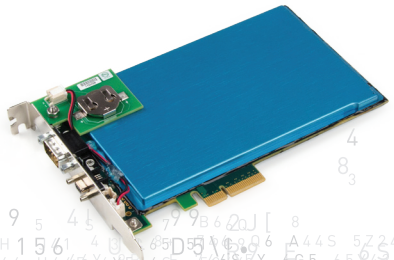
SafeNet
THE DATA PROTECTION COMPANY



ProtectServer Internal-Express

產品簡介

取樣檢查使用者應用程式

- 加密，包含資料庫
- 使用者和資料驗證
- 郵件完整性
- 安全金鑰儲存
- 電子商務金鑰管理
- PKI 金鑰管理
- 電子文件管理
- 電子帳單處理及支付 (EBPP)
- EFT 交易

優點

效能

- 專用的密碼編譯電子化功能，可卸載主機的工作量

安全性

- 通過 FIPS 140-2 Level 3 認證
- 具備防竄改能力的環境

易於管理

- 直覺的 GUI
- 命令列介面
- 就地安全韌體升級
- 網路 HSM 遠端管理

ProtectServer Interlal-Express 為需要高效能對稱和非對稱密碼編譯運作的伺服器和應用程式，提供具防竄改效能的安全硬體。

不同的效能等級

SafeNet ProtectServer Internal-Express 是一張相容於 PCI Express x4 的介面卡，有多種不同效能等級以符合各種系統需求：25、220 或 600 RSA 1024 位元簽章 (每秒)。

多種密碼編譯處理功能

ProtectServer HSM 具備安全儲存和專用的密碼編譯處理器，可提供高速的密碼編譯運作和快速的交易速度。該 HSM 提供多種密碼編譯服務 — 包含電子商務、PKI、文件管理、電子帳單處理和支付 (EBPP)、資料庫加密、金融 EFT 交易和其他操作 — 所需的加密、使用者和資料驗證、郵件完整性、安全金鑰儲存，以及金鑰管理。

強大的安全 — 將金鑰保存在硬體中

對於經常在伺服器安全性低的環境中運作的密碼編譯作業而言，該產品可提供最高等級的防護。ProtectServer Internal-Express 是通過 FIPS 140-2 Level 3 驗證，並且具備防竄改能力的安全產品，可防禦處理敏感資訊的 HSM 遭受實體攻擊。當偵測到實體攻擊時，內部儲存金鑰的記憶體就會自行銷毀。此外，密碼編譯的金鑰絕對不會以明文型式暴露在 HSM 之外。

安全的儲存和處理為客戶帶來軟體產品無法提供的安全，並且提供通過認證的機密性和完整性，可符合客戶期望和產業組織的安全需求。

豐富的 API/工具套件和自訂能力

提供多種應用程式介面 (API)，可協助密碼編譯應用程式遵循產業安全標準和平台環境。其中包含市場上最廣為使用的 PKCS#11 功能組，一個 Java JCA/JCE、JCProv 與 Microsoft CryptoAPI/CNG 提供者實作，並且可以和 Open SSL 無縫整合。這個軟體開發套件提供了絕佳的彈性和擴充性，可以開發出自訂的密碼編譯應用程式 — 包含使用全新演算法 — 並且可安全地下載到 HSM 受保護的環境中使用。此外，其還提供一個 EFT/交易處理命令列，以及一個可以量身打造 HSM 上密碼編譯應用程式的自訂模組。

技術規格

作業系統

- Solaris
- AIX
- Linux
- Windows Server

密碼編譯 API

- PKCS#11、CAPI/CNG、JCA/JCE、JCProv、OpenSSL

密碼編譯處理

非對稱演算法

- RSA (多達 4096 位元)、DSA、ECDSA Diffie Hellman (DH)、ECC Brainpool Curves (指定和使用者定義) 以及其他

對稱演算法

- AES、DES、3DES、CAST-128、RC2、RC4、SEED、ARIA 以及其他
- 支援 ECB、CBC、OFB64、CFB-8 (BCF) 和其他等模式

雜湊演算法

- MD5、SHA-1、SHA-256、SHA-384、SHA-512、MD2、RIPEMD128、RIPEMD160、DES MDC-2 PAD1

郵件驗證編碼

- SHA-1、SHA-256、SHA-384、SHA-512、MD2、RIPEMD128、RIPEMD160、DES MDC-2 PAD1、SSL3 MD5 MAC、AES MAC、CAST-128 MAC、DES MAC、DES3 MAC、DES3 Retail CFB MAC、DES30x9.19 MAC、IDEA MAC、RC-2 MAC、SEED MAC、ARIA MAC、VISA CVV

法規標準認證

- FCC Part 15 — Class B
- 合乎 RoHS
- BAC 和 EAC ePassport 認證
- 通過 FIPS 140-2 Level 3 認證#1550
- FCC Part 15 Class B Unintentional Radiators ANSI C63.4-2003
- EN 55022:1998 Amendment 1:2000，Amendment 2:2003
- EN 55024:1998 Amendment 1:2001

實體特性

連接能力

- PCI Express Base Specification, revision 1.1、PCI Express Card Electromechanical Specification, revision 1.1 x4 link
- 智慧卡備份用 COM 埠

尺寸

- 4.16 英吋 x 6.63 英吋

電源需求

- +5V@3A 最大；+12V@0.2A 最大

運作溫度

- 0°C 到 40°C

儲存溫度

- -20°C 到 +65°C

易於管理

直覺的圖形化使用者介面 (GUI) 使用簡單易懂的導覽和使用者互動操作，簡化了 HSM 設備管理和金鑰管理的工作。您可以由遠端位置進行緊急且即時的工作，如金鑰修改、增加和刪除等，以降低管理成本和縮短回應時間。

彈性的程式開發功能

ProtectServer HSM 為開發者提供絕佳的彈性，可以打造自己的韌體並在 HSM 受保護的環境中使用。該工具組是功能性模組，提供開發和部署自訂韌體所需的所有工具，而全功能的軟體模擬器則可支援這些彈性的開發工具，讓開發者可以方便地在桌上型電腦上測試和偵錯自訂的韌體。這個模擬器也能當成測試應用程式的好工具，而不需真正安裝 ProtectServer HSM。當一切準備就緒後，開發者只要安裝 HSM 並將通訊導向硬體即可，不需要進行任何軟體的改變。

便利性

智慧卡可為安全備份、復原和傳輸密碼編譯金鑰的動作提供最高等級的安全和管理便利性。您可以在現場具效益地進行升級，免去將產品退回服務地點的支出。

多個插槽

ProtectServer Internal-Express 支援多個密碼編譯金鑰的儲存槽。儲存槽的功能類似於擁有多個插槽的智慧卡讀卡機，但是不需要實體讀卡機。這些虛擬插槽是金鑰的安全資料夾，每個保護夾都用唯一的使用者和安全管理密碼加以保護。藉此，一部 PSI-E HSM 可以使用於多個應用程式，省下更多成本並提供更多彈性。

關於 SafeNet

SafeNet 成立於 1983 年，是資訊安全的全球領導者。SafeNet 在資料的整個週期中保護客戶最重要的資產，包括身分、交易、通訊、資料與軟體授權。目前有 100 多個國家超過 25,000 個企業與政府機構客戶信任 SafeNet 所提供的資訊安全性。

聯絡我們：如需所有辦公室位置和聯繫資訊，請瀏覽 **www.safenet-inc.com**
追蹤我們：www.safenet-inc.com/connected