

THALES



Host Security Module 8000

www.thalesgroup.com/esecurity

>> HOST SECURITY MODULE

The HSM is a tamper-resistant device that provides the cryptographic facilities necessary for securing transactions in financial networks.

The HSM is used to secure a multitude of financial applications around the world ranging from ATM and POS networks to interbank funds transfer and share dealing systems. It is available in various performance variants with a wide range of interface options and protocols allowing connection to all types of host system.

The Host Security Module is:

- Used for 70% of the world's card transactions
- Used by all major card associations
- Used for ATM, POS, corporate banking, card issuing, funds transfer and stock/share trading
- Easily customised for user applications

- Visa/MasterCard/American Express PIN and Card Verification Functions
- EMV 3.1.1, EMV 4.0 and 4.1 transaction processing and secure messaging (including PIN Change)
- Remote Key Loading for NCR and Diebold ATMs
- Triple-DES DUKPT and Australian Transaction Key schemes
- RSA key generation, signing and verification
- Async, Ethernet, SNA supported on all models
- ESCON option available
- Message Encryption
- Comprehensive Auditing Functionality
- Europy Security Platform (ESP)

- Available with support for a wide range of connectivity options and transaction protocols.
 - Available in various speed variants to give required transaction throughput.
 - Triple DES capable, using two and three keys, for all functions including the processing of PIN blocks.
 - Integrated within all major financial industry solution providers applications.
- Certified to the most rigorous security standards.

Typical HSM Applications

ATM Interchange

The HSM is designed for the ATM interchange environment and is in use in many of the world's major ATM interchange networks. The HSM can be customized to suit individual networks and, if needed, the particular requirements of each member of the network. The wide and growing variety of host interfaces in the HSM means that the needs of each member's system can be readily accommodated. In particular, the AMEX, MasterCard and VISA commands are an integral part of all standard functionality.

EFTPOS

The HSM supports a number of EFTPOS (Electronic Funds Transfer at Point of Sale) 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 the HSM. Single and Triple-DES versions of the Derived Unique Key Per Transaction and Australian Transaction Key schemes are also available.

Card Production Facility

The HSM is suitable for use within the client card production area. It can provide 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) as well as securely generating PINs and PIN mailers.

Chip Card Support

The HSM supports Credit/Debit and Electronic Purse chip card applications from Visa and MasterCard. The standard HSM software provides transaction processing commands for EMV 3.1.1, EMV 4.0 and 4.1 based systems.

Electronic Purse

The HSM can support VISA Cash, CLIP, and VCEPS processing, enabling card holders to securely reload value to their cards from an ATM or card reload terminal.

Data Integrity

The integrity of information transmitted around and stored within systems is of paramount importance to its users. The integrity of information generated at remote terminals can be secured, using message authentication codes (MACs). The HSM is compatible with WebSentry™ and Smart Card terminals. A number of applications such as Cash Management and Bond Reconciliation can be secured in this way.

HSM 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 high speed variant, the HSM provides industry leading performance (800 Triple-DES PIN Block translate functions per second), significantly reducing transaction processing time and lowering the cost per transaction.

Flexible Key Management System

In practice, the security offered by any application is only as good as the key management system designed for it. The HSM supports a variety of key management schemes, including Master/Session Key, Racal Transaction Key, Australian Transaction Key, DUKPT, and Public Key.

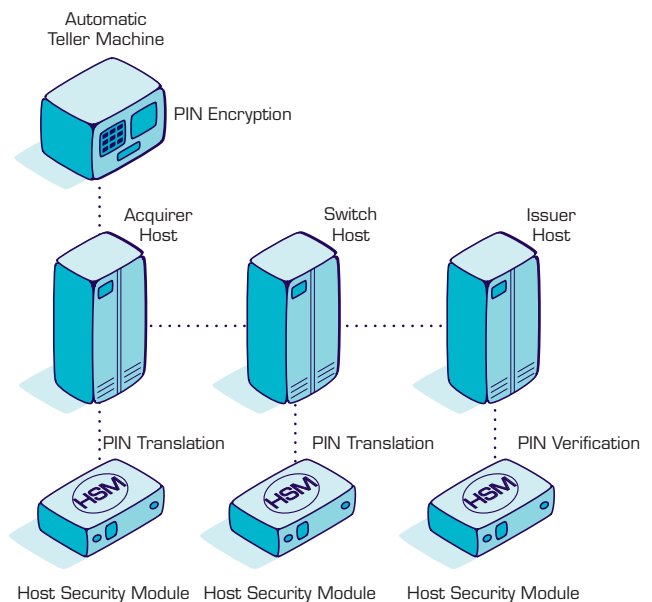
RSA Public Key Support

The HSM offers a high-speed Public Key subsystem. RSA Public Key cryptography is used for two primary functions:

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

The HSM supports RSA key lengths from 320 to 2048 bits. This feature allows the HSM 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.

Typical ATM Interchange Application



ATM Remote Key Loading

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

Security Certification

The HSM utilises the Thales Secure Generic Sub-System (SGSS) for all its cryptographic and security processing. This subsystem is validated to FIPS 140-1 level 4 and FIPS 140-2 level 3.

The HSM 8000 has successfully completed the MEPS accreditation, required to secure transactions on French banking networks.

The HSM is a product designed to exceed the security requirements of today's financial networks.

Secure Key Storage and Generation

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



Extensive Host System Support

The HSM is integrated with applications supplied by all the leading financial industry solution providers.

A range of communications protocols are supported. The standard HSM 8000's support TCP/IP and UDP (through an auto-sensing 10/100 BaseT ethernet interface), SNA and Asynchronous connections. ESCON is available as an option for IBM mainframe systems.

Security Resource Managers

The Security Resource Managers (SRMs) are optional software products for IBM MVS, Tandem Guardian, and UNIX® systems. The SRMs allow multiple applications to use a single Application Programming Interface (API) to access the cryptographic resource provided by a set of HSMs. The SRM allows different HSM models to be used transparently to customer applications.

- IBM version - operates under 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.
- Tandem version - operates under the 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.
- UNIX version – operates under several variants of UNIX. It operates as a server supporting client applications on multiple network machines. The API supports applications written in C or C++.

Technical Specifications

Typical Performance (Triple DES PINBlock Translate)	A range of models supporting up to 800 Triple DES PINBlock translates per second.	
Cryptographic Support	<p>DES and Triple DES Algorithms – Provide PIN encryption and message authentication capabilities.</p> <p>RSA Algorithm – Provides high-level key management including remote key loading for ATMs, and supports the generation and validation of digital signatures. RSA key length is selectable from 320 to 2048 bits.</p> <p>Local Master Key Components – These are stored on Smart Cards (ISO 7816) for secure storage or distribution.</p>	
Communications Interfaces	HSM8-S	TCP/IP and UDP, Ethernet 10/100Base-T; Async, RS232, SNA (v.24/RS-232)
	HSM8-E	ESCON; TCP/IP and UDP, Ethernet 10/100Base-T; Async, RS232, SNA (v.24/RS-232)
Security Certification	The HSM utilises the Thales Secure Generic Sub-System (SGSS) for all its cryptographic and security processing. This subsystem is validated to FIPS 140-1 level 4 and FIPS 140-2 level 3.	
Power	Voltage	90-132 VAC and 175-264 VAC, auto-selected
	Frequency	47-63 Hz
	Fuse	1.6A delayed action
Environmental	Operating Temp.	10° to 40° C
	Humidity	10% to 90%, non-condensing
Physical Dimensions	Height	88 mm (2U)
	Width	480 mm (to fit 19" rack)
	Depth	400 mm
	Weight	12 kg



TM: A certification Mark of NIST which does not imply product endorsement by NIST, the U.S. or Canadian Governments.
FIPS 140-2 logo

EUROPE, MIDDLE EAST, AFRICA

Meadow View House, Crendon Industrial Estate
Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ, UK
Tel: +44 (0)1844 201800, Fax: +44 (0)1844 208550
e-mail: emea.sales@thales-esecurity.com

AMERICAS

2200 N. Commerce Parkway, Suite 200, Weston, Florida 33326, USA
Tel: +1 888 744 4976, +1 954 888 6200, Fax: +1 954 888 6211
e-mail: sales@thalesesec.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

FIPS 140-1™: A validation mark of NIST, which does not imply product endorsement by NIST, the U.S. of Canadian Governments. MasterCard is a registered trademark of MasterCard International Incorporated. Visa is a registered trademark of Visa International Service Association. IBM is a registered trademark of International Business Machines Corporation. American Express and Amex are registered trademarks of American Express Company. UNIX is a registered trademark of The Open Group. HP and Tandem are registered trademarks of Hewlett-Packard Company. NCR is a registered trademark of NCR Corporation. Diebold is a registered trademark of Diebold Corporation. All other logos and product names are trademarks or registered trademarks of their respective companies. The Thales policy is one of continuous development and consequently the equipment may vary in detail from the description and specification in this publication



Certificate no. EMS 73638



Certificate no. FS68836