



> Thales nShield Solo

VORTEILE

- > Kostengünstiges, dediziertes HSM für Server
- > Schützt Schlüsselmaterial und sensible Anwendungsdaten in einer sicheren Hardware-Umgebung
- > Ermöglicht einfache, automatisierte Backups des Schlüsselmaterials mit sicherer Wiederherstellung
- > Verbessert die Sicherheit und kryptografische Leistungsfähigkeit von OEM-Appliances
- > Security World und Fernwartung senken Kosten
- > Vermeidet Engpässe durch hohe Performance
- > Einfach mit Drittanwendungen integrierbar
- > Datenschutz auch in ungesicherten Umgebungen dank CodeSafe-Technologie
- > Compliance mit FIPS und Common Criteria

Hardware Security Module zur Verwaltung von Schlüsseln

Thales nShield Solo, Teil der nCipher-Produktreihe, ist eine Gruppe von HSM-Steckkarten für Server und Appliances zum Schutz von Schlüsselmaterial. Optional können Anwendungen auf dem Modul ausgeführt werden, um verarbeitete Daten noch besser zu schützen. nShield Solo, bisher einfach als „nShield“ bekannt, schützt das Schlüsselmaterial auf Servern mit einem manipulationssicheren Hardwaremodul. nShield Solo ist mit Systemen mit PCI-, PCI-X- und PCI-Express-Schnittstellen kompatibel.



>> Thales nShield Solo

Hardware-sicherheit für kritische Anwendungen

nShield Solo ermöglicht Unternehmen, kritische Anwendungen mit Hardwareschutz zu versehen, so beispielsweise Public Key Infrastructures (PKIs), Datenbanken, Web- und Anwendungsserver. nShield Solo-Module sind als manipulationssichere PCI- und PCI-Express-Karten erhältlich; die PCI-Variante ist mit PCI-X-Schnittstellen kompatibel.

Kostengünstiger Schutz für einzelne Server

Beim Schutz von Schlüsselmaterial auf einem oder wenigen Servern, stellt nShield Solo die kostengünstigste Lösung dar. Kunden, die ein oder mehrere nShield Solo-Module in einem 19-Zoll-Rack montieren wollen, bietet der optionale nShield SmartCard Reader Rackmount eine praktische und saubere Lösung, um Kartenleser im Rechenzentrum einzubinden.



Sicherheit und Performance für OEM-Appliances

Hardwarehersteller können ihre Appliances mit nShield Solo mit verbesserter Sicherheit ausstatten und Compliance mit FIPS und Common Criteria bei der Schlüsselverwaltung anbieten. Sie profitieren außerdem von einer Leistungssteigerung bei kryptografischen Operationen.

Fernwartung und Hochverfügbarkeit

Sollen nShield HSMs per Fernwartung an entfernten Standorten betrieben werden, kann die Option Remote Operator in Verbindung mit einer nShield Solo-Karte im Administrator-Rechner genutzt werden, um Authorisierungen zu ermöglichen. Das ermöglicht eine schnellere Bedienung der Sicherheitsfunktionen und reduziert Reisekosten. nShield Solo kann mit Servern im Cluster eingesetzt werden, um eine Lastenverteilung und maximale Verfügbarkeit zu erzielen.

Security World senkt Kosten

Das Security World-Konzept ermöglicht eine zentrale Verwaltung von nShield Solo, nShield Connect und nethSM, um den Zeitaufwand für Einrichtung und Verwaltung zu verringern. Security World ermöglicht die Fernwartung von HSMs in einem unbemannten Rechenzentrum, Wiederherstellung sogar nach vollständiger Ersetzung von Hardware und die gemeinsame Nutzung von Schlüsselmaterial zwischen einzelnen HSMs, auch bei räumlicher Trennung.

Schlüsselmaterial und Metadaten können automatisch gesichert werden, ohne zusätzliche Hardware oder Personal vor Ort einzusetzen, was die Gesamtkosten des Betriebs senkt.

Hohe Leistung schützt vor Engpässen

nShield Solo bietet Hardwarebeschleunigung für kryptografische Operationen mit bis zu 6.000 Signaturvorgängen pro Sekunde (TPS) mit 1.024-Bit-RSA-Schlüsseln. Mit 2.048-Bit-Schlüsseln werden bis zu 3.100 TPS erreicht.

Einfach mit Drittanwendungen integrierbar

nShield Solo arbeitet mit Anwendungen zusammen, die Standardschnittstellen wie PKCS#11, Java Cryptography Extension (JCE), OpenSSL, Microsoft CAPI und CNG unterstützen. nShield Solo ist kompatibel mit nShield Connect und kann über Optionspakete um neue Funktionen erweitert werden. nShield Solo unterstützt eine breite Palette an Betriebssystemen, darunter Windows 2008/2003/Vista/XP, Linux, Solaris, AIX und HP-UX.

Datenschutz in ungesicherten Umgebungen

Die meisten HSMs schützen Schlüsselmaterial, aber nicht die Daten selbst. Trojaner oder korrupte Administratoren haben Zugriff auf sensible Informationen auf dem Hostsystem. Die CodeSafe-Technologie verarbeitet die Daten innerhalb des HSM statt auf dem Hostsystem, was Ihnen erlaubt, auch kritische Prozesse in ungesicherten Umgebungen auszuführen.

Compliance mit FIPS und Common Criteria

nShield Solo unterstützt eine breite Palette symmetrischer und asymmetrischer Algorithmen, einschließlich einer kompletten Suite B-Implementierung mit optionaler, voll lizenzierter Elliptic Curve Cryptography (ECC). Die Sicherheit von nShield Solo ist nach FIPS 140-2 Level 3 und Common Criteria EAL 4+ validiert. nShield Solo-Module sind in einer günstigeren Variante auch mit Zertifizierung nach FIPS 140-2 Level 2 erhältlich. nShield Solo trennt administrative und betriebliche Aufgaben durch Zwei-Faktoren-Authentifizierung und Mehr-Augen-Prinzip. Der Zugriff kann getrennt nach Anwendung, Rolle, Abteilung oder Standort erfolgen.

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



Thales - Information Systems Security