



HOST SECURITY MODULE

- Supports ATM, EFTPOS, EMV (Europay, Mastercard and Visa), and Chip Card Applications
- Visa/MasterCard/American Express PIN and Card Verification Functions
- Europay Security Platform (ESP) functionality
- FIPS Validated
- DES, Triple DES Two and Three Key, RSA
- Supports ATM Remote Key Loading
- VISA CASH, CLIP and VCEPS
- Supports ANSI, ISO, and Australian Security Standards.

→ 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 standard and high speed variants with a wide range of connectivity options and protocols allowing connection to all types of host systems.

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
- 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, VISA and MasterCard commands are an integral part of all standard firmware releases.

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 Thales Transaction Key method, were pioneered by Thales and implemented in the HSM. 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

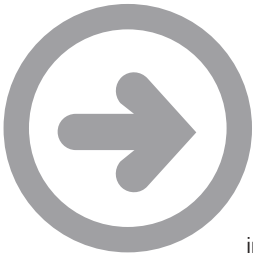
The HSM supports Credit/Debit and Electronic Purse chip card applications from Visa, MasterCard and Europay. The transaction processing functions are available as standard card issuing functions on request. For more information contact your local representative.

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), by Thales PC Security Modules, WebSentry™ and Smart Card terminals for subsequent verification by an HSM. A number of applications such as Cash Management and Bond Reconciliation can be secured in this way.



HSM Features Various Speed Variants

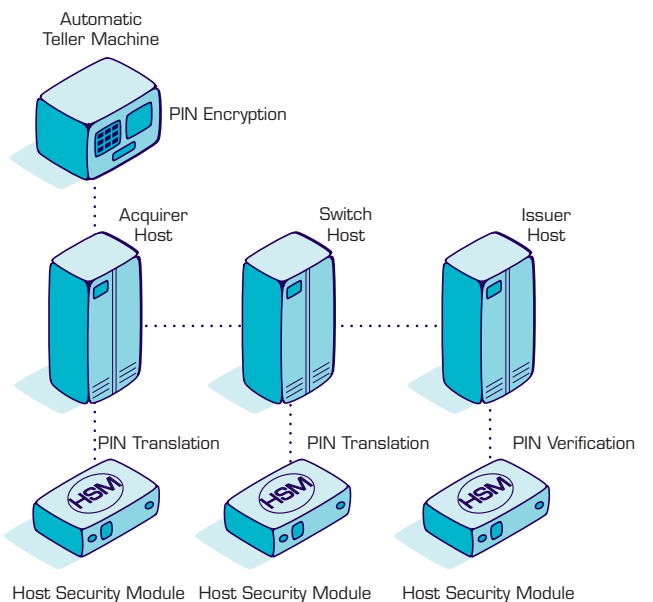
As the banking and financial industries continue to move toward PIN-based and Smart Card security systems, the demand for higher transaction speeds has never been greater.

In its high speed variant, the HSM provides industry leading performance (800 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.

Typical ATM Interchange Application



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 and
- 2) to distribute DES keys encrypted under an RSA Public Key.

The HSM can handle 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.

ATM Remote Key Loading

RSA based functions are provided to support remote key loading for 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 Subsystem (SGSS) for all its cryptographic and security processing. This subsystem is validated to FIPS 140-1 level 4 and is in final stages of validation under the more rigorous FIPS 140-2* standard.

The HSM overall has been submitted for FIPS validation and is expected to achieve FIPS 140-2 level 3* on completion.

The HSM is a product designed to exceed the stringent 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 Software Support

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

The HSM can connect to many different hosts including: Amdahl®, Bull®, IBM, ICL, DEC, HPI®, NCR®, Stratus®, Tandem®, Unisys® and PCs.

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 various flavours of UNIX. It operates as a server to client applications running on the same machine as the SRM or from any machine on the network. The API supports applications written in C or C++.



Technical Specifications

Typical Performance (Triple DES PINBlock Translate)	HSM8-SM	220
	HSM8-EM	220
	HSM8-SH	800
	HSM8-EH	800

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-SM / HSM8-SH	TCP/IP and UDP, Ethernet 10/100Base-T; Async, RS232
	HSM8-EM / HSM8-EH	ESCON; TCP/IP and UDP, Ethernet 10/100Base-T; Async, RS232

Security Certification	<p>The HSM utilises a Secure Generic Sub-System (SGSS) for all cryptographic and security processing this is validated to FIPS 140-1 level 4.</p> <p>The Sub-System is under evaluation at FIPS 140-2 level 4 and the HSM overall at FIPS 140-2 level 3.</p>
-------------------------------	--

Power	Voltage	90-132 VAC and 175-264 VAC, auto-selected
	Frequency	47-63 Hz
	Fuse	1.6A delayed action

Environmental	Operating Temperature	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

*Check on the NIST website for status of these validations.





THALES

Distributed by:
Network Technologies Dtl. GmbH
Bernhardstrasse 10
D-53902 Bad Muenstereifel - GERMANY
Tel: +49 (0)2253-92 42 0, Fax: +49 (0) 2253-92 42 29
e-mail: info@ntdgmbh.de
Internet: www.ntdgmbh.de

FIPS 140-1™: A validation mark of NIST, which does not imply product indorsement by NIST, the U.S. of Canadian Governements.

IBM is a registered trademark of International Business Machines Corporation. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd. HP is a registered trademark of Hewlett-Packard Company. Amdahl is a registered trademark of Amdahl Corporation. Bull is a registered trademark of Bull S.A. DEC is a registered trademark of Digital Equipment Corporation. NCR is a registered trademark of AT&T Global Information Solutions Company. Stratus is a registered trademark of Stratus Corporation. Tandem is a registered trademark of Tandem Computers Inc. Unisys is a registered trademark of Unisys 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.

Publication Number: 089/1002/10309 ©2002.