FORWARD THINKING IT SOLUTIONS

nCipher und THALES HSMs

nShield und payShield Produkte

ergonomics

nCipher und THALES HSMs

nCipher nShield Connect
Netzwerkbasiertes Hardware Security Module

Das nCipher nShield Connect ist Teil der nCipher Produktlinie. Es handelt sich dabei um ein ans Netzwerk angeschlossenes General Purpose Hardware Sicherheits Modul (HSM), das für bis zu 100 Clients kryptographische Funktionen wie Verschlüsselung oder digitale Signatur bereitstellen kann.

Die im Betrieb auswechselbaren und redundant ausgelegten Netzteile und die vor Ort austauschbaren Lüfter machen das nShield Connect fehlertolerant. Mit hoher Verfügbarkeit, Skalierbarkeit und Fernverwaltung verschafft es Organisationen die Möglichkeit, zuverlässige, zukunftssichere kryptografische Dienste aufzubauen und zu nutzen.

Der Sicherheitsstandard des nShield Connect entspricht den Vorgaben von FIPS 140-2 Level 3 und Common Criteria EAL4+.

Merkmale
- Hardwarebasierte Sicherheit für kritische Anwendungen
- Verringerte Kosten für Compliance
- Einfache Verwaltung des Schlüsselmaterials dank dem Security World Konzept
- Sichere Ausführung eigener Anwendungen innerhalb des geschützten Bereichs mit CodeSafe (optional)
- Betriebliche Kontinuität und minimierte Ausfallzeiten durch doppelte Stromversorgung und austauschbare Lüfter
- Kompatibel mit anderen nCipher 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

nShield Solo
HSM als PCI Karte

Die nShield Solo sind ebenfalls Mitglieder der nCipher-Produktfamilie. Die nShield Solo sind HSM-Steckkarten für Server und Appliances zum Schutz von Schlüsselmaterial. Wie beim nShield Connect können optional Anwendungen auf dem Modul ausgeführt werden, um verarbeitete Daten noch besser zu schützen. Das nShield Solo schützt das Schlüsselmaterial auf Servern mit einem manipulationssicheren Hardwaremodul.

nShield Solo ist mit Systemen mit PCI-, PCI-X- und PCI-Express-Schnittstellen kompatibel.

Merkmale
- Kostengünstiges, dediziertes HSM für Server und Appliances
- Schützt Schlüsselmaterial und sensible Anwendungsdaten in einer sicheren Hardwareumgebung
- 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

THALES HSMs

- Einfach mit Drittanwendungen integrierbar
- Datenschutz auch in ungesicherten Umgebungen dank CodeSafe-Technologie
- Compliance mit FIPS und Common Criteria

nCipher nShield Edge
Das portable HSM

Das nCipher nShield Edge ist ein HSM mit USB Schnittstelle. Als Mitglied der nCipher HSM Familie bietet das Edge vollständige HSM Funktionalität mit Chipkartenleser und Quorum Authentifizierung für den Schutz des sensitiven Schlüsselmaterials. Das Edge ist für kleine Transaktionsvolumen geeignet.

Die zertifizierte Plattform übernimmt Schlüsselmanagement, kryptographische Funktionen wie Verschlüsselung und digitale Signatur für eine grosse Anzahl von kommerziellen und individuellen Anwendungen. Mit der Edge lässt sich ohne weiteres eine offline Certificate Authority realisieren oder das Remote Management einer Security World sicherstellen. Das USB Interface ist optimal für den Einsatz mit Notebooks oder virtuellen Maschinen, wo softwarebasierte Sicherheit nicht ausreicht. Im Zusammenhang mit den stetig zunehmenden Compliance Anforderungen bietet die nShield Edge ein klar wahrnehmbares Sicherheitselement.

nCipher Security World
Alle nShield Produkte unterstützen die nCipher Security World Architektur für die effiziente Schlüsselverwaltung. Mit der Security World können administrative Aufgaben wie Backups für die HSMs automatisiert werden.

In einer Security World können alle HSMs auf das gleiche Schlüsselmaterial zugreifen, so dass keine Single Points of Failure entstehen. Zusätzliche HSMs werden bei Bedarf einfach in eine bestehende Security World integriert.

Thales payShield 9000
Das Payment HSM

Das Thales payShield 9000 ist speziell für die Anforderungen von Verarbeitern des elektronische Zahlungsverkehrs ausgelegt.

Das HSM übernimmt Aufgaben wie PINs schützen, umschlüsseln und prüfen, Transaktionen verarbeiten, Kredit- und Debitkarten ausgeben sowie Schlüssel verwalten. Die payShield Modelle sind die weltweit am häufigsten eingesetzten Payment HSMs, so dass geschätzte 80% aller Zahltransaktionen über solche Geräte abgewickelt werden.

Das Design der Thales payShield 9000 basiert auf 25 Jahre Erfahrung von Thales bei der Sicherung von Zahltransaktionen. Dank dieser langjährigen Erfahrung können hohe Sicherheit und einfacher Betrieb vorausgesetzt werden.

Das Thales payShield 9000 wird als externes Gerät im Host- oder Serverumfeld eingesetzt. Der Funktionsumfang und die Zertifizierungen entsprechen den Vorgaben der Internationalen

nCipher und THALES HSMs

Card Schemes, u.a. American Express, Discover, JCB, MasterCard und Visa.

Das payShield 9000 ist FIPS 140-2 Level 3 zertifiziert. Zudem ist das HSM verfügbar in Konfigurationen, welche gemäss der PCI HSM Spezifikation des PCI Security Standards Council zertifiziert sind.

Merkmale
Umfassende und zertifizierte Sicherheit speziell ausgelegt für die Kartenpersonalisierung und den Zahlungsverkehr.

- Unterstützt alle wichtigen Standard Zahlungsverkehrsanwendungen.
- Stellt Hochverfügbarkeit sicher dank redundanter Hardware, austauschbaren Komponenten und Support für Clustering und Failover.
- Vereinfacht Einführung und Wartung. Reduziert die Compliance-Kosten dank einer Auswahl von Softwarepaketen zugeschnitten für Issuers, Processors und Acquirers.
- Unterschiedliche Leistungsklassen sind verfügbar, so dass nur die tatsächlich benötigte Performance erworben werden muss.

Weitere Informationen finden Sie auf unserer Website www.ergonomics.ch.

Ergonomics AG » Nordstrasse 15 » CH-8006 Zürich
info@ergonomics.ch
+41 58 311 10 00