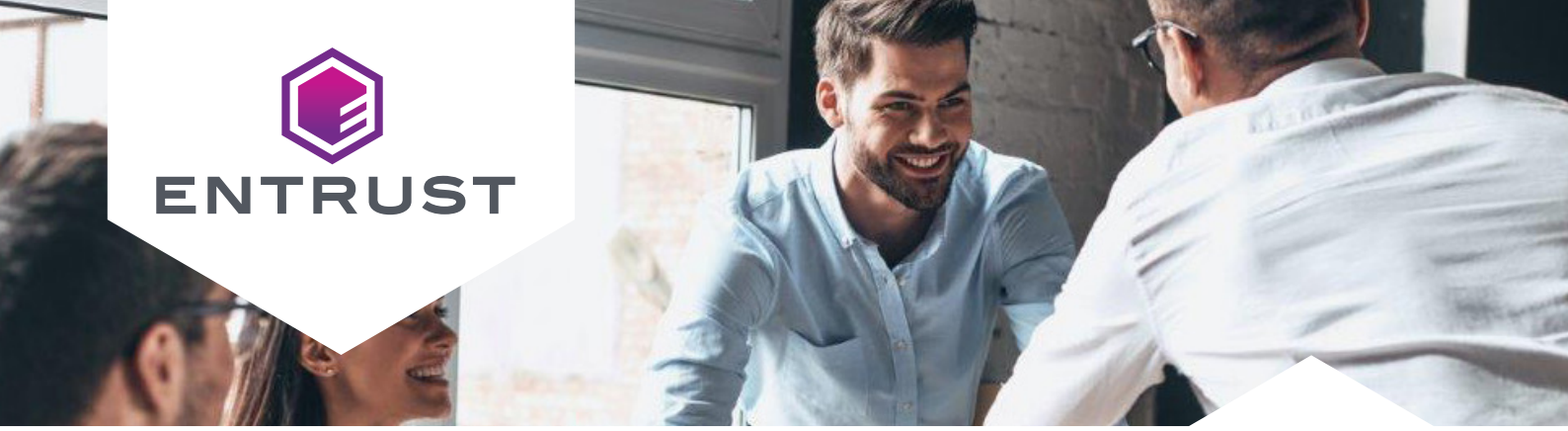


HSM nShield Solo

Schede PCI-Express certificate che forniscono servizi di chiavi di crittografia a server stand-alone

IN EVIDENZA

Gli hardware security module (HSM) nShield Solo sono schede PCI-Express certificate in formato low-profile che forniscono servizi crittografici ad applicazioni ospitate su un server o un'appliance. Queste schede a prova di manomissione 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 e altro ancora.

La serie nShield Solo include nShield Solo+ il nuovo nShield Solo XC ad alte prestazioni.

Architettura ad alta flessibilità

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

Elaborazione più rapida di un maggior numero di dati

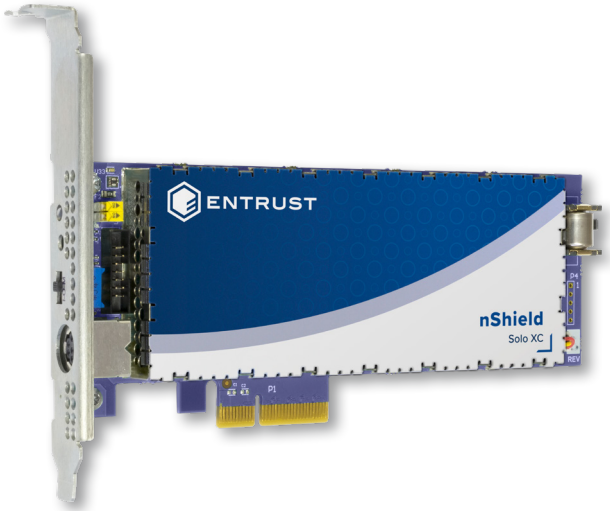
Gli HSM nShield Solo supportano elevate prestazioni e sono pertanto ideali per imprese, retail, IoT e altri ambienti in cui il flusso produttivo costituisce un elemento cruciale.

Proteggi i tuoi dati e le tue applicazioni di proprietà

L'opzione CodeSafe fornisce un ambiente sicuro per l'esecuzione di applicazioni sensibili all'interno dei margini di nShield.

CARATTERISTICHE E VANTAGGI CHIAVE

- Massimizza le prestazioni e la disponibilità con elevate prestazioni crittografiche crittografica elevati e scalabilità flessibile
- Supporta un'ampia gamma di applicazioni tra cui autorità di certificazione, firma del codice e altre ancora
- nShield CodeSafe protegge le tue applicazioni all'interno dell'ambiente di esecuzione sicuro di nShield
- nShield Remote Administration ti aiuta a ridurre i costi e gli spostamenti



SCOPRI DI PIÙ SU ENTRUST.COM/HSM

HSM nShield Solo

SPECIFICHE TECNICHE

Algoritmi di crittografia supportati

- Algoritmi asimmetrici: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA, ECDH, Edwards (X25519, 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
- Implementazione completa della Suite B con ECC con licenza, comprendente Brainpool e curve personalizzate

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
- Ambienti virtuali Solo XC supportati tra cui VMware ESX, Microsoft Hyper-V, Linux KVM e Citrix XenServer

Interfacce di programmazione di un'applicazione (API)

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

Connettività host

- PCI Express versione 2.0; Connettore Solo+: 1 via, connettore Solo XC connector: 4 lane

Conformità agli standard di protezione

- Certificazione FIPS 140-2 livello 2 e livello 3
- Solo+: certificazione Common Criteria EAL4+ (AVA_VAN.5)
- Riconoscimento di Solo+ come dispositivo per la creazione di una firma qualificata (QSCD)
- Solo 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
- Solo XC: conforme a BSI AIS 20/31

Conformità agli standard di sicurezza e ambientali

- UL, UL/CA, CE, FCC, Canada ICES, KC, FCC, VCCI, RCM
- RoHS2, WEEE, REACH

Gestione e monitoraggio

- nShield Remote Administration e nShield Monitor
- Registro di revisione sicuro
- Supporto alla diagnostica Syslog e monitoraggio delle prestazioni di Windows
- Agente di monitoraggio SNMP

MODELLI DISPONIBILI E PRESTAZIONI

Modelli nShield Solo	500+	XC Base	6000+	XC Mid	XC High
Prestazioni di firma RSA (tps) per lunghezze delle chiavi raccomandate dal NIST					
2048 bit	150	430	3.000	3.500	8.600
4096 bit	80	100	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	2.400	7.515[1]	14.400[1]

Dimensioni	Peso		Potenza	
	Solo+	Solo XC	Solo+	Solo XC
56,2 Q 167,1 Q 15,4 mm	230 g	280 g	10 W	24 W
2,2 Q 6,6 Q 0,6 pollici	0,5 lb	0,62 lb		

Nota 1: 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

ENTRUST

Per contattarci:
HSMinfo@entrust.com