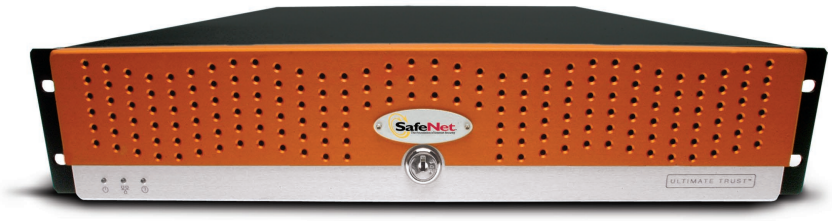
Luna SA

*網路 **HSM** 伺服器*



一個彈性且網路支援的硬體安全模組，
提供強大的加解密運算及硬體密鑰控管，
確保應用程式的安全運作。

保護硬體密鑰控管及加解密運算

Luna SA 為一硬體安全模組，提供硬體密鑰的管理及加速加解密運算，確保其安全性及高效能。Luna SA 內建的硬體安全模組為 FIPS 140-2 認證，可以支援每秒處理 1200 交易的效能 (RSA 1024-bits)，並提供可選擇性的驗證方式來保護最敏感的安全應用程式 (FIPS 140-2 Level 3 模式)

網路可分享性

Luna SA 內建乙太網路的連線提供更彈性化的建置方式。Luna SA 支援 TCP/IP 的網路確保其容易整合入現有網路架構及能夠與其他網路裝置溝通。多重應用程式伺服器可以透過被信任的網路連線來分享 Luna SA 的加解密能力，其網路連線結合了雙因素的電子憑證驗證及 128bit SSL 加密，也因此 Luna SA 端及應用程式伺服器端的連線永遠是在一個被保護的狀態，確保敏感資料的安全性。

彈性化設定方式

Luna SA 的彈性化功能解決了多種安全性問題。Luna SA 的 HSM Partitioning 提供單一 HSM 可以切割為多區塊的 Logical HSM. Luna SA 可以提供最多 20 獨一區塊的切割，每一區塊的可以擁有自己的存取控制及獨立的密鑰存儲。

多重的存取控制及身分驗證

多重管理者身分驗證政策針對敏感的加解密金鑰提供最高安全的保護，除此之外，也避免非法的設定改變。但同時仍提供彈性化的遠端管理及監控機制。透過 Luna PED (PIN Entry Device) 可以來執行管理者功能，它直接連接到 Luna SA 裝置。

支援標準的 Cryptographic API，讓整合工作更容易

Luna SA 支援 PKCS#11、Microsoft CryptoAPI 2.0、JCA (Java Cryptographic Architecture) 及 OpenSSL Cryptographic APIs，簡化了整合程序並確保了應用程式之間的相容性。

主要特性

安全性

Luna SA 的操作介面，軟體及硬體設計都確保加解密運算及金鑰多層次的整合性及安全性。

- 操作控制包含雙因素的身分驗證方式，及軟體存取的安全，防止非法的存取及操作。
- 安全的軟體運作維持系統與 Secure Booth verification 的整合性。PKI 簽核的 code module 也能預防非法軟體的入侵。
- Luna SA 具有防入侵，反竄改的高安全設計，提供主動及被動的自我防護機制。

程式碼簽章避免未授權者的入侵使用

應用程式會經由程式碼簽章來確保只有授權的使用者可以執行使用程式。程式碼簽章程序確保只有被信任的程式碼可以載入 Luna SP 並執行。因此應用程式沒有合法的簽章即無法被變更，程式碼簽章程序確保安全性裝置的邏輯完整性。

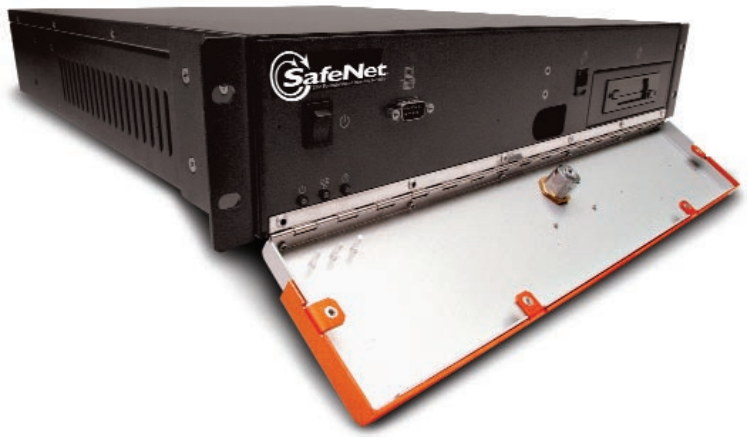
FIPS 140-2 規格

Luna SA 為一 FIPS 140-2 規格的硬體安全模組，保護重要加解密金鑰及加速不同等級安全應用程式的加解密運算。可針對您特殊應用程式來達到 FIPS 140-2 Level 3 及 FIPS 140-2 Level 2 兩個等級的保護。

可擴充性

Luna SA 擁有廣泛的架構選項，能夠隨著應用程式的成長而擴充，以滿足您的需求。核心架構參數可以透過軟體進行升級，因此不必更換硬體就能擴充 Luna SA。

SafeNet®
The Foundation of Information Security



業界標準機架規格

Luna SA 為 2U 19" 的業界標準 機架規格，為企業提供安全但又合乎企業資料中心的標準架構

整合性實體

整合式實體安全性方法包括防盜螺絲，入侵偵測開關，以及防護式接頭以防止硬體受到攻擊。

簡化遠端管理

Luna SA 具有一個安全性命令列介面以簡化遠端系統管理並讓系統的維護合理化，一個本機的中控台連接埠提供安全性的初始設定或直接系統管理。

備份及災難復原

Luna SA 可以透過備份裝置安全的提供資料的存儲，Key Clone, 及災難復原

兩段式管理者認證機制

為了保護現有 HSM 的投資，SafeNet Luna CA 3 加解密的硬體裝置可以透過 PC 卡硬體裝置與 Luna SA 溝通

軟體升級

Luna SA 使用 SafeNet 的可擴充式 Ultimate Trust™ Security Platform 來增加新的功能特性或效能。透過 PKI 驗證的軟體更新功能，可讓您新增最新推出的軟體功能，或將現有的架構特性輕鬆的部署到同一個區域的數個裝置上。

技術規格

加解密 API

- PKCS#11 v2.01
- Microsoft CAPI v2.0
- JCA (Java Cryptographic Architecture)
- JCE (Java Cryptographic Extensions)
- Open SSL

加解密硬體規格

- FIPS 140-2 Level 3, 憑證號 375
- FIPS 140-2 Level 2, 憑證號 436

加解密功能

- 產生硬體加速型亂數 (Annex C of ANSI X9.17)
- 產生對稱及非對稱金鑰配對
- 加密及解密
- RSA
- 數位簽章

加解密效能

每秒處理超過 1200 筆 1024 bits RSA 加解密運算

加密演算法

- 非對稱金鑰
  Diffie-Hellman (1024-4096 bit)
  RSA (512-4096 bit) (PKCS#1 v1.5, OAEP PKCS#1 v2.0)
- 數位簽章
  RSA (1024-4096-bit)、DSA (512-1024-bit)、(PKCS#1 v1.5)
- 對稱金鑰
  3DES (雙倍及三倍金鑰長度)、AES、RC2、RC4、RC5、CAST-128
- Hash Digest 演算法
  SHA-1、SHA-2 (160, 256, 512)、MD-5
- 訊息認證碼 (MAC)
  HMAC-MD5、HMAC-SHA-1、SSL3-MD5-MAC、SSL3-SHA-1-MAC

實體特性

連線能力

- 10/100 Ethernet、CAT5、UTP (最多 2 埠)
- Luna PED 認證埠
- 區域主控台連接埠
- Luna Token PC 卡插槽

尺寸

- 全長 2U，19" 機架型外殼 (與 ANSI/EIA-310-D 相容)
- 19.0" x 20.6" x 3.45" (482.6mm x 523.2mm x 87.7mm)
- 35 磅 (15.9 公斤)

可拆式儲存裝置

PC Card Type II 插槽，5V (+/- 0.25V)

溫度

運作：0°C 至 40°C，存放：-20°C 至 +65°C

安規標準認證

符合 U/L 1950 與 CSA C22.2 安全標準
FCC Part 15 - Class B
ISO - 9002 認證

SafeNet 台灣分公司

台北市 106 敦化南路二段 216 號 20 樓 B2 室
電話：(02) 2735 3736 eMail：*APACEnterprise@safenet-inc.com*
tw.safenet-inc.com

經銷商

SafeNet®
The Foundation of Information Security