

產品介紹

# SafeNet PCIe HSM

(原產品名 SafeNet Luna PCI-E)



金雅拓的 SafeNet 網路 HSM 是需要數字簽名、加密密鑰存儲、事務加速、證書簽章、代碼簽名、批量密鑰生成、數據加密、DNSSEC 等強大安全性的企業的選擇。

金雅拓的 SafeNet PCIe HSM 是市場上應用最廣泛的通用嵌入式硬體安全模塊。憑藉專用的性能和構建完整集成解決方案的能力，SafeNet PCIe HSM 非常適合用於身份驗證，簽名和密鑰發布。

## 安全硬體密鑰管理

SafeNet PCIe HSM 的高保證設計提供專用硬體密鑰管理，以保護整個密鑰生命週期中的敏感密鑰。SafeNet PCIe HSM 的內部安全架構為在 HSM 中生成，使用和存儲的密鑰和敏感數據提供了前所未有的安全級別。

## 嵌入 SafeNet 通用 HSM 功能集以節省運營成本

SafeNet PCIe HSM 受益於強大的前瞻性功能集。這些功能（包括遠程管理，安全傳輸和遠程備份）將大大降低使用 SafeNet PCIe HSM 的解決方案的管理和運營成本。

## 高可用性和可擴展的性能

多個 SafeNet PCIe HSM 卡可以組合在同一台伺服器上，以提供高可用性，負載平衡和可擴展的性能。HA Group 技術共享事務負載，在組成員之間同步數據，並在成員卡發生故障時重新分配處理能力，以保持不間斷的服務。高性能計算能力還可以在單元恢復服務時輕鬆恢復。SafeNet PCIe HSM 還包括對不同伺服器中的卡之間的密鑰同步的 API 支持。使用此 API，組織可以創建自己的高可用性設置。

## 優勢與特點

### 強大的安全性

- > 硬體鍵
- > 遠端管理
- > 高保證交付的安全運輸模式
- > 多級訪問控制
- > 所有訪問控制鍵的多部分分割
- > 防入侵、防篡改的硬體
- > 安全審計記錄
- > 最強大的密碼算法
- > Suite B 算法支持
- > 安全退役

### 示例應用程序

- > PKI 密鑰生成和密鑰
- > 存儲（在線 / 離線 CA 密鑰）
- > 證書驗證和簽名
- > 文檔簽名
- > 交易處理
- > 數據庫加密
- > 智能卡發行
- > 物聯網的信任之根

## 靈活的備份和意外恢復選項

SafeNet PCIe HSM 提供安全，可審計和靈活的選項來簡化備份，複製和意外恢復。可以在本地或遠程執行重要備份，以實現 SafeNet Backup HSM，小型 eTokens 或其他 SafeNet HSM。

## 無需投入昂貴的認證即可實現 **FIPS 140-2** 和通用標準驗證

實現 FIPS 和 Common Criteria 認證可能是一個耗時且成本高昂的過程。由於金雅拓唯一的關注點就是安全性，我們將第三方認證作為優先考慮事項。

我們的團隊在設計符合 FIPS 140-2 和 Common Criteria 的產品方面擁有多年的經驗。在您的設備或服務中使用 SafeNet PCIe HSM 代表了將 FIPS 140-2 和 Common Criteria 驗證解決方案推向市場的具有成本效益的方式。

### 為支持 **ECC** 的資源受限環境開發解決方案

隨著資源受限設備（智能手機，平板電腦，智能電錶）的安全需求不斷增長，供應商必須能夠提供利用 ECC 算法的解決方案。與 RSA 密鑰相比，ECC 提供高密鑰強度，密鑰長度大大縮短。SafeNet PCIe HSM 提供硬件加速 ECC 算法，可用於開發解決方案，而無需購買額外的許可證。

### 共同架構

所有 SafeNet 通用 HSM 均受益於通用架構，其中受支持的客戶端，API，算法和身份驗證方法在整個通用 HSM 產品系列中保持一致。這消除了圍繞特定 HSM 設計應用程序的需要，並且提供了將按鍵從外形因素移到外形因素的靈活性。

### 提供兩種性能模組

SafeNet PCIe HSM 提供兩種性能模型：  
SafeNet PCIe HSM 7000 和 SafeNet PCIe HSM 1700。SafeNet PCIe HSM 7000 是一種

| Algorithm | Model         |               |
|-----------|---------------|---------------|
|           | PCIe HSM 1700 | PCIe HSM 7000 |
| RSA-1024  | 1,800         | 7,300         |
| RSA-2048  | 360           | 1,200         |
| ECC P256  | 580           | 2,000         |
| ECIES     | 200           | 310           |
| AES-GCM   | 3,600         | 3,600         |

### 技術規格

#### 操作系統支援

> Windows，Linux，Solaris

#### API 支援：

> PKCS # 11，Java (JCA / JCE)，微軟 CAPI/CNG/OpenSSL/Ruby/Python 加密

> PKCS # 11，Java (JCA / JCE)，微軟 CAPI/CNG/OpenSSL 加密

> Full Suite B support

> Asymmetric: RSA (1024-8192), DSA (1024-3072), Diffie-Hellman, KCDsa, Elliptic Curve Cryptography (ECDSA, ECDH, ECIES) with named, user-defined and Brainpool Curves

> Symmetric: AES/RC2/RC4/RC5/CAST/DES/Triple DES/ARIA/SEED

> Hash/Message Digest/HMAC: SHA-1, SHA-2 (224-512), SSL3-MD5-MAC, SSL3-SHA-1-MAC

> Random Number Generation: FIPS 140-2 approved DRBG (SP 800-90 CTR mode)

#### 物理特性

> 尺寸：全高，半長 4.16"x 6.6" (106.7mm x 167.65mm)

> 功耗：最大 12W，典型值 8W

> 溫度：運行 0°C - 50°C

#### 安全認證

> FIPS 140-2 2 級和 3 級

> 通用標準 EAL4 + (進行中)

> BAC&EAC 電子護照支援

#### 安全和環境合規性

> UL，CSA，CE

> FCC，KC Mark，VCCI，CE

> RoHS，WEEE

#### 主機接口

> PCI-Express X4，PCI CEM 1.0a

#### 可靠性

> MTBF 216,204 小時