產品優點

整合的實體安全防護功能

Luna PCI 通過 FIPS 140-2 第 2 級和第 3 級認證。所有型號都安全地裝在特殊設計的機殼內，以符合對於避免損害和異物入侵的嚴厲要求。

可在 Windows 作業平台上隨插即用 (Plug and Play)

支援 Microsoft Windows 2000、Windows XP 和 Windows Server 2003 的隨插即用功能，讓您更容易在各式各樣的應用程式上部署 Luna PCI，這些應用程式包括 IIS Server、Microsoft Certificate Service、ISA Server 和 RMS Server。

完全支援 Cryptographic API，讓您可以輕鬆地進行整合

Luna PCI 支援 PKCS#11、Microsoft CryptoAPI、Java JCA(Java Cryptographic Architecture)和 Open SSL Cryptographic APIs，讓您能簡化開發程序，還能加快應用程式的部署。

Developer's ToolKit (開發人員的工具組)

對開發人員而言，有了功能強大且容易使用的 Luna Toolkit 後，將能輕鬆地在您自己的應用程式中加上安全的、以硬體為主的加密處理過程。

Luna PCI

硬體安全防護模組

Luna® PCI 是高安全性加密 PCI 加速卡家族系列產品 - 可用來啟動備受好評的、廣被全世界的主要政府單位、財金機構和大型企業所採用的 Luna SA

硬體金鑰管理

Luna PCI 提供專用的硬體金鑰管理功能來保護重要的加密金鑰不受到攻擊。這項硬體設計的安全性相當高，能確保加密金鑰在整個使用的生命週期中都能受到完整的保護。所有數位簽署和確認作業都會在 HSM 內部進行以提升效能和維護安全。Luna PCI HSM 能在一系列提供多種安全防護、效能和作業功能選項的產品型號和設定中，產生有硬體保護的金鑰並加以儲存，提供安全金鑰備份和加快加密的速度。

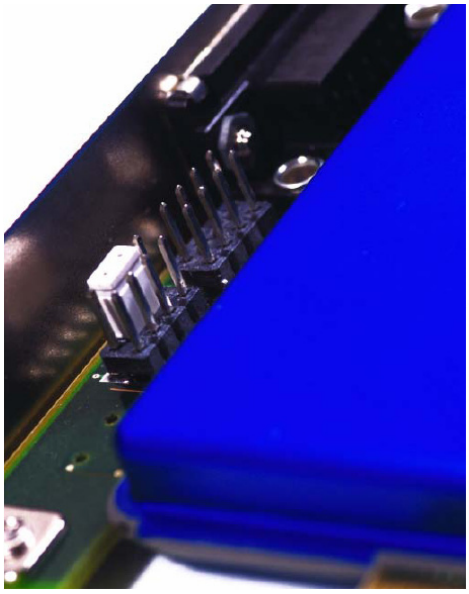
高效能加密程序

Luna PCI 以專用的硬體加速來減少金鑰的應用程式處理瓶頸。而高階 Luna PCI 型式能在通過 FIPS 認證硬體的安全防護下，每秒提供高達 7000 個非對稱 1024 位元 RSA 作業。

硬體認證

Luna PCI 卡通過了許多重要的安全防護認證，包括 FIPS (Federal Information Processing Standards，聯邦資訊處理標準)140-2 第 2 級和第 3 級認證。Common Criteria 的 EAL 4+ 級和 German Digital Signature Law(德國數位簽章法)的驗證正在進行中。

SafeNet
The Foundation of Information Security



安全認證和存取控制

Luna PCI 提供了有效的二階段認證(two-factor authentication)方式和多種管理員角色，能夠預防此未經授權而存取重要的加密資料。支援 FIPS 140-2 第 3 級作業的 Luna PCI 可藉由 Luna PED(PIN Entry Device，PIN 碼輸入裝置)來提供 True Trusted Path(真實可信路徑)。Luna PED 是一個整合的手提認證裝置，它不需要用到市面上的鍵盤或[illegible]能讓管理人員輸入 PIN 碼

加密功能

Luna PCI 支援各式各樣的非對稱金鑰加密(asymmetric key encryption)和金鑰交換功能(key exchange capabilities)，另外也支援了所有標準對稱加密運算。Luna PCI 還支援所有標準散列運算(hashing algorithms)和訊息認證碼(message authentication codes)。此外，Luna PCI 也支援了以 ANSI X9.31 的

技術規格

支援的 Client API

PKCS#11 v2.01、Microsoft CryptoAPI 2.0、Java JCA/JCE 和 Open SSL

支援的作業系統

- Microsoft Windows 2000、Windows XP 和 Windows Server 2003
- Linux Kernels 2.4、2.6

加密過程

非對稱金鑰加密和金鑰交換(Asymmetric Key Encryption and Key Exchange)

- RSA(512-4096 位元)(PKCS#1 v1.5、OAEP PKCS#1 v2.0)、Diffie-Hellman(512-1024 位元)、DSA(512-1024)

對稱運算(Symmetric Algorithms)

- DES、3DES、(2 倍和 3 倍的金鑰長度)RC2、RC4、RC5、AES

散列運算(Hashing Algorithms)

- SHA-1、SHA-256、SHA-384、SHA-512、MD-2、MD-5

訊息認證碼(Message Authentication Codes, MAC)

- HMAC-MD5、HMAC-SHA-I、HMAC-SHA-256、HMAC-SHA-384、HMAC-SHA-512、SSL3-MD5-MAC、SSL3-SHA-I-MAC

Random Number Generation (亂數產生器)

- Luna PCI 支援以 ANSI X9.31 的 Appendix A 2.4 為基礎的 Random Number Generation(亂數產生器)

實體規格

PCI 卡型式

- PCI 卡，3.3V

作業溫度

- 0°C到 50°C之間

儲存溫度

- -20°C 到 65°C 之間

法規標準認證

- 1950 & CSA C22.2 safety compliant FCC Part 15 – Class B

公司地址：4690 Millennium Drive, Belcamp, Maryland 21017 USA

電話：+1 410.931.7500 或 800.533.3958

電子郵件：*info@safenet-inc.com*

www.safenet-inc.com

Australia +61 3 9882 8322
Brazil +55 11 4208 7700
Canada +1 613.723.5077
China +86 10 885 19191
Finland +358 20 500 7800
France +33 1 41 43 29 00
Germany +49 18 03 72 46 26 9
Hong Kong +852.3157.7111
India +91 11 26917538
Japan +81 45 640 5733
Korea +82 31 705 8212
Mexico +52 55 5575 1441
Netherlands +31 73 658 1900
Singapore +65 6297 6196
Taiwan +886 2 27353736
UK +44 1276 608 000
U.S. (Massachusetts) +1 978.539.4800
U.S. (Minnesota) +1 952.890.6850
U.S. (New Jersey) +1 201.333.3400
U.S. (Virginia) +1 703.279.4500
U.S. (Irvine, California) +1 949.450.7300
U.S. (San Jose, California) +1 408.452.7651
U.S. (Torrance, California) +1 310.533.8100

Distributors and resellers located worldwide.

SafeNet
The Foundation of Information Security