



Luna EFT

PRODUCT BRIEF

Benefits

Strongest Security

- Increased PIN and key mailer security with PIN and custodian key data printed directly to the mailer stationery
- FIPS 140-2 Level 3 certification (in process)

High Performance

- Up to 1200 Visa PIN Verify (PVV) operations per second
- Up to 600 RSA signatures per second
- 64 concurrent host connections

Functionality and Support

- Strong EMV support
- Paypass and Paywave supported
- DUKPT support
- APACS 70 support
- Italian Debit support

The Luna EFT (PH-EFT) is a network-attached Hardware Security Module (HSM) designed for retail payment system processing environments for credit, debit, e-purse 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

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

Strong Security

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

In addition, Luna EFT 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.

Luna EFT 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.

Multiple Command Set & API Support

Luna EFT 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. The Mark II command set, as well as the AMB (Australian Major Banks) command set, which is designed to suit the Australian market, supports the APCA interface standards.

Customizations

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

Technical Specifications

APIs

- Mark II including Card Issuance and Online Banking Module
- Australian Major Banks
- Custom Solutions

Security Validations

- FIPS 140-2 Level 3 validated (in progress)
- APCA approved
- TR-31 Interoperability

Cryptographic Performance

- Up to 1200 TDEA-based (or 3DES) operations per second
- 600 1024-bit RSA signatures per second

Cryptographic Algorithms

- DEA/TDEA
- SEED
- RSA
- SHA-1
- 3DES

Digital Signing

Asymmetric Key

- RSA

Symmetric Keys

- 3DES
- DES
- 3DES-3Length

Hash Digest

- SHA-1

Message Authentication Codes (MAC)

- X9

Physical Characteristics

Connectivity

- Asynchronous Serial V.24 Async
- Raw Ethernet (ISO 8803) with optional ISO 8802 selectable
- TCP/IP over Ethernet supports 2 NIC

Dimensions

- 1U rackmount chassis 19"x20.6"x1.725"
- 9.5 kg (21 lbs)

Temperature

- Operating 0°C to 40°C
- Storage -20°C to +65°C

Power Requirements

- 100V-250V

Regulatory Standards

- U/L 1950 & CSA C22.2 compliant
- FCC Part 15 - Class B
- RoHS compliant



Network Key Transfer

Luna EFT 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 Luna EFT to another. It is also possible to move keys between units on smart card. Keys can be entered via the console and stored directly in the Luna EFT secure memory, making changing to a new master key easier since there is no specific key migration required. More than 15,000 instances of each key can exist at any given time. Luna EFT supports multiple key management schemes including: master/session keys, DUKPT, remote ATM initialization (NCR and Diebold), and Australian AS2805 key management.

Supports General Purpose Crypto Processing

Luna EFT 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, Luna EFT supports up to 600 RSA signatures per second.

Graphic User Interface (GUI) Based Console Operations

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.

Secure Software Upgrade from CD-ROM, USB Memory Stick, or Host Interface

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 SafeNet software can be installed. In addition, if the software upgrade is incomplete, Luna EFT will automatically restart from the last successful start.



COMPLIANT

Contact Us: For all office locations and contact information, please visit www.safenet-inc.com

Follow Us: www.safenet-inc.com/connected

©2010 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners. PB (EN)-08.19.10