

解決方案手冊

# nShield® 通用硬體安全模組

Cyberworld 科明大同

ENTRUST
SECURING A WORLD IN MOTION

# 目錄


您可信賴的安全性 3

nShield 系列產品 4

支援多種用途 5

nShield 系列功能特色 6

與產業領導者合作 10

多功能性與高性能 11

為企業 KMS 而設的 nShield 信任根 11

業界標準認證 11



# 您可信賴的安全性

Entrust nShield 硬體安全模組 (HSM) 是經過加固的防篡改裝置，可保護您公司最敏感的資料。這些獲得 FIPS 認證的模組可執行加密功能，例如產生、管理及儲存加密和簽署金鑰，以及在其受保護的邊界內執行敏感功能。

nShield HSM 可讓您的安全堆疊如虎添翼，幫助您：

- 實現更高層級的資料安全性及信任度
- 滿足並超越重要監管標準
- 運用量子安全技術為資料安全性提供未來保障

# nShield 系列產品

為了滿足您的特定環境需求，nShield 通用 HSM 系列包含下列機型：

## 網路連接式 HSM

nShield HSM 可為分佈於網路上的應用程式提供加密服務。提供功能強大的 nShield 5c 全新機型及既有的 nShield Connect XC 成熟機型。



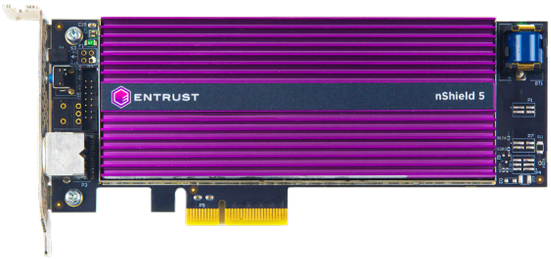

## 可攜式 USB HSM

nShield Edge HSM 是為操作簡便及價格經濟而設計的桌上型裝置。nShield Edge 是開發人員的理想選擇，並且支援小量根金鑰產生等應用。




## PCIe 嵌入式 HSM

nShield HSM 採用小尺寸 PCIe 卡的形式，可為伺服器或裝置上託管的應用程式提供加密服務。提供一系列較新的 nShield 5s 高規格機型及既有的 nShield Solo XC 成熟機型。




## nShield 雲端服務

以訂閱為基礎的模式，提供對專用 FIPS 認證 nShield HSM 的存取權。它具備與地端 HSM 相同的特性及功能（包括支援後量子演算法），同時結合雲端服務部署的優點。這可讓客戶實現雲端優先目標，並將這些裝置的維護作業交由 Entrust 專家負責。

有了 nShield 雲端服務，您便擁有自己的金鑰（而非 HSM）。由於它採用與地端 nShield HSM 部署相同的獨特 Security World 金鑰管理架構，您可以輕鬆將密碼作業從地端遷移至雲端 —— 或採取混合模式，混合使用地端及雲端 HSM，以增強備援能力及可靠性。

nShield 雲端服務現已在歐盟（德國）、英國、美國及澳洲的完全備援資料中心推出。區域資料中心可支援地理圍欄，以便滿足雲端資料安全及資料主權要求。我們可提供一系列服務選項以因應各種客戶需求。對於價格敏感的客戶，可在客戶偏好的地點提供自我管理的單一 HSM 實作。標準版、進階版及企業版客戶可指定首選 HSM 位置，以滿足其營運、災難復原和資料主權需求，同時選擇最適配的效能及價位。

# 支援多種用途

Entrust 客戶使用 nShield HSM 作為各種商業應用的信任根，包括：

- 公鑰基礎建設 (PKI)
- TLS/SSL 加密金鑰保護
- 程式碼簽章
- 數位簽章
- 5G 電信應用
- 區塊鏈

隨著物聯網 (IoT) 的成長帶動對裝置 ID 及憑證的更大需求，nShield HSM 將繼續支援關鍵的安全措施，例如使用數位憑證執行裝置驗證。

nShield HSM 也支援各種加密演算法，包括：

- **全新 NIST 標準化抗量子演算法**幫助您為未來的後量子時代做好準備
- **橢圓曲線加密演算法**非常適合現今的低功耗運算環境，例如智慧電錶裝置
- **5G 相容演算法** 適用於電信應用

# nShield HSM 系列功能特色

## 雲端友善的 Web 服務介面

nShield Web Service RESTful 介面提供創新的部署方式，無需直接將應用程式與 nShield 整合，並且摒除對作業系統及架構設計選擇的依賴。

## 後量子安全保障

nShield HSM 系列的設計目標是透過支援後量子加密演算法，協助組織為量子未來做好準備。nShield HSM 符合 NIST 的後量子加密標準化標準，可支援您採用具備硬體加速性能的抗量子安全技術。



## 為地端或雲端提供容器化支援

nShield Container Option Pack 可助您無縫開發及部署以我們高度保證 HSM 為基礎的容器化應用程式或程序。此選項提供一套預先配套的腳本，可大幅簡化將 nShield HSM 整合至容器應用環境的作業，同時支援應用程式和容器化主機的動態擴充需求。

## 利用 Entrust 的 nShield 雲端整合選項套件為您的雲端資料提供更強大的金鑰管理

nShield Cloud Integration Option Pack 支援自帶金鑰 (BYOK) 部署，無論您使用的是 Amazon Web Services、Google Cloud Platform、Microsoft Azure 或 Salesforce，都能讓您在地端部署的 nShield HSM 內產生強大的金鑰，並安全輸出至您的雲端應用程式。透過 BYOK，您可加強金鑰管理實作的安全性、獲得對金鑰更大的控制權，並確保您能分擔保護雲端資料安全的責任。

BYOK 結合 nShield HSM 可為您帶來以下優勢：

- 更安全的金鑰管理實作，加強雲端敏感資料的安全性
- 使用受 FIPS 認證硬體保護的 nShield 高熵隨機數產生器，強化金鑰產生
- 在您自己的環境內使用自己的 Shield HSM 建立金鑰並安全輸出至雲端，同時保留您自己的備份，進而加強對金鑰的控制

## 利用自持金鑰 (HYOK) 實現最大的金鑰控制

受管制之產業的選擇一般取決於安全與資料處理政策、政府要求（例如資料主權考量）以及組織的整體安全勢態。資料主權最近成為歐盟的燙手山芋，Schrems II 案件的判決結果令超過 5,000 家歐盟企業組織不得不審慎思考其加密金鑰及加密資料的儲存位置。為此，雲端服務供應商 AWS 推出其金鑰管理服務外部金鑰存放區 (AWS KMS XKS)，讓企業組織能夠掌控其地端或雲端解決方案中的加密金鑰，自行擁有、持有及管理這些金鑰而完全獨立於 AWS 生態系統之外。nShield HSM 可與 AWS KMS XKS 無縫整合。在 Microsoft Azure 資訊保護 (AIP) 環境內，nShield HSM 可支援雙重金鑰加密，協助企業保護 Microsoft 365 中最敏感的內容。

## 使用遠端管理簡化運作

nShield 網路連接及 PCIe HSM 適用的 nShield 遠端管理可幫助您：

- 降低運作成本，同時全天候掌握 HSM 資產的動態。
- 使用 nShield Monitor 向您的員工提供有關負載趨勢、使用統計數據、篡改事件、警告及警報的資訊，實現最佳化的 HSM 效能、基礎設施規劃及正常運作時間。
- 透過強大且安全的介面輕鬆管理 HSM，從而減少差旅成本並節省時間。

## 遠端組態設定

nShield 網路連接機型提供序列控制台選項，將 HSM 的實體安裝簡化成架設、佈線及通電三步完成。而所有其他 HSM 和網路組態設定均可透過遠端執行。無需重新造訪資料中心，即可輕鬆完成部署及重新部署。此功能支援供應商/租戶模式，由供應商控制網路組態，而租戶則可完全控制其重要資料。

## 高度靈活的 Security World 架構

nShield Security World 透過建立獨特、靈活的金鑰管理環境支援 Entrust nShield HSM。它可讓您結合不同的 nShield HSM 機型，建立一個統一的生態系統，提供可擴充性、無縫故障轉移和負載平衡。無論您部署一個或數百個 HSM，都能提供互通操作性，讓您管理不限數量的金鑰，並可自動從遠端備份及還原金鑰資料。

nShield Security World 提供以下優勢：

- 協助您隨著需求成長輕鬆擴充 nShield HSM 資產
- 保持系統韌性
- 摒除耗時的 HSM 備份，節省時間

## 利用 KeySafe 5 提供集中遠端管理

Entrust KeySafe 5 提供集中及遠端管理設定與組態的能力，可查看 Security World 可擴充式架構的狀態，適用於 nShield 及 nShield 雲端服務 HSM 的混合資產。

## 保護執行環境

除了保護您的敏感金鑰之外，nShield 網路連接式 HSM 及 PCIe HSM 也為您的專有應用程式運作提供一個安全的環境。CodeSafe® 軟體開發人員工具套件可讓您在 nShield HSM 的 FIPS Level 3 實體邊界內開發及執行程式碼，保護您的應用程式免受潛在攻擊。

CodeSafe 工具套件可協助您：

- 在經過認證的環境內執行敏感應用程式並保護應用程式資料端點，實現高保障度
- 保護安全敏感應用程式免受內部人員攻擊、惡意軟體和進階持續性威脅等危害
- 使用程式碼簽章解除未經授權的應用程式變更或惡意軟體感染的風險
- 使用在 nShield HSM 的 FIPS 邊界內執行的後量子選項套件與 CodeSafe 軟體開發工具套件，部署後量子演算法（如 LMS）

## 支援加密敏捷性

加密敏捷性是指組織無縫採用新興加密方法的能力。隨著第一波後量子加密演算法的標準化以及其他演算法的持續推出，此能力更顯重要。

nShield 5 HSM 透過其安全處理器提供開箱即用的加密敏捷性，這是一個可透過軟體更新隨時重新編程的現場可程式化閘陣列 (FPGA)。這可減少昂貴且耗時的硬體更新，並且提高對量子電腦的防禦能力，量子電腦可能破壞我們目前所依賴的加密技術。

在我們準備迎接量子電腦挑戰的來臨之際，HSM 對於 IT 系統、雲端和網際網路的安全性和信任度至關重要。nShield 5 HSM 原生支援 ML-DSA 等 NIST 標準化 PQC 演算法。



# 與產業領導者合作

Entrust 與領先的技術供應商合作提供強化的解決方案，以應對廣泛的產業安全挑戰，並協助客戶達成數位轉型的目標。透過 Entrust Ready 技術合作夥伴計劃，我們與合作夥伴協力合作，將 nShield HSM 整合至各種安全解決方案中，包括：

- 憑證及 PKI
- 資料庫安全
- 程式碼簽章
- 數位簽章
- 特權帳戶管理
- 5G
- 應用程式交付
- 雲端智慧
- 大數據智慧

nShield HSM 支援我們合作夥伴的安全應用程式，提供最強大的加密處理、金鑰保護及金鑰管理，同時促進遵循政府和產業資料安全法規。

我們對於 nShield 的全新雲端友善功能（包括 nShield 雲端服務）為客戶帶來的可能性感到興奮。這些新功能充分體現市場正在發生變化；企業需要雲端全方位服務 HSM 的功能，才能釋放創新和商業優勢。」

**MATT LANDROCK · CRYPTOMATHIC 企業總監**

「Entrust 推出的 nShield 雲端服務為 F5 客戶提供更多安全選擇，讓他們能以訂閱為基礎的模式實現資料主權。將安全從資本支出轉為營運支出，為組織帶來更大的靈活性及成本效益。」

**JOHN MORGAN · F5 NETWORKS 安全副總裁兼總經理**

「Entrust nShield HSM 是最先進的技術，讓我們能在自己的技術中使用更精密、更安全的晶片」。

**BILL KAVADAS · MEMJET 資訊系統資深總監**

# 多功能性與高性能

nShield 網路連接 HSM 和 PCIe 規格 HSM 提供三種效能級別，不論您的交易速率適中，或者您的應用程式需要高傳輸率，都能滿足您的環境需求。nShield 雲端服務是我們採用訂閱模式的解決方案，以我們最高效能的網路連接 HSM 為基礎，可讓您在雲端存取 nShield HSM。

# 為企業 KMS 而設的 nShield 信任根

如果您的組織正在尋找以 HSM 信任根為基礎的企業金鑰管理服務，請考慮 Entrust 加密安全平台。其金鑰與機密管理解決方案結合傳統的金鑰生命週期管理、分散式儲存庫架構以及全面的中央政策與合規管理儀表板，因此可重新定義加密金鑰管理。此平台可跨越企業的密碼生態系統提供分散式的安全性與集中式的可視性 —— 如此強大的組合將有助於確保資料受保護，同時符合嚴苛的合規要求。

Entrust 加密安全平台可滿足在日益複雜的數位環境中全面加密資產管理之不斷增長的需求。它以 nShield HSM 信任根為基礎，結合豐富的功能操作 PKI、憑證生命週期管理、金鑰管理和機密管理，從而統一密碼管理。

# 業界標準認證

Entrust 遵循嚴苛的標準，可協助您在受監管的環境中展現合規性，同時對 nShield HSM 的安全性及完整性提供高度信心。以下是我們遵守的部分標準清單。完整清單可參見我們的網站及產品說明書。

### FIPS 140-2/FIPS 140-3

全球公認的聯邦資訊處理標準 (FIPS) 140-2 是美國國家標準暨技術研究院 (NIST) 的認證，用於驗證加密模組的安全性穩健度。2022 年，該標準由新的 NIST FIPS 140-3 標準取代。nShield Solo XC 和 Connect XC HSM 已通過既有的 FIPS 140-2 標準認證。nShield 5s 和 5c 已通過新的 FIPS 140-3 3 級標準認證。

FIPS Level 3 Validated 140-2

FIPS 140-3™

通過 FIPS 140-3 驗證，
4745 號憑證

## 符合共同準則及 eIDAS

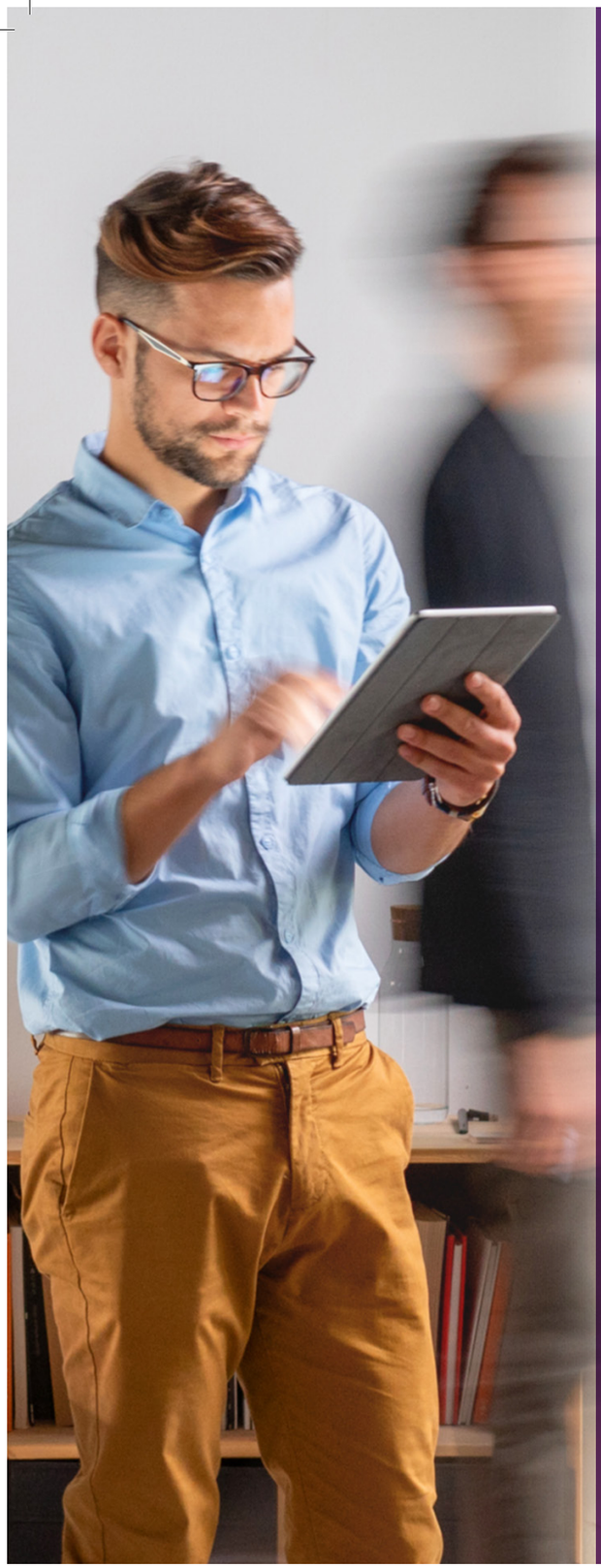
nShield XC 和 nShield 5 HSM 已通過共同準則 EAL4+ 認證，並獲得 eIDAS 法規認可為合格簽章產生裝置 (QSCD)。我們已通過共同準則 EAL4+ 認證的 Entrust Remote QSCD 可支援 TSP 和簽章系統整合商 (SI) 提供符合現行 eIDAS 法規且經 eIDAS 認證的遠端簽章服務。Entrust Remote Type 2 QSCD 結合 **Entrust 簽章啟動模組 (SAM)** 與 **Entrust Solo XC HSM**，可建立高度安全且滿足未來需求的遠端簽章及標章服務所需的信任根。

此外，nShield XC 和 nShield 5 HSM 符合共同準則保護輪廓 EN 419 221-5「信任服務加密模組」。因此，nShield HSM 可作為歐盟成員國和企業數位化的安全骨幹。這包括啟用國家身分證計畫和跨境服務、合格的電子文件和交易簽章服務，以及身分驗證、時間戳記、安全電子郵件和長期文件保存服務。這些認證是作為歐洲法規之一部分建立，並持續獲全球許多國家採用。

Common Criteria

## 如需更多資訊

請造訪 **entrust.com/HSM** ，了解我們如何保護您在地端、雲端及虛擬環境中的業務關鍵資訊和應用程式。



## 關於 ENTRUST

Entrust 透過以身分為核心的全面安全解決方案保護人員、裝置及資料，抵禦詐欺和網路威脅。

我們的解決方案可協助企業和政府全方位保護關鍵系統，實現安全註冊上線及簽發，提供日常身份保護，並賦予跨金鑰、機密和憑證的 360 度可視性及協調能力，讓他們能自信地交易及擴充業務。深耕於我們數十年來作為建立信任先驅與創新者的地位，Entrust 擁有全球性的合作夥伴網路，支援超過 150 個國家地區的客戶。

Cyberworld 科明大同 | 中国区总代理

公司网站 www.cyberworld.com.cn
业务联系 info@cyberworldchina.com
售后支持 support@cyberworldchina.com

关注公众号

©2025 Entrust Corporation。保留所有權利。Entrust、Datacard 及六角形標誌為 Entrust Corporation 在美國及/或其他國家的商標、註冊商標及/或服務標誌。所有其他品牌或產品名稱均為其各自所有者的財產。HS26Q1-nshield-family-br

entrust.com

ENTRUST
SECURING A WORLD IN MOTION