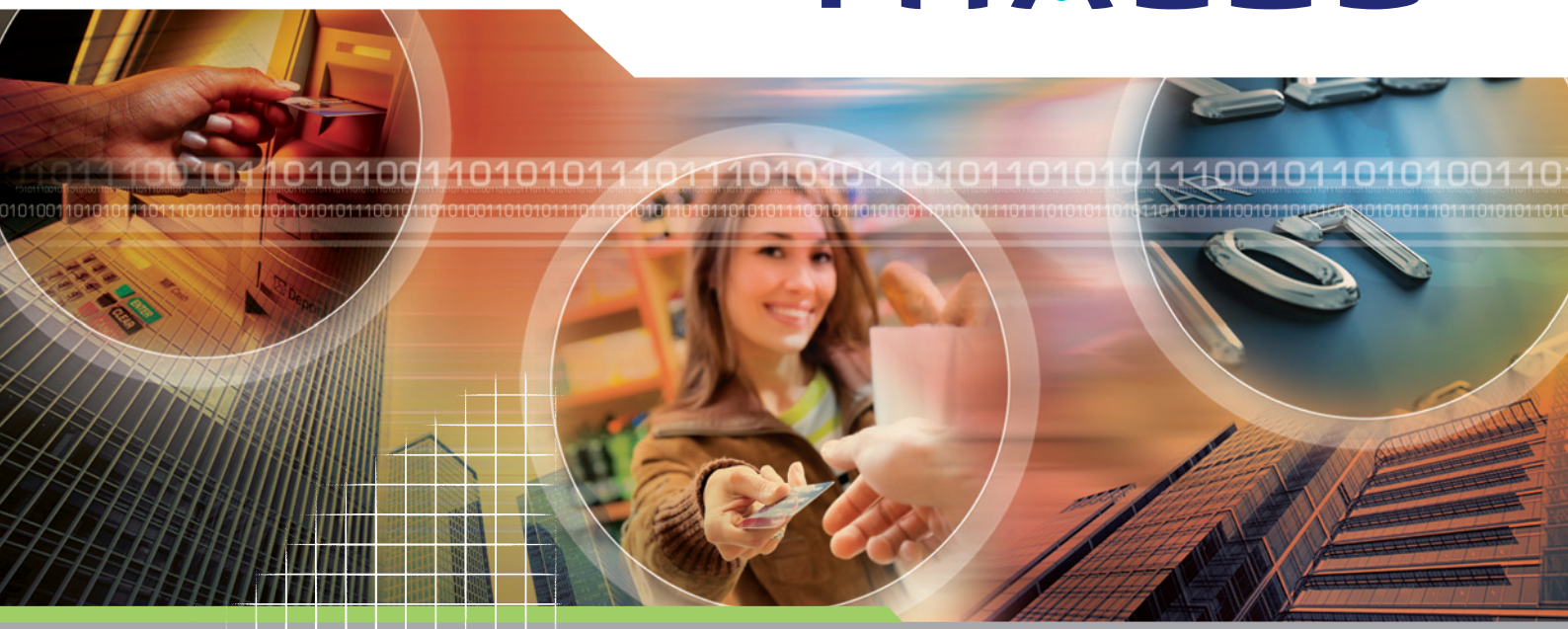
THALES

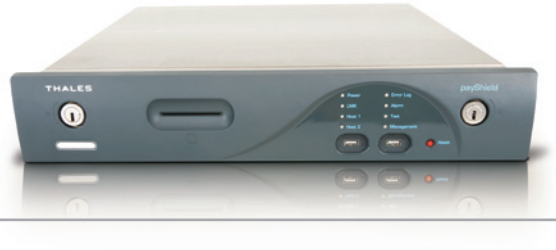


Thales e-Security payShield 9000

The hardware security module that secures the world's payments

KEY BENEFITS

- Simplified audit compliance leveraging existing FIPS and PCI HSM certifications
- Lower operating costs enabled by robust remote management
- High resilience features maximizing device uptime
- Flexible and secure key component management using the Key Management Device (KMD)
- Capacity planning simplified by built-in utilization statistics



The Thales payShield 9000 is a hardware security module (HSM) built specifically for payment security that generates, protects and stores encryption keys and customer PINs based on globally recognized encryption standards. It incorporates a market-leading combination of high resilience features, extensive diagnostics, cryptographic performance and most importantly independent security validation.

payShield 9000 offers functionality to support the latest card scheme payment applications for contact chip, contactless chip and mobile secure elements and focuses on supporting evolving standards from leading industry organizations including PCI SSC, Global Platform and Multos International. Customers have flexibility in choosing the best performance model and base software package for their specific needs, maximizing investment and lowering costs.

Thales payment hardware security modules (HSMs) are the most widely deployed and integrated globally with all leading payment application software. Customers trust Thales HSM technology to help deliver a secure issuing and processing environment essential for credit and debit card transactions.

>> payShield 9000

Technical Specifications*

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 Public Key
> DUKPT for PIN and data encryption
> Master/Session Key Scheme
> Racal Transaction Key Scheme
> AS2805 support

Cryptographic algorithms supported

> DES and Triple-DES (two and three key)
> AES (128, 192 and 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 optimise 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 v1
> APCA
> MEPS
> NIST SP800-20, SP800-90(A)

Financial services standards supported

> ISO: 9564, 10118, 11568, 13491, 16609
> ANSI: X3.92, X9.8, X9.9, X9.17, X9.24, X9.31, X9.52, X9.97
> 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
> Europay Security Platform (MasterCard stand-in processing)
> Integration with all major payment authorization and switching applications

Management facilities

> 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 using Thales Security Resource Manager (SRM) application
> SNMP
> Built-in error logs

Security features

> 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 C
> **Humidity:** 10% to 90% (non-condensing)

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

Americas: Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific: Unit 4101 41/F 248, Queen's Road East, Wanchai, Hong Kong, PRC • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa: Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com