nCIPHER

www.ncipher.com

nShield® 通用型
硬體安全模組(HSM)

Contents

您能信賴的安全性 3

nShield 系列產品 4

nShield Connect 4

nShield Edge 4

nShield Solo 4

支援各種廣泛應用 5

nShield 系列產品特色 6

適用雲端環境的網路服務介面(Web Interface) 6

nShield BYOK 為您的雲端資料提供更強大的金鑰管理功能 6

透過遠端監控及管理簡化維運作業 7

Security World 具備高度彈性的架構 7

CodeSafe - nShield 的安全執行環境 8

與業界領導廠商合作 9

多樣性及高效能 10

通過業界標準認證 11

FIPS 140-2 11

CC共同準則與eIDAS 11

了解更多資訊 11

您能信賴的安全性

nCipher Security 的 nShield 硬體安全模組(HSM)是經過強化的防篡改設備，可妥善保護您公司內最機敏的資料。這些通過 FIPS 140-2 認證的HSM可執行加密功能，如生成、管理、儲存加密和簽章金鑰，同時將您具機敏性的程式功能，在HSM內受保護的記憶體區塊執行。

nShield HSM 能強化您的安全架構，進而協助您：

- 達到更高層級的資料安全性與信賴度
- 符合且優於重要法規標準
- 維持高度服務等級及商業應用靈活度

nShield 系列產品

nShield 通用型HSM為配合您特有的使用環境，提供以下平台選擇：

NSHIELD CONNECT

網路連接設備

nShield Connect HSM 為分布在整個網路的應用程式提供加密服務。
nShield Connect HSM 提供兩種系列：一般型nShield Connect+ HSM 與高效能 nShield Connect XC HSM 系列。

NSHIELD EDGE

可攜式 USB 模組

nShield Edge HSM是以便利性和經濟效益而設計的桌機裝置。
Edge是開發人員的理想選擇，支援低用量、無效能需求的使用場景。

NSHIELD SOLO

可嵌入設備或伺服器的 PCIe 卡

nShield Solo HSM 具 PCI-Express卡介面，適合單機使用，能為伺服器或設備上的應用程式提供加密服務。
nShield Solo HSM 提供兩種系列：一般型nShield Solo+ HSM與高效能 nShield Solo XC HSM系列。

支援各種廣泛用途

nCipher 客戶使用 nShield HSM 作為不同商業應用程式的信任基礎，包括公開金鑰基礎設施(PKI)、SSL/TLS加密金鑰保護、程式碼簽章、數位簽章與區塊鏈。

隨著IoT物聯網的成長，裝置識別碼及憑證的需求也逐漸增加，nShield HSM將持續支援各種重要安全措施，如使用數位憑證作為裝置間的驗證機制。

nShield HSM 也支援多種加密演算法，包括ECC橢圓曲線加密演算法，最適合為現今緊湊的環境及業界最廣泛使用的作業系統及應用程式介面(API)，提供高速交易的演算能力。

nShield 系列產品特色

適用雲端環境的網路服務介面

選購 nShield Web Services Crypto API 能透過網路服務呼叫執行指令，簡化應用程式與HSM之間的介接。這項創新方法無須直接將應用程式整合至nShield，可加速部署，且不需仰賴作業系統及架構設計選擇。Web Services Crypto API 可介接架設在雲端及傳統數據中心的應用程式，是適用雲端環境的解決方案。

nShield BYOK 為您的雲端資料提供更強大的金鑰管理功能

nShield BYOK 讓您在本地端的nShield HSM生成高強度的金鑰，並能安全地將金鑰匯出至雲端應用程式，無論是在AWS、Google Cloud Platform、Microsoft Azure，或是三者皆具的雲端環境。

透過 nShield BYOK，您不僅能強化金鑰管理實務的安全性，更能妥善控管金鑰，確保雲端資料的安全。

nShield BYOK可創造以下效益：

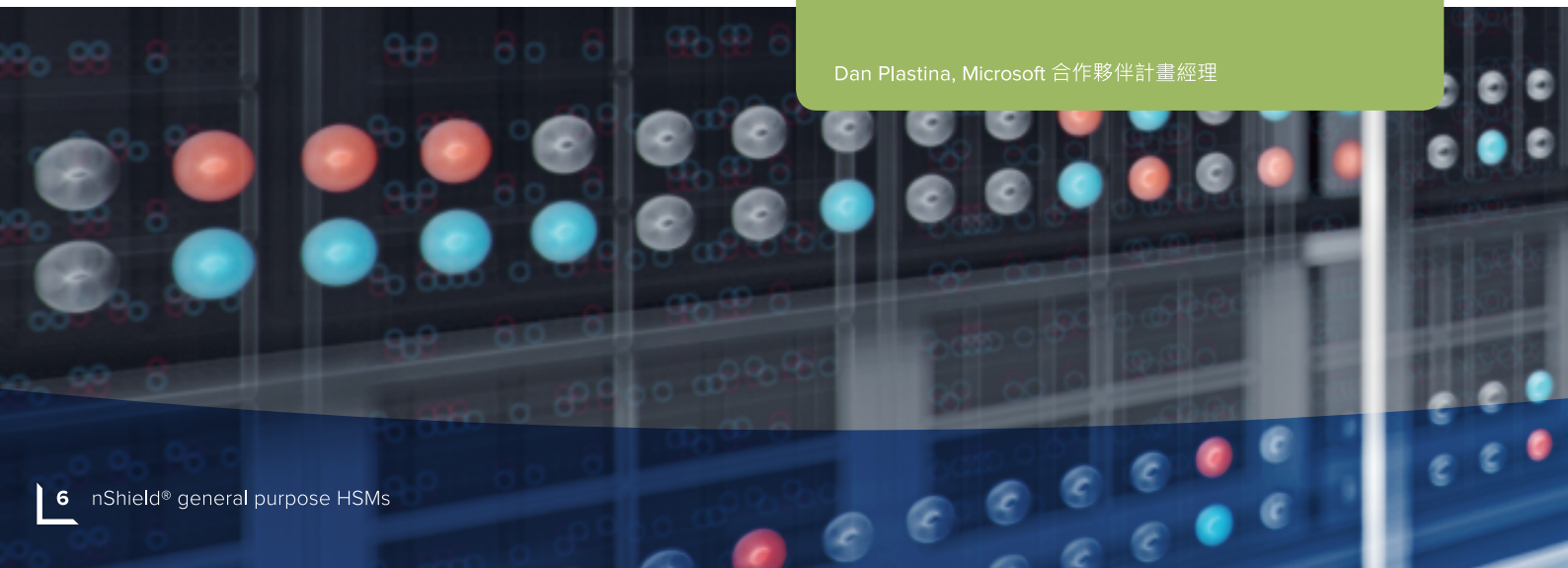
- 提高金鑰管理實務安全，強化雲端機敏資料的安全
- 透過nShield的亂數產生器產出更高強度的金鑰，並由通過FIPS認證的硬體加以保護。
- 更好的金鑰管控力 - 使用企業在本地端的 nShield HSM 來產出金鑰且安全地匯出至雲端。

Azure　aws

Google Cloud

「由於我們的合作，客戶能自行產出主金鑰並上傳至雲端HSM，對金鑰的完全掌控也讓客戶確信其資料確實受到保護。」

Dan Plastina, Microsoft 合作夥伴計畫經理



透過遠端監控及管理簡化維運作業

nShield Solo與Connect HSM提供nShield Monitor和 nShield Remote Administration，協助您降低維運成本，並能隨時掌握資料、進行 HSM 設備24x7的全天候運作。

nCipher遠端監控和管理產品能協助您：

- nShield Monitor 可優化 HSM 性能、基礎設施規劃及正常運作時間，並提供管理人員負載趨勢、使用情形統計、篡改事件、警告和告警等資訊。
- 透過 nShield Remote Administration 強大而安全的介面來管理HSM，可降低差旅成本並節省時間。

Security World 具備高度彈性的架構

nShield HSM 是 nCipher Security World 架構不可或缺的一環，可建構獨特、靈活的金鑰管理環境。透過 Security World，您可以整合不同的 nShield HSM 機型，建立一致系統環境，提供可擴充性、無縫備援機制及負載平衡。

無論您部署一台還是數百台HSM，Security World 都能提供跨平台的操作，讓您管理無限量的金鑰，並自動遠端備份、恢復金鑰資料。

nShield Security World 具備以下優點：

- 可隨需求成長，輕鬆擴充 nShield HSM 設備
- 維持系統彈性
- 無須費時進行 HSM 備份，節省時間

「nShield HSM一直是提供兼具卓越性能與可擴充性服務的重要構件。」

Steve Collins, Barclays 新興市場群總監

「nCipher nShield HSM 提供快速有效的方法來取得新金鑰。我們對 CodeSafe 的功能尤其印象深刻，讓我們能在 HSM 範圍內執行受到保護的安全關鍵程式碼。所有功能皆渾然天成。」

Ryan Smith, Chain 技術長

CodeSafe - nShield 的安全執行環境

除了保護機敏金鑰外，nShield Solo 和 Connect HSM 還能提供安全環境，執行您專有的應用程式。CodeSafe 選購品項讓您能在 nShield 具備 FIPS 140-2 Level 3 標準的範圍內，開發、執行程式碼，保護應用程式免於潛在攻擊。

CodeSafe 可協助您：

- 在通過認證的環境內，執行機敏應用程式並保護應用程式數據端點，進而達到高可信度
- 保護機敏應用程式免於內部攻擊、惡意軟體及進階持續威脅(APT)等危害
- 使用程式碼簽章，排除未經授權的應用程式變更或感染惡意軟體等風險

與業界領導廠商合作

nCipher 與領導技術廠商合作，提供強化解決方案來解決各種產業安全挑戰，並協助客戶實現數位轉型的目標。透過 nCipher 技術合作夥伴計畫，nCipher 與合作夥伴攜手共事，將 nShield HSM 整合至各種安全解決方案中，包括認證、PKI、資料庫安全、程式碼簽章、數位簽章、特權帳戶管理、應用程式交付、雲端及大數據應用等。

nShield HSM 支援合作夥伴的安全應用程式，藉此提供最強大的加密處理、金鑰保護和金鑰管理功能，同時加速對政府和產業資料保護規範的合規。

「F5對 nShield HSM的支援，為加密金鑰帶來最高等級的實質保護，使企業能夠達到最新政府規範和安全架構的合規要求。」

Siva Mandalam, F5 Network 產品管理部資深協理

「我們為眾多不同的企業提供管理服務 PKI，而我們管理的 PKI 解決方案，全部仰賴 nShield HSM，因其具備強大安全性和操作簡便性，可用於金鑰備份等關鍵功能。」

Robert Hann, Trustis 業務開發協理

多樣性及高效能

nShield Connect 和 Solo HSM 具備三種效能等級可供選擇，以符合您的環境需求，無論您的交易量多寡或應用程式所需的效能高低，nShield HSM 均可滿足。

通過業界標準認證

nCipher通過嚴格標準，不僅協助您在法規環境下證明合規性，同時讓您對nShield HSM安全性及完整性充滿信心。以下如列幾項我們所通過的認證標準，完整內容請見nCipher官網。

FIPS 140-2

全球公認的FIPS 140-2是美國政府NIST標準，能驗證加密模組的安全穩定性。nCipher旗下所有nShield HSM產品均通過FIPS 140-2 Level 2和Level 3認證，您可依需求購買所需級別。

CC共同準則與EIDAS

nShield Solo+ 和 Connect+ 平台通過CC (EAL)4+認證，且被核准為合格簽章創建設備(QSCD)。nShield HSM 作為 QSCD，有充分的能力可成為歐洲數位簽章 (eIDAS) 、驗證服務、數位簽章和時間戳記等全球認可解決方案的安全骨幹。

了解更多資訊

請至 nCipher 官網 www.nCipher.com/products/general-purpose-hsms，進一步了解我們如何在本地端、雲端及虛擬環境下，保護您的關鍵業務資料和應用程式。

www.ncipher.com

關於 nCipher Security

當今快速發展的數位環境，提高了客戶滿意度、競爭優勢和經營效率，卻也同時增加了安全上的風險。nCipher Security 是通用型硬體安全模組(HSM)的領導品牌，為世界頂尖企業的重要業務資訊和應用程式提供可信度、完整性與管控力。

nCipher Security 的加密解決方案可以保護雲端應用、IoT物聯網、區塊鏈、電子支付等新興技術，並滿足各種合規要求。nCipher Security 提供客戶所需的成熟技術來保護機敏資料、網路通訊和基礎設施免於威脅。任何時候，nCipher Security 都能為您的關鍵業務應用程式提供可信度，確保資料的完整性，並給予您充分的管控力。

了解更多資訊，請到 www.ncipher.com

Search: nCipherSecurity

TRUST. INTEGRITY. CONTROL.