The Thales payShield 9000 is a payment hardware security module (HSM) that provides the cryptographic protection needed for Automated Teller Machine (ATM) and Point of Sale (POS) credit and debit card issuance and transactions. The cryptographic functionality and management features meet or exceed the card application and security audit requirements of the major international card schemes, including American Express, Discover, JCB, MasterCard, UnionPay and Visa. It is deployed as an external peripheral for mainframes and servers running card issuing, mobile provisioning and payment processing software applications for the electronic payments industry.

**Key Benefits**
- Delivers comprehensive, certified security specially designed for cards and mobile secure elements
- Provides off-the-shelf support for all major payment applications
- Maximizes business continuity with high resilience features
- Reduces the cost of compliance with a choice of software options tailored for issuers, processors, and acquirers
- Offers a range of scalable, high-performance models
Key management standards supported
- Thales Key Block support (compliant with ANSI X9.24; superset of X9 TR-31)
- X9 TR-31 Key Block support
- RSA Remote Key Transport
- DUKPT
- Master/Session Key Scheme
- Racial Transaction Key Scheme
- AS2805 support

Cryptographic algorithms supported
- DES and Triple-DES key lengths 112 bit, 168 bit
- AES key lengths 128 bit, 192 bit, 256 bit
- RSA (up to 2048 bits)
- FIPS 198-1, MD5, SHA-1, SHA-2

Performance options
- Range of performance options up to 1500 Triple-DES PIN block translates / second using key blocks
- Multi-threading to optimize performance

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

Certifications / validations
- Cryptographic module certified to FIPS: 140-2 Level 3, 46, 81, 180-3, 186-3, 198
- PCI HSM*
- APCA
- GBIC
- MEPS
- NIST SP800-20, SP800-90(A)

Financial services standards supported
- ISO: 9564, 10118, 11568, 13491, 16609
- X9 TR-31, X9 TG-3/TR-39, APACS 40 & 70, AS2805 Pt 14

Card payments support
- 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
- MasterCard On-behalf Key Management (OBKM)
- Integration with all major payment authorization and switching applications

Management facilities
- Secure Host Communications option for TLS/SSL authenticated sessions on Ethernet host ports
- Graphical User Interface (GUI) option for standard PC hardware over Ethernet - local and remote modes supported
- Key Management Device (KMD) option to form keys from components
- Console interface for “dumb” terminals
- Clustering interface for Thales Security Resource Manager (SRM) application
- SNMP
- Utilization statistics, health check diagnostics and error logs

Security features
- Multiple master keys option enabling cryptographic isolation
- Two-Factor Authentication of security officers using smart cards
- Dual physical locks and/or smart cards control authorization levels
- Tamper-resistance exceeding requirements of PCI HSM and FIPS 140-2 Level 3
- Detection of cover removal in addition to alarm triggers for motion, voltage and temperature
- Device ‘hardening’ - ability to disable functions not required by the host application
- Audit trails

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
- Electrical Supply: 100 to 240V AC Universal input, 47 to 63 Hz. Dual power supply option on all models for resilience
- Power Consumption: 100W (maximum)
- Operating Temperature: 0 deg C to 40 deg
- Humidity: 10% to 90% (non-condensing)

* Customers must explicitly specify a PCI HSM compliant product at the time of order. Special software, delivery and configuration conditions apply when ordering a PCI HSM compliant product.