Funzionare completamente offline (nessuna dipendenza cloud).
- Resistere ad attacchi offline di brute-force sul file cassaforte.
- Rilevare manomissioni/corruzioni della cassaforte (tamper-evident).
- Prevenire replay/rollback di versioni precedenti del vault.
- Applicare key separation (nessun riuso della stessa chiave per scopi diversi).
- Evitare persistenza su disco di dati sensibili in chiaro (best-effort).
- Minimizzare la permanenza in memoria dei dati sensibili (best-effort).

THREAT MODEL (perimetro dichiarato) - ATTORI, CAPACITÀ, COPERTURA (riferimenti al documento)

IN SCOPE (coperto da architettura e test user-space):

- Attaccante con pieno accesso al file vault cifrato (furto/copia).
- Brute-force offline.
- Corruzione/manomissione dei file.
- Replay/rollback di versioni vecchie del vault (mitigazione best-effort user-space, non protezione forense).
- Ispezione "user-space" (es. tentativi di abuso a livello applicativo).
- Uso improprio crittografico (es. key reuse, KDF debole) ridotto/mitigato dal design (KDF robusta, AEAD, separazione contesti dove applicata).

ATTORI OSTILI (semplificati) - cosa significa "IN SCOPE / OUT OF SCOPE":

- Attaccante locale (utente Windows standard):
- Capacità: può copiare file accessibili e tentare attacchi OFFLINE sul file rubato.
- Copertura: vale il perimetro "IN SCOPE" (attacchi offline su file + manomissione + rollback).

- Attaccante locale con privilegi amministratore:

- Capacità: può ispezionare processi e aumentare la capacità di acquisire informazioni dal sistema.
- Copertura: solo mitigazioni "best-effort" user-space + policy/lockdown.
- Limite: scenari OS-level/forensi restano OUT OF SCOPE.

- Attaccante con dump RAM (user-space):
- Capacità: può acquisire snapshot del processo a livello user-space.
- Copertura: mitigazioni "best-effort" di minimizzazione permanenza.
- Nota: durante la visualizzazione/copia, il dato può esistere temporaneamente in chiaro nei buffer UI (limite strutturale user-space).

- Attaccante con accesso fisico (furto PC/USB/disk):
- Capacità: può rubare i file e tentare analisi offline.
- Copertura: vale il perimetro "IN SCOPE" (attacchi offline sul file).

- Malware attivo (keylogger/clipboard/screenshot):
- Capacità: può catturare input/output mentre l'utente usa il PC.
- Copertura: riduzione superficie tramite policy/lockdown (es. blocchi operativi), ma se il sistema è compromesso durante l'uso interattivo la confidenzialità
dell'input/output non è garantibile dal solo perimetro user-space.

OUT OF SCOPE (non oggetto di audit formale in questa release):
- Attacchi kernel/hypervisor-level.
- Dump forensi della memoria a livello OS (es. kernel-level) e analisi avanzata swap.
- Attacchi hardware-assisted.
- Certificazioni formali (es. FIPS).

NOTA: pur senza validazione forense dedicata, il design riduce l'esposizione (least exposure), limita la permanenza in memoria e separa le chiavi/logiche di derivazione per ridurre il rischio anche in scenari ad alta criticità.

In modo semplice:

- Se qualcuno ruba il file della cassaforte, non può leggerlo.
- Se qualcuno prova a modificarlo, la manomissione viene rilevata.
- Versioni vecchie della cassaforte sono soggette a controlli anti-rollback best-effort a livello user-space (non costituisce protezione forense OS-level).
- Le chiavi crittografiche non vengono riutilizzate per scopi diversi.
- Nessuna password o segreto viene lasciato in chiaro su disco.
- I dati sensibili restano in memoria solo per il tempo strettamente necessario.
- NOTA RAM (best-effort, user-space): i campi sensibili nel vault in RAM sono mantenuti cifrati "at-rest" (wrapper di sessione) e decifrati solo on-demand per l'interfaccia.
- Guard-rail: prima del salvataggio vengono rimossi i wrapper RAM e il write è bloccato se restano dati "di sessione".
- Durante la visualizzazione/copia, il dato può esistere temporaneamente in chiaro in RAM nei buffer dell'app/GUI (limite strutturale dei runtime user-space).

Security Testing Results (Summary) I test di sicurezza sono stati eseguiti tramite suite automatizzate e deterministiche, in sandbox isolata, senza accesso a dati reali (test riproducibili).

Primitive verificate (high level):
- KDF: Argon2id (memory-hard) - parametri configurati per contesto (vault / firme / chiavi locali), con profili memory-hard differenziati.
- AEAD: XChaCha20-Poly1305 - confidenzialità + integrità (tamper-evident)

Test (sicurezza) Risultato
- Verifica parametri KDF (Argon2id) PASS
- Resistenza brute-force offline (costo KDF elevato) PASS
- AEAD roundtrip + rilevazione manomissione (tamper) PASS
- Roundtrip save/load della cassaforte PASS
- Rilevazione corruzione/manomissione del vault PASS
- Integrità dei file critici (anti-tamper) PASS
- Controlli anti-replay/rollback (best-effort user-space) PASS
- Key separation (assenza key reuse tra contesti) PASS

- Export/backup cifrati: password errata ? fallisce PASS
- Export/backup cifrati: file alterato/tamper ? rilevato PASS
- Allegati cifrati: roundtrip + rilevazione manomissione PASS
- Audit cifrato: generazione e verifiche di coerenza/integrità PASS
- MFA TOTP (generazione/verifica) PASS
- Singola istanza (anti-collisione) PASS
- Lockout progressivo + contromisure operative (configurabili) PASS
- Zero plaintext su disco (best-effort, sandbox scan) PASS
- Mitigazioni RAM (presenza meccanismi: wipe/lock buffer) PASS

Note:
- "Zero plaintext su disco (best-effort)" è verificato scansionando i file prodotti nei flussi testati in sandbox alla ricerca di marker lunghi e univoci
derivati da credenziali di test; non costituisce prova forense OS-level.
- Le mitigazioni RAM sono verificate come presenza di meccanismi (secure wipe / buffer locking), non come prova forense.

Valutazione interna (nel perimetro dichiarato): livello di sicurezza ELEVATO. La valutazione è basata su test deterministici riproducibili in sandbox isolata e sul threat model esplicitamente dichiarato nel presente documento. Non costituisce certificazione formale, audit indipendente o validazione forense a livello di sistema operativo.

Nota sul punteggio:
- Il punteggio è una valutazione interna basata su test deterministici riproducibili in sandbox e sul threat model dichiarato.
- Il residuo 1 riflette esclusivamente scenari OS-level forensi (es. dump RAM kernel-level / hypervisor) non inclusi nell'audit formale di questa release.

Perimetro di audit (limiti dichiarati):
- Le valutazioni e i test forensi a livello di sistema operativo (es. dump RAM kernel-level, attacchi con privilegi elevati, kernel/hypervisor-level, hardware-assisted)

non sono stati oggetto dell'audit eseguito e risultano fuori dal perimetro di verifica formale.

- Tuttavia, l'architettura di KeyCrypta è stata progettata tenendo conto anche di questi scenari ad alta criticità (minimizzazione esposizione, riduzione permanenza in memoria, separazione chiavi), pur in assenza di validazione forense dedicata.

2) COMPATIBILITÀ E SUPPORTO

- Supporto ufficiale: Microsoft Windows 10 e Windows 11.
- Distribuzione: installazione locale o modalità portabile chiavetta USB (vedi sezione 7).
- Nessuna dipendenza cloud per l'uso quotidiano.

3) PRINCIPI DI SICUREZZA (HIGH LEVEL POLICY)

3.1 Data-at-Rest by design

- Tutti i dati sono cifrati localmente.
- I file critici sono protetti contro manomissioni.
- Le operazioni critiche sono progettate per rilevare manomissioni e incoerenze (tamper-evident).

3.2 Least exposure

- Nessun salvataggio in chiaro di password o segreti.
- Gestione restrittiva dei file temporanei.

3.3 Separation of duties (enterprise)

- Policy amministrative applicabili (read-only, blocchi export/import, ecc.).
- Audit cifrato delle operazioni sensibili (vedi sezione 6).

3.4 Defense-in-depth

- Cifratura autenticata (AEAD).
- Controlli di integrità.
- Protezioni operative contro tentativi non autorizzati e rilevazione ambienti ostili.

4) ARCHITETTURA CRITTOGRAFICA (PUBBLICA)

4.1 PRIMITIVE E PARAMETRI CRITTOGRAFICI

- Derivazione chiavi (KDF): Argon2id (memory-hard)

Parametri per modulo:

- Vault principale (locale):

t = 6 m = 512 MiB p = 2

- Formati cifrati avanzati / export protetti (es. KC.CLOUD):

t = 7 m = 1 GiB p = 2

- KC Share Offline:

t = 7 m = 1 GiB p = 2 KeyCrypta applica preset Argon2id differenziati in base al contesto operativo, con configurazioni orientate a elevata resistenza contro attacchi offline.

- Cifratura simmetrica: XChaCha20-Poly1305
- AEAD (Authenticated Encryption with Associated Data)
- Integrità e autenticazione integrate

- Firme digitali:
- Utilizzate nei flussi che richiedono verifica di autenticità

e integrità crittografica

4.2 Gestione chiavi

- Chiavi derivate localmente dall'utente.
- Nessuna master key su server.
- Permanenza in memoria ridotta (best effort).

4.3 Post-Quantum (roadmap)

- KeyCrypta è predisposta per integrare firme post-quantum in modo opzionale.
- La funzionalità (es. Dilithium3 via liboqs o equivalenti) verrà abilitata in una futura release, subordinatamente alla disponibilità e stabilità della libreria.
- In assenza di abilitazione, i componenti post-quantum restano disattivati (default OFF).

5) AUTENTICAZIONE, ACCESSO E CONTROLLO (ENTERPRISE)

5.1 Modello di accesso KeyCrypta implementa un modello di accesso multi-fattore "a livelli", progettato per adattarsi a contesti enterprise con requisiti di sicurezza differenziati. Il modello può includere, a seconda della configurazione e delle policy:

- Autenticazione primaria basata su credenziale di accesso dell'utente.
- Fattore aggiuntivo di tipo "knowledge" (es. risposta segreta).
- Fattore MFA TOTP opzionale, attivabile dall'utente o imposto da policy aziendale.

Il modello è pensato per consentire un incremento progressivo del livello di sicurezza senza compromettere l'operatività.

5.2 MFA (TOTP) - opzionale

- Supporto a MFA TOTP per rafforzare l'autenticazione in scenari enterprise.
- L'uso dell'MFA può essere:
- facoltativo per l'utente,
- oppure obbligatorio in base a policy IT aziendali.
- L'abilitazione dell'MFA non richiede servizi cloud obbligatori.

5.3 Policy amministrative e modalità di lockdown In contesti enterprise, KeyCrypta consente l'applicazione di restrizioni amministrative configurabili, tra cui (a seconda della policy adottata):

- Modalità SOLA LETTURA (blocco di scrittura e modifica dei dati - disattivato di default).
- Blocco degli screenshot (abilitabile/disabilitabile via policy - attivato di default).
- Disabilitazione di funzionalità opzionali (es. verifica password violate tramite servizi online - attivato di default).
- Blocco delle funzioni di export/import e di trasferimento dati (abilitabile/disabilitabile via policy - disattivato di default).
- Attivazione della cassaforte per un periodo di tempo limitato (utilizzi eccezionali o controllati) - disattivato di default.

Tali policy sono progettate per supportare requisiti di compliance, segregazione dei ruoli e riduzione della superficie di attacco.

5.4 Emergency Access / Business Continuity (opzionale) È prevista una procedura opzionale di Recupero di Emergenza Amministratore, pensata per garantire la continuità operativa in contesti

enterprise, ad esempio in caso di:

- offboarding di un utente,
- indisponibilità prolungata dell'utente titolare della specifica cassaforte locale.

L'abilitazione del recupero di emergenza:

- è una scelta esplicita dell'organizzazione,
- deve essere governata da policy interne,
- richiede un controllo degli accessi IT adeguato.

In assenza di configurazione esplicita, il recupero di emergenza resta disattivato per impostazione predefinita.

6) TRACCIABILITÀ E AUDIT

- Audit log cifrato per tutte le azioni sensibili.
- Report di sicurezza esportabili.
- Nessuna dipendenza da cloud.

7) FORMATI DI BACKUP / EXPORT E PORTABILITÀ (ENTERPRISE)

7.1 Formati cifrati di backup ed export KeyCrypta supporta esclusivamente formati di backup ed export cifrati, progettati per garantire continuità operativa e trasferimento sicuro anche in ambienti enterprise complessi. Sono supportati, tra gli altri:

- Backup/export cifrato "portable" (.kc.cloud), pensato per spostare la cassaforte come singolo file cifrato, utilizzabile anche su canali non fidati senza mai perdere la cifratura.
- Backup/export cifrato locale (.kc.local), destinato a procedure on-premise, repository aziendali e workflow IT interni.
- Export in formato "sequenza parole" (TXT) per scenari di recovery controllato e documentato, sempre governato da policy amministrative.

In tutti i casi, l'export non produce dati in chiaro se non esplicitamente previsto e autorizzato dalle policy.

7.2 Gestione degli allegati cifrati Gli allegati associati alle voci della cassaforte sono gestiti tramite

un archivio cifrato dedicato (.kc.attachments). Caratteristiche principali:

- Cifratura end-to-end degli allegati.
- Apertura controllata dei file.
- Gestione sicura dei file temporanei, con rimozione best-effort al termine dell'utilizzo.

Questo approccio riduce il rischio di esposizione accidentale di dati sensibili su disco.

7.3 Modalità portabile su USB cifrata (vantaggio enterprise) KeyCrypta può essere utilizzato in modalità completamente portabile, caratteristica particolarmente rilevante per contesti enterprise. La modalità portabile consente:

- Esecuzione dell'intera applicazione (programma, cassaforte e backup) da supporto USB cifrato (es. BitLocker To Go o tecnologie equivalenti).
- Riduzione delle tracce persistenti sulle workstation ospitanti.
- Utilizzo in scenari di mobilità, postazioni condivise o ambienti air-gapped.

Best practice enterprise consigliate:

- Utilizzare esclusivamente supporti rimovibili con cifratura reale.
- Gestire distribuzione, inventario e revoca tramite policy IT.
- Separare le casseforti per utente, ruolo o progetto (principio di segregazione).

8) PROTEZIONI OPERATIVE (HIGH LEVEL)

8.1 Anti-forza bruta / anti-intrusione KeyCrypta implementa meccanismi di protezione operativa contro tentativi di accesso non autorizzati e attacchi di forza bruta.

In particolare:

- Lockout progressivo e gestione dei tentativi errati su finestra temporale.
- Rallentamento e limitazione delle operazioni sensibili in presenza di pattern sospetti.
- In condizioni di sicurezza critiche, KeyCrypta può attivare contromisure robuste, inclusa una protezione "distruttiva" della cassaforte dopo un

numero definito di tentativi di accesso errati. Tali contromisure, se attivate, sono irreversibili e devono essere considerate parte di una strategia di sicurezza difensiva avanzata, governata da

policy.

8.2 Rilevazione di ambienti ostili KeyCrypta include meccanismi di rilevazione di ambienti potenzialmente ostili o di analisi non autorizzata.

In caso di rilevazione:
- Alcune funzionalità possono essere limitate.
- L'operatività può essere bloccata in modo controllato, al fine di ridurre il rischio di compromissione o analisi forzata.
Le azioni intraprese dipendono dalla configurazione e dalle policy di sicurezza adottate.

8.3 Singola istanza e sicurezza di sessione Per ridurre vettori di abuso e collisioni operative, KeyCrypta applica:
- Avvio in modalità singola istanza.
- Controlli di sessione per evitare accessi concorrenti non previsti.
- Timeout automatici per ridurre l'esposizione accidentale di dati sensibili in caso di inattività.
Queste misure contribuiscono a rafforzare la sicurezza operativa nell'uso quotidiano.

8.4 Sicurezza dei file temporanei (allegati e report) KeyCrypta gestisce i file temporanei in modo controllato e restrittivo. In particolare:
- Creazione dei temporanei solo quando strettamente necessario.
- Apertura controllata dei file allegati e dei report.
- Rimozione dei temporanei al termine dell'utilizzo.
- Cancellazione sicura "best effort" dove tecnicamente applicabile, con fallback robusti in caso di file in uso.

9) INFORMATIVA PRIVACY (SINTESI PUBBLICA)
KeyCrypta non raccoglie né invia automaticamente dati personali.

Comunicazioni verso l'esterno (se abilitate dall'utente o dalla policy):
1) Attivazione/ri-attivazione licenza:
- può richiedere l'invio volontario dell'UUID del dispositivo (da parte dell'utente/IT) per vincolo

licenza.

2) Verifica "Password Violate" (opzionale):

- se attivata, utilizza il modello k-anonymity (invio del solo prefisso hash SHA-1 a 5 caratteri a HaveIBeenPwned, senza inviare la password in chiaro).

Nessun contenuto della cassaforte viene trasmesso automaticamente. Nessuna sincronizzazione cloud è richiesta per l'uso del prodotto. Nessuna telemetria e nessuna necessità di internet per funzionare.

10) RISK & COMPLIANCE STATEMENT (PUBBLICO)

10.1 Cosa protegge

- Protezione dei dati in caso di copia del file cassaforte (attacchi offline).
- Rilevazione manomissioni sui componenti critici.
- Riduzione superfici di attacco tramite isolamento offline e policy amministrative.

10.2 Cosa NON promette (limiti dichiarati)

- Nessun software può garantire protezione assoluta su hardware/firmware completamente compromessi.
- In presenza di compromissione totale del sistema operativo (malware con privilegi elevati), un attacker può impattare la sicurezza operativa (es. intercettazione input).
- La robustezza contro tentativi di forza bruta dipende anche dalla qualità/entropia della password scelta.

10.3 Allineamento a principi ISO-style (senza certificazione)

- Principi ispirati a controllo accessi, segregazione, auditabilità e gestione del rischio (approccio "ISO-style").
- Il prodotto è predisposto per valutazioni interne e audit di sicurezza, ma non dichiara certificazioni formali salvo diversamente indicato in contratti dedicati.

11) DEPLOYMENT & OPERATIONS (GUIDA PUBBLICA)

11.1 Distribuzione enterprise (pattern consigliati)

- Standalone per utente: una cassaforte per persona (o per ruolo).
- Portable secure: esecuzione da USB cifrata con policy IT.
- Workstation secured: installazione su workstation hardenizzata (EDR, least privilege, patching).

11.2 Backup & Restore (processo)

- Definire una policy di backup: frequenza, retention, controllo accessi.
- Conservare copie cifrate in repository aziendale (anche offline), con controllo versioni e integrità.
- Pianificare procedure di restore testate (disaster recovery).

11.3 Offboarding / Revoca

- Separazione per utente facilita l'offboarding.
- Se configurato, il Recupero di Emergenza Amministratore può supportare business continuity su credenziali aziendali.
- Revoca operativa: ritiro supporto, disattivazione policy e gestione licenza secondo contratto.

12) LICENZA E LIMITAZIONE DI RESPONSABILITÀ (SINTESI)

- Software concesso in licenza secondo termini EULA.
- Vietata copia/alterazione/distribuzione non autorizzata.
- Il software è fornito "così com'è", senza garanzie implicite o esplicite; l'organizzazione deve adottare le proprie policy di backup e sicurezza operativa.

13) CONTATTI

Per richieste enterprise (procurement, NDA, security questionnaire, deployment support): Email: info@keycrypta.com