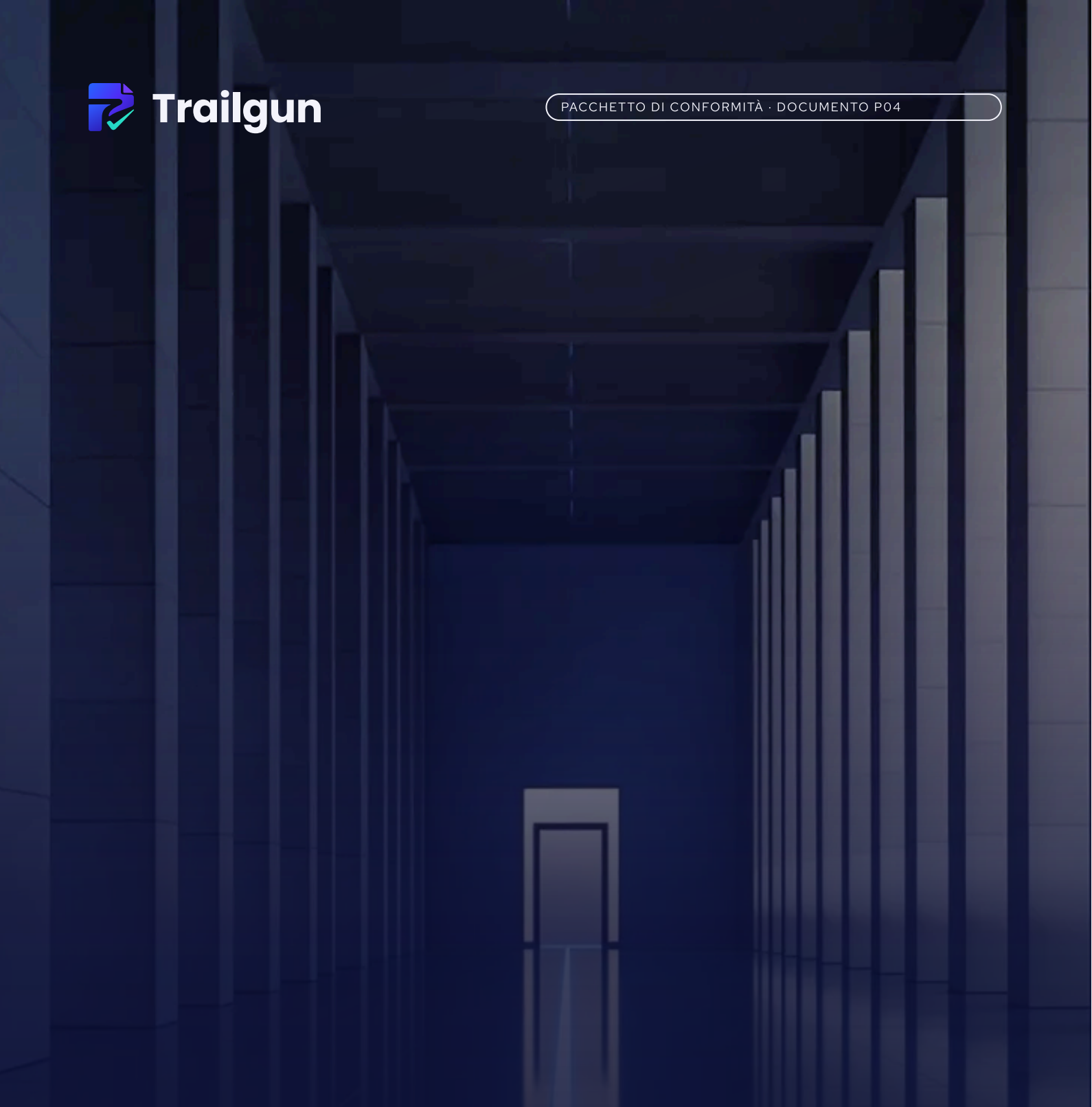
Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO P04



VERSIONE 2.0 · DICEMBRE 2026

Politica di crittografia e gestione delle chiavi

Che cosa si cifra, con quali algoritmi, chi custodisce le chiavi, come si ruotano chiavi e segreti e come si consegnano i dati cifrati ai Clienti.

CODICE	TITOLARE	REVISIONE	STATO
P04 · POL-04	Responsabile della sicurezza	Annuale	al 01/12/2026

POLITICA P04 · POL-04

Politica di crittografia e gestione delle chiavi

Che cosa si cifra, con quali algoritmi, chi custodisce le chiavi e come si ruotano.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P04 (POL-04)	Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale e a ogni cambio di algoritmo o servizio	personale tecnico; uffici ICT risk e CISO dei Clienti	Riservato · per il Cliente

DOCUMENTI COLLEGATI
P03, P09, P11; procedura 23 (Gestione delle chiavi e dei segreti); procedura 28 (Restituzione e cancellazione a fine contratto)

AMBITO
Dati a riposo e in transito della piattaforma, copie di sicurezza, segreti, chiavi API, firme dei webhook, esportazioni verso i Clienti.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
8.24, 5.17, 8.20, 8.21	DORA art. 9(4)(d); Reg. del. (UE) 2024/1774 art. 6; GDPR art. 32(1)(a)

1 Scopo e ruoli

La cifratura protegge i dati dei Clienti quando un altro controllo cede: un supporto smarrito, una copia trasferita, una connessione intercettata. Il Responsabile della sicurezza sceglie algoritmi e servizi, custodisce le chiavi e i segreti e ne tiene l'inventario (procedura 23); le chiavi KMS sono gestite dal servizio AWS Key Management Service e non escono mai in chiaro.

2 Dati a riposo

2.1 Il disco dati e il disco di sistema di ogni istanza sono volumi EBS cifrati con AES-256 tramite AWS KMS. Gli snapshot e le loro copie in Irlanda sono cifrati.

2.2 Il bucket temporaneo per Textract e Transcribe usa la cifratura lato server (SSE-S3), blocca l'accesso pubblico, accetta solo connessioni TLS e cancella gli oggetti entro 1 giorno; l'app li cancella a fine analisi.

2.3 I segreti sono SecureString in SSM Parameter Store, cifrati con KMS; sul server il file di configurazione è leggibile solo dal servizio.

2.4 La protezione a riposo è quella del volume e delle copie: database e file non hanno una seconda cifratura applicativa. Per questo chi può accedere al sistema in esecuzione è regolato dalla politica P03 (credenziali temporanee, sessioni registrate, registro degli accessi del personale).

2.5 Le chiavi KMS sono gestite da AWS, con rotazione annuale automatica. Le chiavi gestite da Trailgun (KMS CMK) per volumi, database e file fanno parte della nuova piattaforma (Percorso, tappa R12).

3 Dati in transito

3.1 Tutto il traffico pubblico passa da HTTPS con TLS 1.2 o superiore (1.3 preferito), HTTP/3, reindirizzamento da HTTP a HTTPS, HSTS di un anno e intestazioni di sicurezza (CSP, X-Content-Type-Options, Referrer-Policy, frame-ancestors). I certificati sono di Let's Encrypt e si rinnovano automaticamente; la loro scadenza è sotto allarme.

3.2 Le chiamate ai fornitori (AWS, posta, firma, banche dati) usano sempre HTTPS; le richieste ai modelli su Amazon Bedrock sono firmate con SigV4 dal ruolo dell'istanza, senza chiavi su disco.

3.3 I webhook in uscita verso i sistemi degli studi sono firmati HMAC-SHA256 con timestamp (`Trailgun-Signature`); quelli in entrata si verificano con Svix (tolleranza 5 minuti) o con un segreto condiviso, e senza segreto la rotta risponde 503.

3.4 Ogni consegna di dati a un Cliente fuori dall'app, compresa l'esportazione complessiva a fine contratto, avviene in un archivio cifrato tramite un link temporaneo; l'indice dei file porta le impronte SHA-256 (procedura 28; esportazione in autonomia: Percorso, tappa R02).

4 Algoritmi

4.1 **Ammessi:** AES-256 per la cifratura simmetrica; TLS 1.2 e 1.3 con suite AEAD; SHA-256 o superiore per impronte e hash; HMAC-SHA256 per le firme; SRP per l'autenticazione degli utenti; SigV4 per le richieste ai servizi AWS.

4.2 **Vietati** per scopi di sicurezza: MD5, SHA-1, TLS inferiore a 1.2, algoritmi o implementazioni crittografiche scritti in proprio. Le librerie crittografiche sono quelle della piattaforma (Node.js, AWS).

4.3 Le chiavi API degli studi si conservano solo come hash SHA-256; le password non si conservano mai presso Trailgun; i file del pacchetto di deposito portano l'impronta SHA-256.

5 Chiavi e segreti

ELEMENTO	ROTAZIONE	CUSTODE
Chiavi KMS	annuale automatica	AWS KMS
Segreti dei fornitori	ogni 12 mesi e subito dopo un sospetto di compromissione o l'uscita di una persona con accesso; data annotata nell'inventario	Responsabile della sicurezza (SSM)
Certificati TLS	automatica (Let's Encrypt, 90 giorni), scadenza sotto allarme	Caddy
Chiavi API degli studi	a cura dello studio, consigliata ogni 12 mesi; revoca immediata	lo studio (Trailgun conserva solo l'hash)
Credenziali del personale	temporanee, a ogni sessione (IAM Identity Center)	la persona

5.1 Un segreto non si trasmette mai per email o chat in chiaro, non si scrive nei log e non entra nel repository: la scansione dei segreti (gitleaks) controlla tutta la storia del repository a ogni verifica della CI.

5.2 Un segreto esposto si revoca e si ruota subito, si toglie dalla storia del repository e l'evento si tratta come incidente (procedura 23 e procedura 25).

6 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Cifratura dei volumi e delle copie	IN ESSERE volumi e snapshot cifrati in Germania e in Irlanda	infrastruttura come codice; inventario 42
TLS, HSTS e intestazioni	IN ESSERE configurazione del proxy	verificabile dall'esterno su app.trailgun.ai
Inventario e rotazione dei segreti	IN ESSERE data di creazione e ultima rotazione di ogni segreto	procedura 23; riesame annuale
Scansione dei segreti	IN ESSERE job «secrets» della verifica della CI	a ogni pull request e prima di ogni rilascio

7 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8; nessuna eccezione ammette un algoritmo vietato. Riferimenti: DORA art. 9, par. 4, lett. d); Reg. del. (UE) 2024/1774 art. 6; GDPR art. 32, par. 1, lett. a); ISO/IEC 27001:2022 controlli 8.24, 5.17, 8.20 e 8.21.