

最重要的必須萬無一失

全方位保護關鍵應用程式、資料和身分

Thales 與 Imperva 已於 2024 年完成合併，共同成為全球資安領域的 5 大領導者之一，隨著 Imperva 加入，Thales 的資安產品組合將提供高度互補的解決方案，幫助客戶保護數位生態系統的核心：應用程式、資料和身份。

在邁向數位轉型時，企業在維護資料安全上，面對越來越多重要的決策，不論是加密策略建構、資料移轉至雲端，或是滿足資料合規要求，都帶來了許多資安問題，包括：複雜性增加、可見性降低、資料控制及隱私問題加劇等，進而導致資料外洩風險增加及合規挑戰。

Thales 透過創新、整合的平台協助全球超過 35,000 個企業組織，防禦網路威脅、加速合規，並為數十億消費者提供安全、值得信賴的數位服務。



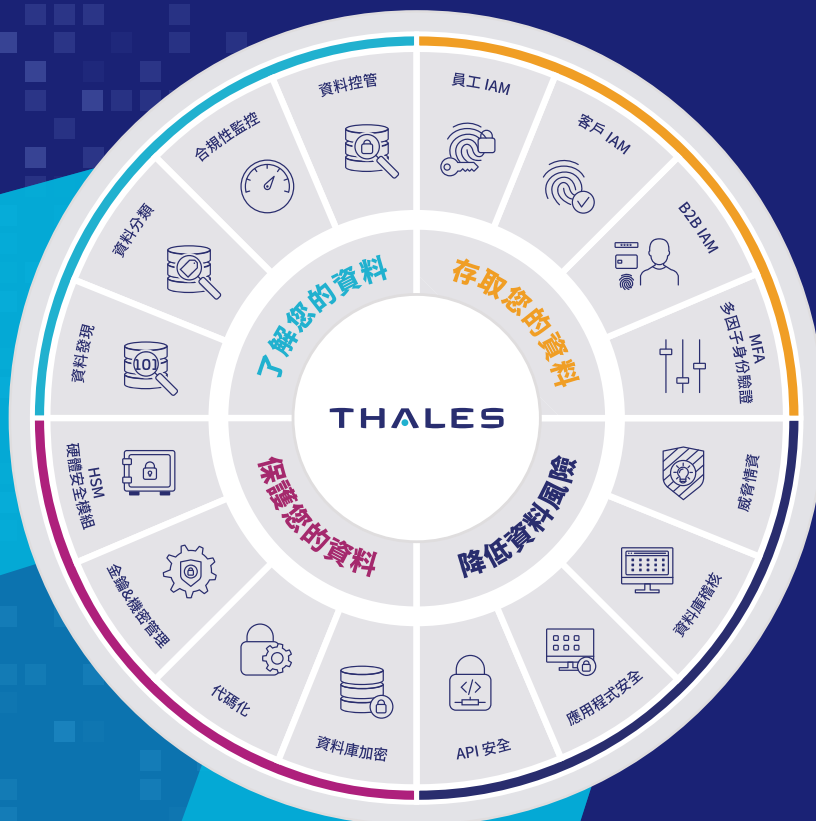
Imperva Application Security
應用程式及API自動保護



CipherTrust Data Security Platform
發現、保護、控管機敏資料



Imperva Data Security Fabric
即時偵測威脅及保護數據



CipherTrust 資料保護平台

加密並控制重要資料的存取

資料外洩事件持續以驚人的速度不斷發生，機敏資料的安全維護對所有企業而言都至關重要。此外，企業積極遵循全球和區域性的資料隱私法規，並尋求在加速採用雲端技術的同時確保存取安全。資安單位需要以資料為中心的方案，藉此維護資料從網路移動到應用程式和雲端時的安全。當邊界網路控制與端點安全措施失效時，靜態資料保護便成為最後一道防線。

CipherTrust 資料安全平台整合了資料的發現、分類、保護，以及前所未有的分級存取控制，並提供集中化金鑰管理。CipherTrust 解決方案移除了資料保護的複雜性、加速法規遵循，並確保雲端轉移安全，減少投資資安營運所需的資源；同時提供無所不在的法規遵循控管，大幅降低企業整體風險。



主要特色

- 集中管理主控台
- 監控及報表功能
- 資料發現與分類
- 以資料可視性進行風險分析
- 資料保護技術
 - 檔案、資料庫與容器的透明加密
 - L7 應用層資料保護
 - 保留資料格式的加密(FPE)
 - 代碼化(Tokenization)與動態資料遮罩
 - 靜態資料遮罩
 - 特權使用者存取控制
- 集中化企業金鑰管理
 - FIPS 140-2 認證
 - 支援 KMIP 生態系統
 - 支援多雲環境的金鑰管理
 - 資料庫加密金鑰管理(Oracle TDE, big data, MS SQL, SQL Server Always Encrypted等)

法規遵循

CipherTrust 資料安全平台支援全球各大安全和隱私法規，包括：

- GDPR
- PCI DSS
- HIPAA
- SOX/GLBA
- CCPA
- FIPS140-2
- FISMA, FedRAMP
- NIST 800-53 rev.4
- 南非 POPI Act
- ISO/IEC 27002:2013
- 日本 My Number Compliance
- 南韓 PIPA
- 印度 Aadhaar Act
- 菲律賓 Data Privacy Act
- 新加坡 Monetary Act
- 澳洲 Privacy Amendment

關鍵效益

• 簡化資料保護

借助新一代資料保護解決方案，發現、保護、控管每一處的機敏資料。CipherTrust 資料保護平台透過集中管理主控台這個單一平台簡化資料安全管理，為企業提供強大的工具來發現、分類機敏資料、對抗外部威脅、防範內部人員濫用，並建立持續的控制，即便資料儲存在雲端或外部服務供應商的基礎設施內亦是如此。組織可以輕鬆查找並縮小隱私缺口、確定保護的優先順序，在實施數位轉型前就擬定正確的隱私與安全決策。

• 加速合規時程

監管與稽核單位要求企業必須控管那些受管制和具機敏性的資料，並提出報告佐證。CipherTrust 資料保護平台所具備的功能，如資料發現與分類、加密、存取控制、稽核日誌、代碼化及金鑰管理等，能支援這些資料安全和隱私要求。平台的集中性和模組(connector)佈署可快速延伸、增加，以因應不斷變化的合規要求。

• 安全的雲端轉移

CipherTrust 資料保護平台提供進階加密與集中化金鑰管理方案，讓企業能夠安全的將機敏資料儲存在雲端；同時也提供先進的多雲自帶加密(BYOE)方案，避免受限於雲端供應商的加密方案，並透過集中、獨立的加密金鑰管理功能，確保資料可以安全而有效率地跨越多重雲端環境。

無法執行 BYOE 的企業仍可以從外部透過 CipherTrust 雲端金鑰管理(Cloud Key Manager)管理金鑰，以遵循業界最佳實務規範；且 CipherTrust 雲端金鑰管理支援在多個雲端架構和 SaaS 應用服務中自帶金鑰(BYOK)。CipherTrust 資料保護平台為企業在雲端的機敏資料和應用程式提供最強的保護，協助任何地方建立、使用或儲存的資料合規並獲得更大的資料控制權。

CipherTrust 資料保護平台產品

CipherTrust Manager 集中管理系統

CipherTrust Manager 是平台的中央管理系統，也是業界領先的企業金鑰管理方案，提供金鑰集中管理、分級存取控制和安全政策配置功能。CipherTrust Manager 管理金鑰的生命週期任務，包括生成、輪替、銷毀、匯入和匯出，提供金鑰和政策的 role-based 存取控制，支援強大的稽核與報告，以及易於開發、管理的 REST API。CipherTrust Manager 提供實體與虛擬版方案，並具備 FIPS 140-2 level 3 的合規標準。CipherTrust Manager 也可搭配 Thales Luna 和 Luna Cloud HSM 等硬體安全模組使用。

CipherTrust 資料發現與分類

CipherTrust 資料發現與分類可在跨雲、大數據和傳統資料存儲途徑中找出需受監管的資料，包括結構化和非結構化的數據。透過單一管理平台可以輕鬆掌握機敏資料及其風險，進而對安全漏洞、法規遵循與修補優先順序等作業做出更好的決策。CipherTrust 資料發現與分類解決方案提供流暢的工作流程，從政策配置、資料發現、分類到風險分析與報告等，以協助排除資安盲點與複雜性。

CipherTrust 透明加密

CipherTrust 透明加密提供靜態資料加密、特權用戶存取控制和詳細的資料存取日誌記錄。代理程式可橫跨雲端和大數據環境中的實體與虛擬伺服器，保護 Windows、AIX 和 Linux 等作業系統中的檔案及資料庫數據。CipherTrust 透明加密的 Live Data Transformation 延展功能提供免停機的資料加密與金鑰更換。此外，安全情資日誌與報告也運用了先進的 SIEM 系統，可簡化合規報告並加速威脅檢測。

CipherTrust Tokenization 代碼化

CipherTrust Tokenization 提供 Vault 和 Vaultless 版本，協助降低資料法規遵循（如 PCI-DSS）所需的成本與複雜性。Tokenization 將敏感數據替換為代碼（token），以確保機敏資料的安全，與資料庫和非授權使用者及系統保持隔離。Vaultless 版本包括基於政策的動態資料遮罩功能，兩種方案都讓應用程式的重要資料代碼化變得更容易。

CipherTrust Database Protection 資料庫自帶加密功能整合

CipherTrust 資料庫保護解決方案透過安全、集中化的金鑰管理，整合資料庫內建的敏感欄位加密功能，且不需修改資料庫應用程式。CipherTrust 資料庫保護解決方案支援 Oracle、MS SQL、IBM DB2 和 Teradata 資料庫。

CipherTrust 金鑰管理

CipherTrust 金鑰管理提供強大且基於標準的加密金鑰管理方案，簡化了諸多加密金鑰管理的挑戰，確保金鑰安全且僅提供給獲得授權的合法加密服務使用。

CipherTrust 金鑰管理支援多種使用情境，包括：

- **CipherTrust 雲端金鑰管理**

為 AWS、Azure、Salesforce 和 IBM Cloud 提供精簡優化的 BYOK 管理。解決方案提供完整的雲端金鑰生命週期管理與自動化，以強化資安團隊效率、簡化雲端金鑰管理。

- **CipherTrust TDE 金鑰管理**

支援多種資料庫，如 Oracle、Microsoft SQL 和 Microsoft Always Encrypted。

- **CipherTrust KMIP Server**

集中管理 KMIP client，如全磁碟加密(FDE)、大數據、IBM DB2、磁帶備份、VMware vSphere 和 vSAN 加密等。

CipherTrust CTE-RWP 透明加密勒索軟體防護

CipherTrust CTE-RWP (Transparent Encryption Ransomware Protection) 以低資源消耗且非侵入性的保護方式，保護文件、資料夾免受勒索軟體攻擊。CTE-RWP 使用機器學習模型來動態偵測可疑的檔案 I/O 活動，無需修改任何終端機或伺服器上的應用程式、設定對每個文件及資料夾的限制性存取控制和加密策略，即可在偵測到異常時發出警報或阻止。

CipherTrust Manager 技術規格表

硬體規格 (k470, k570)

尺寸	19.0"(寬) x 21"(深) x 1.75" (高)
重量	12.7kg (28lbs)
CPU 處理器	Intel Xeon E3-1275v5
記憶體	16 GB
硬碟空間	1 X 2TB SATA SE (Spinning Disk)
Serial 序列埠	1
網路介面	4x1GB or 2x10GB/2X1GB
電源供應器	• 平均耗電量 (Watts) 0.7A @120V (84W) • 最大耗電量 (Watts) 0.83A @120V (100W) • 電壓: 100-240V 50-60Hz
電源線	• PSE 認證 • 多國規格配置
平均故障間隔時間	153,583
機殼入侵偵測	防篡改密封. k570 內建的 HSM 若偵測到破壞性侵入，將自動清空資料
運作溫度	0 to ~35°C
非運作時溫度	-20 to 60 °C
運作相對濕度	5% ~ 95% 非凝結狀態
FIPS 140-2 認證	https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3519
嵌入的 HSM 管理	k570 (內建 HSM), 管理介面及 REST API 都允許設定或介接 HSM
硬體安裝	含滑軌安裝套件

軟體規格

管理介面	Management Console, REST API, ksctl (Command Line Interface), NAE XML			
最大金鑰數量	k470	k570	k170v	k470v
	1M	1M	50K	1M
最大分區數(multi-tenancy)	1000			
API 支援	REST, NAE-XML, KMIP, PKCS#11, JCE, .NET, MCCAPI, MS CNG			
登入認證方式	• 本地認證 • AD/LDAP • 憑證驗證登入 • K570: 利用Local or Remote PED 進行主密鑰的建立及設置			
支援的 HSM	Luna Network HSM, Luna T-Series Network HSM, Luna Cloud HSM, Data Protection on Demand, AWS CloudHSM			
叢集支援(Cluster)	Active/Active. Max Nodes=10 cluster 叢集成員可以是實體或虛擬版. k170v 僅限為 2-node clusters.			
備份	手動/排程; 支援以 HSM 金鑰加密備份			
網管	SNMP v1, v2c, v3, NTP, Syslog-TCP			
日誌格式	RFC-5424, CEF, LEEF			
認證	k570: FIPS 140-2 L3 k470, k170v 及 k470v 可介接 Luna Network HSM 確保主密鑰安全強度			

虛擬版硬體需求

	k170v	k470v
最小 CPU 數	2	4
最小記憶體(GB)	4	16
最小硬碟空間(GB)	100	200
最小虛擬網路埠數量	1	2

Thales Luna Network HSM



在 Thales Luna Network 硬體安全模組 (HSM) 中儲存、保護、管理金鑰，能以效能領先業界的高安全性、防竄改、網路連結功能，保障機敏資料和重要應用程式的安全。且 Luna Network HSM 可整合各種應用程式加速加密作業、保障金鑰週期安全、為整體加密設計提供最安全的信任基礎架構。

主要特色

卓越效能

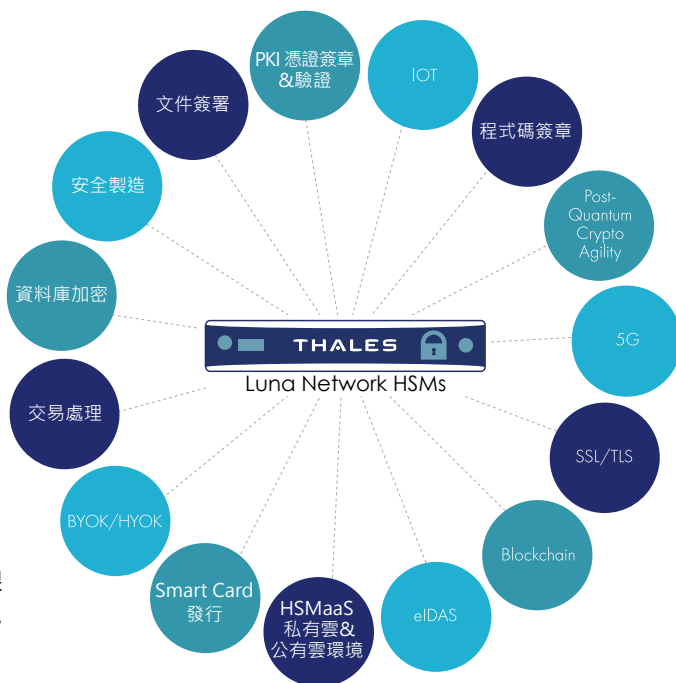
- 超過每秒 20,000 ECC 和 10,000 RSA 作業的高效運行，滿足企業對高效能的需求
- 延遲時間更短，效能更高

最高的安全性與合規規格

- 金鑰儲存在通過 FIPS 驗證、防竄改的硬體中
- 符合 GDPR、eIDAS、HIPAA、PCI-DSS 等要求
- 符合雲端現存標準
- 多重角色，實現高度權責分離
- M of N 多人特徵控制及多因素驗證，提升安全性
- 確保稽核記錄安全性
- 具備安全傳輸模式的高保證度傳遞效能
- 以外部 Quantum RNG 植入的高品質金鑰
- 可使用 Luna backup HSM 安全地備份、複製金鑰，或根據需要，使用資料保護將金鑰備份、複製到雲端，以實現效能運用、可靠性和災難恢復

降低成本並節省時間

- 支援 HSM 遠端管理，無需奔波
- 減少稽核與合規開銷負擔
- 企業系統自動化，透過 REST API 管理 HSM
- 多應用程式或租戶可共享 HSM，提高資源利用
- 彈性分割區規則，符合您的金鑰管理與合規需求



- Luna Client 可在容器中使用，便於移動、提高效率並減少經常性開銷
- 功能模組
 - 延伸原生 HSM 功能
 - 於 HSM 安全規範中建立、佈署客製化程式

技術規格

支援作業系統

- Windows、Linux、Solaris、AIX
- Virtual: VMware、Hyper-V、Xen、KVM

支援應用程式編程介面

- PKCS#11、Java (JCA/JCE)、Microsoft CAPI 與 CNG、OpenSSL
- REST API 管理

支援加密演算法

- 完整支援 Suite B
- 非對稱式演算法：RSA、DSA、Diffie-Hellman、Elliptic Curve 加密演算法 (ECDSA、ECDH、Ed25519、ECIES)，搭配命名、使用者自訂和 Brainpool curves、KCDISA 等
- 對稱式演算法：AES、AES-GCM、Triple DES、DES、ARIA、SEED、RC2、RC4、RC5、CAST 等
- 雜湊 / 訊息摘要 / HMAC：SHA-1、SHA-2、SHA-3、SM2、SM3、SM4 等
- Key Derivation：SP800-108 Counter Mode
- Key Wrapping：SP800-38F
- Random Number Generation：設計符合 AIS 20/31 對 DRG.4 使用以硬體為基礎的真雜訊來源，並配合 NIST 800-90A 相容 CTR-DRBG
- Digital Wallet Encryption：BIP32
- 用於用戶身份驗證的 5G 加密機制：Milenage、Tuak 和 COMP128

安全憑證

- FIPS 140-2 Level 3：密碼與多因素驗證 (PED)
- 針對保護規範 EN 419 221-5 的通用標準 EAL4 + (AVA_VAN.5 和 ALC_FLR.2)
- 符合 eIDAS 要求的合格簽章生成裝置 (QSCD) 清單

主機介面

- 2 個選項：4 個可單獨設定的 1G 自動感應 Ethernet LAN port 或 2 個 10G SFP port 和 2 個 1G RJ45 port (copper)
- 支援 IPv4 和 IPv6

實體規格

- 標準 1U 19 英吋機架式規格
- 尺寸：482.6 mm x 533.4mm x 43.815mm
- 重量：28 磅 (12.7 公斤)
- 輸入電壓：100-240V，50-60Hz
- 耗電量：最高 110W，一般 84W
- 散熱性：最高 376BTU / 小時，一般 287BTU / 小時
- 溫度：作業溫度 0°C–35°C

可靠性

- 雙熱插拔電源
- 平均故障間隔 (MTBF) 171,308 小時

管理及監控

- HA 災難修復
- 將硬體備份、復原到地端或雲端硬體
- SNMP、Syslog

硬體型號規格

Luna A 系列 - 密碼驗證，簡易管理

A700	A750	A790
2 MB 記憶體	16 MB 記憶體	32 MB 記憶體
Partitions : 5	Partitions : 5	Partitions : 10
Maximum Partitions : 5	Maximum Partitions : 20	Maximum Partitions : 100
標準效能 RSA-2048 : 1,000 tps ECC P256 : 2,000 tps AES-GCM : 2,000 tps	企業效能 RSA-2048 : 5,000 tps ECC P256 : 10,000 tps AES-GCM : 10,000 tps	最大效能 RSA-2048 : 10,000 tps ECC P256 : 22,000 tps AES-GCM : 17,000 tps

Luna S 系列 - 多因素 (PED) 驗證，最高安全性部署環境

S700	S750	S790
2 MB 記憶體	16 MB 記憶體	32 MB 記憶體
Partitions : 5	Partitions : 5	Partitions : 10
Maximum Partitions : 5	Maximum Partitions : 20	Maximum Partitions : 100
標準效能 RSA-2048 : 1,000 tps ECC P256 : 2,000 tps AES-GCM : 2,000 tps	企業效能 RSA-2048 : 5,000 tps ECC P256 : 10,000 tps AES-GCM : 10,000 tps	最大效能 RSA-2048 : 10,000 tps ECC P256 : 22,000 tps AES-GCM : 17,000 tps

tps = 每秒交易處理量

payShield 10K 金融支付產業專用

專為信用卡支付系統與行動支付安全所設計的 硬體安全模組(HSM)，保障全球支付安全

- 適合銀行、第三方支付業者使用，符合國際發卡機構安全稽核要求
- 擁有業界領先的效能：最高可達 2,500 tps
- 提供高可用性及完善的金鑰管理機制
- 符合 FIPS 140-2 安全等級，提供硬體強化的防竄改環境、防外力破壞



主要特色

- payShield 10K 是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，payShield 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。
- 擁有高可用性與高效能的金融交易專用 HSM，可同時處理最高每秒 2,500 筆交易量，滿足金融業瞬間大量交易需求。
- 與 payShield 9000 設備相容，不需要改變既有資安政策，可共用現有的 LMK IC 晶片卡，且原本的 payShield 9000 客製化功能可升級到 payShield 10K。
- 滿足零售業導入 mPOS 系統的行動支付安全，從讀卡機產生密鑰，並確保 PIN 碼全程被保護，以及解密資料必須與商家網路隔絕。確保消費者信用卡個資不外流，提升商家交易安全信賴度。
- 保護終端模擬 (Host Card Emulation, HCE) 模式的行動支付安全。發卡者使用 HSM 可安全地產生並集中儲存支付憑證，且能彈性決定當離線授權時在何時、有多少金鑰可被存在手機中；而在線上授權時，發卡者則可即時驗證手機支付 App 的密文。
- payShield 10K 獨特功能讓行動支付中的各環節能安全配置相關應用，包括支付 App 的發行到手機。同時也能安全配置其他使用非接觸式支付的應用，如 NFC 或 P2P 支付應用等。
- 卡片 / 行動支付支援：payShield 10K 提供全面性功能，在以下多個領域提供主要支付品牌支援 (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 HSM 標準，如主要支付品牌的 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

法規遵循

- 整機符合支付交易安全要求 FIPS 140-2 Level 3 加解密模組最廣泛採用的安全標準。
- 符合最新導入的支付卡系統 HSM 標準 Payments Card Industry Hardware Security Module standard (PCI HSM v3)。
- 加密性能與管理功能符合或超越國際支付機構安全稽核要求，包括美國運通、Discover、JCB、Visa、Mastercard 以及銀聯。
- payShield 10K 符合 Global Platform Card Specification 以及 EMV Card Personalization Specification，能建立與行動支付安全元件之間的安全對話。

應用 - payShield 10K 專為信用卡支付設計包含發卡與支付作業

支付方式、載具變化，從傳統 ATM、信用卡等接觸式，衍生出行動支付、NFC 等非接觸式卡片，近年來亦發展出第三方支付，收單部分有無線化、行動化的趨勢。國內甚至有第三方支付專法通過，第三方支付產業預期可蓬勃發展，國內外電商及銀行也紛紛著手建置適用的交易平台與服務。

這樣的變化回歸原點，使用者是否能接受除了考慮方便性外，最重要的還是交易是否安全可靠。因此支付交易始終遵循國內外主管機關訂製嚴格的交易機制，HSM 在其中扮演至關重要的角色，負責金鑰管理、身分驗證、密碼驗證、交易資料加密等關鍵工作，HSM 除了確保安全性之外，同時也可以簡化作業過程，降低管理複雜度。

接觸式支付方式

- ▶ EMV
- ▶ DUKPT
- ▶ POS 收單系統
- ▶ 置發卡作業
- ▶ PCI DSS
- ▶ 磁條卡交易
- ▶ ATM 交易
- ▶ 信用卡交易
- ▶ 網路銀行

非接觸式支付方式

- ▶ TSM 金流信任管理平台
- ▶ PSP 支付服務業者
- ▶ mPOS 行動支付
- ▶ NFC 近場通訊
- ▶ HCEP2PE 點對點加密
- ▶ VISA/Master/JCB/
美國運通/銀聯



技術規格

支援加密演算法

- 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)
- FIPS 186-3 中定義的 ECC (P-256, P-384 & P-521)
- HMAC、MD5、SHA-1、SHA-2、SHA-224、SHA-256、SHA-384 & SHA-512

物理安全性

- 防篡改和回應式設計
- 一旦遭受任何竊改攻擊，機敏資料會立即清除
- 具備移動、電壓和溫度警報觸發器

邏輯安全性

- 本地端主金鑰 (LMK) 選項：variant 和 key block
- 資安人員須使用 Smart Card 進行雙因子身份驗證 (2FA)
- 雙重控制授權 - 實體鑰匙或 Smart Card
- 預設執行最高強度的安全設定
- 結合用戶控制事件範圍記錄的 Audit log
- 乙太網路主機 port 的 TLS 驗證 session

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

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、1,000、2,500 和 10,000 次調用 (cps)
- 可透過 payShield Manager、payShield Monitor 和 payShield 信任管理裝置 (TMD) 實現遠端管理及監控
- 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 英吋機架安裝
- 尺寸：482.6 mm x 736.6 mm x 44.5 mm
- 重量：35 磅 (15.9 公斤)
- 電源：90-264 VAC
- 功耗：60W (最大值)
- 作業溫度：0°C - 40°C