



Come proteggiamo i dati

Sicurezza spiegata semplice — senza termini tecnici

La nostra garanzia

Solo il titolare, in possesso della propria CHIAVE PRIVATA, può leggere i contenuti.

La chiave viene generata dal sistema e mostrata all'utente una sola volta. Nel database viene conservato solo un'impronta digitale (hash Argon2ID) **dalla quale è impossibile risalire alla chiave originale. Nemmeno AVANET può recuperarla.**

Senza la chiave privata, i dati restano incomprensibili. **Anche per noi.**

Tre elementi distinti

Per proteggere i dati vengono utilizzati **3 elementi distinti**. Ognuno ha un ruolo diverso:

 CHIAVE PRIVATA	 PASSWORD	 CODICE OTP
A cosa serve: Criptare i dati e decriptarli per la lettura	A cosa serve: Accedere all'account	A cosa serve: Confermare l'identità (secondo controllo)
Chi la possiede: SOLO IL TITOLARE (trasmessa una sola volta su canale cifrato TLS 1.3)	Chi la possiede: Il titolare (scelta in fase di registrazione)	Chi la possiede: Inviato via Email o WhatsApp ad ogni accesso
Cosa protegge: I CONTENUTI (documenti, password, note)	Cosa protegge: L'ACCESSO all'account	Cosa protegge: L'ACCESSO (doppio controllo)

Perché è importante capire la differenza?

Anche se qualcuno dovesse scoprire la password (o compromettere l'account), **senza la CHIAVE PRIVATA non potrebbe comunque leggere i contenuti**. I dati resterebbero incomprensibili.

La CHIAVE PRIVATA (in dettaglio)

Funziona come la combinazione di una cassaforte fisica. Senza di essa, nessuno può aprire la Cassaforte Digitale.

 Cosa significa per l'utente	 Importante da sapere
• È unica e solo il titolare la possiede • Viene generata dal sistema in modo casuale • Sul server viene salvata solo l'impronta (hash Argon2ID), MAI la chiave in chiaro	• Trasmessa UNA SOLA VOLTA su canale cifrato • Va conservata in un luogo sicuro • Se viene persa, non è recuperabile • <i>(Per questo esistono i Delegati!)</i>

- Nemmeno AVANET può recuperarla

⚙ Come funziona (spiegato semplice)

1	L'utente carica un documento o inserisce una password
2	Il contenuto viene criptato con la CHIAVE PRIVATA utilizzando AES-256
3	Sul server viene salvata solo la versione criptata — incomprensibile senza chiave
4	Solo il titolare (con la propria chiave) può decriptare e leggere i contenuti

🔒 Esempio: come appare un dato protetto

Ecco cosa succede quando viene inserita un'informazione nella Cassaforte:

✗ PRIMA (dato inserito dall'utente)

Appunto personale: Codice allarme casa 4821

⬇ La cifratura AES-256 con la CHIAVE PRIVATA lo trasforma in... ⬇

✅ DOPO (dato cifrato con AES-256 e archiviato sui server)

xK9mQ7pLwR3nVbYc8fTjHs2dA5gUiOeZ0kNvBx1rMqW4yFaP...

👉 Questo è ciò che viene salvato sui server AVANET: il dato, **protetto da cifratura AES-256**, appare come una **sequenza di caratteri senza significato**.

Solo con la chiave privata del titolare è possibile tornare al dato originale.

📦 Due modalità d'uso

La Cassaforte Digitale può essere utilizzata in due modi, a seconda delle esigenze:

🔒 SOLO CASSAFORTE

Archivio personale sicuro

- Conservare password e credenziali
- Archiviare documenti riservati
- Proteggere dati sensibili
- Accesso solo con la propria chiave

Nessun Delegato, nessun "Tutto OK?"

👥 CASSAFORTE + CONTINUITÀ

Archivio sicuro + trasferimento ai Delegati

- Tutte le funzioni della cassaforte
- Designazione di Delegati di fiducia
- Sistema "Tutto OK?" attivo
- Rilascio ai Delegati in caso di indisponibilità (graduale o simultaneo)

Continuità operativa garantita

💡 È possibile iniziare con la modalità "Solo Cassaforte" e attivare i Delegati in un secondo momento.

🕒 Il sistema "Tutto OK?" e i Delegati

Periodicamente viene inviato un messaggio semplice: **"Tutto OK?"** — via WhatsApp, Email o App.

✅ Se il titolare **RISPONDE**

Un click e tutto resta protetto. La Cassaforte rimane sigillata fino al prossimo controllo.

⌚ Se il titolare **NON RISPONDE**

Dopo il periodo di grazia (72 ore), si attiva il protocollo di emergenza. I Delegati designati ricevono le informazioni in sequenza (VERDE per primo, GIALLO per secondo, ROSSO per ultimo) oppure, se configurato dal titolare, tutte insieme contemporaneamente.

La frequenza è personalizzabile: **ogni 7, 14, 30 o 60 giorni**. Modificabile in qualsiasi momento.

🏖️ Vacanze in programma? È possibile mettere in pausa le notifiche dalla dashboard.

I Delegati ricevono un **PINCODE temporaneo** (validità max 30 giorni, revocabile in qualsiasi momento) per accedere alle informazioni, secondo le priorità impostate dal titolare (in sequenza o tutte insieme):

Livello	Cosa può contenere (esempi)	Quando arriva
🟢 VERDE	Es. contatti urgenti, scadenze immediate	Per primo
🟡 GIALLO	Es. documenti importanti, polizze, contratti	Per secondo
🔴 ROSSO	Es. informazioni riservate, dati sensibili	Per ultimo

📌 I contenuti indicati sono solo esempi. Il titolare decide liberamente cosa inserire in ogni livello. È inoltre possibile configurare il rilascio di tutti i livelli contemporaneamente.

🛡️ Misure di sicurezza

🔒 Protezione dei contenuti

- I dati vengono criptati con AES-256 al momento dell'archiviazione
- Sui server esistono solo dati cifrati, incomprensibili
- Solo il titolare può decriptarli

🔒 Protezione dell'accesso (3 fattori indipendenti)

- Password (scelta dall'utente)
- + Codice OTP (via Email o WhatsApp)
- + Chiave Privata (PIN Master) per decriptare i contenuti
- Triplo controllo = 3 fattori indipendenti

🌐 Server sicuri

- Server in 4 paesi europei (IT, FR, DE, CH)
- Conformità GDPR e normativa privacy
- Backup automatici e ridondanti

🔍 Controlli periodici

- Test di sicurezza regolari
- Miglioramento continuo
- Documentazione disponibile su richiesta

🏢 Per aziende e professionisti

Su richiesta è possibile ottenere:

- **Documentazione tecnica dettagliata** sulle misure di sicurezza

- **DPA** (accordo per il trattamento dati)

? Domande?

Siamo a disposizione! Scrivere a info@lacassafortedigitale.it o chiamare il **+39 0171 050110**