HSM nShield Connect

La sicurezza delle tue applicazioni dipende dal luogo in cui tieni le chiavi

IN EVIDENZA

Funzionalità a 360°

Gli hardware security module (HSM) nShield Connect sono appliance certificate secondo FIPS 140-2 e Common Criteria EAL4+ (EN 419 221-5) che forniscono servizi di chiavi di crittografia scalabili e a elevata disponibilità tra le reti.

- Tassi di transazione crittografica elevati ed estrema flessibilità
- Integrazione con oltre 150 soluzioni di fornitori di applicazioni leader nel settore
- Opzione CodeSafe per proteggere le applicazioni e la logica di business all'interno dell'ambiente di esecuzione sicuro di nShield

Gli HSM nShield Connect sono piattaforme a prova di manomissione che eseguono funzioni come crittografia, firma digitale e generazione e protezione delle chiavi per un'ampia gamma di applicazioni, tra cui:

- Autorità di certificazione
- Firma del codice
- Software personalizzato
- Applicazioni su cloud e containerizzate
- Servizi web
- Blockchain
- Crittografia del database

La serie nShield Connect include nShield Connect+ e nShield Connect XC ad alte prestazioni.

SCOPRI DI PIÙ SU ENTRUST.COM/HSM

HSM nShield Connect

CARATTERISTICHE E VANTAGGI CHIAVE

Architettura ad alta flessibilità

L'esclusiva architettura Security World permette di combinare i modelli di HSM nShield per costruire un patrimonio misto in grado di fornire scalabilità flessibile, failover e bilanciamento dei carichi.

Elaborazione più rapida di un maggior numero di dati

Gli HSM nShield Connect supportano elevate prestazioni e sono pertanto ideali per ambienti in cui il flusso produttivo costituisce un elemento cruciale, come imprese, retail e IoT.

EFFICIENTI FUNZIONALITÀ DA REMOTO

Elimina la necessità di raggiungere fisicamente il data center

nShield Remote Administration: permette di presentare in tutta sicurezza da remoto le smart card di autorizzazione agli HSM remoti per eseguire attività di manutenzione come aggiornamenti del firmware, aggiunta di nuovi HSM e riassegnazione/riconfigurazione degli HSM esistenti. È disponibile una scheda tecnica distinta.

Remote Configuration: la versione a console seriale di Connect XC permette una facile installazione per il personale del data center, la configurazione della rete da remoto e le impostazioni del pannello anteriore.

nShield Monitor fornisce un unico dashboard per tutti gli HSM nShield per aiutarti a ottimizzare le operazioni e incrementare l'uptime. È disponibile una scheda tecnica distinta.

Proteggi le tue applicazioni di proprietà

L'opzione CodeSafe fornisce un ambiente sicuro per l'esecuzione di applicazioni sensibili all'interno di un confine fisico nShield certificato secondo lo standard FIPS 140-2. Per maggiori informazioni, consulta la scheda tecnica di CodeSafe.

MODELLI DISPONIBILI E PRESTAZIONI

Modelli nShield Connect	500+	XC Base	1500+	6000+	XC Mid	XC High
Prestazioni di firma RSA (tps) per lunghezze delle chiavi raccomandate dal NIST						
2048 bit	150	430	450	3.000	3.500	8.600
4096 bit	80	100	190	500	850	2.025
Prestazioni di firma a curva principale ECC (tps) di punta per lunghezze delle chiavi raccomandate dal NIST						
256 bit	540	680	1.260	2.400	7.515[2]	14.400[2]
Licenze client						
incluse	3	3	3	3	3	3
Massimo	10	10	20	illimitate[1]	20	illimitate[1]

Nota 1: richiede la licenza client di tipo enterprise.

Nota 2: le prestazioni indicate richiedono l'attivazione della funzione RNG ECDSA rapida disponibile gratuitamente tramite richiesta al supporto nCipher.

SCOPRI DI PIÙ SU ENTRUST.COM/HSM

HSM nShield Connect

SPECIFICHE TECNICHE

Algoritmi di crittografia supportati (inclusa l'implementazione completa della Suite B di NIST)

- Algoritmi asimmetrici: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA (incluse le curve NIST, Brainpool e secp256k1), ECDH, Edwards (Ed25519, Ed25519ph)
- Algoritmi simmetrici: AES, Arcfour, ARIA, Camellia, CAST, DES, MD5 HMAC, RIPEMD160 HMAC, SEED, SHA-1 HMAC, SHA-224 HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC, Tiger HMAC, 3DES
- Hash/message digest: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160

Piattaforme supportate

- Sistemi operativi Windows e Linux comprendenti distribuzioni da RedHat, SUSE e i principali fornitori di servizi cloud in esecuzione come macchine virtuali o in container

Interfacce di programmazione di un'applicazione (API)

- PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI/CNG e Web Services (richiede Web Services Option Pack)

Connettività host

- Doppie porte Gigabit Ethernet (due segmenti di rete)

Conformità agli standard di protezione

- Certificazione FIPS 140-2 livello 2 e livello 3
- Certificazione di conformità IPv6 e USGv6 Ready
- Connect XC: certificazione eIDAS e Common Criteria EAL4 + AVA_VAN.5 e ALC_ FLR.2 secondo il profilo di protezione EN 419 221-5, in base allo schema NSCIB olandese
- Connect+: certificazione Common Criteria EAL4+ (AVA_VAN.5)
- Riconoscimento di Connect+ come dispositivo per la creazione di una firma qualificata (QSCD)
- Connect XC: conforme a BSI AIS 20/31

Conformità agli standard di sicurezza e ambientali

- UL, CE, FCC, RCM Canada ICES RoHS2, WEEE

Elevata disponibilità

- Archiviazione interamente allo stato solido
- Vassoio ventole manutenibile in loco, alimentatori doppi sostituibili a caldo

Gestione e monitoraggio

- nShield Remote Configuration (disponibile su modelli Connect XC configurati con console seriale)
- nShield Remote Administration (acquistabile separatamente)
- nShield Monitor (acquistabile separatamente)
- Secure Audit Logging
- Supporto alla diagnostica Syslog e monitoraggio delle prestazioni di Windows
- Agente di monitoraggio SNMP

Caratteristiche fisiche

- Montaggio su rack standard 1U 19 pollici. Dimensioni: 43,4 x 430 x 705 mm
- Peso: 11,5 kg
- Tensione in ingresso: 100-240 V CA commutazione automatica 50-60 Hz
- Consumo energetico: fino 2.0 A a 110 V CA, 60 Hz | 1.0 A a 220 V CA, 50 Hz
- Dissipazione del calore: da 327.6 a 362.0 BTU/h (carico completo)
- Affidabilità - MTBF (ore)[3], Connect XC: 107.384 ore, Connect+: 99.284 ore

Nota 3: calcolato a una temperatura operativa di 25 °C utilizzando lo standard MTBF Telcordia SR-332 "Reliability Prediction Procedure for Electronic Equipment"

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