www.ncipher.com

使用 nCipher 服務與 HSM 硬體安全模組部署、維護安全的身份辨識管理解決方案

- 保護個人身份與裝置
- 開展正確的流程與步驟
- 評估現有 PKI 部署的妥適性
- 移轉 PKI 以滿足擴展需求
- 加速資安稽核與合規

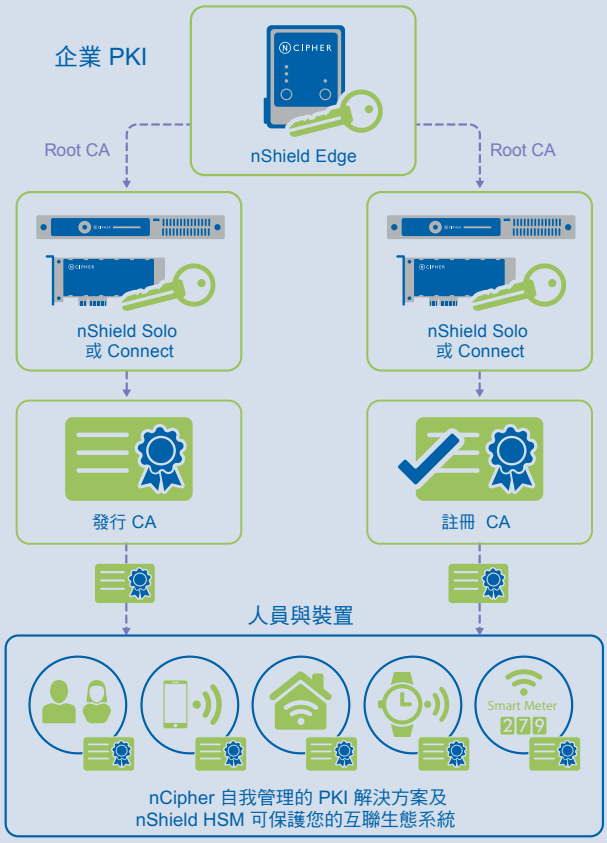
nCipher 提供能自我管理的 PKI 解決方案，以滿足企業特定的安全需求

問題：隨著互連技術採用的增加，公鑰基礎設施 (PKI) 的運用也日益提升，新的 PKI 系統建立需求亦隨之而生。

隨著可加密應用程式的使用增加及 IoT 物聯網的影響，對 PKI 也出現前所未有的新需求。 擴大憑證運用的需求，以及將設備和感測器安全連接到密不可分的網絡生態系統的管理需求，正促使企業重新評估其現有 PKI 的妥適性。 隨著資安標準的改變，企業也重新思考其 PKI 實施策略，並在某些特定情況下重新設計並移轉成更新、更強大的部署。

挑戰：在企業 PKI 中維持強健的安全信任根，並滿足對機敏應用程式的運作需求。

對使用 PKI 的機敏應用程式來說，保護基礎私鑰的安全相當重要。 根據 2018 年 Ponemon Institute 的 PKI 趨勢研究顯示，使用數位憑證的前五大應用，分別為供大眾瀏覽的網站 SSL / TLS、虛擬專用網路、公有雲端應用程式、email 電子郵件及設備身份驗證。 數位憑證可用來識別應用程式與設備，並為可信的生態系統進行身份驗證 (authentication)。 這需要透過自動、可信的方式保護管理越來越多的私鑰。



nCipher 提供能自我管理的 PKI 解決方案以滿足企業特定的安全需求

解決方案：NCIPHER 自我管理的 PKI 解決方案結合顧問服務與正確的安全硬體，協助客戶從確認需求、部署到訓練的每個階段。

企業的 PKI 需求通常因人而異，取決於其業務、客戶和所支援的應用。 nCipher 自我管理的PKI 解決方案結合對 PKI 設計、執行的技術專長，以及為系統提供強大安全信任根的安全硬體。 服務包括初步需求評估和步驟、流程的開展，以及設計、執行所需的基礎設備，確保客戶能部署滿足當前和未來需求的 PKI。

顧問服務可協助需要高可用性、備援性，或是有實驗室環境的操作設定，幫助客戶發展自身的 PKI 能力。 對於首次部署 PKI 的客戶，將提供文件化和結合安全硬體的部署服務。至於已部署 PKI 和增加 PKI 部署的客戶，則將提供妥適性檢查和移轉服務，包括結合安全硬體的 SHA 移轉服務。

nCipher nShield HSM 硬體安全模組提高了 PKI 部署的保障層級，可保護、管理受認證隔離環境中的基礎私鑰。nCipher nShield HSM 使用標準加密應用程式介面 (CAPI)，支援 Microsoft、Red Hat、Entrust、RSA、Safelayer 和 Insta。

為什麼要用 NCIPHER HSM及自我管理PKI 解決方案

由於重要機敏應用程式和連網設備的部署增加，帶動更多對 PKI 的需求，希望能保護跨領域發佈的個人和設備憑證之 Root CA 私鑰和憑證的註冊登記。

未使用 HSM 保護私鑰的 PKI，可能容易受到駭客攻擊而產生嚴重後果。 HSM 提供一個強化的環境，可保護重要機敏的私鑰，免於被竊或盜用，並支援故障切換 (failover)，達到完整的生命週期管理。 從 CA 安全性遭到破壞的案例中，我們了解到，透過 HSM 將憑證發行結合身份檢查及核准是必要的。nCipher nShield HSM 除了通過嚴格的安全標準認證，包括 FIPS 140-2 Level 3 ，共同準則 CC EAL 4 +) ，還能滿足以下需求：

- 將 Root CA 和註冊金鑰儲存在安全且防篡改的環境中
- 透過以智能卡為基礎的政策和雙因子認證，進行管理者存取權限管理
- 滿足公部門、金融服務和企業的監管合規要求

NCIPHER

nCipher nShield HSM 簡化整個企業（包括虛擬化環境）的身份憑證管理，幫助組織滿足稽核及合規要求，如 PCI DSS。nCipher HSM 提供以下型號，可滿足不同客戶的特定需求：

- nShield Edge：USB 介面可攜式 HSM，供離線 Root CA 及開發者應用程式使用
- nShield Solo / Solo+ / Solo XC：PCIe 卡介面的高效 HSM，供單一伺服器使用
- nShield Connect / Connect+ / Connect XC：可連接網路的高效 HSM，供資料中心使用

了解更多資訊

進一步了解 nCipher Security 如何為您的關鍵業務資訊和應用程式提供可信度、完整性和管控力，請到 ncipher.com