Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO 23

VERSIONE 2.0 · DICEMBRE 2026

Procedura di gestione delle chiavi e dei segreti

L'inventario delle chiavi e dei segreti della piattaforma, dove stanno, chi li usa e quando si ruotano; come si creano, si conservano e si revocano; la scansione dei segreti su tutta la storia del codice e che cosa si fa se uno è esposto.

SEGRETI DELL'APP
SSM Parameter Store, cifrati KMS

ROTAZIONE
ogni 12 mesi e all'uscita

CIFRATURA A RIPOSO
AES-256, chiavi KMS

SCANSIONE
gitleaks a ogni verifica

PROCEDURA 23 · PROC-23

Gestione delle chiavi e dei segreti

Dove serve un segreto, ce n'è uno solo per ambiente, conservato cifrato, noto all'inventario per nome e mai per valore, ruotato con una data.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
PROC-23	Responsabile della sicurezza (Franco Puppo, CEO)	Organo amministrativo, [data della delibera]	2.0 · stato al 01/12/2026

REVISIONE	DESTINATARI
annuale e dopo ogni segreto esposto	chi sviluppa e amministra la piattaforma; CISO e ICT risk dei Clienti

DOCUMENTI COLLEGATI

politica P04; documento 20, Gestione dei cambiamenti; documento 21, Ingresso e uscita del personale; documento 22, Revisione degli accessi; documento 25, Risposta agli incidenti; documento 42, Inventario degli asset; documento 05, Sicurezza delle informazioni

1 Scopo e ambito

1.1 La procedura copre ogni informazione che, in mano a un terzo, gli darebbe accesso a un sistema o a dati: chiavi di cifratura, chiavi API, segreti dei webhook, credenziali di servizio, certificati, credenziali delle persone che amministrano la piattaforma.

1.2 Principio: dove si può, nessun segreto. L'app accede ai servizi AWS (Amazon Bedrock per i modelli, Textract, Transcribe, la posta di Cognito) con il ruolo dell'istanza e credenziali temporanee, firmate e ruotate da AWS; l'integrazione continua accede ad AWS con OIDC; le persone con IAM Identity Center. Le password degli utenti Trailgun non le conserva: il login usa Amazon Cognito con il protocollo SRP e l'app di autenticazione.

2 Inventario

L'inventario dei segreti si tiene con l'inventario degli asset (documento 42): nome, sistema, ambiente, titolare, scopo, data di creazione e dell'ultima rotazione. Mai il valore.

CHE COSA	DOVE STA, COME È PROTETTO	CHI LO USA	ROTAZIONE
Segreti dell'app: chiavi dei fornitori (posta, firma e visure, banca dati, notifiche, pagamenti), segreti dei webhook in entrata	SSM Parameter Store, un parametro per ambiente, SecureString cifrato con KMS; sul server un file leggibile solo dal processo; in production non entrano mai valori finti	l'app del proprio ambiente	ogni 12 mesi; subito al sospetto di compromissione o all'uscita di una persona con accesso
Accesso ai servizi AWS dall'app	nessuna chiave: ruolo dell'istanza con privilegi limitati, credenziali temporanee	l'app	automatica, da AWS
Credenziali amministrative AWS	IAM Identity Center, credenziali temporanee con MFA; nessuna chiave statica; utente root con MFA, non usato	personale autorizzato	a ogni sessione
Integrazione continua	OIDC di GitHub verso un ruolo per ambiente, concesso solo al branch omonimo; nessuna chiave AWS in GitHub	GitHub Actions	a ogni esecuzione
Chiavi di cifratura dei dischi, delle copie in entrambe le regioni, dei segreti	AWS KMS, AES-256	servizi AWS	annuale, automatica
Certificati TLS	Let's Encrypt, emessi e rinnovati da Caddy; chiave privata sul disco dati cifrato	proxy HTTPS	automatica, validità 90 giorni
Chiavi API degli studi	mostrate una volta alla creazione; Trailgun conserva solo l'impronta SHA-256 e il prefisso visibile	sistemi dello studio	a cura dello studio, consigliata ogni 12 mesi; revoca immediata dall'Organizzazione
Firma dei webhook in uscita (API dello studio)	HMAC-SHA256 con timestamp; un segreto per chiave API, generato da Trailgun, mostrato una volta allo studio e conservato nel database sul disco cifrato	app e sistemi dello studio	a cura dello studio: un webhook nuovo ha un segreto nuovo; con la chiave revocata il webhook si ferma
Account di Trailgun presso i fornitori (console, banca dati giuridica)	archivio cifrato delle credenziali [strumento], accesso personale con MFA	personale autorizzato	ogni 12 mesi e all'uscita di una persona con accesso

CHE COSA	DOVE STA, COME È PROTETTO	CHI LO USA	ROTAZIONE
Fattori di autenticazione degli utenti	segreti TOTP custoditi da Cognito; mai visibili a Trailgun	utenti	a cura dell'utente; ripristino solo con verifica dell'identità

3 Ciclo di vita

1. **Creazione.** Un segreto si crea solo per uno scopo e un ambiente, con l'ambito minimo che il fornitore consente, generato dal fornitore o da un generatore casuale robusto. Ogni ambiente ha i suoi segreti: un segreto di production non si usa mai in development o staging, che lavorano con servizi esterni finti.
2. **Conservazione.** Il segreto va subito nel Parameter Store dell'ambiente, attraverso lo script di rilascio. Non sta mai nel repository, nell'immagine del container, nel modello dell'infrastruttura, nei log, in email, chat o ticket. La copia di lavoro sulla postazione amministrativa è fuori dal repository (esclusa da git) e su disco cifrato.
3. **Uso.** L'app legge i segreti all'avvio; un segreto cambiato entra in vigore con il riavvio. I log applicativi non riportano mai segreti né token, e i log di accesso HTTP non registrano il corpo delle richieste né i token.
4. **Rotazione.** Ordine fisso: si crea il segreto nuovo; si aggiorna il Parameter Store; si riavvia l'app; si verifica che il servizio del fornitore risponda; solo allora si revoca il vecchio presso il fornitore. La data entra nell'inventario. Il calendario delle rotazioni annuali sta nell'inventario e si controlla alla revisione trimestrale degli accessi (documento 22).
5. **Revoca.** Un segreto che non serve più si revoca presso il fornitore e si toglie dal Parameter Store nello stesso cambiamento; all'uscita di una persona si ruotano tutti i segreti a cui aveva accesso (documento 21).

4 Scansione dei segreti

4.1 Ogni verifica dell'integrazione continua (ogni pull request verso un branch di ambiente e ogni rilascio) esegue gitleaks su **tutta la storia** del repository, non solo sulle modifiche, con la versione dello strumento fissata e controllata con la sua impronta SHA-256. Se trova un segreto, la verifica fallisce e nulla arriva su una macchina.

4.2 Chi sviluppa esegue la stessa scansione in locale sull'albero di lavoro prima di un commit.

4.3 Le eccezioni stanno nel file di configurazione dello strumento, solo per falsi positivi dimostrati e ciascuna con il motivo scritto (per esempio le chiavi del registro dei prompt, che sono identificativi e non credenziali). Un segreto vero non va mai in eccezione: si ruota e si toglie dalla storia.

5 Se un segreto è esposto

1. **Revocare subito** il segreto presso chi lo ha emesso (fornitore, AWS, GitHub), anche prima di sapere se è stato usato; per una chiave API di uno studio, revoca dall'Organizzazione o dal backoffice e avviso all'amministratore dello studio.
2. **Sostituire** con un segreto nuovo seguendo il passo 4 del paragrafo 3, con un rilascio urgente se serve (documento 20).
3. **Capire se è stato usato**: CloudTrail, registri di accesso del fornitore, log di accesso HTTP e applicativi, registro delle attività degli studi, per tutto il periodo dall'esposizione.
4. **Registrare l'evento** come incidente (documento 25) e valutare la violazione dei dati personali (documento 26). Se il segreto è stato usato contro dati dei Clienti, i tempi di notifica partono da quando lo si sa.
5. **Togliere il segreto dalla storia** del repository, se vi era finito, e rieseguire la scansione completa.
6. **Correggere la causa** (regola della scansione, passo di lavoro, permessi) e annotare il tutto nel registro degli incidenti e nell'inventario.

6 Cifratura

A riposo: AES-256 sui dischi e sulle copie di sicurezza in Germania e in Irlanda (EBS con AWS KMS) e sull'archivio temporaneo del riconoscimento del testo (S3, cifratura lato server). In transito: TLS 1.2 o superiore, 1.3 preferito, con HSTS di un anno; verso i fornitori sempre HTTPS. Le chiavi gestite da Trailgun in KMS (CMK) arrivano con la nuova piattaforma (Percorso, tappa R12, documento 12).

7 Evidenze e riferimenti

7.1 Evidenze: inventario dei segreti con le date di rotazione; esiti della scansione gitleaks di ogni verifica; configurazione di rotazione delle chiavi KMS; CloudTrail per gli accessi ai parametri e alle chiavi; registro degli incidenti per ogni segreto esposto; verbali di uscita (documento 21).

7.2 Riferimenti: DORA, art. 9, par. 4, lett. d); Reg. del. (UE) 2024/1774, art. 6 (cifratura e controlli crittografici); GDPR, art. 32, par. 1, lett. a); ISO/IEC 27001:2022, controlli 5.17 (informazioni di autenticazione), 8.24 (uso della crittografia) e 8.4 (accesso al codice sorgente).

Trailgun

On target.

In a flash.

Dai documenti al lavoro finito: agenti AI per pratiche legali e finanziarie.

SICUREZZA E INCIDENTI, 24/7
security@trailgun.ai

REPERIBILITÀ PRIORITÀ 1
[+39 ...]

PRIVACY E DPO
privacy@trailgun.ai

Procedura 23 del pacchetto di conformità Trailgun, versione 2.0, stato al 01/12/2026. Attua la politica P04 (crittografia e gestione delle chiavi). Documento riservato, destinato al Cliente e alle sue autorità di vigilanza.