



> payShield 9000

The hardware security module securing the world's payments

KEY BENEFITS

- > Comprehensive security for card issuing and payment processing
- > Widespread global integration with major payment applications
- > Field-upgradeable functionality
- > Range of host connectivity options
- > Designed to exceed FIPS 140-2 Level 3 requirements
- > Modular software options
- > Software customisation available through Thales Professional Services team

The Thales payShield 9000 is a payment hardware security module (HSM) that generates, protects and stores encryption keys and customer PINs. It is a critical element in protecting Automated Teller Machine (ATM) and Point of Sale (POS) credit and debit card transactions. The cryptographic functionality and management features present in the payShield 9000 satisfy the card application and security audit requirements of the major international card schemes, including American Express, Discover, JCB, MasterCard and Visa.

It is deployed as an external peripheral for mainframes and servers running card issuing and payment processing software applications for the electronic payments industry.

A wide range of performance options are available to suit individual user needs. With this flexibility and their comprehensive range of functionality, Thales payment HSMs are the most widely deployed in the world, processing an estimated 70% of all payment card transactions.



>> payShield 9000

Technical Specifications*

Key management

- > Multiple Local Master Keys (LMKs) for secure storage and distribution of keys providing comprehensive separation of key types, applications or customer data as required
- > Known test LMK for use in non-production environments
- > Thales Key Block support (superset of ANSI X9.24)
- > X9 TR-31 Key Block support
- > RSA Public Key
- > DUKPT (DES and Triple-DES)
- > Master/Session Key
- > Racal Transaction Key
- > AS2805 Key (DES and Triple-DES)

Cryptographic support

- > DES and Triple-DES (two and three key)
- > RSA (up to 2048 bits)
- > AES and ECC via software upgrade

Performance

- > Range of performance models up to 1500 Triple-DES PIN block translates/second using key blocks
- > Multi-threading to exploit full performance capability
- > Clustering option when used in conjunction with Thales Security Resource Manager (SRM) application

Host connectivity

- > Asynchronous (v.24, RS-232)
- > TCP/IP & UDP (10/100/1000 Base-T)
- dual ports for resilience

Certifications

- > FIPS 140-2 Level 3 (in progress)
- > MEPS (in progress)
- > APCA (in progress)
- > PCI HSM (in progress)

Financial industry standards

- > American Express/MasterCard/VISA PIN and Card Verification functions
- > EMV 3.X and 4.X transactions and messaging (inc. PIN Change)
- > Remote Key Loading to NCR, Diebold and Wincor-Nixdorf ATMs
- > Europay Security Platform (MasterCard stand-in processing)
- > Integration with all major payment authorisation and transaction switching applications

Management facilities

- > Console interface for "dumb" terminals
- > Graphical User Interface (GUI) option for standard PC hardware over Ethernet - local and remote modes supported
- > Ability to manage clusters of payShield 9000 devices via external Thales Security Resource Manager (SRM) product

Security

- > Two-Factor Authentication of operators using Smart Cards
- > Dual physical locks or smart cards control setting of modes
- > Tamper-resistance designed to exceed requirements of FIPS 140-2 Level 3
- > Detection of removal of covers
- > Multiple alarm triggers for motion and voltage and temperature
- > Device 'hardening' - ability to disable functions not required by the host application

Physical characteristics

- > **Form Factor:** 2U 19" rack mount
- > **Height:** 85mm (3.35")
- > **Width:** 478mm (18.82")
- > **Depth:** 417mm (16.42")
- > **Weight:** 7.3kg (16lb) with single PSU
7.5kg (16.5lb) with dual PSU
- > **Voltage:** 100 to 240V AC Universal input
- > **Frequency:** 47 to 63Hz
- > **Power Consumption:** 100W (maximum)
- > **Operating Temperature:** 10°C to 40°C
- > **Humidity:** 10% to 90% (non-condensing)

*All specifications are preliminary and subject to change - contact Thales for further information.

Thales - Information Systems Security

