nShield Connect HSM

Für die Sicherheit Ihrer Anwendungen ist es entscheidend, wo Sie Ihre Schlüssel aufbewahren

HIGHLIGHTS

Umfangreiche Funktionen

nShield Connect Hardware Sicherheitsmodule (HSM) sind gemäß FIPS 140-2 und Common Criteria EAL4+ (EN 419 221-5) zertifizierte Geräte, die netzwerkübergreifende skalierbare und hochverfügbare kryptographische Schlüsseldienste anbieten.

- Hohe kryptographische Transaktionsraten und flexible Skalierung
- Können mit über 150 Lösungen führender Anbieter integriert werden
- Optional schützt CodeSafe Ihre Anwendungen und Geschäftsprozesse in der sicheren Ausführungsumgebung von nShield.

nShield Connect HSM sind manipulationssichere Plattformen, die unter anderem für die folgenden Anwendungen Verschlüsselung, digitale Signaturen sowie Schlüsselerstellung und -schutz anbieten:

- Zertifizierungsstellen
- Code-Signatur
- Benutzerdefinierte Software
- Cloud- und containerisierte Anwendungen
- Webdienste
- Blockchain
- Datenbankverschlüsselung

Die nShield-Connect-Reihe umfasst nShield Connect+ und das leistungsstarke nShield Connect XC.

WEITERE INFORMATIONEN AUF ENTRUST.COM/HSM

nShield Connect HSM

WICHTIGE FUNKTIONEN UND VORTEILE

Hochflexible Architektur

Mit unserer einzigartigen Security-World-Architektur können Sie nShield-HSM-Modelle zum Aufbau einer gemischten Infrastruktur kombinieren, die flexible Skalierbarkeit sowie nahtlosen Failover und Lastenausgleich bietet.

Mehr Daten schneller verarbeiten

nShield Connect HSM unterstützen hohe Transaktionsraten und sind daher perfekt für Umgebungen geeignet, in denen der Durchsatz entscheidend ist, wie z. B. in Unternehmen, im Einzelhandel und im Bereich IoT.

OPTIONAL LEISTUNGSSTARKE REMOTE-FUNKTIONEN

Besuche im Rechenzentrum werden unnötig

nShield Remote Administration: Wartungsaufgaben wie Firmware-Upgrades, Bereitstellung neuer HSM und die Neuzuweisung/Neukonfiguration bestehender HSM können dank sicherer Remote-Authentifizierung von Smartcards per Fernzugriff erfolgen. Separate Datenblätter erhältlich.

Fernkonfiguration: Die serielle Konsolenversion von Connect XC ermöglicht eine einfache Installation im Rechenzentrum, Netzwerkkonfiguration und Einstellung der Frontplatte per Fernzugriff.

Der nShield Monitor bietet ein einziges Dashboard für alle Ihre nShield-HSM und sorgt somit für eine Optimierung des Betriebs und erhöhte Verfügbarkeit. Separate Datenblätter erhältlich.

Schützen Sie Ihre proprietären Anwendungen

Optional bietet CodeSafe eine sichere Umgebung, um sensible Anwendungen innerhalb der nach FIPS 140-2 zertifizierten physischen Grenzen von nShield auszuführen. Entsprechende Informationen finden Sie im Datenblatt zu CodeSafe.

VERFÜGBARE MODELLE UND LEISTUNG

nShield Connect-Modelle	500+	XC Base	1.500+	6.000+	XC Mid	XC High
RSA Signing Performance (tps) für NIST-empfohlene Schlüssellängen						
2048 Bit	150	430	450	3.000	3.500	8.600
4096 Bit	80	100	190	500	850	2.025
ECC Prime Curve Signing Performance (tps) für NIST-empfohlene Schlüssellängen						
256 Bit	540	680	1.260	2.400	7.515[2]	14.400[2]
Client-Lizenzen						
Inbegriffen	3	3	3	3	3	3
Maximum	10	10	20	unbegrenzt[1]	20	unbegrenzt[1]

Hinweis 1: Erfordert eine Client-Lizenz für Unternehmen.

Hinweis 2: Die angegebene Performance erfordert die schnelle Aktivierung der RNG-Funktion von ECDSA, die der Support von nCipher kostenlos zur Verfügung stellt.

nShield Connect HSM

TECHNISCHE DATEN

Unterstützte kryptographische Algorithmen (einschließlich vollständiger NIST-Suite-B-Implementation)

- Asymmetrische Algorithmen: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA (einschließlich NIST, Brainpool & secp256k1-Kurven), ECDH, Edwards (Ed25519, Ed25519ph)
- Symmetrische Algorithmen: 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-/Hashwert: MD5, SHA-1, SHA-2 (224, 256, 384, 512 Bit), HAS-160, RIPEMD 160

Unterstützte Plattformen

- Windows- und Linux-Betriebssysteme einschließlich Distributionen von RedHat, SUSE und großen Cloud-Anbietern, die als virtuelle Maschinen oder Container ausgeführt werden

Anwendungsprogrammier-Schnittstellen (APIs)

- PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI/CNG und Web Services (erfordert das Web Services Option Pack)

Host-Konnektivität

- Dual Gigabit Ethernet-Anschlüsse (zwei Netzwerksegmente)

Sicherheits-Compliance:

- Nach FIPS 140-2 Level 2 und Level 3 zertifiziert
- Nach IPv6 zertifiziert und USGv6-Ready-konform
- Connect XC: eIDAS und Common Criteria EAL4 + AVA_VAN.5 und ALC_ FLR.2-Zertifizierung gemäß dem Schutzprofil EN 419 221-5 laut dem niederländischen NSCIB-System
- Connect+: Nach Common Criteria EAL4+ (AVA_VAN.5) zertifiziert
- Connect+ ist als qualifiziertes Signaturerstellungsgerät (Qualified Signature Creation Device) anerkannt
- Connect XC: BSI-AIS-20/31-konform

Einhaltung von Sicherheits- und Umweltstandards

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

Hohe Verfügbarkeit

- Alle Solid-State-Speicher
- Vor Ort einsetzbare Lüfter, duale Hot-Swap-Netzteile

Verwaltung und Überwachung

- nShield Remote Configuration (verfügbar bei mit der seriellen Konsole konfigurierten Connect XC-Modellen)
- nShield Remote-Verwaltung (separat erhältlich)
- nShield Monitor (separat erhältlich)
- Sichere Audit-Protokollierung
- Syslog-Diagnose-Unterstützung und Windows Leistungsüberwachung
- Agent für SNMP-Überwachung

Physische Eigenschaften

- Standard 1HE 19 Zoll Rackmontage Abmessungen: 43,4 x 430 x 705 mm (1,7 x 16,9 x 27,8 Zoll)
- Gewicht: 11,5 kg
- Eingangsspannung: 100-240 V AC automatische Umschaltung 50-60 Hz
- Stromverbrauch: bis zu 2,0 A bei 110 V AC, 60 Hz | 1,0 A bei 220 V AC, 50 Hz
- Wärmeableitung: 327,6 bis 362,0 BTU/Std (voll geladen)
- Zuverlässigkeit: MTBF (Stunden)[3], Connect XC: 107.384 Stunden, Connect+: 99.284 Stunden

Hinweis 3: Bei 25 °C Betriebstemperatur mit dem MTBF-Standard Telcordia SR-332 „Reliability Prediction Procedure for Electronic Equipment“ berechnet.

Mehr Informationen zu Entrust nShield HSMs

HSMinfo@entrust.com
entrust.com/HSM

ÜBER ENTRUST CORPORATION

Entrust ermöglicht vertrauenswürdige Identitäten und Zahlungen sowie verlässlichen Datenschutz und hält damit die Welt sicher in Bewegung. Ein nahtloses und sicheres Umfeld ist heute mehr denn je unerlässlich, sei es bei Grenzübertritten, beim Einkaufen, beim Zugriff auf E-Government-Dienste oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet für genau diese Interaktionen eine unübertroffene Bandbreite an Lösungen für digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen. Mit 2.500 Mitarbeitern und einem weltweiten Partnernetzwerk ist Entrust für Kunden in über 150 Ländern tätig, die sich bei ihren sensibelsten Operationen auf uns verlassen.

Weitere Informationen auf
entrust.com/HSM

Kontakt:
HSMinfo@entrust.com