NCIPHER

www.ncipher.com

CodeSafe：在安全環境中執行程式碼

- 在防篡改硬體安全模組（HSMs）內執行機密應用系統，以保護其資料安全
- 透過數位簽章和驗證程式碼，協助確保資料的完整性
- 透過執行政策規定，提供一個安全的金鑰管理環境
- 將金鑰和憑證獨立地連結至應用系統，以提供強大的存取控制
- 以遠端 CodeSafe 工具提供便利的方案

nCipher Security CodeSafe®

經認證適用於機密應用系統之硬體保護工具

nCipher Security CodeSafe®

CodeSafe 是一組可讓開發人員在符合美國聯邦資訊處理標準（FIPS）認證之 nShield HSMs 防篡改保護範圍內編寫和執行機密應用系統的工具。應用系統在安全的執行環境中運行，可作加密、解密和資料處理，同時也可受益於 HSM 用以管理應用系統之金鑰的政策。

支持廣泛的應用系統

CodeSafe可用以保護任何類型的應用系統，當中包括與銀行業務、智慧型電表、驗證代理、數位簽章代理及自訂加密程序等相關的加密技術和商業邏輯。

確保 CODESAFE 應用系統的完整性

CodeSafe 提供工具，在 nShield 的安全執行環境中對應用系統進行數位簽章，因此能在執行期間透過 HSM 驗證簽章的完整性。

CODESAFE 關鍵政策執行和存取控制

CodeSafe 讓軟體持有者可定義管理使用應用系統數據 — 包含金鑰和憑證 — 的政策並會執行這些政策，以提供安全的金鑰管理環境。同時，CodeSafe 將金鑰和憑證獨立地連結至應用系統，以確保強大的存取控制。

安全的 SSL/TLS 端點

CodeSafe 應用系統開發人員可在系統中嵌入OpenSSL函式庫，以終止 nShield HSM 內的 SSL/TLS 會話，以便進行端對端加密、加強數據傳輸層的安全性，以及減少攻擊面。

遠程部署和更新

管理員可以從中央位置進行應用系統的部署，無需實際前往存取 HSMs。

nShield 的相容性

CodeSafe 可用於 FIPS 140-2第3 級認證的 nShield Solo PCI-e 和網路附加的 nShield Connect HSMs。相容型號包括所有支援的 nShield Solo 和 Connect HSMs 產品，包括 XC 系列。

HSM 開發環境

CodeSafe能與以下程式設計應用系統相容：

- 內嵌應用系統的 C 和 C++ 程式語言
- 主機伺服器上的 C、C++ 和 Java

開始使用CODESAFE

如欲使用 CodeSafe，您需要：

- FIPS 140-2第3 級認證的 nShield Solo 或 Connect HSM
- CodeSafe 開發人員工具包
- CodeSafe 啟動授權

CodeSafe 開發人員工具包內含教程、相關文件和程式範例，協助您整合您的應用系統和 nShield HSMs。nCipher 專業服務團隊亦會提供專業服務協助您進行整合。

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。