Archivio per chiavi ad alta scalabilità

Gestione simultanea di milioni di chiavi ad alte prestazioni

IN EVIDENZA

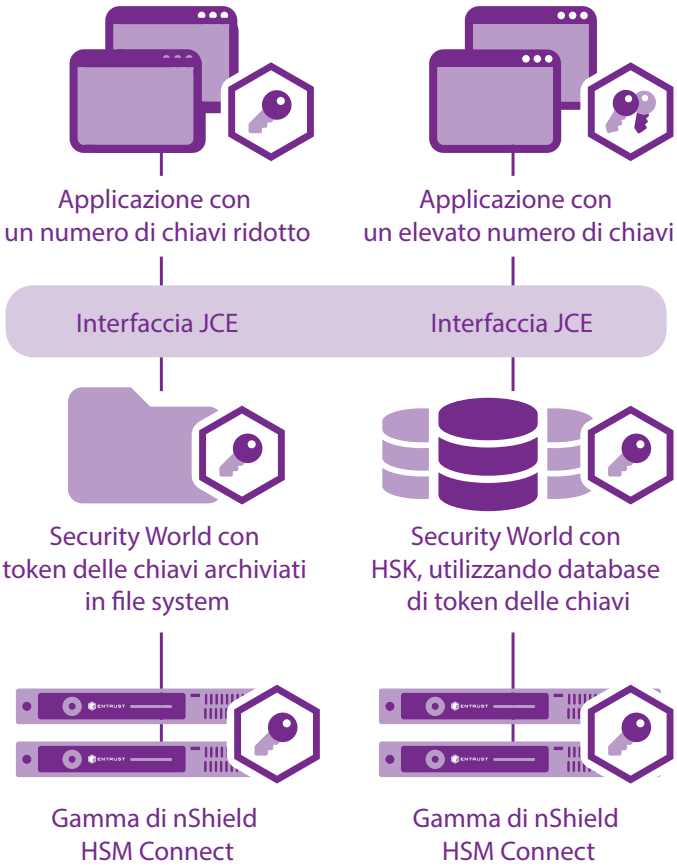
- Una soluzione ad alte prestazioni e a elevata scalabilità per specifici casi d'uso con HSM nShield® di Entrust
- Supporta un elevato numero di chiavi crittografiche attive simultaneamente
- Evita colli di bottiglia a livello dei sistemi operativi

Alcuni casi d'uso di HSM (Hardware Security Module) necessitano di un utilizzo simultaneo di un elevato numero di chiavi crittografiche, rischiando colli di bottiglia nei file system dei computer connessi agli HSM. Gli archivi per chiavi ad alta scalabilità (HSK, dall'inglese High-scalability keystore) supportano un elevato numero di chiavi ad alte prestazioni.

Caratteristiche principali

La soluzione HSK vanta le seguenti caratteristiche:

- Scalabile fino a milioni di chiavi RSA
- Prestazioni invariate con l'aumento delle chiavi
- Supporta la generazione delle chiavi RSA e del CSR, la creazione e la verifica di firme digitali, la cifratura e la decifratura dei dati.
- Sincronizzazione automatica tra più computer in chiamata
- Soluzione scalabile e personalizzabile per qualunque esigenza aziendale



SCOPRI DI PIÙ SU ENTRUST.COM/HSM

HSM nShield Edge

Come funziona

Gli HSM nShield di Entrust garantiscono tassi di transazioni ad alte prestazioni elevati, fino a qualche migliaia al secondo. (Le prestazioni dipendono dal modello dell'HSM e dall'operazione di crittografia specifica. Per un approfondimento sulle prestazione degli HSM, consultare le schede tecniche dei modelli nShield.)

L'architettura di Entrust Security World, flessibile e sicura, archivia chiavi crittografiche esternamente all'HSM come token. Le chiavi all'interno dei "token" sono protette efficacemente dalle chiavi master dell'HSM tramite crittografia, vincoli di utilizzo, controllo degli accessi e autenticazione, sommando la sicurezza con i vantaggi rappresentati da scalabilità, bilanciamento del carico, failover, espansione o contrazione semplificata del numero di HSM, scambio delle appliance e backup facilitato di token delle chiavi senza dover utilizzare dispositivi aggiuntivi.

L'architettura standard Security World archivia questi "token" nei file system dei computer in chiamata (con supporto per la sincronizzazione) utilizzando un unico file per ciascun token. Questo approccio è adatto per la maggior parte dei casi d'uso che tipicamente hanno un numero limitato di chiavi attive in ciascun computer.

In alcuni casi d'uso, la prestazione degli HSM nShield può essere limitata dalla latenza nel file system del sistema operativo del computer in chiamata. L'HSK offre alte prestazioni quando viene utilizzato un elevato numero di chiavi grazie all'introduzione di un database per archiviare i token delle chiavi nel computer del cliente.

Il team di servizi professionali Entrust saranno lieti di valutare l'adeguatezza dell'HSK per le necessità aziendali, fornendo anche assistenza nella sua integrazione nell'ambiente, inclusa la personalizzazione in base alle specifiche esigenze.

Casi d'uso esemplificativi

- Sicurezza delle e-mail aziendali per un ampio numero di utenti
- Firma dei documenti aziendali
- IoT (Internet of Things) con molti dispositivi connessi
- Applicazioni mobili con un elevato numero di utenti finali
- Sistemi di portafoglio elettronico per scambiare criptovalute

Dettagli tecnici

- Libreria JCE (Java Cryptography Extension) utilizzando gli HSM nShield
- Web Services Option PACK con moduli JSON RESTful
- Archivia "token" delle chiavi di HSM nShield in un database, invece di utilizzare un file system
- Opera con software popolari di database relazionali tra cui MSSQL, Oracle e Derby (con l'aggiunta di database aggiuntivi)
- Opera con un unico HSM o più HSM in una gamma con carichi bilanciati

Scopri di più su

Per ulteriori informazioni sugli HSM nShield di Entrust, visita il sito **entrust.com/HSM**. Per saperne di più sulle soluzioni di sicurezza digitale di Entrust per identità, accesso, comunicazioni e data, visita il sito **entrust.com**

Scopri di più su
entrust.com/HSM

Per contattarci:
HSMinfo@entrust.com