

payShield 10K

專為信用卡支付系統與行動支付安全所設計硬體安全模組，保障全球支付安全。

payShield 10K

- 簡化在黑暗數據資料中心 (自動化數據資料中心) 的部署
- 提供高可用性及完善的金鑰管理機制
- 專為信用卡支付系統設計，即時提供最廣泛的卡片和行動應用程式支援
- 提供性能升級，無需更換硬體
- 與現有Thales payment HSM 設備相容，不需改變現有資安政策



技術規格

payShield 10K 是一個專為信用卡支付系統與行動支付安全所設計硬體安全模組 (HSM)，在全球支付生態系統中受到發卡方、服務提供者、收單行、處理方和支付網路廣泛使用。對於面對面和遠端支付服務，這套模組在保護支付認證頒發、用戶身份驗證、卡片驗證和機敏資料保護的過程，提供領先的安全與支付技術。

常見用例

- 支付認證頒發 - 卡片、行動安全元素、穿戴式裝置、互聯裝置以及主機卡模擬 (HCE) 應用
- PIN 碼路由
- 點對點加密 (P2PE)
- 安全代碼化 (針對 PCI DSS 合規性)
- EMV 支付代碼化
- 卡片和行動支付授權
- POS、mPOS 和 SPoC 金鑰管理
- PIN 碼和 EMV 密碼驗證
- 遠端金鑰載入

完善的整合選擇服務

- 提供所有主要支付授權，交換應用程式整合
- 技術合作夥伴詳情請見：
www.thalessecurity.com/partners/technology-partners

卡片 / 行動支付支援

- payShield 10K 提供全面性功能，在以下多個領域支援領先支付品牌 (美國運通、Discover、JCB、Mastercard、銀聯和 Visa) 的需求，包括：
 - 符合最新導入的支付卡系統硬體安全模組標準，例如所有主要支付品牌的 PIN 碼和卡片驗證功能
 - EMV 交易授權和訊息傳遞
 - 行動支付交易授權和金鑰管理
 - ATM 和 POS 裝置遠端金鑰載入
 - 區域 / 全國金鑰管理 (包括澳洲、德國和義大利)
 - Mastercard 代理金鑰管理 (OBKM) 支援
 - 支援磁條和 EMV 的資料準備和個人化，包括行動佈建方式
 - PIN 碼生成和列印

密碼演算法

- DES 和 Triple-DES 金鑰長度 112 和 168 位元
- AES 金鑰長度 128、192 和 256 位元
- RSA (最高 4096 位元)
- HMAC、MD5、SHA-1、SHA-2

金融服務標準

- ISO : 9564、10118、11568、13491、16609
- ANSI : X3.92、X9.8、X9.9、X9.17、X9.19、X9.24、X9.31、X9.52、X9.97
- ASC X9 TR-31、X9 TG-3/TR-39
- APACS 40 和 70

物理安全性

- 防篡改和回應設計
- 一旦遭到任何篡改攻擊，機敏資料會立即清除
- 行動、電壓和溫度的警報觸發器

邏輯安全性

- 本地主金鑰 (LMK) 選項 - 變體和金鑰塊
- 使用智慧卡對安全人員進行雙重身份驗證 (2FA)
- 雙重控制授權 - 實體鑰匙或智慧卡
- 預設情況下提供最高強度的安全設定
- 使用者控制記錄事件範圍的審計跟蹤

產品型號和選項

- 所有型號均標配雙熱拔插電源和風扇
- 效能等級範圍 - 每秒 25、60、250、1000 和 2500 次調用 (cps)
- 透過 payShield 遠端管理 (VM)、payShield 監控 (VM) 和 payShield 可信管理裝置 (TMD) 實現遠端管理和監控選項
- 格式保留加密 (FPE) 選項
- 多個 LMK 選項 - 每個 HSM 最多 20 個分區
- 台灣財金資訊公司指令集選項

主機連接

- TCP/IP 和 UDP (1Gbps) - 雙連接埠
- 乙太網路主機連接埠上 TLS 認證工作階段的安全主機通訊管理選項

安全認證

- FIPS 140-2 Level 3
- PCI HSM v3

實體規格

- 外形規格 : 1U 19 英寸機架安裝
- 尺寸 : 482.6 x 736.6 x 44.5 公釐 (19 x 29 x 1.75 英寸)
- 重量 : 15.9 公斤 (35 磅)
- 電源 : 90-264 VAC
- 功耗 : 60W (最大值)
- 作業溫度 : 0°C-40°C
- 運輸溫度 : -25°C-70°C
- 儲存溫度 : -5°C-45°C
- 濕度 : 10%-90% (非冷凝)

安全和環境合規性

- UL、UL/CA、UL-AR、CE、BIS、FCC、Canada ICES、RCM、KC、VCCI
- RoHS2、REACH、WEEE