payShield 10K
The hardware security module that secures the world’s payments

- Simplifies deployment in dark data centers
- Delivers high resilience and availability
- Offers the broadest support of card and mobile applications in a timely manner
- Supports performance upgrades without hardware change
- Maintains backwards compatibility with all legacy Thales payment HSMs
Technical specifications

payShield 10K is a payment hardware security module (HSM) used extensively throughout the global payment ecosystem by issuers, service providers, acquirers, processors and payment networks. It plays a fundamental security role in securing the payment credential issuing, user authentication, card authentication and sensitive data protection processes for both face-to-face and digital remote payments.

Common use cases

• Payment credential issuing – cards, mobile secure elements, wearables, connected devices and host card emulation (HCE) applications
• PIN routing
• Point to point encryption (P2PE)
• Security tokenization (for PCI DSS compliance)
• EMV payment tokenisation
• Card and mobile payment authorization
• POS, mPOS and SPoC key management
• PIN and EMV cryptogram validation
• Remote key loading

The choice of integrators

• Integration with all major payment authorization and switching applications
• Technology partner details can be found at: www.thalesesecurity.com/partners/technology-partners

Card/mobile payment support

• payShield 10K has a comprehensive range of functions that supports the needs of the leading payment brands (American Express, Discover, JCB, Mastercard, UnionPay and Visa) in a number of areas including:
  * PIN and card verification functions for all major payment brands
  * EMV transaction authorization and messaging
  * Mobile payment transaction authorization and key management
  * Remote Key Loading for ATM and POS devices
  * Regional/National key management (including Australia, Germany and Italy)
  * Mastercard On-behalf key management (OBKM) support
  * Magnetic stripe and EMV-based data preparation and personalization including mobile provisioning
  * PIN generation and printing

Cryptographic algorithms

• DES and Triple-DES key lengths 112 & 168 bit
• AES key lengths 128, 192 & 256 bit
• RSA (up to 4096 bit)
• HMAC, MD5, SHA-1, SHA-2

Financial services standards

• ISO: 9564, 10118, 11568, 13491, 16609
• ASC X9 TR-31, X9 TG-3/TR-39
• APAC 40 & 70

Physical security

• Tamper resistant and responsive design
• Sensitive data erased immediately in the event of any tamper attack
• Alarm triggers for motion, voltage and temperature

Logical security

• Local Master Key (LMK) options – variant and key block
• Two-factor authentication (2FA) of security officers using smart cards
• Dual control authorization – physical keys or smart cards
• Strongest security settings implemented by default
• Audit trails with user control over the scope of events recorded

Product models and options

• Dual hot-swappable power supply units and fans standard across all models
• Range of performance levels – 25, 60, 250, 1000 & 2500 calls per second (cps)
• Remote management and monitoring options via payShield Manager, payShield Monitor and payShield Trusted Management Device (TMD)
• Format preserving encryption (FPE) options
• Multiple LMK options – up to 20 partitions per HSM

Host connectivity

• TCP/IP & UDP (1Gbps) – dual ports
• Secure Host Communications Management option for TLS authenticated sessions on Ethernet host port

Security certifications

• FIPS 140-2 Level 3 (security sub-system) in progress
• PCI HSM v3 (selected software versions)

Physical characteristics

• Form factor: 1U 19” rack mount
• Dimensions: 482.6 x 736.6 x 44.5mm (19 x 29 x 1.75”)
• Weight: 15.9 kg (35 lbs)
• Electrical Supply: 90 to 264 VAC
• Power Consumption: 60W (maximum)
• Operating Temperature: 0 deg C to 40 deg C
• Transportation Temperature: -25 deg C to 70 deg C
• Storage Temperature: -5 deg C to 45 deg C
• Humidity: 10% to 90% (non-condensing)

Safety and environmental compliances

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