Attestazione e confidential computing

Condizioni e informazioni del servizio. Per il cliente fanno fede il contratto, l’ordine e gli allegati sottoscritti.

1. Scheda tecnica del servizio

LoricAI protegge documenti, chiavi ed elaborazione nel perimetro di confidential computing. Questa scheda, versione 2026-11-12, descrive piattaforme, percorso dei dati e procedura di verifica. Le evidenze firmate della configurazione assegnata permettono al referente IT di verificare l’ambiente: la scheda descrittiva non sostituisce le evidenze.

2. Piattaforme hardware

L’infrastruttura LoricAI offre enclave hardware su NVIDIA RTX PRO 6000 Blackwell Server Edition e NVIDIA B200. CPU AMD e GPU NVIDIA partecipano alla verifica dell’ambiente protetto. Il profilo assegnato identifica piattaforma, modalità di protezione e configurazione del cliente. La configurazione del servizio identifica CPU, GPU, firmware, driver e modalità di confidential computing. La sola sigla commerciale della GPU non dimostra che la modalità protetta sia attiva: si controllano le evidenze CPU e di ogni GPU assegnata.

3. Modello e località

Il modello AI è Qwen 3.8 Flash Next.
Qwen è un modello aperto, sviluppato da Alibaba.
Lo facciamo funzionare solo sui nostri server protetti.
Alibaba non riceve nulla: né documenti, né domande. I documenti sono elaborati in Finlandia, nell’Unione Europea, sui server di Verda.
Le chiavi sono gestite a parte, con Google Cloud KMS. Cloudflare - rete; archivio R2 cifrato nell’Unione Europea.
Backblaze - copie di sicurezza cifrate B2 nell’Unione Europea. La scheda di configurazione del cliente associa modello/versione AI, software autorizzato e identità del servizio al profilo di esecuzione.

4. Documento cifrato, elaborazione protetta

La cifratura sul dispositivo protegge il trasferimento e l’archivio. Per elaborare una richiesta, i dati vengono decifrati soltanto all’interno dell’enclave autorizzata, dove opera il modello AI. La risposta torna al tuo spazio attraverso un canale protetto. La memoria e i canali del perimetro protetto sono parte della configurazione verificata. Il contenuto non viene inviato ad API AI esterne né usato per addestramento. Ogni cliente ha una chiave dedicata, gestita separatamente dai documenti tramite il servizio di gestione delle chiavi. Il servizio di gestione delle chiavi non riceve i documenti. La policy di rilascio autorizza l’ambiente protetto dopo i controlli di integrità; credenziali, ruoli e tracciamento degli accessi governano le operazioni sulla chiave.

5. Passo 1: identificare il profilo

Acquisire l’identificativo del servizio, CPU, GPU assegnate, versione del modello, software approvato, valori di riferimento e policy di rilascio delle chiavi. Verificare che il profilo corrisponda allo spazio del cliente.

6. Passo 2: raccogliere le evidenze

Acquisire attestazioni CPU e GPU, catene di certificati e una prova fresca collegata alla sessione. Una prova vecchia o relativa a un altro ambiente non descrive la sessione attuale. Prima di inviare un documento, la tua app chiede al chip una prova firmata da AMD e NVIDIA.
La prova dice che l'area blindata è chiusa e che dentro gira solo il programma che abbiamo pubblicato.
Se la prova non torna, il documento non parte nemmeno.

7. Passo 3: verificare firma e configurazione

Utilizzare i verificatori ufficiali AMD e NVIDIA compatibili con il profilo. Controllare firme, validità e revoca dei certificati; confrontare misure, firmware, modalità protetta e identità del software con i valori autorizzati. Ripetere per ogni GPU. L’attestazione GPU non sostituisce quella CPU e viceversa.

8. Passo 4: controllare la policy delle chiavi

Verificare che evidenze non valide, scadute o difformi impediscano il rilascio della chiave. Eseguire la verifica sul percorso concordato con dati dimostrativi, senza inviare documenti di produzione. Conservare esito, orario, configurazione e versioni dei verificatori nel registro del cliente.

9. Protezioni e continuità

L’attestazione verifica ambiente e policy, non qualità delle risposte, autorizzazioni applicative o disponibilità. Teniamo copie di sicurezza cifrate per 5 anni.
Sono protette dalla tua chiave: senza, nessuno le può leggere. Richieste di autorità e trasferimenti sono disciplinati separatamente dalla località di elaborazione e dalla prova hardware.

10. Riferimenti operativi

Guida LoricAI: https://loricai.io/verifica-tecnica/
AMD SEV: https://www.amd.com/en/developer/sev.html
NVIDIA Attestation: https://docs.nvidia.com/attestation/
Piattaforme NVIDIA: https://docs.nvidia.com/confidential-computing/containers/v1.1.0/supported-platforms
Contatto tecnico: support@loricai.io.