The ProtectHost White HSM specifically meets the needs of payment processors, card issuers, merchants and e-payment solution providers to adhere to American Express, JCB, MasterCard and Visa security standards.

Application-level cryptographic and key management processing is performed by the ProtectHost White HSM on behalf of the host computer to which it is attached. It delivers secure key storage, DES, 3DES and RSA cryptographic processing, PIN encryption, digital signature generation and verification, secure key loading, plus PIN and key mailer printing. Tamper-resistant secure casing, including physical key locks, provides physical and logical protection to cryptographic keys preventing unauthorized access to highly sensitive key information. Automatic cryptographic key erase upon tamper detection and battery removal ensures the ultimate level of secrecy and integrity of keys and sensitive data.

GUT-based (Graphic User Interface) console operations incorporate a menu-based navigation system with intuitive dialog box interaction. Software upgrades can be cost-effectively performed at the in-field location avoiding the cost of returning the product to the service facility.

Typical usage applications include securing retail payment systems such as ATM and EFTPOS networks, e-purse systems, clearing and settlement systems, wagering, Internet/mobile banking, and other financial transaction systems.

ProtectHost White performs EFT/payment processing, card issuance and online banking security functionality utilizing SafeNet’s portfolio of command sets. Out-of-the-box integration with the leading software applications of the most important global and regional payment processing, card issuance and Internet banking vendors facilitates rapid and cost-effective deployment.
**Secure**

Hardware Security Modules (HSMs) provide a tamper-protected environment to deliver the highest level of physical and logical protection to the storage and processing of highly sensitive information, such as cryptographic keys, PINs and other data.

- **Security Features**
  - Tamper-protected physical security
  - Secure, battery-backed memory for key storage
  - Multi-threading

- **Security Benefits**
  - Physical security consisting of tamper-resistant casing incorporating physical key locks, plus tamper-responsive circuitry ensures that all information stored within the secure memory is cleared in the event of a tamper or break-in attempt to the device.
  - Battery-backed secure key storage is provided for cryptographic keys (Symmetric – DES, 3DES etc; Asymmetric – RSA etc) and other sensitive data. Batteries also provide back-up power to the tamper-sensing electronics when no system power is available. Any detected tamper event, including battery removal, will immediately result in memory erasure.
  - The direct attachment of a keyboard and monitor ensures physical administrator presence at the location of the HSM when performing device management tasks. This avoids the security implications of malicious remote penetration into the device.
  - Support both symmetric and asymmetric algorithms and associated key management ensures diverse functionality within a single device. Please refer to the command set of interest for specific use and application cryptographic algorithms.

**Random Number Generator (RNG)**

ProtectHost White utilizes a Random Number Generator (RNG) that has been designed and confirmed to satisfy the statistical tests of FIPS 140-2 level 3. This generation of truly random cryptographic keys ensures the required level of entropy essential for the highest levels of security.

- **RNG**
  - Performs rapid processing of cryptographic commands. Specialized cryptographic electronics, including a dedicated data cipher microprocessor, memory and a Random Number Generator (RNG), offloads the cryptographic processing from the host system freeing it to respond to more requests.

**Performance**

ProtectHost White performs rapid processing of cryptographic commands. Specialized cryptographic electronics, including a dedicated data cipher microprocessor, memory and a Random Number Generator (RNG), offloads the cryptographic processing from the host system freeing it to respond to more requests.

- **Performance Features**
  - Broad range of performance levels
  - Multiple HSM scalability and Workload Distribution (WLD)
  - Multi-threading
  - RSA accelerator (optional)

- **Performance Benefits**
  - ProtectHost White can be configured to suit numerous performance levels in order to meet the specific needs of your application. Figures below apply to typical EFT host functions such as Visa PVV operations, to confirm others, please contact your SafeNet representative.
    - **Mark II**
      - Asyc
      - PI 20 host functions (~20 operations/sec)
      - PI 140 host functions (~140 operations/sec)
      - PI 280 host functions (~280 operations/sec)
      - PI 560 host functions (~560 operations/sec)
      - PI 1200 host functions (~1200 operations/sec)
  - High levels of scalability, reliability and increased throughput can be easily achieved at no restriction on the number of HSMs that can work in unison, or the number of keys that can be managed. In addition, the application can be relieved from Workload Distribution (WLD) processing to focus on primary tasks by implementing the available WLD support option.
  - SafeNet’s cryptographic APIs are fully thread-safe allowing multi-threaded applications to be used to obtain greater HSM throughput.
  - A RSA accelerator is available to increase the throughput of all RSA cryptographic operations.

**Easy Management**

Easy management is critical to a competent security system. The ProtectHost White HSM enables trouble-free configuration, operation and key management.

- **Management Features**
  - Intuitive, menu-based command set
  - Provision for in-field secure firmware upgrade via CD or FTP
  - Secure, battery-backed key storage
  - Symmetric and asymmetric key management
  - Auxiliary interfaces for secure PIN and key management

- **Management Benefits**
  - The regular task of configuring and managing cryptographic and key component settings through a command line interface can be relieved and simplified through the use of a 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.
  - 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.
  - Additionally, internal certificate-based security mechanisms ensure that only authentic, digitally signed software can be installed, eliminating the possibility of non-proprietary software compromising the security of the device.
  - Built-in support to directly attach a PIN and key mailing printing device to ProtectHost White ensures the highest level of security by avoiding the risk of sensitive data passing through an insecure intermediate device. This provides performance efficiency to direct HSM invoked printing of PIN and key mailers, without incurring any additional investment in print server equipment.

**Command Sets for ProtectHost White**

SafeNet delivers one of the most comprehensive portfolios of cryptographic command sets on the market. These enable users and developpers to facilitate seamless integration of cryptography and HSMs into a large array of third-party solutions, or custom applications.

- **Command Set**
  - **SafeNet Solution**
    - **Mark II**
    - **Australian Major Bank (AMB)**
    - **Card Issuance**
    - **Online Banking Module**
    - **Custom Solutions**
**Security**

Hardware Security Modules (HSMs) provide a tamper-protected environment to deliver the highest level of physical and logical protection to the storage and processing of highly sensitive information, such as cryptographic keys, PINs and other data.

**Security Features**

- **Tamper-protected physical security**: Physical security consisting of tamper-resistant casing incorporating physical key locks, plus tamper-responsive circuitry ensures that all information stored within the secure memory is cleared in the event of a tamper or breach attempt to the device.
- **Secure, battery-backed memory for key storage**: Battery-backed secure key storage is provided for cryptographic keys (Symmetric, DES, 3DES, etc., Asymmetric RSA, etc.) and other sensitive data. Batteries also provide back-up power to the tamper-sensing electronics when no system power is available. Any detected tamper event, including battery removal, will immediately result in memory erasure.
- **Direct attachment of standard console (VGA monitor and keyboard) to HSM**: The direct attachment of a keyboard and monitor ensures physical administrator presence at the location of the HSM when performing device management tasks. This avoids the security implications of malicious remote penetration into the device.
- **Smart card key transfer**: Cryptographic keys stored on smart cards facilitates rapid configuration of identically-keyed HSMs whilst also minimizing the possibilities of human error. Additionally, the storage of keys on smart cards delivers secure key back-up in the event of tamper-activated memory erasure, upgrade, maintenance, or key transfer from one HSM to another.
- **Supports symmetric and asymmetric/public key ciphers**: The support of both symmetric and asymmetric algorithms and associated key management ensures diverse functionality within a single device. Please refer to the command set of interest for specific use and application cryptographic algorithms.

**Performance**

ProtectHost White performs rapid processing of cryptographic commands. Specialized cryptographic electronics, including a dedicated data cipher microprocessor, memory and a Random Number Generator (RNG), off-loads the cryptographic processing from the host system freeing it to respond to more requests.

**Performance Features**

- **ProtectHost White** can be configured to suit numerous performance levels in order to meet the specific needs of your application. Figures below apply to typical EFT host functions such as Visa PIN-POS operations, to confirm others, please contact your SafeNet representative.
  - **Asynch**: PL 20 host functions (~140 operations/sec)
  - **PL 140 host functions (~140 operations/sec)**
  - **PL 280 host functions (~280 operations/sec)**
  - **PL 560 host functions (~560 operations/sec)**
  - **PL 1200 host functions (~1200 operations/sec)**

- **Multiple HSM scalability and Workload Distribution (WLD)**: High levels of scalability, reliability and increased throughput can be easily achieved as there is no restriction on the number of HSMs that can work in unison, or the number of keys that can be managed. In addition, the application can be relieved from Workload Distribution (WLD) processing to focus on primary tasks by implementing the available WLD support option.

- **Multi-threading**: SafeNet's cryptographic APIs are fully thread-safe allowing multi-threaded applications to be used to obtain greater HSM throughput.

- **RSA accelerator (optional)**: A RSA accelerator is available to increase the throughput of all RSA cryptographic operations.

**Easy Management**

Easy management is critical to a competent security system. The ProtectHost White HSM enables trouble-free configuration, operation and key management.

**Management Features**

- **Intuitive, menu-based Graphic User Interface (GUI) for key management**: The regular task of configuring and managing cryptographic and key component settings through a command line interface can be relieved and simplified through the use of a 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.
- **Provision for in-field secure firmware upgrade via CD or FTP**: 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.
- **Symmetric and asymmetric key management**: ProtectHost White provides comprehensive key management capabilities for both symmetric and asymmetric keys within a single device. Both HSM-stored and/or host-stored keys can be selected to best suit customer’s needs in terms of flexibility, card and key volumes, performance and security.
- **Auxiliary interfaces for secure PIN and key mailer printing**: Built-in support to directly attach a PIN and key mailer printing device to ProtectHost White ensures the highest level of security by avoiding the risk of sensitive data passing through an insecure intermediate device. This provides performance efficiency to direct HSM-invoked printing of PIN and key mailers, without incurring any additional investment in print server equipment.

**Command Sets for ProtectHost White**

SafeNet delivers one of the most comprehensive portfolios of cryptographic command sets on the market. These enable users and developers to facilitate seamless integration of cryptography and HSMs into a large array of third-party solutions, or custom applications.

**Command Set**

**SafeNet Solution**

**Mark II**

The **Mark II** functionality provides comprehensive, standards-compliant, cryptographic and key management support for online retail transactions initiated using magnetic stripe cards and chip cards (e.g. EMV).

The security and functionality delivered by **Mark II** ensures compliance with international payment schemes such as American Express, JCB, MasterCard and Visa.

**Australian Major Bank (AMB)**

The **AMB** functionality provides comprehensive, standards-compliant, cryptographic support for card payment transactions that employ Australian key management schemes.

The security and functionality delivered by **AMB** executes adherence to standards defined by the Australian Payments Clearing Association (APCA).

**Card Issuance**

The **Card Issuance** functionality provides the required cryptographic and key management processing involved in the production and issuance of consumer transaction cards. This includes magnetic stripe cards and EMV-based chip cards.

**Online Banking Module**

The **Online Banking Module** provides true end-to-end encryption security to sensitive information used in Internet transactions, such as online banking. Encryption is initiated at the customer’s computing device (PC, mobile phone etc) creating a secure channel between the customer’s PC and the host computing system, all the way beyond the web server.

**Custom Solutions**

SafeNet works closely with customers to extend its standard EFT products to incorporate customer-defined functionality. In addition, solutions are commonly developed with total custom functionality, not based on any standard SafeNet product, to ensure the unique needs of the customer can be delivered.
Technical Specifications

Cryptographic Algorithms
- Symmetric: DES, 3DES (two and three key), plus others on request
- Asymmetric: RSA plus others on request

For full details of supported algorithms, message authentication, key operations, digital signatures, hashing, certificates etc; please refer to the command set relevant to your interest.

Algorithms are updated as required; please check with SafeNet for the latest updates.

Host Platforms
ProtectHost White can optionally operate in conjunction with the host-based cryptographic API, ProtectToolkit EFT.

ProtectHost White provides the following features:
- Asynchronous Serial (V24/V32) and/or parallel (V24/V32, 3270 Control Unit, IUD Devices)
- Raw Ethernet (ISO 8802) with optional ISO 8802 selectable
- TCP/IP over Ethernet, TCP/IP over Token Ring
- IBM Channel

Standard Compliance
Please refer to the Command Set and Cryptographic API relevant to your interest.

Dimensions
- 430mm x 187mm x 550mm or 16.9” x 7.4” x 21.7” (w/h/d)
- Weight: 18kg (39lb, 11oz)

Power Requirements
- Voltage: 90 to 240 Volts - 50/60 Hz
- Power consumption: 150 Watts
- Temperature: 0° to 40°C (32 to 104 °F)
- Relative Humidity: 5% to 95%

Technological highlights:
- Tamper-resistant secure casing, including physical key locks, provides physical and logical security functionality utilizing SafeNet’s portfolio of command sets. Out-of-the-box integration with the leading software applications of the most important global and regional payment processors, card issuers, merchants and e-payment solution providers to adhere to American Express, JCB, MasterCard and Visa security standards.

Application level cryptographic and key management processing is performed by the ProtectHost White HSM on behalf of the host computer to which it is attached. It delivers secure key storage, DES, 3DES and RSA cryptographic processing, PIN encryption, digital signature generation and verification, secure key loading, plus PIN and key mailing printing.

Tamper-resistant secure casing, including physical key locks, provides physical and logical protection to cryptographic keys, preventing unauthorized access to highly sensitive key information. Automatic cryptographic key erase upon tamper detection and battery removal ensures the ultimate level of secrecy and integrity of keys and sensitive data.

GUI-based (Graphic User Interface) console operations incorporate a menu-based navigation system with intuitive dialog box interaction. Software upgrades can be cost-effectively performed at the in-field location avoiding the cost of returning the product to the service facility. Typical usage applications include securing retail payment systems such as ATM and EFTPOS networks, e-purse systems, clearing and settlement systems, wagering, Internet/mobile banking, and other financial transaction systems.

ProtectHost White performs EFT/credit card payment processing, card issuance and online banking security functionality utilizing SafeNet’s portfolio of command sets. Out-of-the-box integration with the leading software applications of the most important global and regional payment processing, card issuance and Internet banking vendors facilitates rapid and cost-effective deployment.

All other product names are trademarks of their respective owners.