THALES nShield Connect 概觀

Thales nShield Connect 500、 nShield Connect 1500 及 nShield Connect 6000 是 Thales 最新一代的網路型 HSM(硬體安全模組)，承自 nCipher netHSM 優異的品質與效能，nShield Connect 500/1500/6000 內含兩個可熱插拔(dual，hotswap)的電源供應器及可現場拆換的(redundant，field-replaceable)風扇，使得它俱備高度的容錯能力(fault tolerant)。因提供了高可用性與順應規模變遷的能力(high availability， scalability)及遠端管理，企業可以建立一個可依賴的、勿須擔心未來規模變遷的加密服務系統。

nShield Connect 500/1500/6000 已獲得 FIPS 140-2 Level 3 及 Common Criteria EAL4+認證。

效益

- ✧ 增強關鍵應用系統的安全性。
- ✧ 降低設備成本。
- ✧ 簡化加密與簽章金鑰管理。
- ✧ 加密運算在安全的硬體內執行，保護敏感資料。
- ✧ 協助確保事業營運連續(business continuity)與最小化停機時間(minimize downtime) 。
- ✧ 相容於 nCipher nShield and nCipher netHSM 系列產品，應用系統不須更動。
- ✧ nShield Connect 6000 可同時連接 100 台應用系統伺服器，提供優異的規模適應效能(Scalability) 。
- ✧ 符合 FIPS 140-2 Level 3 及 Common Criteria EAL4+。

THALES nShield Connect 功能

提供應用系統硬體安全

nShield Connect 讓企業得以在許多關鍵應用系統上增加硬體保護能力，例如公開金鑰基礎建設(PKIs)、資料庫、網站、及應用系統伺服器。 使用業界標準加密運算介面，,nShield Connect 可以立即與市場主流系統整合，例如 Microsoft Certificate Services (PKI) 、Entrust Authority Security Manager、RSA Certificate Manager、Oracle Database、Microsoft SQL Server，及其他應用系統。

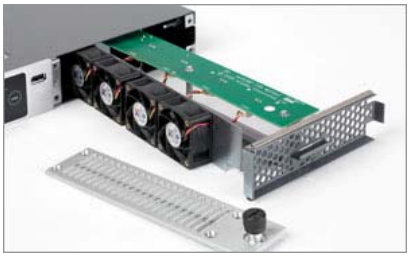
玉山科技股份有限公司
http://www.asiapeak.com
(02)77128295

Type	Applications	Benefits
Public key infrastructure (PKI)	• Microsoft Certificate Services (PKI) • Entrust Security Manager • RSA Certificate Manager • Many more	• Adds internal controls to protect root and subordinate-level private keys • Accelerates key generation and OCSP responses
Database encryption	• Oracle Database • Microsoft SQL Server	• Enable central key management • Add internal controls to protect master keys
Web and application servers	• Microsoft Internet Information Server • Apache Web Server • Websphere • Oracle WebLogic	• Add internal controls to protect SSL keys • Accelerate SSL connection setups • Secure data processing

高可靠性

特別為了營運連續性(business continuity)所設計，nShield Connect 是全球 HSM 中首款採用兩個可熱插拔的電源供應器，將此設備接上兩個不同電力來源，避免任一電力中斷造成系統停擺。電源供應器可在不停機情況下由操作人員在現場置換，不須整機送回供應商，確保服務不中斷。

nShield Connect 還有多個風扇，如有任一風扇故障，其他風扇仍可提供冷卻機體溫度的功能，風扇也可現場更換，這些設計就是為了增強設備的可用性，多台 HSM 可提供彼此備援及負載平衡(clustered and load balanced) 。



管理方便

Security World 管理軟體可以中央式管理 nShield Connect 500/1500/6000、Thales nShield 與 Thales netHSM 系列產品以降低設定及管理時間。Security World 支援安全地遠端操作在機房內的 HSM，災難復原時的硬體置換，不同地點的各個 HSM 的金鑰分享。所有金鑰及其相關資訊都可自動備份而不需額外的硬體設備，降低整體操作成本。

當企業佈置越來越多的硬體安全模組或有大量加密金鑰時，與其他廠牌 HSM 相較，Security World 的設計方式在操作及成本優勢上更為明顯：

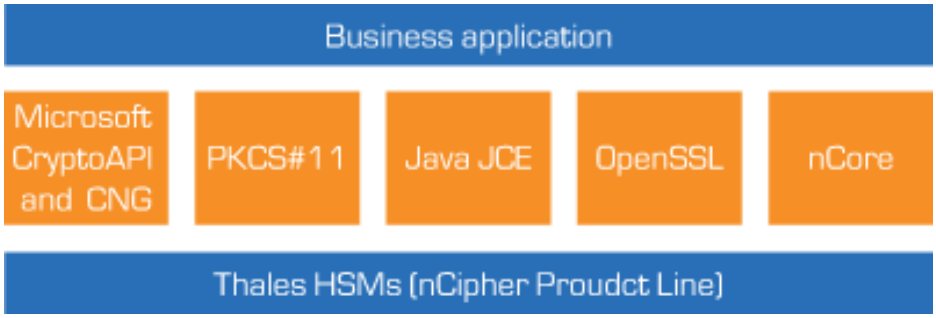
玉山科技股份有限公司
http://www.asiapeak.com
(02)77128295

它牌 HSM 做法 所有金鑰在 HSM 裡	Thales Security World 用 HSM Module Key 保護
✧ 備份在昂貴的專屬硬體上 ✧ 備份需要麻煩的人工與實體操作 ✧ 安全的儲存區是有限的，升級時需要額外的專屬硬體 ✧ 理論上做不到災難復原(Disaster recovery)，Clustering 會非常複雜 ✧ 過時的安全做法，造成操作方式非常麻煩與昂貴	✧ 自動化備份在省錢的檔案伺服器裡，不需人工介入，降低操作成本 ✧ 安全的儲存區是無限與便宜的，因為它使用檔案伺服器的空間 ✧ 災難復原做法有彈性，因為只使用處理 Security World files 與管理者法定最低人數 ✧ Clustering 容易又有彈性 ✧ 相同的安全等級卻更容易操作與管理

規模化與彈性

為提供高達 100 台連線機器的加密服務需求， nShield Connect 使用加密運算的加速晶片，使它成為當今網路型 HSM 中效能最高的硬體安全模組，每秒可達 6000 次的 1024 位元 RSA 金鑰的簽章速度(TPS)。National Institute of Standards and Technology (NIST) 建議 2010 年後應使用的 2048 位元 RSA 金鑰的簽章，nShield Connect 6000 可高達每秒 3000 次的 2048 bits 金鑰簽章。 網站伺服器如 Microsoft IIS 與 Apache，也可使用 nShield Connect 來增加 SSL 能力(throughput)，因為它可以將 SSL 連線運算移到 nShield Connect 上執行，卸載(off-loading) 網站伺服器的負擔。

nShield Connect 與應用系統整合是經由標準介面，包括 PKCS#11, Java Cryptography Extension (JCE), Microsoft CAPI and CNG.



nShield Connect 與其他 Thales (nCipher) nShield 及 netHSM 產品完全相容，並且可以升級採用選擇套件(Option Packs)以支援其他額外功能。nShield Connect 廣泛地支援各種作業系統，包括 Windows 2008/2003/Vista/XP、Linux、Solaris、AIX 與 HPUX。兩個 Gigabit Ethernet ports 讓這 HSM 可同時服務兩個網段。

密碼學與法規遵循

nShield Connect 支援廣泛的公開金鑰與對稱式演算法，還包括可選擇的 full Suite B implementation、完整授權的 elliptic curve cryptography (ECC)。 nShield Connect 符合 FIPS 140-2 Level 3 與 Common Criteria EAL 4+。管理者與操作者權責分開、雙因素認證(two-factor authentication)、多人控制(k of n)。操作員群組可依應用系統、角色、部門、地域來區別存取金鑰的權限。

整合的服務

Thales 另提供專業服務可確保客戶使用 Thales HSM 最佳實務。客戶可從 Thales 的開發人員的支援以整合 Thales HSM 與客制化應用系統，或是開發在 Thales HSM 環境下保護敏感性資料的客制化應用系統。

THALES nShield Connect 規格

實體規格

Physical dimensions: 19” rack unit, 1U, 705mm depth (43.4 x 430 x 705 mm)

Unpackaged weight: 11.5 Kg

Packaged dimensions: 190 x 590 x 890 mm

Packaged weight: 19.5 Kg

Power consumption: up to 1.2A at 110V AC 60Hz or 0.6A at 220V AC 50Hz

操作溫度

Normal range: 10 to 35 C

Operating range: 5 to 40 C

Storage range: -20 to 70 C

前面

Touch wheel

Smart card reader

Vents with easy access to field-replaceable, redundant fans

USB connector for keyboard

Color LCD display and associated soft keys

Power button

Clear button

Warning / Attention indicator lamp

玉山科技股份有限公司
http://www.asiapeak.com
(02)77128295

THALES

後面

Dual, hot-swap power supplies (each with IEC 320 mains socket & rocker switch)

2x 1 Gigabit Ethernet ports

演算法

Public key algorithms: RSA, Diffie-Hellman, DSA, El-Gamal, KCDSA, ECDSA, ECDH

Symmetric algorithms: AES, Arcfour, ARIA, Camellia, CAST, DES, MD5 HMAC, RIPEMD160 HMAC, SEED, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, Tiger HMAC, Triple DES.

效能

以下效能係指每秒可執行簽章交易的次數(TPS)。效能數字可能因作業系統、應用程式、網路架構及其他因素而有所差異 (NIST recommends using RSA 2,048 bit keys from year 2010)

Key length	nShield Connect 500	nShield Connect 1500	nShield Connect 6000
RSA 1024 bits	Up to 500 TPS	Up to 1,500 TPS	up to 6,000 TPS
RSA 2048 bits	Up to 150 TPS	Up to 500 TPS	up to 3,000 TPS
RSA 4096 bits	Up to 65 TPS	Up to 150 TPS	up to 550 TPS

認證

FIPS 140-2 Level 3

Common Criteria EAL4+

平台

Windows 2008/2003/Vista/XP

Solaris

HP-UX

AIX

Linux

應用程式介面

PKCS #11

Microsoft CryptoAPI / CNG

Java JCE

OpenSSL

nCore

玉山科技股份有限公司
http://www.asiapeak.com
(02)77128295