cpl.thalesgroup.com

THALES
Building a future we can all trust

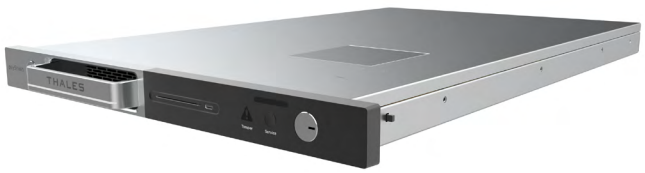
payShield 10K

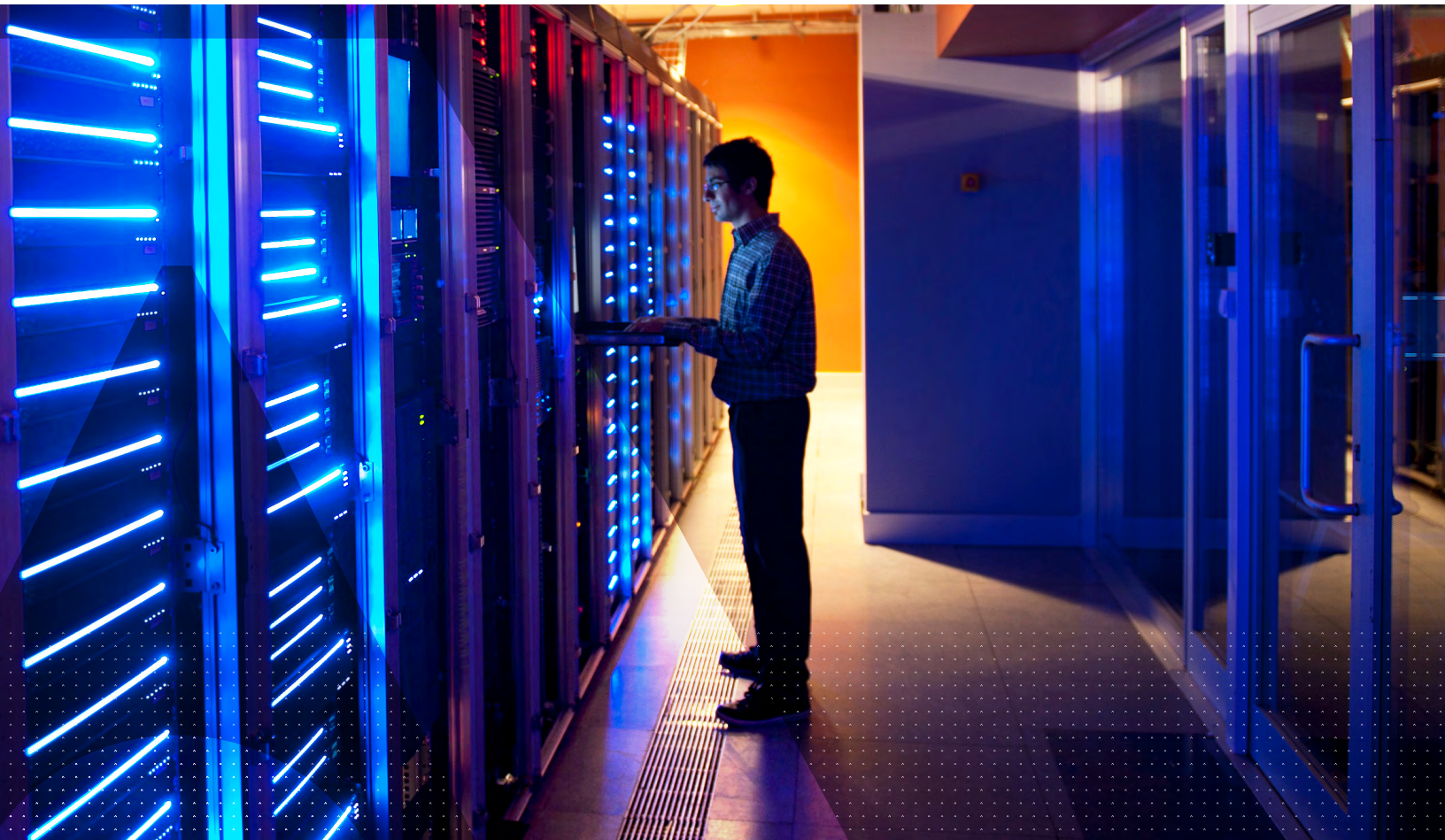
The hardware security module that secures the world's payments

payShield 10K

- 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

Now also available via the payShield Cloud HSM subscription service.





Overview

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: cpl.thalesgroup.com/partners/partner-search

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, Belgium, 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)
- ECC as defined in FIPS 186-3 (P-256, P-384 & P-521)
- HMAC, MD5, SHA-1, SHA-2, SHA-224, SHA-256, SHA-384 & SHA-512

Financial services standards

- 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 TR-34, X9 TG-3/TR-39
- APACS 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 logs with user control over the scope of events recorded
- TLS authenticated sessions on Ethernet host ports

Product models and options

- Range of performance levels – 25, 60, 250, 1000, 2500 & 10000 calls per second (cps)
- PS10-S 1Gbps dual host ports, Standard
- PS10-D 10Gbps dual host ports, platinum rated power supplies
- PS10-F FICON single host port, platinum rated power supplies
- Dual hot-swappable power supply units and fans standard across all models
- 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

Security approvals

- FIPS 140-2 Level 3 (for the TASP security subsystem)
- PCI HSM v3 including RAP
- PCI HSM v3 KLD (for payShield TMD)
- AusPayNet
- CB HSM (SAFIRE v2.2 methodology)
- GBIC pre-evaluation
- Bancontact certificate holder

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:
  - PS10-S - 60 W max
  - PS10-D - 70 W max (with 4 x optical transceivers); 80 W max (with 4 x copper transceivers)
  - PS10-F - 80 W max (with 1 x FICON transceiver)
- 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

- Nemko C/US, CE, BIS, FCC, Canada ICES, RCM, KC, VCCI, ZICTA, BSMI, UKCA, EAC, NOM
- RoHS3, REACH, WEEE, TCSA

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> cpl.thalesgroup.com <

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us