nCIPHER
AN ENTRUST DATACARD COMPANY

www.ncipher.com

兼具便利性與安全性的雲端

- 更安全的金鑰管理實務作法，以強化對雲端上敏感性資料的保障
- 透過使用經由美國聯邦資訊處理標準（FIPS）認證的硬體來保護的 nShield高熵隨機亂數產生器來生成更高強度的金鑰
- 加強金鑰的控管能力 — 在您內部環境使用自己的 nShield HSMs來建立金鑰，並將金鑰安全地匯出至雲端
- 不論您的金鑰是用在雲端還是內部部署，均可享更一致的金鑰管理操作

nShield 自帶金鑰（BYOK）

協助雲端客戶加強數據安全控管

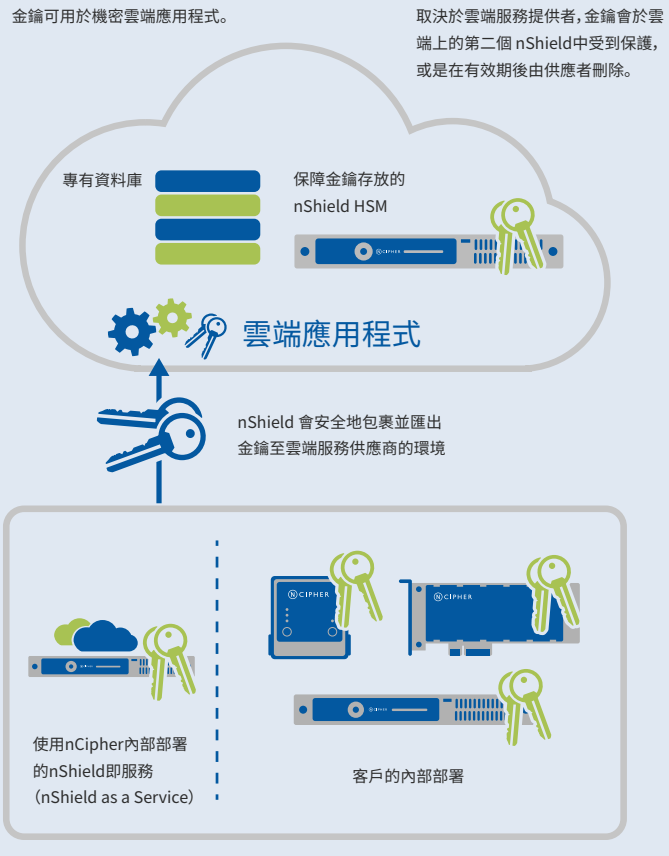
透過 nCipher Security 的 nShield 硬體安全模組（HSMs），無論您使用的是 Amazon Web Services（AWS）、Google Cloud Platform（GCP）或 Microsoft Azure，您都可以自帶金鑰（BYOK）到雲端應用程式。

nShield 高保證HSMs使您能夠繼續享受雲端服務的靈活性與經濟效益，同時強化您的金鑰管理實務之安全性，更有效地控管您的金鑰。

Azure

aws

Google Cloud



nCipher 獨特的 Security World 架構為主金鑰（Master Key）提供安全的長期存放和災難復原保護。

nShield 自帶金鑰 (BYOK)
功能概述

nShield BYOK 有哪些功能

透過 nShield BYOK，您可以使用您的 nShield HSMs來生成、儲存和管理您的金鑰，以保護雲端上運行的機密應用程式、資料庫和儲存的大量資料。nShield BYOK提供下列功能：：

- 仰賴硬體信任根 (Root of Trust)。您的 nShield HSMs是值得信賴，且符合美國聯邦資訊處理標準 (FIPS) 140-2 第3 級認證的防篡改設備。這些 HSMs做為您雲端服務的信任根，讓您能夠安全地生成及保護您的加密和簽署金鑰。
- 使用 nShield 來管理您的金鑰。當存放敏感性資料於雲端上裝載的應用程式時，您可以倚賴nShield HSMs來生成和包裹您的金鑰，並將金鑰安全地傳輸到雲端應用程式。
- 掌握金鑰的可用性。由於您擁有nShield HSMs的專屬控制權，不論是在內部部署，還是使用nShield即服務 (nShield as a Service)，您均可決定何時生成和匯出金鑰。透過控制主金鑰，您還可以掌握何時以及是否進一步將其匯出至雲端供應商。
- 選擇您的雲端供應商。透過 nShield BYOK，您可以決定每個雲端供應商使用的金鑰。這讓您能夠靈活地從您的內部部署或nShield即服務 (nShield as a Service) 環境中，為不同的應用選擇適當的雲端服務，同時都能受惠於 nShield 高保證的金鑰生成與保護。

nShield BYOK如何運作

在nCipher的機制下，您可以使用您的 nShield HSM 來生成金鑰、保障長期存放，並將金鑰匯出到雲端。當金鑰從您的內部部署或nShield即服務 (nShield as a Service) 環境中匯出到雲端後，您將根據下列其中一種方式來管理金鑰：

如果您正在使用 AWS 或 GCP...

您將把金鑰暫借（lease）給 AWS 或 GCP，以供在雲端中臨時使用。在預設的時間後，您於雲端的金鑰將被銷毀。如有需要，您可以再次借出儲存在 HSM 中的金鑰。

如果您正在使用 Microsoft Azure...

您將把金鑰安全地傳輸到在 Azure 基礎設施中運行的 nShield HSM，因此兩端均可享受HSM的安全保障。

無論您選擇那一種公共雲端服務，生成自己專屬的金鑰並控制其匯出，均有助您為雲端中的敏感性資料和應用程式建立強大的保障

開始使用nShield BYOK

如要開始於AWS、GCP或Azure使用 nShield BYOK，您會需要一個 nShield HSM。您可以選擇下列方案：

- nShield Connect：網路連接的設備。
- nShield Solo：崁入於伺服器的PCIe 卡。
- nShield Edge：USB 外接裝置，適合小批量的應用。
- nShield 即服務（nShield as a Service）：使用基於訂閱的nShield Connect HSMs。

如要在AWS或GCP上使用nShield BYOK，您需要以下 nCipher 套件：

Cloud Integration Option Pack

此Option Pack包含所有您於使用內部nShield HSMs時需要的工具，以生成並借用（lease）你的金鑰給AWS或GCP。
您可以自行將 nShield BYOK 與 AWS 或 GCP 整合，也可以使用 nCipher 專業服務協助您無縫及有效地連線。

如要在Azure上使用nShield BYOK，您可以選購以下套件：

自帶金鑰，Azure Professional Services

此套件包括 nShield Edge、nCipher 專業服務團隊提供的整合服務，以及一年的維護。
您亦可以分別購買 nShield Connect、Solo 或 Edge HSMs 和其他專業服務。

了解更多

若要進一步了解 nCipher Security 如何為您關鍵的資料與應用系統提供可信度，確保資料的完整性，並給予您充分的管控力，請造訪 nCipher.com。