Benefits

Strongest Security

Increased PIN and key mailer security with PIN and custodian key data printed directly to the mailer stationary

FIPS 140-2 Level 3 certification (in process)

Secure key transfer with existing SafeNet ProtectHost White device

High Performance

Up to 1200 Visa PIN Verify (PVV) operations per second, which provides for faster and more efficient transactions

Ease of Use and Support

Strong EMV support

Ability to produce postscript PIN mailers on a laser printer

SafeNet ProtectHost EFT

The SafeNet ProtectHost EFT (PH EFT) is a stand alone Hardware Security Module (HSM) designed for retail Electronic Funds Transfer (EFT) payment system processing environments for credit, debit, chip card and internet applications. It offers general purpose cryptographic processing, key storage and generation, and PIN generation and verification.

Comprehensive EMV Support

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

Strong Security

SafeNet PH 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 PH EFT Pin Mailer System allows for printing of the Pins directly to secure PIN envelopes.

SafeNet PH EFT also offers true end-to-end internet and mobile transaction security. All transactions are RSA encrypted from the client to the host, and Java applet at client browser or phone.

Multiple Command Set & API Support

The SafeNet PH 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. The CI (Card Issuing) command set provides functionality for the Card Issuers especially those with Chip Card/EMV requirements. The AMB (Australian Major Bank) command set is designed to suit the Australian market and supports the APCA interface standards.

Customizations

SafeNet works closely with customers to extend its standard EFT and Payments products to incorporate customer-defined functionality. The PH EFT allows for custom functionality to be readily implemented in support of non-standard EFT systems including electronic purse, mobile banking, and gaming. The PH EFT uses proprietary cryptographic methods: Issuer PIN management.

Key Management

SafeNet's PH 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 PH EFT to another. It is also possible to move Keys around between units on smart card. Keys can be entered via the console and stored directly in the PH EFT secure memory, making changing to a new master key easier since there is no specific key migration required.

Supports General Purpose Crypto Processing

SafeNet's PH EFT provides for the encryption or Message Authentication Code (MAC) generation for large files, and tasks can be split into multiple supported function calls. The variable length field structure in the PH EFT offers flexibility in defining any size data field during a function call.

SafeNet®
The Foundation of Information Security

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 in the PH EFT 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 Pen Drive, 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 PH EFT security mechanisms ensure that only genuine SafeNet software can be installed. In addition, if the software upgrade is incomplete, PH EFT will automatically restart from the last successful start. This gives users confidence that their sensitive data will not be lost and will remain secure.

RoHS COMPLIANT

Technical Specifications

Platform
- A variety of interfaces to a wide variety of host types

APIs
- Payment Industry
- Mark II
- Australian Major Bank
- Card Issuance
- Online Banking Module
- Custom Solutions

Hardware Validations
- FIPS 140-2 Level 3 validated (certificate number in progress)
- RoHS compliant

Cryptographic Performance
- 2400 operations per second

Ethernet and Asynchronous interface support

Cryptographic Algorithms
- Asymmetric Key
- RSA

Digital Signing

Symmetric Keys
- 3DES
- DES

Hash Digest
- SHA-1

Message Authentication Codes (MAC)
- ANSI X9

Physical Characteristics

Connectivity
- Asynchronous Serial
- Raw Ethernet (ISO 8803) with optional ISO 8802 selectable
- TCP/IP over Ethernet

Dimensions
- 1U RoHS compliant
- 7.21lb (15.9kg)

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

Power Requirements
- 1.5A@120V Max

Regulatory Standards Certification
- U/L 1950 & CSA C22.2 compliant
- FCC Part 15 - Class B
- ISO - 9002 Certification

Corporate Headquarters: 4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel.: +1 410 931 7500 or 800 533 3958, Fax: +1 410 931 7524, Email: info@safenet-inc.com

EMEA Headquarters: Tel.: + 44 (0) 1276 608 000, Email: info.emea@safenet-inc.com

APAC Headquarters: Tel: + 852 3157 7111, Email: info.apac@safenet-inc.com

For all office locations and contact information, please visit www.safenet-inc.com/company/contact.asp

www.safenet-inc.com

SafeNet® The Foundation of Information Security