

# SafeNet Luna Payment HSM



The SafeNet Luna Payment HSM from Thales is a network-attached Hardware Security Module (HSM) designed for retail payment system processing environments for credit, debit, e-wallet and chip cards, as well as Internet payment applications. It offers secure PIN and card processing, message authentication, comprehensive key management, and general-purpose cryptographic processing.



## Comprehensive EMV support

The SafeNet Luna Payment HSM specifically meets the needs of payment processors, card issuers, acquirers, merchants, and e-payment solution providers who need to adhere to EMV security standards. The SafeNet Luna Payment HSM offers comprehensive EMV support from transaction processing to card issuance capabilities.

## Strong security features

Tamper-evident seals, intrusion detection switches, and shielded connectors designed into the SafeNet Luna Payment HSM minimize exposure to direct physical attacks.

The SafeNet Luna Payment HSM ATM Key Management System provides key mailer security by allowing the custodian key data to print directly to secure key envelopes; it also allows for automatic ATM key distribution and initialization (NCR & Diebold). Likewise, the PIN Mailer System allows for printing of the PINs directly to secure PIN envelopes.

The SafeNet Luna Payment HSM also offers true end-to-end internet and mobile transaction security. In addition to providing secure login through RSA-encrypting the PIN/password, SNMP is now supported, facilitating resource management from your central monitoring service.

## Comprehensive command set & API support

The SafeNet Luna Payment HSM provides command set support for a wide variety of clients. The Mark II command set provides the functionality required by the vast majority of issuing and acquiring banks, payment processors, and ATM systems, including functionality for card issuance whilst the AMB command set supports Australia Major Bank requirements. The SafeNet Luna Payment HSM is backward compatible with previous releases. The SafeNet Luna Payment HSM also supports other common Payment HSM command sets, and third-party APIs.

## Benefits

### Strongest Security

- Keys in hardware
- Remote management with two-factor access control
- Web-based configuration
- Intrusion-resistant, tamper-evident hardware
- PCI-HSM 2.0 and APCA CECS Certification\*

### Secure audit logging

- User operations are automatically audited and contain who, what, and when to help meet regulatory compliance requirements.
- Increased security to provide tamper-evident logging

### Performance and Scalability

- Up to 2000 Visa PIN verification operations per second
- Scalable up to 20 cryptographically isolated partitions
- Available in a variety of performance options to suit individual use case needs
- In-field upgradeability between performance levels to protect your investment
- Dual hot-plug redundant power supply

### Example Applications

- Card Issuance
- PCI P2PE Compliance
- EMV
- Transactions Processing
- DUKPT
- Remote Key Loading
- Contactless Payments

## Security for Host Card Emulation

With the growing popularity of mobile payments and the emergence of Host Card Emulation (HCE), new software-based standards have been developed by major payment players to digitize card credentials and enable secure, device-based payment transactions. With SafeNet Luna Payment HSM banks, card issuers and payment service providers can now offer customers contactless payment applications that are compliant with these specifications. The SafeNet Luna Payment HSM plays a central role in protecting payment data by managing the entire cryptographic process that secures the enrollment, provisioning, and tokenization of payment card credentials and payment operations.

## Scalability with secure partitions

A single SafeNet Luna Payment HSM can be separated into 20 cryptographically isolated partitions, with each partition functioning as if it was an independent HSM. This provides a tremendous amount of scalability and flexibility, as a single HSM can perform tasks for multiple payment applications concurrently.

## Customizations

Thales works closely with customers to extend its standard payment products to incorporate customer-defined functionality. The SafeNet Luna Payment HSM allows custom functionality to be readily implemented in support of non-standard EFT systems including e-wallet, mobile banking, and gaming. The SafeNet Luna Payment HSM uses proprietary cryptographic methods.

## Network key transfer

SafeNet Luna Payment HSM has the option to store keys internally or on the host. Keys can also be backed up to a smart card and the keys can be loaded directly from one SafeNet Luna Payment HSM to another. It is also possible to use a smart card to move keys between units. Keys can be entered via the console and stored directly in the SafeNet Luna Payment HSM secure memory, making changing to a new master key easier since there is no specific key migration required. HSM internal secure key memory allows for storage of up to 9,999 keys of each key type. SafeNet Luna Payment HSM supports multiple key management schemes including: master/session keys, DUKPT, remote ATM initialization (NCR and Diebold), and Australian AS2805 key management.

## Support for 3-D Secure payment transactions

3-D Secure is an added layer of security for online credit and debit card transactions, offered as MasterCard SecureCode, or Verified by Visa. The SafeNet Luna Payment HSM host functions now provide support for Visa 3-D Secure and MasterCard SecureCode protocols for payment transactions.

This includes support for the calculation of CAW (Card Authentication Verification Value) and providing TLS (Transport Layer Security) related crypto-operations.

## Web-based configuration management

The regular task of configuring and managing cryptographic and key component settings often executed through a command line interface is simplified through the use of an easy to use GUI. A well-structured menu-based navigation system, coupled with intuitive dialog box interaction, reduces the risk of manual input errors and speeds up the administrative process.

\*When granted, PCI SSC approval is provided by PCI SSC to ensure certain security and operational characteristics important to the achievement of PCI SSC's goals, but PCI SSC approval does not under any circumstances include any endorsement or warranty regarding the functionality, quality or performance of any particular product or service. PCI SSC does not warrant any products or services provided by third parties. PCI SSC approval does not under any circumstances include or imply any product warranties from PCI SSC, including, without limitation, any implied warranties of merchantability, fitness for purpose, or non-infringement, all of which are expressly disclaimed by PCI SSC. All rights and remedies regarding products and services which have received PCI SSC approval shall be provided by the party providing such products or services, and not by PCI SSC.

## Secure software upgrade

Upgrades can be cost-effectively performed at the in-field location avoiding the need and cost of returning the HSM to the service location, or opening or disassembling the unit. Built-in security mechanisms ensure that only genuine Thales software can be installed. In addition, if the software upgrade is incomplete, the SafeNet Luna Payment HSM will automatically restart from the last successful start.

## Supports general purpose crypto processing

SafeNet Luna Payment HSM provides for the encryption or Message Authentication Code (MAC) generation for large files, and tasks can be split into multiple supported function calls. In addition, SafeNet Luna Payment HSM supports up to 384 RSA signatures per second.

## About Thales Cloud Protection & Licensing

Today's enterprises depend on the cloud, data and software in order to make decisive decisions. That's why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive information and software wherever it is created, shared or stored – from the cloud and data centers to devices and across networks. Our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day.

## Technical specifications

### Operating System

- Windows, Linux, Solaris, AIX, HP-UX
- Virtual: VMware, Hyper-V, Xen

### Cryptographic APIs

- SafeNet Mark II Payments API
- SafeNet Eracom AMB Payments API
- Third Party payments API

### Functionality and Support

- EMV
- Contactless & NFC Payment Support
- 3D-Secure
- Italian Debit
- American Express
- TR-31
- Visa Cloud
- Format Preserving Encryption

### Cryptography

- Symmetric: AES, DES, Triple DES, SEED
- Asymmetric: RSA (1024-7168)
- Hash/Message Digest/HMAC: SHA-1, SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512), MD5
- Random Number Generation: FIPS 140-2 approved DRBG (SP 800-90 CTR mode)

### Physical Characteristics

- Standard 1U 19in. rack mount chassis
- Dimensions: 19" x 21" x 1.725" (482.6mm x 533.4mm x 43.815mm)
- Weight: 28lb (12.7kg) > Input Voltage: 100-240V, 50-60Hz
- Power Consumption: 180W maximum, 155W typical
- Temperature: operating 0°C – 35°C, storage -20°C – 60°C
- Relative Humidity: 5% to 95% (38°C) non-condensing

### Security Certifications

- PCI-HSM 2.0
- APCA CECS

### Safety and Environmental Compliance

- UL, CSA, CE
- FCC, KC Mark, VCCI, CE
- RoHS, WEEE