cpl.thalesgroup.com

THALES
Building a future we can all trust

Thales ProtectServer 3 Network HSMs

ProtectServer 3 External
ProtectServer 3+ External

Thales ProtectServer 3 網路硬體安全模組 (HSM) 是強化安全的網路加密伺服器，保護加密金鑰免受外洩，同時提供加密、簽章和身份認證服務以保護機敏應用程式。

ProtectServer 3 External HSM

ProtectServer 3+ External HSM

最高安全性

ProtectServer 網路 HSM 包含一個加密模組，以高保障的方式執行安全加密處理。 這些設備採用具有防篡改安全性的重型鋼製硬體，可防止物理攻擊，並為加密金鑰、PIN 碼和其他高度機敏資訊的儲存和處理，提供最高級別的物理和邏輯保護。 安全儲存和處理是指加密金鑰永遠不會以明確的形式暴露在 HSM 之外，為客戶提供軟體相似產品無法企及的安全級別，且設備通過機密性和完整性的認證，可滿足行業/組織安全性需求。

靈活的編程

ProtectServer HSM 為應用程式開發人員提供了獨特的靈活性，可以創建自己的韌體並在 HSM 的安全範圍內執行。 被稱為功能模組的工具包，提供一個全方位的環境來開發和部署客製韌體。 加入功能齊全的軟體模擬器使開發工具集更加完整，開發人員僅需桌上電腦即可方便地測試和調試客製韌體。 在無需安裝 ProtectServer HSM狀態下，模擬器還可作為測試應用程式的重要工具。 準備就緒後，開發人員只需安裝 HSM 並將通訊重定向到硬體 — 無需更改軟體。

效益

效能

- 3500 個 RSA-1024 簽章/秒

安全

- FIPS 140-2 3 級驗證*
- 防竄改硬體保護
- 真實隨機數生成器
- 金鑰材質的智慧卡備份

可靠性

- 高品質元件

易於管理

- 直觀的圖形用戶界面
- 場域安全升級
- 遠程管理

互操作性

- 支援 ANSI X9 TR-31 金鑰模組

易於管理

直觀的圖形用戶界面 (GUI) 使用易於理解的導航和用戶互動體驗，來簡化 HSM 設備管理和金鑰管理。 可以從遠程位置安全地執行緊急和時間緊迫的管理任務，例如金鑰修改、添加和刪除，進而降低管理成本和回應時間。

ProtectServer 3+ HSM

除了 ProtectServer 3 HSM 提供的特性和功能外，ProtectServer 3+ HSM 還採用雙可插拔交流電源，防止電源故障，以保障資料中心的高可用性，並透過將設備連接到兩個獨立的電源，以防止其中一個電源可能發生故障，實現業務不中斷。 對故障電源或電源供給執行維護時，提供了必要的靈活性，並確保您的設備將持續運營。

高效能和可擴展性

ProtectServer Network HSM 實現快速執行和處理加密命令。 專門的密碼電子設備，包括專用的資料密碼微處理器、記憶體和真正的隨機數生成器 (RNG)，從主機系統中分擔加密處理，使其能夠騰出資源回應更多請求。

ProtectServer Network HSM 支援各式的對稱和非對稱加密性能標準，可滿足各種安全應用程式的處理要求，速度高達每秒 3500 次 RSA-1024 簽章作業。 包含的雙網口界面，使 HSM 可以整合在相同或不同的子網中，並在不同的網路之間共享，以保護多個業務網域或在單一網路中提供冗餘。

此外，由於對可協同工作的 HSM 數量或可以管理的金鑰數量沒有限制，因此可輕鬆實現高擴展性、可靠性、冗餘性，及更高吞吐量。

便利性

智慧卡為加密金鑰的安全備份、復原和傳輸提供了最高的安全性和便利的管理功能。 可以在現場執行升級，節省將產品送還服務據點的費用，以節省成本。 ProtectServer HSM 還支援透過兼容的 PIN 鍵盤輸入金鑰組件。

多因素身份認證

ProtectServer HSM 支持多因素身份認證。 這種認證方案需要包括腦中的token PIN碼和SafeNet 110 OTP 產生器隨機生成的 6 位數密碼，來增加另一層安全性。

技術規格

供應機型

- PSE 3 可用於 PL25、PL220 和 PL3500 性能型號
- PSE 3+ 僅在 PL3500 性能型號中可用

支援作業系統

- Windows, Linux

加密APIs

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

加密

- 非對稱：RSA、DSA、Diffie-Hellman、橢圓曲線密碼演算法（ECDSA、ECDH、Ed25519），具有命名曲線、用戶定義曲線和 Brainpool 曲線等
- 對稱式演算法：AES、AES-GCM、AES-CCM、AES-GMAC、Triple DES、DES、CAST 128、RC2、RC4、SEED、ARIA 等
- 雜湊：SHA-1、SHA-2、SHA-3、MD5、MD2、RIPEMD 128、RIPEMD 160、DES MDC2 PAD1 等
- 訊息摘要：SHA-1、SHA-2、SHA-3、MD2、RIPEMD128、RIPEMD160、DES MDC-2 PAD1、SSL3 MD5 MAC、AES MAC、CAST-128 MAC、DES MAC、DES3 MAC、DES3零售CFB MAC、DES30x9.19 MAC、IDEA MAC、RC-2 MAC、SEED MAC、ARIA MAC, VISA CVV
- Digital Wallet Encryption: BIP32
- 用於用戶身份認證的 5G 加密機制：MILENAGE 和 TUAK
- ANSI X9 TR-31 Key Block 支援互操作性

實體規格

- 機架式安裝
  - 標準 1U 19 英吋機架式規格
- 尺寸
  - 17.20” x 9.84” x 1.73” (437 mm x 270 mm x 44 mm) (PSE 3)
  - 19” x 21” x 1.725” (482.6mm x 533.4mm x 43.815mm) (PSE 3+)
- 重量
  - 6.83磅 (3.1 公斤) (PSE 3)
  - 28磅 (12.7公斤) (PSE 3+)
- 輸入電壓
  - 100–240V, 50–60Hz (PSE 3)
  - 100–240V, 50–60Hz (PSE 3+)
- 耗電量
  - 最高 90W , 58W typical (PSE 3)
  - 最高100W , 84W typical (PSE 3+)
- 溫度
  - Operating 0°C to 35°C, storage –20° to 60°C
- 相溼度
  - 5% to 85% (38°C) 非冷凝 (PSE 3)
  - 5% to 95% (38°C) 非冷凝 (PSE 3+)

主機接口

- 2 Gigabit Ethernet ports with Port Bonding (PSE 3)
- 4 Gigabit Ethernet ports with Port Bonding (PSE 3+)
- IPv4 和 IPv6

安全認證

- FIPS 140-2 3 級*

管理和監控

- 高可用性 (HA) / 工作負載分配 (WLD) g
- SNMP, Syslog
- 備份/復原

安全和合規環境

- UL, CSA, CE
- FCC、KC 標誌、VCCI、CE
- RoHS, WEEE
- 印度 BIS [IS 13252（第 1 部分）/IEC 60950-1]

可靠性

- 雙熱插拔電源 (PSE 3+)
- 平均故障間隔時間 (MTBF) 165637 小時 (PSE 3)
- 平均故障間隔時間 (MTBF) 171,308 小時 (PSE 3+)

* pending

關於Thales

重視個人機密隱私的公司，將 Thales 解決方案作為保護資料安全的首選。 在資料安全方面，企業面臨越來越多的關鍵時刻。 無論是建構加密策略、轉移到雲端還是滿足合規性要求，您都可以依賴 Thales實現數位化轉型。

Decisive technology for decisive moments.