LA Cassaforte DIGITALE

IL FUTURO DIGITALE, AL SICURO.

LA CASSAFORTE DIGITALE

WHITE PAPER TECNICO

Architettura di Sicurezza, Infrastruttura
e Piano di Continuità del Servizio

Versione 1.0 — Febbraio 2026
Classificazione: Pubblico
AVANET SRL — Cuneo, Italia
P.IVA 03772060046

INDICE

1. Premessa e scopo del documento

Il presente documento descrive in modo tecnico e trasparente l'architettura di sicurezza, l'infrastruttura e le garanzie di continuità de La Cassaforte Digitale, piattaforma sviluppata e gestita da AVANET SRL

Lo scopo è fornire a decisori tecnici, responsabili IT, consulenti e professionisti le informazioni necessarie per una valutazione razionale e informata dell'affidabilità del servizio. Questo non è un documento commerciale: è una disclosure tecnica.

Domanda centrale a cui questo documento risponde: «Perché dovrei affidare le mie informazioni più sensibili a questa piattaforma?»

La risposta si basa sulla struttura tecnica del sistema: la protezione dei dati è garantita dall'architettura crittografica, indipendentemente da qualsiasi scenario esterno. I dati restano protetti e inaccessibili a terzi per vincolo matematico.

2. Architettura di sicurezza

2.1 Principio fondamentale: Zero-Knowledge

La Cassaforte Digitale adotta un'architettura zero-knowledge. Questo termine tecnico indica un modello in cui il gestore del servizio non ha, in nessun momento e in nessuna circostanza, la possibilità tecnica di accedere ai contenuti degli utenti.

Non si tratta di una scelta organizzativa («noi non guardiamo i vostri dati»), ma di un'impossibilità strutturale («non possiamo guardare i vostri dati»). La differenza è sostanziale:

Modello tradizionale	Modello Zero-Knowledge (LCD)
Il fornitore cifra i dati con le proprie chiavi	L'utente cifra i dati con la propria chiave, prima dell'invio
Il fornitore può decifrare in caso di richiesta legale o violazione	Nessuno può decifrare senza la Chiave Privata dell'utente
Una violazione dei server espone i dati in chiaro	Una violazione dei server espone solo dati cifrati, inutilizzabili
La sicurezza dipende dall'affidabilità del fornitore	La sicurezza dipende dalla crittografia, non dal fornitore

2.2 Flusso crittografico

Il processo di cifratura segue questi passaggi:

Fase 1 — Registrazione e generazione della Chiave Privata

Al momento della configurazione iniziale, il sistema genera una Chiave Privata (PIN Master) univoca. Questa chiave viene mostrata all'utente una sola volta e non viene mai trasmessa né salvata in chiaro sui server. L'utente è responsabile della sua custodia.

Fase 2 — Derivazione della chiave crittografica

Dalla Chiave Privata viene derivata la chiave crittografica effettiva tramite l'algoritmo PBKDF2 (Password-Based Key Derivation Function 2) con i seguenti parametri:

Parametro	Valore
Algoritmo hash	SHA-256
Iterazioni	150.000 (centocinquantamila)
Lunghezza chiave output	256 bit (32 byte)
Salt	Composto da hash dell'email utente + salt random univoco

Le 150.000 iterazioni rendono computazionalmente impraticabile un attacco brute-force: anche con hardware dedicato, ogni tentativo richiede un tempo significativo, rendendo irrealizzabile la prova sistematica di tutte le combinazioni possibili.

Fase 3 — Cifratura dei contenuti

Ogni documento, nota, credenziale o file caricato dall'utente viene cifrato con l'algoritmo AES-256-CBC (Advanced Encryption Standard) utilizzando la chiave derivata nella Fase 2. La cifratura avviene interamente sul dispositivo dell'utente (browser), prima che qualsiasi dato venga trasmesso ai server.

Parametro	Valore
Algoritmo	AES-256-CBC
Lunghezza chiave	256 bit — standard militare e governativo
Vettore di inizializzazione (IV)	16 byte random, unico per ogni operazione di cifratura
Dove avviene la cifratura	Sul dispositivo dell'utente (client-side), mai sul server

Fase 4 — Trasmissione e archiviazione

I dati cifrati vengono trasmessi ai server tramite connessione TLS 1.3 (il protocollo più recente e sicuro per le comunicazioni internet). Sui server arrivano esclusivamente dati già cifrati: sequenze di byte prive di qualsiasi significato senza la Chiave Privata dell'utente.

Nessun operatore AVANET, nessun tecnico di sistema, nessun amministratore di database può leggere, interpretare o ricostruire i contenuti archiviati. Questo vale anche in caso di ordine giudiziario: AVANET può consegnare solo dati cifrati, tecnicamente indecifrabili senza la Chiave Privata.

2.3 Misure di protezione aggiuntive

Misura	Descrizione
Protezione brute-force	Sistema progressivo di blocco: dopo tentativi errati la Chiave Privata viene temporaneamente bloccata con tempi di attesa

	crescenti, fino al reset automatico dell'account dopo superamento della soglia massima
Audit trail completo	Ogni accesso, modifica, download e operazione viene registrata con timestamp, indirizzo IP e tipo di azione. Il registro è consultabile dall'utente in qualsiasi momento
TLS 1.3	Tutte le comunicazioni tra dispositivo e server utilizzano il protocollo di crittografia in transito più recente
Certificati SSL/TLS	Certificato valido con catena completa, configurazione moderna e cipher suite aggiornate. Record CAA configurati per prevenire emissione non autorizzata di certificati
Controllo accesso delegati	I Delegati ricevono un PINCODE dedicato con hash separato. L'accesso dei Delegati è limitato nel tempo (scadenza 30 giorni) e tracciato indipendentemente
Headers di sicurezza	Strict-Transport-Security, X-Content-Type-Options, X-Frame-Options, Content-Security-Policy implementati secondo le best practice OWASP

2.4 Tre livelli di sicurezza indipendenti

La piattaforma separa la protezione in tre elementi distinti, ciascuno con una funzione specifica. La compromissione di uno solo di essi non consente l'accesso ai contenuti:

Elemento	Funzione	Chi lo possiede	Cosa protegge
Chiave Privata (PIN Master)	Cifrare e decifrare i contenuti archiviati	Solo il titolare (scaricabile una sola volta)	I contenuti (documenti, password, note, video)
Password	Autenticarsi e accedere all'account	Il titolare (scelta in fase di registrazione)	L'accesso all'account
Codice OTP	Confermare l'identità con un secondo fattore	Generato ad ogni accesso, inviato via Email o WhatsApp	L'accesso (doppia verifica)

Implicazione pratica: anche se un attaccante dovesse ottenere la password dell'utente e intercettare il codice OTP, senza la Chiave Privata non potrebbe comunque leggere i contenuti archiviati. I dati resterebbero sequenze di byte incomprensibili. Analogamente, il possesso della sola Chiave Privata senza password e OTP non consente l'accesso all'account.

Questo modello a tre fattori separati elimina ogni singolo punto di vulnerabilità (single point of failure) nel processo di accesso.

2.5 Rappresentazione concreta della cifratura

Per illustrare concretamente cosa accade ai dati, consideriamo un esempio reale. Quando un utente inserisce un'informazione nella piattaforma:

Stato	Contenuto
Dato inserito dall'utente	Password banca: MarioRossi2024!
Dato archiviato sui server	U2FsdGVkX1+vupppZksvRf8x3EiNsR4pJB5mQ7...

La seconda riga è ciò che esiste sui server AVANET: una sequenza di caratteri priva di qualsiasi significato. Senza la Chiave Privata del titolare, è tecnicamente impossibile risalire al dato originale. Questo vale per ogni singolo elemento archiviato: documenti, note, credenziali, video messaggi.

2.6 Due modalità operative

La piattaforma può essere utilizzata in due configurazioni, a seconda delle esigenze dell'utente:

Solo Cassaforte	Cassaforte + Continuità
Archivio personale cifrato. Conservazione sicura di password, credenziali, documenti riservati e dati sensibili. Accesso esclusivo con la propria Chiave Privata.	Tutte le funzioni dell'archivio sicuro, più: designazione di Delegati di fiducia, sistema di Controllo Vitale attivo, rilascio graduale delle informazioni in caso di indisponibilità.
Nessun Delegato, nessun Controllo Vitale. Funziona come una cassaforte digitale personale.	Continuità operativa garantita: le informazioni critiche raggiungono le persone giuste al momento giusto.

È possibile iniziare con la modalità «Solo Cassaforte» e attivare i Delegati e il sistema di continuità in qualsiasi momento successivo, senza perdita di dati o riconfigurazioni.

2.7 Versatilità architetturale: l'utente decide cosa e come proteggere

La Cassaforte Digitale non impone un modello di utilizzo predefinito. La piattaforma è progettata per accogliere qualsiasi strategia di organizzazione delle informazioni critiche che il titolare ritenga più efficace per la propria realtà.

L'archivio cifrato può contenere credenziali e password di accesso, documenti riservati e contratti, video messaggi personali, istruzioni operative per collaboratori e familiari, riferimenti a professionisti di fiducia, indicazioni su dove reperire documentazione conservata altrove, o qualsiasi combinazione di questi elementi.

La protezione crittografica è identica indipendentemente dalla natura del contenuto: ogni elemento viene cifrato con AES-256 sul dispositivo dell'utente e segue le regole di rilascio graduale configurate dal titolare.

Questa versatilità non è un utilizzo secondario, ma una caratteristica progettuale. Ogni persona, ogni azienda, ogni studio professionale ha esigenze diverse e un proprio modo di organizzare le informazioni critiche. La piattaforma si adatta all'utente, non il contrario.

Il risultato è sempre lo stesso: in caso di necessità, le persone giuste ricevono le informazioni giuste, nel modo e nei tempi stabiliti dal titolare.

3. Infrastruttura server e localizzazione dei dati

3.1 Distribuzione geografica

I dati cifrati degli utenti vengono replicati su server distribuiti in quattro paesi dell'Unione Europea e dello Spazio Economico Europeo:

Paese	Ruolo	Giurisdizione	Ridondanza
Italia	Primario	GDPR + normativa IT	Copia completa
Francia	Replica	GDPR + CNIL	Copia completa
Germania	Replica	GDPR + BDSG	Copia completa
Svizzera	Replica	nLPD (equiv. GDPR)	Copia completa

3.2 Implicazioni della distribuzione

Resilienza ai guasti: la perdita completa di un datacenter non comporta perdita di dati. Il servizio può essere ripristinato da qualsiasi delle altre tre copie.

Protezione giurisdizionale: nessun singolo governo può ordinare la cancellazione o il sequestro di tutte le copie simultaneamente, poiché risiedono sotto giurisdizioni legali differenti.

Conformità territoriale: tutti i server si trovano in paesi con legislazione sulla protezione dei dati equivalente o superiore al GDPR europeo. Nessun dato transita o viene archiviato al di fuori dello Spazio Economico Europeo.

3.3 Cosa è archiviato sui server

Sui server sono presenti esclusivamente:

- **Dati cifrati** — sequenze di byte incomprensibili senza la Chiave Privata
- **Hash della Chiave Privata** — per la verifica dell'identità (non reversibile)
- **Salt crittografico** — componente pubblica necessaria alla derivazione della chiave
- **Metadati operativi** — timestamp, log di accesso, stato del Controllo Vitale

Non sono mai presenti: la Chiave Privata in chiaro, le chiavi crittografiche derivate, i contenuti in forma leggibile.

4. Gestione delle chiavi di cifratura

4.1 Ciclo di vita della Chiave Privata

Fase	Cosa accade	Dove
Generazione	Chiave univoca generata in modo casuale	Sul server, mostrata all'utente una sola volta
Custodia	L'utente salva la chiave (stampa, file, cassaforte fisica)	Esclusivamente presso l'utente
Utilizzo	Inserita ad ogni sessione per derivare la chiave AES-256	Derivazione sul client, verifica hash sul server
Perdita	Impossibilità permanente di accesso ai dati cifrati	Nessun recupero possibile (by design)
Rigenerazione	Nuova chiave generata, dati precedenti resi inaccessibili	Reset completo dell'archivio cifrato

4.2 Perché la perdita della chiave è irreversibile

La scelta di non prevedere un meccanismo di recupero della Chiave Privata è intenzionale e rappresenta il fondamento stesso della sicurezza del sistema. Se esistesse una «porta secondaria» per recuperare i dati senza la chiave dell'utente, quella stessa porta sarebbe utilizzabile da un attaccante, da un dipendente infedele o sotto coercizione legale.

L'assenza di backdoor è una garanzia, non una limitazione. È lo stesso principio adottato da sistemi come Signal, ProtonMail e altri servizi crittografici riconosciuti a livello internazionale.

4.3 Sistema di Controllo Vitale e meccanismo Delegati

Il sistema di Controllo Vitale (denominato «Tutto OK?») è il meccanismo che garantisce la continuità digitale. Periodicamente, la piattaforma invia al titolare una richiesta di conferma tramite i canali configurati (WhatsApp, Email o notifica in-app).

Funzionamento del Controllo Vitale

Parametro	Dettaglio
Frequenza configurabile	Ogni 7, 14, 30 o 60 giorni, modificabile in qualsiasi momento dalla dashboard
Canali di notifica	WhatsApp, Email, notifica in-app — configurabili dall'utente
Risposta del titolare	Un singolo click/tap per confermare. La Cassaforte resta sigillata fino al prossimo controllo

Modalità Vacanza	Sospensione temporanea delle notifiche con data di riattivazione automatica. Previene falsi allarmi durante assenze programmate
Mancata risposta	Dopo il periodo di sicurezza configurato, si attiva il protocollo di emergenza verso i Delegati

Rilascio graduale ai Delegati (tre livelli)

In caso di mancata risposta prolungata, le informazioni vengono rilasciate ai Delegati designati in modo graduale, secondo tre livelli di priorità preconfigurati dal titolare:

Livello	Contenuto tipico	Tempistica di rilascio
VERDE	Contatti urgenti, scadenze immediate, istruzioni operative prioritarie	Per primo — immediatamente dopo l'attivazione del protocollo
GIALLO	Documenti importanti, polizze, contratti, credenziali operative	Dopo 24-48 ore dal rilascio del livello Verde
ROSSO	Informazioni riservate, dati sensibili, contenuti ad accesso limitato	Per ultimo — secondo la tempistica configurata dal titolare

Questo meccanismo a rilascio progressivo garantisce che le informazioni più urgenti arrivino subito, mentre i contenuti più riservati vengano rilasciati solo dopo un periodo di ulteriore attesa, riducendo il rischio di attivazioni accidentali.

Sicurezza crittografica dei Delegati

Quando il protocollo di emergenza si attiva, i Delegati designati ricevono un PINCODE dedicato che permette l'accesso ai contenuti secondo i livelli preconfigurati. La chiave crittografica necessaria viene derivata dal PIN Master dell'utente attraverso un processo sicuro (PBKDF2 con 50.000 iterazioni e chiave AES-256-CBC dedicata) che non espone mai la Chiave Privata originale ai Delegati.

Il PINCODE dei Delegati ha una validità limitata a 30 giorni e ogni accesso viene registrato nell'audit trail con timestamp, indirizzo IP e operazioni effettuate. Al termine della validità, l'accesso viene revocato automaticamente.

Revoca immediata dei Delegati

Il titolare dell'account mantiene in ogni momento il pieno controllo sui propri Delegati. In qualsiasi circostanza — anche durante un'emergenza già attivata — il titolare può:

- **Revocare immediatamente** l'accesso di uno o più Delegati con effetto istantaneo
- **Modificare** i Delegati designati, aggiungerne di nuovi o rimuovere quelli esistenti
- **Riassegnare i livelli** di accesso (Verde, Giallo, Rosso) in base alle nuove esigenze
- **Disattivare completamente** il sistema di Controllo Vitale, tornando alla modalità «Solo Cassaforte»

Se il titolare rientra in disponibilità dopo l'attivazione del protocollo di emergenza, può revocare immediatamente tutti gli accessi concessi ai Delegati. Dal momento della revoca, i PINCODE

precedentemente emessi cessano di funzionare e i Delegati non possono più accedere ad alcun contenuto. Il titolare riprende il controllo esclusivo della propria Cassaforte Digitale.

5. Modello di minaccia e garanzie strutturali

Di seguito analizziamo i principali scenari di rischio e le protezioni strutturali in atto:

Scenario di minaccia	Rischio effettivo	Protezione
Violazione dei server (data breach)	L'attaccante ottiene solo dati cifrati AES-256, inutilizzabili senza la Chiave Privata di ciascun utente	Cifratura zero-knowledge: i dati sono protetti dalla crittografia, non dalla sicurezza perimetrale
Dipendente infedele	Nessun dipendente AVANET possiede le chiavi per decifrare i contenuti	Impossibilità tecnica di accesso, non policy organizzativa
Ordine giudiziario / sequestro	AVANET può consegnare solo blob cifrati e metadati	I contenuti restano illeggibili anche per l'autorità giudiziaria senza la Chiave Privata
Indipendenza strutturale	I dati sui server sono protetti dalla crittografia, non dall'infrastruttura aziendale. Sono inaccessibili a qualsiasi soggetto terzo	Separazione architetturale completa tra gestore del servizio e contenuti degli utenti
Intercettazione comunicazioni	Doppia protezione: i dati sono cifrati prima della trasmissione E il canale è protetto da TLS 1.3	Cifratura end-to-end + cifratura in transito
Attacco brute-force sulla Chiave	PBKDF2 a 150.000 iterazioni rende ogni tentativo computazionalmente costoso	Blocco progressivo dopo tentativi errati + reset automatico account

6. Piano di continuità del servizio (BCP)

6.1 Ridondanza e disaster recovery

La distribuzione su quattro datacenter europei garantisce che il servizio possa essere ripristinato entro tempi definiti anche in caso di disastro:

Metrica	Valore
RTO (Recovery Time Objective)	Massimo 4 ore per il ripristino completo del servizio
RPO (Recovery Point Objective)	Massimo 1 ora di dati — replica sincrona tra datacenter
Disponibilità target (SLA)	99,9% uptime annuo (massimo 8,76 ore di downtime/anno)
Backup	Backup giornalieri cifrati con retention di 90 giorni

6.2 Monitoraggio e manutenzione

L'infrastruttura è monitorata 24/7 con sistemi di alert automatici. Gli aggiornamenti di sicurezza vengono applicati entro 24 ore dalla pubblicazione per vulnerabilità critiche (CVSS 9+) e entro 7 giorni per vulnerabilità di gravità inferiore.

7. Indipendenza strutturale dei dati e continuità del servizio

7.1 AVANET SRL: 30 anni nel settore IT

AVANET SRL è un'azienda con sede a Cuneo, attiva da oltre 30 anni nel settore informatico e delle telecomunicazioni. Operando come Internet Service Provider e fornitore di servizi IT per oltre 1.000 clienti, l'azienda dispone di competenze consolidate nella gestione di infrastrutture di rete, sicurezza informatica e servizi cloud.

La Cassaforte Digitale nasce da questa esperienza trentennale e dalla conoscenza diretta delle esigenze di PMI, studi professionali e professionisti italiani in materia di organizzazione e protezione delle informazioni critiche.

7.2 Separazione architetturale: gestore e dati

Una delle proprietà più rilevanti dell'architettura zero-knowledge è la separazione strutturale tra chi gestisce l'infrastruttura e chi possiede i dati.

AVANET SRL gestisce i server, la piattaforma e l'infrastruttura tecnologica. Gli utenti possiedono le chiavi di cifratura e, di conseguenza, il controllo esclusivo sui propri contenuti. Queste due sfere sono completamente indipendenti.

Questa separazione non è organizzativa (una policy interna), ma architetturale (un vincolo del sistema). Significa che la protezione dei dati non dipende dall'azienda: dipende dalla crittografia. I contenuti sono protetti dalla matematica in qualsiasi scenario, presente e futuro.

In termini concreti: le chiavi di cifratura non esistono sui server. Non esiste un «archivio chiavi» accessibile a nessuno. Sui server sono presenti esclusivamente blob binari cifrati con AES-256, privi di qualsiasi valore informativo senza le Chiavi Private dei singoli utenti.

7.3 Impegni di continuità e trasparenza

AVANET SRL si impegna a garantire la massima continuità e qualità del servizio attraverso impegni concreti verso i propri utenti:

Impegno	Dettaglio
Esportazione dati	Gli utenti possono esportare tutti i propri dati in qualsiasi momento, in formato standard leggibile, attraverso la funzione di export dedicata

Comunicazione proattiva	Qualsiasi modifica rilevante al servizio viene comunicata con largo anticipo (minimo 180 giorni) via email, PEC e notifica in-app
Investimento continuo	Aggiornamenti di sicurezza, nuove funzionalità e miglioramenti della piattaforma vengono rilasciati costantemente, garantendo un servizio sempre allineato alle migliori pratiche del settore
Cancellazione certificata	Su richiesta dell'utente, cancellazione completa e certificata di tutti i dati da tutti i datacenter, conforme alle linee guida NIST 800-88
Documentazione aperta	Il White Paper Tecnico è pubblico e può essere sottoposto a revisione indipendente da qualsiasi esperto di sicurezza informatica

7.4 Garanzia architetturale permanente

La separazione tra gestore dell'infrastruttura e contenuti degli utenti rappresenta una garanzia superiore a qualsiasi clausola contrattuale: non si tratta di promettere che i dati non verranno letti, ma di rendere tecnicamente impossibile la loro lettura da parte di chiunque non sia il legittimo titolare.

Questa proprietà è permanente e intrinseca all'architettura del sistema. Non dipende da decisioni aziendali, da accordi commerciali o da evoluzioni organizzative. È un vincolo matematico che protegge i dati in qualsiasi scenario.

8. Garanzie contrattuali e strumenti di tutela

8.1 Diritti dell'utente

Ogni utente de La Cassaforte Digitale ha diritto a:

• **Portabilità completa:** esportazione di tutti i propri dati in qualsiasi momento, in formato standard leggibile.

• **Cancellazione immediata:** eliminazione completa e certificata di tutti i dati su richiesta, da tutti i datacenter.

• **Trasparenza:** accesso completo ai log di accesso e alle operazioni effettuate sul proprio account.

• **Comunicazione proattiva:** minimo 180 giorni di preavviso per qualsiasi modifica rilevante al servizio.

8.2 Responsabilità dell'utente

L'architettura zero-knowledge implica una responsabilità simmetrica:

• **Custodia della Chiave Privata:** la perdita della Chiave Privata comporta l'impossibilità permanente di accesso ai dati. AVANET non può recuperarli.

• **Aggiornamento Delegati:** l'utente è responsabile di mantenere aggiornati i riferimenti dei propri Delegati.

• **Risposta al Controllo Vitale:** l'utente deve rispondere alle verifiche periodiche per evitare l'attivazione del protocollo di emergenza.

9. Conformità normativa

Normativa / Standard	Stato di conformità
GDPR (Reg. UE 2016/679)	Piena conformità. Infrastruttura interamente UE/SEE. DPA (Data Processing Agreement) disponibile su richiesta per aziende e professionisti. Privacy by design e by default
D.Lgs. 196/2003 (Codice Privacy IT)	Piena conformità. Informativa privacy disponibile. Registro trattamenti aggiornato
AES-256 (FIPS 197)	Standard crittografico approvato NIST, utilizzato da governi e forze armate a livello globale
OWASP Top 10	Misure di mitigazione implementate per le principali vulnerabilità web
nLPD (Svizzera)	Conformità per il datacenter svizzero. Legislazione equivalente al GDPR

Per aziende e professionisti è inoltre possibile richiedere documentazione tecnica aggiuntiva sulle misure di sicurezza, oltre al DPA (Data Processing Agreement) per il corretto inquadramento del trattamento dati ai sensi del GDPR.

10. Conclusioni

La sicurezza de La Cassaforte Digitale non si basa su promesse, ma su vincoli matematici e architetturali:

1. I dati non possono essere letti da AVANET perché la cifratura avviene prima che i dati raggiungano i server, e le chiavi restano esclusivamente in possesso dell'utente.

2. I dati non possono essere letti da un attaccante perché l'algoritmo AES-256 non ha vulnerabilità note e il brute-force è computazionalmente impossibile.

3. I dati sono strutturalmente indipendenti dal gestore perché la separazione architetturale tra infrastruttura e contenuti è un vincolo permanente del sistema. I dati sono protetti dalla matematica in qualsiasi scenario.

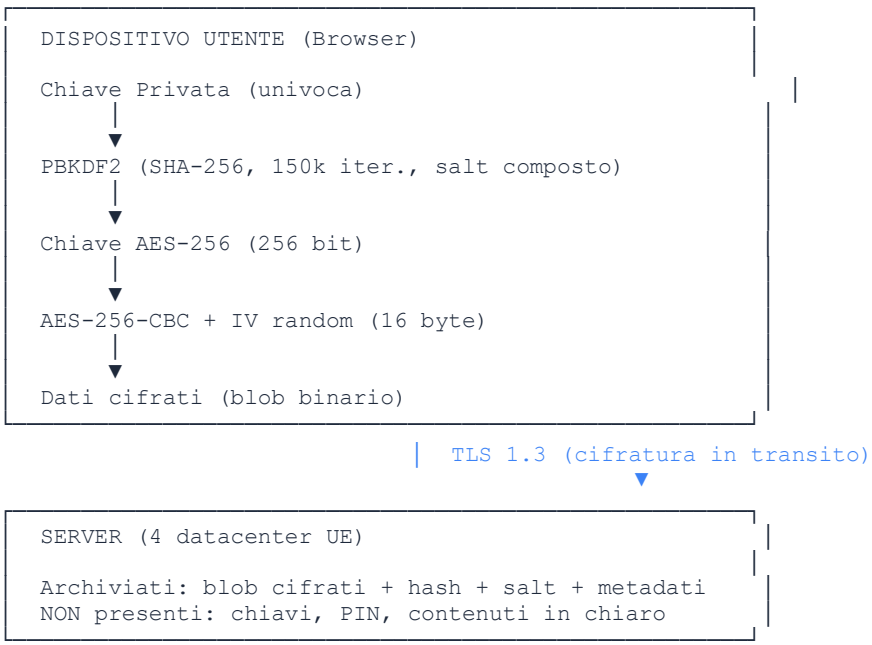
4. I dati non possono essere persi perché la replica su quattro datacenter europei garantisce la sopravvivenza anche in caso di disastro fisico.

La fiducia che chiediamo non è emotiva, ma razionale: non chiediamo di credere che proteggeremo i vostri dati. Chiediamo di verificare che, per come è progettato il sistema, non potremmo accedervi nemmeno volendo.

Questo documento è pubblico e può essere sottoposto a revisione indipendente da parte di qualsiasi esperto di sicurezza informatica.

Appendice A — Schema crittografico dettagliato

Rappresentazione testuale del flusso crittografico:



Appendice B — Glossario tecnico

Termine	Definizione
AES-256	Advanced Encryption Standard con chiave a 256 bit. Standard crittografico simmetrico adottato dal governo statunitense e considerato inviolabile con la tecnologia attuale.
Brute-force	Tentativo di violare una chiave provando sistematicamente tutte le combinazioni possibili. Impraticabile con AES-256 e PBKDF2 ad alto numero di iterazioni.
CBC	Cipher Block Chaining. Modalità operativa che utilizza un vettore di inizializzazione (IV) per garantire che dati identici producano output cifrati diversi.
Client-side encryption	Cifratura che avviene sul dispositivo dell'utente prima della trasmissione. Il server riceve solo dati già cifrati.
Controllo Vitale	Meccanismo periodico di verifica («Tutto OK?»). L'utente conferma la propria disponibilità con un click. L'assenza di risposta attiva il rilascio graduale ai Delegati.
Dead Man's Switch	Termine tecnico inglese per il Controllo Vitale: il sistema verifica periodicamente che l'utente sia attivo. L'assenza di risposta attiva il protocollo di emergenza.
Delegato	Persona di fiducia designata dal titolare per ricevere le informazioni archiviate in caso di indisponibilità prolungata del titolare stesso.
DPA	Data Processing Agreement. Accordo per il trattamento dei dati personali tra titolare e responsabile del trattamento, richiesto dal GDPR.
Escrow	Deposito presso terzi. Nel contesto software, indica il deposito del codice sorgente presso un soggetto indipendente.
GDPR	General Data Protection Regulation (Reg. UE 2016/679). Normativa europea sulla protezione dei dati personali.
OTP	One-Time Password. Codice usa e getta inviato via Email o WhatsApp ad ogni accesso come secondo fattore di autenticazione.
PBKDF2	Password-Based Key Derivation Function 2. Algoritmo che trasforma una password in una chiave crittografica attraverso iterazioni ripetute, rallentando gli attacchi.
RPO	Recovery Point Objective. Quantità massima di dati che può essere persa in caso di disastro.
RTO	Recovery Time Objective. Tempo massimo per il ripristino del servizio dopo un'interruzione.
Salt	Valore casuale aggiunto alla password prima della derivazione della chiave. Impedisce attacchi basati su tabelle precalcolate.
TLS 1.3	Transport Layer Security versione 1.3. Protocollo più recente per la cifratura delle comunicazioni internet.

2FA	Two-Factor Authentication. Autenticazione a due fattori: richiede sia la password sia un codice OTP per accedere all'account.
Zero-Knowledge	Architettura in cui il fornitore del servizio non ha la possibilità tecnica di accedere ai contenuti degli utenti.

AVANET SRL — Via Luigi Einaudi, 23 — 12100 Cuneo (CN) — Italia
P.IVA 03772060046 — REA CN-311788
info@lacassafortedigitale.it — www.lacassafortedigitale.it