



> Thales nShield Connect

HAUPTVORTEILE

- > Verbesserte Sicherheit für kritische Anwendungen
- > Verringerte Kosten für Compliance
- > Vereinfachte Verschlüsselung und einfache Verwaltung von Schlüsselmaterial
- > Sichere Ausführung eigener Anwendungen innerhalb des geschützten Bereichs mit CodeSafe (optional)
- > Betriebliche Kontinuität und minimierte Ausfallzeiten durch doppelte Stromversorgung und redundante Lüfter
- > Kompatibel mit anderen Thales HSMs
- > Unerreichte Skalierbarkeit mit unübertroffener Performance für bis zu 100 Clients
- > Zertifiziert nach FIPS und Common Criteria und entspricht somit den Anforderungen des BSI IT-Grundschutzes

Netzwerkbasiertes Hardware Security Modul

Thales nShield Connect, Teil der nCipher Produktreihe, ist ein netzwerkbasiertes Hardware Security Modul (HSM), das bis zu 100 Clients schützt, indem es deren Schlüsselmaterial geheim hält und sensible Daten auf einer gesicherten Appliance verarbeitet. Seine einzigartige doppelte, hot-swap-fähige Stromversorgung und seine redundanten Lüfter machen nShield Connect fehlertolerant. Die hohe Verfügbarkeit, einfache Skalierbarkeit und die Möglichkeit der Fernwartung ermöglichen es Organisationen, zuverlässige und zukunftssichere kryptografische Dienste zu erstellen. Die Sicherheitsfunktionen von nShield Connect sind nach FIPS 140-2 Level 3 und Common Criteria EAL4+ zertifiziert und erfüllen damit die Anforderungen des BSI IT-Grundschutzes.



>> Thales nShield Connect

Hardware-sicherheit für Anwendungen

nShield Connect ermöglicht Unternehmen, ihre kritischen Systeme wie beispielsweise Public Key Infrastrukturen (PKIs), Datenbanken, Web- und Anwendungsserver mit hardwarebasiertem Schutz auszustatten. Mit standardkonformen kryptografischen Schnittstellen integriert sich nShield Connect problemlos in Microsoft Certificate Services (PKI), Entrust Authority Security Manager, RSA Certificate Manager, Oracle Database, Microsoft SQL Server und viele andere Anwendungen.

nShield Connect besteht aus einer manipulationssicheren 19-Zoll-Hardware, die Anwendungsschlüssel innerhalb der Sicherheitszone generiert. Mit der Option CodeSafe ist es möglich, eigene Anwendungen innerhalb des geschützten Raums auszuführen, um vor Insiderangriffen und Trojanern sicher zu sein.

Betriebliche Kontinuität

Mit seiner besonderen Auslegung auf ununterbrochenen Betrieb hin ist nShield Connect das einzige HSM der Welt, das eine doppelte, hot-swap-fähige Stromversorgung und vor Ort wartbare Lüfter besitzt. So werden lange Transportzeiten für Reparaturen vermieden. Um die Verfügbarkeit noch weiter zu erhöhen, können mehrere HSMs zur Lastverteilung und als Ausfallsicherung kombiniert werden. Die Unterstützung von SNMP ermöglicht eine Fernüberwachung der Stromversorgung, der Temperaturen, Lüfterdrehzahlen und anderer Parameter.



Skalierbarkeit und Flexibilität

Um bis zu 100 Clients bedienen zu können, bietet nShield Connect eine Hardwarebeschleunigung für kryptografische Operationen. Damit stellt nShield Connect mit bis zu 6.000 Signaturvorgängen pro Sekunde (TPS) mit 1024-Bit RSA-Schlüsseln das schnellste netzwerkbasierte HSM dar.* Mit 2048-Bit-Schlüsseln erreicht nShield Connect bis zu 3.000 TPS.*

nShield Connect integriert sich über Standardschnittstellen in anderen Anwendungen, darunter PKCS# 11, OpenSSL, Java Cryptography Extension (JCE), Microsoft CAPI und CNG. Es ist mit nShield Solo (nShield PCI/PCle) und netHSM kompatibel und kann mit Optionspaketen für zusätzliche Funktionen ausgerüstet werden. nShield Connect unterstützt eine große Bandbreite an Betriebssystemen, darunter Windows 2008/2003/Vista/XP, Linux, Solaris, AIX und HP-UX. Zwei Gigabit-Ethernet-Anschlüsse ermöglichen dem HSM die Integration in zwei Netzwerksegmente.

Kryptographie und Compliance

nShield Connect unterstützt eine große Bandbreite an symmetrischen und asymmetrischen Algorithmen, einschließlich einer vollständigen Suite-B-Implementierung mit optionaler, voll lizenzierter Elliptic Curve Cryptography (ECC). Die Schlüsselverwaltung von nShield Connect ist nach FIPS 140-2 Level 3 und Common Criteria EAL 4+ zertifiziert. Als Best Practice und um Complianceanforderungen zu erfüllen, bietet nShield Connect eine Aufgabentrennung mit Zwei-Faktoren-Authentifizierung und Vier-Augen-Prinzip. Organisationen können den Zugriff nach Anwendung, Abteilung und Standort regeln.

Modelle

nShield Connect ist in drei verschiedenen Varianten verfügbar:

Modellnummer	500	1500	6000
Stromversorgungen	2	2	2
Geschwindigkeit (TPS RSA 1024)*	500	1500	6000
Geschwindigkeit (TPS RSA 2048)*	150	500	3000
Enthaltene Client-Lizenzen	3	3	3
Maximale Anzahl an Clients	10	20	100
Frontblende	Schwarz	Schwarz	Silber

*Die Leistung hängt unter anderem von der Anwendung, dem Betriebssystem, dem Netzwerkaufbau und weiteren Faktoren ab.

Weitere Informationen erhalten Sie unter www.thalesgroup.com/iss.

Thales - Information Systems Security

