

# THALES



## payShield 9000

The hardware security module  
securing the world's payments



# payShield 9000

## Table of Contents

<b>Introduction</b>	<b>4</b>
<b>Thales Hardware Security Module</b>	<b>5</b>
<b>Overview of Cryptographic Services</b>	<b>5</b>
<b>Typical HSM applications</b>	<b>6</b>
ATM interchange	6
EFTPOS	6
Card issuing	6
Transaction processing	7
Data security	7
<b>payShield 9000 features</b>	<b>7</b>
Performance options	7
Flexible key management system	7
RSA public key support	8
Remote management	8
ATM remote key loading	8
Security certification	9
Secure key storage and generation	9
Extensive host system support	9
Security Resource Managers	9
<b>About Thales</b>	<b>11</b>



# Introduction

## Hardware Security Module

As an organisation in the payment card industry, you face the challenges of supporting increases in transaction volumes, replacing magnetic stripe cards with contact and/or contactless smart cards, securing remote delivery channels such as mobile or internet while still needing to differentiate your services for competitive advantage. The constant need to defeat new security threats is a major consideration in your IT investment year-on-year. In addition to the increasing burden of regulation, your solutions must incorporate cryptographic security that meets the latest payment card industry (PCI) mandates and is able to grow and adapt to support your emerging needs.

The payShield 9000, the latest hardware security module (HSM) from Thales, meets these challenges. Its software options address the needs of card issuers, merchant acquirers, switches, third party payment processors, card schemes and ATM network providers. The core security component of the payShield 9000, which delivers the critical security functionality, is designed to exceed the requirements of FIPS 140-2 Level 3 - the most widely adopted certification standard for cryptographic modules which is mandated by the card schemes. The payShield 9000 is fully backward compatible with the HSM 8000 and RG7000 ranges which it succeeds.



Designed specifically as a tamper-resistant peripheral, the payShield 9000 connects to the host system without the need for host client software. It provides the full range of cryptographic facilities necessary for issuing payment cards and securing credit and debit card transactions in financial networks.

As a dedicated payment HSM, it is used to secure a wide range of financial infrastructures around the world including Automated Teller Machine (ATM) and point-of-sales (POS) networks, inter-bank funds transfer systems and share dealing systems. The software functionality enables it to support the latest types of remote delivery channel (such as mobile and internet) both in terms of transaction security and user authentication/data security protection if required. It is available in various performance variants (to match individual user needs) with a wide range of connectivity options and protocols allowing connection to all types of host systems.



## Thales Hardware Security Modules are:

- Involved in securing over 70% of the world's payment card transactions
- Deployed by leading card schemes and payment processors for a variety of key management, payment switching and authorisation purposes
- Capable of being fully managed remotely from the data centre
- Proven in delivering strong security for ATM, POS, corporate banking, card issuing, funds transfer and share trading systems
- Easy to customise for individual user applications
- Designed to support a wide range of host interface connectivity options
- Available in various performance variants to match user transaction processing requirements
- Upgradeable in terms of functionality through secure auditable software license downloads
- Integrated with all major payment applications provided by leading vendors
- Independently certified to the most rigorous global and national security standards



## Overview of Cryptographic Services

- Visa/MasterCard/American Express PIN and Card Verification Functions,
- EMV 3.x and EMV 4.x transaction processing and secure messaging (including PIN Change),
- Remote Key Loading for NCR, Diebold and Wincor-Nixdorf ATMs,
- Fully compliant with 3 key Triple DES standards for all relevant functions including PIN block processing,
- Triple-DES DUKPT, APACS, and AS2805 transaction key schemes,
- RSA key generation, signing and verification,
- ANSI X9.24 Part 1 and X9 TR-31 for enhanced key management using key blocks.



## Typical HSM applications

### ATM interchange

payShield 9000 is designed for the ATM interchange environment and can be customized to suit individual networks and, if needed, the particular requirements of each member of the network. The wide variety of host interface options and PIN management commands available in the payShield 9000 family means that the specific needs of each member's system can be readily accommodated. In particular, specific functions designed around AMEX, Visa and MasterCard processing requirements are an integral part of the core software packages.

### EFTPOS

Thales payment HSMs support a large number of Electronic Funds Transfer at Point of Sale (EFTPOS) systems in use around the world. Many of the key management concepts required to secure EFTPOS, such as the Racal Transaction Key scheme, were pioneered by Thales and implemented in RG7000 and HSM 8000 product families and now have been migrated to the payShield 9000. Single and Triple-DES versions of the Derived Unique Key per Transaction, APACS, and AS2805 transaction key schemes are also available.

### Card issuing

A range of software modules available in the payShield 9000 make it a secure, highly reliable component for use within a card production area for both magnetic stripe and chip-based cards. It has proven integration with leading card management systems worldwide. Providing a secure means of generating cryptographic card values such as Visa's CVV (Card Verification Value), MasterCard's CVC (Card Verification Code) and American Express CSC (Card Security Code), it can also be used for secure PIN block and PIN mailer generation. The full range of EMV data preparation options for all major contact and contactless applications are available for use directly by the issuer host system.



## Transaction processing

PayShield 9000 supports the transaction processing requirements of the full range of credit and debit card applications from the major card schemes, namely American Express (AMEX), JCB, MasterCard and Visa. The difference in requirements between magnetic stripe, contact chip and contactless chip cards are fully implemented. The core payShield 9000 transaction processing software provides transaction processing commands for EMV 3.x and EMV 4.x based systems for issuers and acquirers supporting EMV chip cards.

## Data security

The integrity of information transmitted around and stored within systems is of paramount importance to its users. Normally information generated at remote terminals will be secured using Message Authentication Codes (MACs). payShield 9000 supports a wide range of MAC processing options to suit individual user needs together with encryption/decryption commands where privacy is required. Many Thales HSM customers have already taken advantage of these facilities to assist with their PCI DSS compliance.



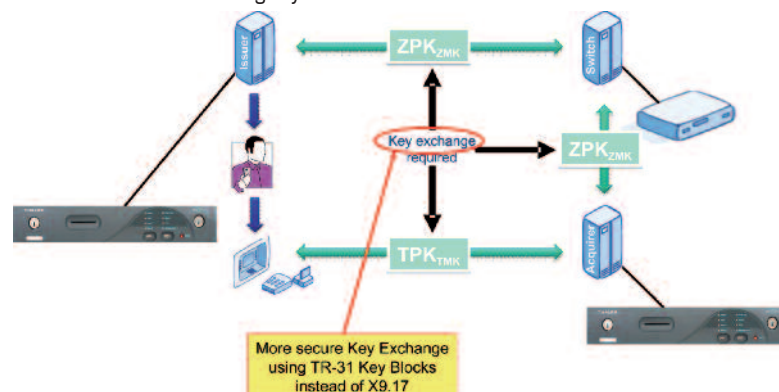
## payShield 9000 features

### Performance Options

As the banking and financial industries continue to move toward PIN-based and smart card security systems, the demand for higher transaction speeds has never been greater. In its highest speed variant, the payShield 9000 provides 1500 Triple-DES PIN Block translate functions per second (tps), significantly reducing transaction processing time and lowering the cost per transaction. For environments or applications where such high levels of performance is not essential, the option to deploy one of the other models in the payShield 9000 models (starting at 20 tps) allows you choose the most cost-effective model for your particular system.

### Flexible key management system

In practice, the security offered by any application is only as good as the key management system designed for it. payShield 9000 supports a variety of key management schemes, including Master/Session Key, APACS/Racal Transaction Key, AS2805, DUKPT and Public Key. There is also full support for the variant LMK scheme in addition to the key block scheme (based on ANSI X9.24 and X9 TR-31) in both standard and custom software to enable customers to use security best practices and eliminate know weaknesses with legacy standards such as ANSI X9.17.



## RSA Public Key Support

payShield 9000 offers a high-speed public key subsystem. RSA Public Key cryptography is used for two primary functions:

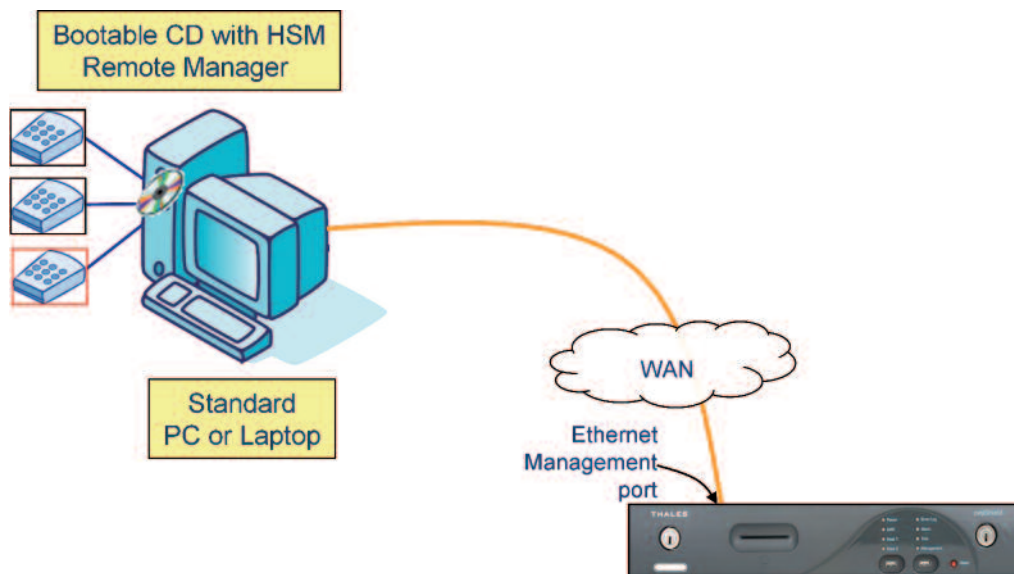
- To generate and verify digital signatures,
- To distribute DES keys encrypted under an RSA Public Key.

payShield 9000 supports RSA key lengths from 320 to 4096 bits in steps of 16 bits.

This feature allows payShield 9000 to be used in systems where different key lengths are used for different functions, such as digital signatures and key management. In addition, it protects an organisation's technology investment, as the industry is expected to increase key length requirements to keep ahead of increased threats.

## Remote Management

The deployment of the Thales Remote HSM Manager solution provides a significant reduction in operating costs by offering a modern, secure way to manage both HSM 8000 and payShield 9000 devices remote from the data centre. An intuitive, faster to use user interface, providing greater flexibility enables easy integration into the existing organisational structure with minimal training overheads.



## ATM remote key loading

RSA based functions are provided to support remote key loading for NCR, Diebold and Wincor-Nixdorf ATMs. This enables the initialisation of ATM master keys to be automated, providing significant cost savings.

## Security certification

payShield 9000 uses the Thales Secure Processing Platform (TSPP) for the management and processing of all cryptographic keys, PINs and other sensitive data. This subsystem is designed to exceed the requirements of FIPS 140-2 Level 3. Like its predecessor, the HSM 8000, the payShield 9000 is undergoing certification under the MEPS accreditation scheme, required to secure transactions on French banking networks and under the APCA scheme for the Australian market. payShield 9000 is a product designed to meet the Payment Card Industry (PCI) HSM standard, exceeding the mandatory security requirements of today's financial networks and keeping transactions secure now and in the future.

## Secure key storage and generation

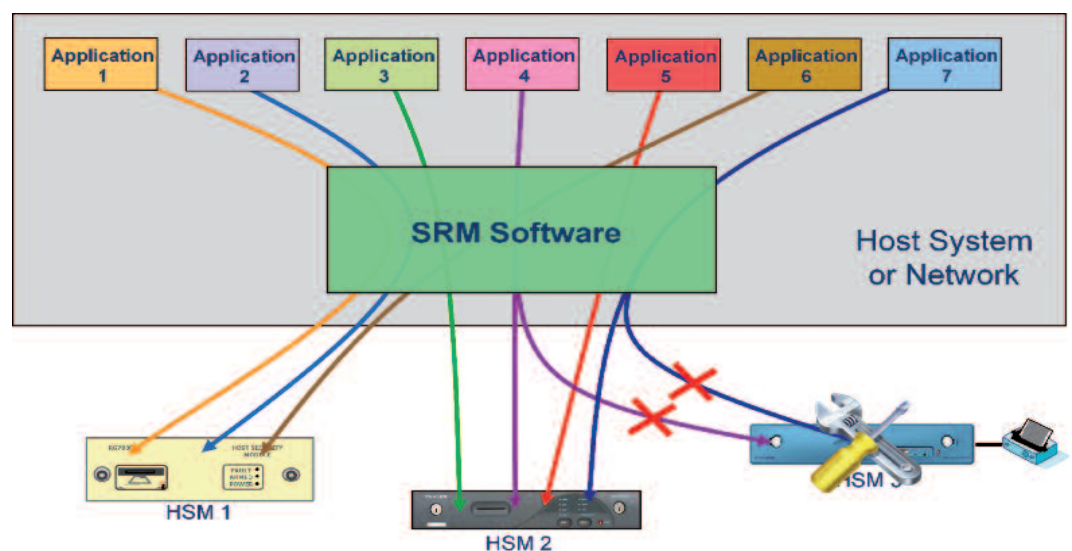
Once the Local Master Key (LMK) has been formed within the payShield 9000, all other keys are stored encrypted under this key on the host and optionally within the HSM itself. payShield 9000 uses Smart Card technology to back up the key components of the LMK.

## Extensive host system support

payShield 9000 is integrated with applications supplied by all the leading financial industry solution providers. A range of communications protocols are supported. The standard payShield 9000 supports TCP/IP and UDP (through an auto-sensing 10/100/1000 BaseT Ethernet interface) and Asynchronous connections.

## Security Resource Managers

The Security Resource Managers (SRMs) are optional software products for z/OS and OS/390, HP NonStop (Tandem Guardian), and IP-connected systems. The SRMs allow multiple applications to use a single Application Programming Interface (API) to access the cryptographic resource provided by a "farm" of payShield 9000 units. The SRM allows different Thales HSM models (RG7000, HSM 8000 and payShield 9000) to be used transparently to customer applications. In the event that any particular HSM is not available, the SRM automatically routes the request to another available device.



IBM version - operates under z/OS or OS/390 and provides support for CICS, IMS, and Batch Applications. Support is also provided for assembly language programs as well as high level languages such as COBOL and PL/1.

HP NonStop version - operates under the NSK (formerly Tandem Guardian) operating system as a Pathway application and accepts requests either via an application interface module or a server interface. It can also provide applications with a key database that can be managed either by the application or by a supplied key management user interface.



---

## About Thales

Thales is a leading international electronics and systems group, addressing defence, aerospace and security markets worldwide.

Thales's leading-edge technology is supported by 22,000 R&D engineers who offer a capability unmatched in Europe to develop and deploy field-proven mission-critical information systems.

To this end, the group's civil and military businesses develop in parallel and share a common base of technologies to serve a single objective: the security of people, property and nations.

The group builds its growth on its unique multi-domestic strategy based on trusted partnerships with national customers and market players, while leveraging its global expertise to support local technology and industrial development.

Thales employs 68,000 people in 50 countries with 2008 revenues of €12.7 billion.

**Thales**  
Security Solutions & Services  
Information Systems Security



**Americas**

2200 North Commerce Parkway  
Suite 200  
Weston, Florida  
33326

Tel.: +1 888 744 4976 or +1 954 888 6200  
Fax: +1 954 888 6211  
E-mail: [sales@thalessec.com](mailto:sales@thalessec.com)



**Asia Pacific**

Units 2205-06  
22/F Vicwood Plaza  
199 Des Voeux Road Central  
Hong Kong, PRC

Tel.: +852 2815 8633  
Fax: +852 2815 8141  
E-mail: [asia.sales@thales-esecurity.com](mailto:asia.sales@thales-esecurity.com)



**Europe, Middle East, Africa**

Meadow View House  
Long Crendon  
Aylesbury  
Buckinghamshire  
HP18 9EQ. UK

Tel.: +44 (0)1844 201800  
Fax: +44 (0)1844 208550  
E-mail: [emea.sales@thales-esecurity.com](mailto:emea.sales@thales-esecurity.com)