Hardware Security Module di scopo generale nShield®

ENTRUST

SECURING A WORLD IN MOTION

Indice

Sicurezza affidabile

Gli hardware security module (HSM) nShield di Entrust sono dispositivi affidabili a prova di manomissione in grado di proteggere i dati più sensibili della tua azienda. Certificati secondo lo standard FIPS 140-2, i nostri moduli supportano un'ampia gamma di attività crittografiche, come la creazione, la gestione e l'archiviazione di chiavi di firma e di crittografia, oltre a fornire margini di protezione per l'esecuzione di funzioni sensibili.

Gli HSM nShield rappresentano un potente strumento da aggiungere alle soluzioni per la sicurezza già implementate dalle aziende e possono contribuire a:

- Raggiungere livelli più elevati di sicurezza e affidabilità dei dati
- Soddisfare e superare i requisiti di importanti standard normativi
- Mantenere livelli superiori di servizio e flessibilità

La famiglia nShield

Per rispondere alle esigenze specifiche dettate dall'ambiente di ciascuna impresa, la famiglia di HSM di scopo generale nShield include i modelli seguenti:

nShield Connect

Dispositivi di rete

Sviluppati per fornire servizi crittografici alle applicazioni distribuite sulla rete, gli HSM nShield Connect sono disponibili in due serie: gli HSM standard nShield Connect+ e quelli della serie ad alte prestazioni nShield Connect XC.

nShield Edge

Moduli portatili con collegamento USB

Gli HSM nShield Edge sono dispositivi desktop sviluppati per garantire praticità e risparmio. nShield Edge è la soluzione ideale per gli sviluppatori e supporta applicazioni come la generazione di chiavi di root a bassi requisiti prestazionali.

nShield Solo

Schede PCIe da incorporare all'interno di appliance o server

Gli HSM nShield Solo sono moduli compatti basati su scheda PCI Express, che forniscono servizi crittografici alle applicazioni installate su server o appliance. Sono disponibili in due serie: gli HSM standard nShield Solo+ e quelli ad alte prestazioni della serie nShield Solo XC.

nShield as a Service

Sottoscrizione per accesso agli HSM nShield in cloud

nShield as a Service permette la sottoscrizione di un accesso dedicato agli HSM nShield Connect XC, certificati secondo lo standard FIPS 140-2 di livello 3. La soluzione offre le stesse caratteristiche e funzionalità degli HSM on-premise, con il valore aggiunto dell'implementazione del servizio su cloud, che consente ai clienti di raggiungere i propri obiettivi "cloud first", lasciando la manutenzione dei dispositivi nelle mani degli esperti di Entrust. Il servizio è disponibile con un modello di gestione autonoma da parte del cliente o completa.

Supporto per un'ampia gamma di utilizzi

I clienti di Entrust utilizzano gli HSM nShield come root of trust per una vasta gamma di applicazioni aziendali, tra cui infrastrutture a chiave pubblica (PKI), protezione delle chiavi di crittografia tramite SSL/TLS, firma del codice, apposizione di firme digitali e blockchain. Con l'evoluzione dell'Internet of Things, la richiesta di certificati e identità dei dispositivi sta diventando sempre più consistente. Sviluppati per affrontare le sfide del futuro, gli HSM nShield continueranno a supportare misure di sicurezza di importanza decisiva, come l'autenticazione dei dispositivi mediante certificati digitali,

oltre a un'ampia gamma di algoritmi di crittografia, tra cui quelli della crittografia ellittica, che offrono transazioni a velocità elevate perfette per gli ambienti di elaborazione compatti di oggi e per i sistemi operativi e le API più diffusi nel settore.

Caratteristiche della famiglia nShield

Interfacce Web services predisposte per il cloud

Il pacchetto opzionale nShield Web Services Option Pack consente di eseguire comandi mediante chiamate ai servizi Web, ottimizzando la comunicazione tra le applicazioni e gli HSM. Grazie a questo approccio innovativo, che elimina la necessità di integrare le applicazioni negli HSM nShield, i clienti non sono vincolati al proprio sistema operativo e all'architettura scelta. nShield Web Services Option Pack è in grado di comunicare con le applicazioni installate nel cloud e nei data center tradizionali.

Supporto containerizzato on-premise e nel cloud

nShield Container Option Pack agevola lo sviluppo e l'implementazione di applicazioni e processi containerizzati basati sulla sicurezza degli hardware security module di Entrust. Il set di script preconfigurati forniti semplifica enormemente l'integrazione degli HSM nShield, supportando le esigenze dinamiche di scalabilità delle applicazioni e degli host eseguiti in container.

Gestione delle chiavi più sicura per i dati sul cloud con nShield BYOK

La tua azienda utilizza Amazon Web Services, Google Cloud Platform o Microsoft Azure (oppure una combinazione di tutti e tre)? Grazie a nShield BYOK (Bring Your Own Key), è possibile generare chiavi sicure negli HSM nShield on-premise ed esportarle in tutta sicurezza alle applicazioni sul cloud. nShield BYOK incrementa i livelli di sicurezza dei processi di gestione e offre ai clienti un maggiore controllo sulle chiavi, il tutto assicurando che la responsabilità della sicurezza dei dati nel cloud risulti condivisa.

Tra i vantaggi di nShield BYOK spiccano:

- Processi di gestione delle chiavi che aumentano la sicurezza dei dati sensibili nel cloud
- Maggiore affidabilità delle procedure di creazione delle chiavi grazie al generatore di numeri casuali a elevata entropia di nShield, protetto dall'hardware certificato secondo lo standard FIPS
- Maggiore controllo sulle chiavi: i clienti utilizzano i propri HSM nShield all'interno del loro ambiente per creare ed esportare le chiavi al cloud in tutta sicurezza

Per la massima sicurezza e l'adozione di controlli rigorosi sul trasporto e l'utilizzo delle chiavi di crittografia, utilizza nCipher BYOK con Microsoft Azure. Se hai bisogno di ricevere assistenza in sede per l'integrazione e l'implementazione, scegli il nostro BYOK Deployment Service Package. Questo pacchetto include un HSM nShield Edge, assistenza all'integrazione da parte del personale dei servizi professionali di Entrust e un anno di manutenzione.

Il Cloud Integration Option Pack (CIOP) di Entrust è progettato per i clienti che utilizzano BYOK con Amazon Web Services oppure Google Cloud Platform e contiene quanto necessario a utilizzare gli HSM nShield on-premise per generare e trasferire le chiavi a tali servizi. Inoltre, il CIOP offre supporto per il nuovo meccanismo di piattaforma aperta Microsoft Azure BYOK.

Operazioni semplificate grazie al monitoraggio e alla gestione da remoto

nShield Monitor e nShield Remote Administration, disponibili per gli HSM nShield Solo e Connect, contribuiscono a ridurre i costi operativi lasciando ai clienti il controllo totale sui propri HSM.

- I vantaggi delle soluzioni per il monitoraggio e la gestione da remoto di Entrust includono:
- Ottimizzazione delle prestazioni degli HSM, pianificazione e uptime dell'infrastruttura grazie a nShield Monitor, che tiene informato il personale sulle tendenze di carico, le statistiche relative all'uso, i tentativi di manomissione, gli avvisi e le notifiche
- Riduzione dell'investimento in tempo e denaro grazie alla gestione degli HSM tramite l'interfaccia sicura di nShield Remote Administration

Configurazione da remoto

I modelli nShield Connect XC offrono una console seriale opzionale per semplificare l'installazione nel rack, la cablatura e il collegamento all'alimentazione dell'HSM, mentre i passaggi rimanenti di configurazione del dispositivo e della rete possono essere completati da remoto. In questo modo, si elimina la necessità di riorganizzare il data center, semplificando il processo di implementazione. Questa funzionalità supporta un modello provider/tenant in base al quale il provider controlla la configurazione della rete e il tenant mantiene il pieno controllo sulle chiavi.

Architettura Security World ad alta flessibilità

nShield Security World supporta gli HSM Entrust nShield mediante la creazione di una ambiente di gestione delle chiavi esclusivo e flessibile. Con nShield Security World, è possibile combinare diversi modelli HSM nShield per costruire un ecosistema unificato che offre scalabilità, failover senza problemi e bilanciamento dei carichi.

"Grazie agli innovativi HSM nShield di Entrust, abbiamo potuto utilizzare un chip più sofisticato e sicuro per la nostra tecnologia."

Bill Kavadas, Senior Director for Information Systems, Memjet

nShield Security World garantisce inoltre l'interoperabilità nel caso di implementazione di un numero qualsiasi di HSM, assicura la gestione di chiavi illimitate e consente di effettuare il backup e di ripristinare le chiavi in modo automatico da remoto.

I vantaggi offerti da nShield Security World includono:

- Scalabilità semplice degli HSM nShield in risposta alle esigenze di crescita dell'azienda
- Conservazione della resilienza del sistema
- Risparmio di tempo mediante l'eliminazione delle lunghe operazioni di backup dell'HSM

CodeSafe: l'ambiente per l'esecuzione sicura di nShield

Oltre a proteggere le chiavi sensibili, gli HSM nShield Solo e Connect forniscono un ambiente sicuro per l'esecuzione di applicazioni proprietarie. L'opzione CodeSafe consente di sviluppare ed eseguire il codice all'interno del perimetro di sicurezza conforme allo standard FIPS 140-2 di livello 3 di nShield, proteggendo le applicazioni da potenziali attacchi.

CodeSafe consente di:

- Raggiungere un elevato livello di sicurezza grazie all'esecuzione di applicazioni sensibili in ambiente certificato, oltre alla protezione degli endpoint e dei dati da questi processati
- Proteggere le applicazioni sensibili da attacchi dall'interno, malware e minacce persistenti avanzate
- Eliminare il rischio di modifiche non autorizzate alle applicazioni e di infezioni da malware grazie alla firma del codice

Collaborazione con le aziende leader del settore

Entrust collabora con provider di tecnologia all'avanguardia allo sviluppo di soluzioni efficaci per vincere le sfide di sicurezza del settore e aiutare i clienti a raggiungere i propri obiettivi di trasformazione digitale. Assieme ai partner che partecipano al programma dedicato dell'azienda, Entrust lavora all'integrazione degli HSM nShield all'interno di un'ampia gamma di soluzioni per la sicurezza, tra cui l'emissione di credenziali, la PKI, la sicurezza dei database, la firma del codice, le firme digitali, la gestione degli account riservati, il rilascio delle applicazioni, il cloud e l'intelligence per i big data. Gli HSM nShield supportano le applicazioni di sicurezza dei nostri partner offrendo elaborazione crittografica di alto livello, protezione e gestione delle chiavi e agevolando la conformità alle normative vigenti sulla sicurezza dei dati, a livello pubblico e di settore.

"Guardiamo con entusiasmo alle possibilità offerte ai nostri clienti dalle nuove funzionalità predisposte per il cloud di nShield, tra cui nShield as a Service. Dimostrano la capacità di riconoscere che il mercato sta cambiando e che le organizzazioni devono affidarsi ad HSM completamente gestiti nel cloud per trarre il massimo dall'innovazione e cogliere i vantaggi commerciali offerti."

Ed Wood, Director of Product Management, Cryptomathic

"Il lancio di nShield as a Service di Entrust offre ai clienti di F5 un più ampio ventaglio di soluzioni per la sicurezza tra cui scegliere, oltre all'opportunità di preservare la sovranità dei dati con un modello a sottoscrizione basato sul cloud. La sicurezza, un tempo considerata una spesa in conto capitale, diventa così un costo operativo, da cui derivano una maggiore flessibilità e convenienza per le organizzazioni."

John Morgan, VP & GM of Security, F5 Networks

Versatilità ed elevate prestazioni

Gli HSM nShield Connect e Solo sono disponibili in tre livelli di prestazioni per adattarsi ad ambienti aziendali di ogni tipo, da quelli con volumi moderati di transazioni a quelli con applicazioni che richiedono un throughput elevato. nShield Connect XC, il nostro HSM dalle prestazioni migliori, è alla base della nostra soluzione nShield as a Service, che consente di accedere agli HSM nShield nel cloud.

Certificazione secondo gli standard di settore

Il rispetto di standard rigorosi da parte di Entrust consente di soddisfare gli obiettivi di conformità degli ambienti regolamentati, garantendo un livello elevato di fiducia nella sicurezza e nell'integrità degli HSM nShield. Di seguito è riportato un elenco parziale degli standard di cui soddisfiamo i requisiti; l'elenco completo è disponibile sul nostro sito Web e nelle schede di dati dei nostri prodotti.

FIPS 140-2

Emesso dal National Institute of Standards and Technology dell'amministrazione statunitense, FIPS 140-2 è uno standard riconosciuto a livello mondiale per la convalida della sicurezza e dell'efficacia dei moduli di crittografia. Tutti gli HSM nShield di Entrust sono certificati secondo lo standard FIPS 140-2 di livello 2 e 3.

FIPS Level 3 Validated 140-2

Common Criteria

Common Criteria e conformità al Regolamento eIDAS

Gli HSM nShield XC e nShield+ sono certificati secondo i Common Criteria EAL 4+ e riconosciuti come dispositivi per la creazione di una firma qualificata (QSCD) ai sensi del regolamento eIDAS. Gli HSM nShield Solo XC e Connect XC sono inoltre conformi al profilo di protezione EN 419 221-5 "Moduli crittografici per servizi fiduciari" secondo i Common Criteria. La famiglia di HSM nShield rappresenta quindi la colonna portante della digitalizzazione degli Stati membri e delle imprese dell'Unione europea, che include il supporto allo sviluppo di sistemi di identificazione a livello nazionale, oltre a servizi transfrontalieri, per i documenti elettronici e la firma delle transazioni, l'autenticazione, le marcature temporali, la sicurezza della posta elettronica e l'archiviazione di documenti a lungo termine. Sebbene queste certificazioni siano state introdotte in seguito all'entrata in vigore di un regolamento europeo, molti Paesi di tutto il mondo ne stanno approvando l'adozione.

Per saperne di più

Visita **entrust.com/HSM** per scoprire come possiamo proteggere le informazioni e le applicazioni business-critical della tua azienda, on-premise, nel cloud e negli ambienti virtuali.

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

Per contattarci:
HSMinfo@entrust.com