



## Host Security Module HSM 8000

Securing payment transactions

### Key Benefits

- > Optimised for payment applications
- > Delivers cryptographic security required by payments industry
- > Cost-effective and field-upgradable performance and functionality options
- > Continuing development programme and bespoke customisation meet all users' needs
- > All key certifications and compliances
- > Supports all major payment authorisation and transaction switching applications

The Thales HSM 8000 is a secure peripheral for hosts running software for the electronic payments industry. It provides the security and cryptographic functions mandated for electronic payments by the payments industry. Being an external device, the HSM 8000 can be used with any type of host. A wide choice of performance options are available to cost effectively meet the needs of all types of users. With this flexibility and their comprehensive range of functionality, Thales HSMs are the most widely deployed in the world, processing an estimated 70% of all payment card transactions.

# >> Host Security Module

## Technical specifications

### Key management

- > Multiple Master Keys for secure storage and distribution of keys. Separation of different key types, applications or clients, and of development and production use
- > TR-31 Key Block support for key exchange
- > Thales Key Block support for secure key storage
- > RSA Public Key
- > DUKPT (DES and Triple-DES)
- > Master/Session Key
- > Racal Transaction Key
- > AS2805 Australian Transaction Key (DES and Triple-DES)
- > Mastercard On-Behalf Key Management

### Cryptographic support

- > DES and Triple-DES (two and three key)
- > RSA

### Performance

- > Range of performance models up to 800 Triple-DES pin block translates/sec.
- > Multi-threading to exploit full capacity
- > Clustering capability

### Host connectivity

- > Asynchronous (v.24, RS-232)
- > TCP/IP & UDP (10/100 Base-T)
- > SNA (v.24, RS-232)
- > ESCON

### Certifications

- > Secure Generic Sub-System (SGSS) certified at FIPS 140-2 Level 3
- > RoHS
- > MEPS

### Financial industry standards

- > VISA/MasterCard/American Express PIN and Card Verification functions
- > EMV 3.1.1, 4.0, and 4.1 transactions and messaging (inc. PIN Change)
- > Remote Key Loading to NCR, Diebold and Wincor Nixdorf ATMs
- > Europay Security Platform
- > Integration with all major payment authorisation and transaction switching applications

### Management facilities

- > Console interface for "dumb" terminals
- > Graphical User Interface option for standard PC hardware over Ethernet
- > Management of HSM 8000 clusters by Host applications

### Security

- > Two-Factor Authentication of operators using Smart Cards
- > Dual physical locks control setting of modes
- > Tamper-resistance certified to FIPS 140-2 Level 3
- > Detection of removal of covers
- > Disabling of unneeded functionality

### Physical characteristics

Form Factor: 2U 19" rackmount, 400mm depth

Weight: 12Kg

Voltage: 90-132 and 175-264 VAC, auto-selected

Environment: 10°C-40°C, Humidity: 10%-90%, non-condensing



#### Europe, Middle East, Africa

THALES eSECURITY LTD. Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ. UK  
T: +44 (0)1844 201800 F: +44 (0)1844 208550 E: [emea.sales@thales-esecurity.com](mailto:emea.sales@thales-esecurity.com)

#### Americas

THALES eSECURITY, INC. 2200 North Commerce Parkway, Suite 200, Weston, Florida 33326. USA  
T: +1 888 744 4976 or +1 954 888 6200 F: +1 954 888 6211 E: [sales@thalesesec.com](mailto:sales@thalesesec.com)

#### Asia Pacific

THALES TRANSPORT & SECURITY (HONG KONG) LTD. Units 2205-06, 22/F Vicwood Plaza, 199 Des Voeux Road Central, Hong Kong, PRC  
T: +852 2815 8633 F: +852 2815 8141 E: [asia.sales@thales-esecurity.com](mailto:asia.sales@thales-esecurity.com)

**Thales**  
Security Solutions & Services