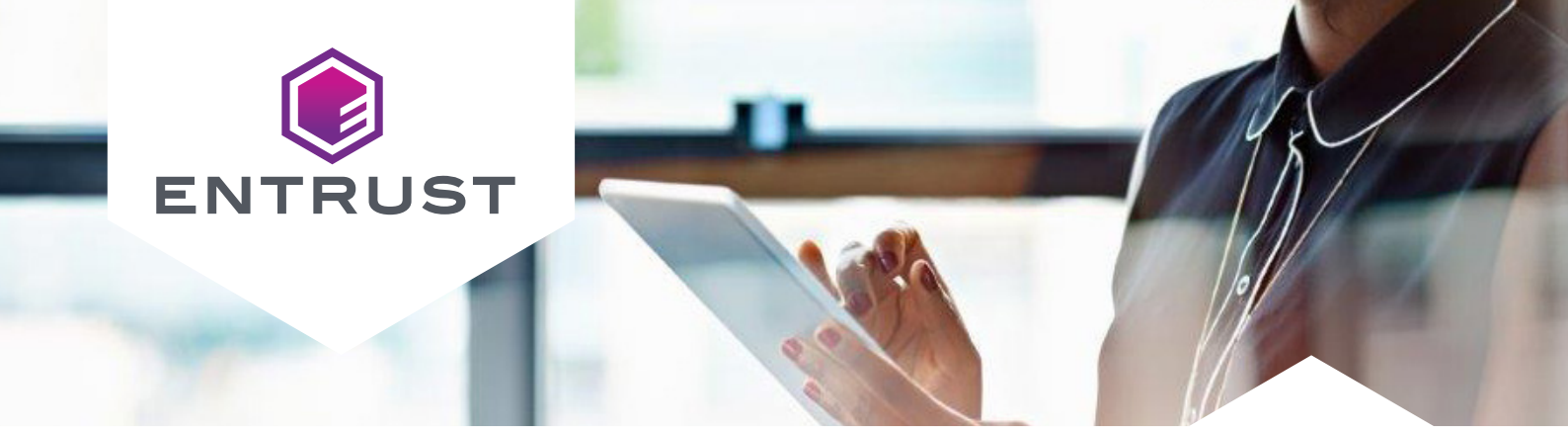

nShield Database Security Option Pack

Integrazione ottimizzata dei database SQL Server di Microsoft con hardware security module nShield a elevata affidabilità

IN EVIDENZA

Root of trust affidabile per implementazioni di database Microsoft SQL Server

- Protegge le chiavi di crittografia dei database negli hardware security module (HSM) certificati secondo le best practice FIPS e Common Criteria
- Garantisce sia la crittografia a livello di cella che la crittografia dati trasparente (TDE)
- Protegge i dati critici di un'organizzazione da possibili violazioni

Per la maggior parte delle organizzazioni, i database costituiscono un significativo archivio di informazioni sensibili. I database aziendali possono contenere dati delle carte di credito dei consumatori, informazioni concorrenziali riservate e proprietà intellettuale. La perdita o lo smarrimento dei dati mette severamente a repentaglio la reputazione delle organizzazioni e può danneggiare il marchio oltre che portare a sanzioni severe. Proteggendo i dati critici dalle minacce interne ed esterne, le organizzazioni limitano i rischi di violazione dei dati e si allineano ai mandati normativi e legislativi, incluso il Payment Card Industry Data Security Standard (PCI DSS). A questo proposito, la sezione 3.6 dell'ultimo standard PCI DSS (v3.2.1) specifica che "le chiavi di crittografia devono essere memorizzate... all'interno di un dispositivo crittografico protetto come un HSM". Inoltre, la sezione 3.6 definisce la migliore pratica in materia di gestione delle chiavi come una funzione di un HSM, ovvero il doppio controllo.

Metti al sicuro il tuo database con il più elevato livello di protezione

Crittografare i dati nel database ti permette di proteggere i dati, ma è necessario salvaguardare anche le chiavi di crittografia che permettono di accedere ai dati. L'utilizzo degli hardware security module (HSM) mette al sicuro le chiavi di crittografia memorizzandole separatamente dai dati su una piattaforma affidabile e protetta. Gli HSM nShield applicano le tue policy di sicurezza interna mediante la richiesta di autorizzazioni basate sui ruoli e la distinzione tra sicurezza e amministrazione dei database, agevolando il processo di dimostrazione della conformità ai revisori.

È disponibile sotto forma di una scheda PCIe dedicata per un unico server o un'appliance di rete condivisa per ambienti virtualizzati.

nShield Database Security Option Pack (per Microsoft SQL Server), conosciuto anche come il provider di SQLEKM, è l'API Extensible Key Management (EKM) fornita per il server SQL Server di Microsoft.

nShield Database Security Option Pack

Microsoft SQL Server è disponibile con due funzionalità di crittografia integrate per proteggere i tuoi dati: TDE e crittografia a livello di cella. Queste funzioni ti permettono di mettere in sicurezza l'intero database o proteggere esclusivamente i campi sensibili del database, e possono essere attivate senza alterare le applicazioni, le strutture del database e i processi in essere.

Proteggi il tuo marchio e i tuoi dati

Convalidati conformemente ai più elevati standard di sicurezza, come FIPS e Common Criteria, gli HSM Entrust nShield sono pronti a proteggere i tuoi dati anche nelle situazioni di sicurezza più impegnative ed esigenti. Il controllo granulare degli accessi degli HSM nShield ti permettono di gestire le chiavi di crittografia per Microsoft SQL Server. Per consentire l'applicazione delle tue policy, le funzionalità di sicurezza sono separate dalle funzioni amministrative.

Gli HSM Entrust nShield forniscono:

- **Protezione delle chiavi hardware**: memorizzano le chiavi di crittografia del database in un ambiente protetto a prova di manomissione per impedire la copia o l'alterazione
- **Applicazione di utenti e ruoli**: consentono un controllo più rigoroso per l'accesso ai dati crittografati in Microsoft SQL Server
- **Rigido controllo delle chiavi**: utilizzano l'autenticazione delle smart card degli amministratori per il controllo affidabile di chiavi di crittografia del database
- **Separazione dei ruoli**: suddividono tra più amministratori le responsabilità legate ad importanti attività e procedure
- **Configurazione e integrazione semplificate**: gli HSM Entrust nShield si integrano senza problemi con Microsoft SQL Server per fornire:
  - crittografia TDE e a livello di cella con protezione chiavi

Oltre a offrire la scalabilità necessaria per soddisfare le mutevoli esigenze, gli HSM nShield sono progettati per integrarsi sin da subito con altre applicazioni enterprise leader nel settore, tra cui server web e applicativi e infrastrutture a chiave pubblica (PKI).

Gli HSM di rete nShield Connect possono essere condivisi da diversi server ed offrono:

- **Supporto per ambienti virtualizzati**: archiviazione delle chiavi basata su hardware per server virtualizzati, compresi Hyper-V e VMware
- **Supporto del cluster di failover** incluso il gruppo di disponibilità AlwaysOn
- **Amministrazione semplificata**: gestione delle chiavi di crittografia per molti database e delle chiavi utilizzate da altre applicazioni
- **Capacità di failover**: nei casi in cui l'elevata disponibilità sia essenziale, gli utenti hanno la possibilità di utilizzare un altro HSM quando un HSM non è più disponibile
- **Disaster recovery**: processi semplici e sicuri per l'archiviazione ed il ripristino delle chiavi
- **Risorse a costi contenuti**: l'utilizzo condiviso del modulo tra più server riduce i costi legati ad hardware, licenze e operativi.

nShield Database Security Option Pack

SPECIFICHE TECNICHE

Configurazioni supportate

- Richiede il software nShield Security World v12.40.2 o v12.60.x o versioni successive.
- Microsoft SQL Server (edizione enterprise) versione 2019 x64, 2017 x64
- Supporto del sistema operativo di Windows Server 2019 R2 x64, 2016 R2 x64
- HSM supportati
  - Compatibile con tutti i modelli di HSM nShield Solo e Connect

Algoritmi di crittografia supportati

- Asimmetrici - comprese lunghezze delle chiavi RSA 2048, 3072 e 4096 bit
- Simmetrici - comprese lunghezze delle chiavi AES 128, 192 e 256 bit

FUNZIONALITÀ NSHIELD SUPPORTATE

L'integrazione di un HSM nShield con Microsoft SQL Server garantisce le seguenti funzionalità:

Funzionalità	Supporto
Set di smarcard 1 di N	Sì
Set di smarcard K di N	Sola
Softcard	Sì
Sola protezione di modulo	Sola
Ripristino della chiave	Sì
Importazione della chiave	Parziale[1]
Bilanciamento dei carichi	Sì
Failover	Sì
Supporto strict FIPS (FIPS 140-2 livello 3)	Sì[2]

1. L'importazione delle chiavi è supportata esclusivamente per le chiavi nCore. L'API nCore è l'interfaccia di programmazione delle applicazioni nativa per i moduli nShield 2. Per maggiori dettagli, consulta le note di rilascio e la guida per l'utente.

Scopri di più

Per ulteriori informazioni sugli HSM Entrust nShield, 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**

Per ulteriori informazioni sugli HSM Entrust nShield, visita il sito

HSMinfo@entrust.com
entrust.com/HSM

ENTRUST CORPORATION

Entrust permette al mondo di continuare a muoversi in sicurezza attraverso sistemi di identificazione, pagamento e protezione dei dati ad alta affidabilità. Oggi più che mai, le persone si aspettano esperienze sicure e ottimizzate, che si tratti di attraversare le frontiere tra Stati, effettuare un acquisto, accedere ai servizi elettronici della pubblica amministrazione o collegarsi a una rete aziendale. Entrust offre un'ineguagliabile gamma di soluzioni di sicurezza digitale ed emissione di credenziali, il vero fondamento di tutte queste interazioni. Con oltre 2.500 colleghi, una rete di partner globali e clienti in più di 150 Paesi, non sorprende che le organizzazioni più fidate al mondo scelgano noi.

Scopri di più su
entrust.com/HSM

ENTRUST

Per contattarci:
HSMinfo@entrust.com