



# ProtectServer Orange External

## Hardware Security Module



**ProtectServer Orange External** provides cryptographic services including high-speed encryption, user and data authentication, message integrity and key storage via a FIPS 140-1 level 3 validated cryptographic core processor. The HSM features tamper-protection security that safeguards it against physical attacks and offers easy-to-perform remote administration via an intuitive graphic user interface .



**ProtectServer Orange External is a network-attached HSM that connects via TCP/IP to a single machine or complete network (LAN) to perform as a central cryptographic subsystem delivering symmetric and asymmetric cryptographic services. All operations that would otherwise be performed on the insecure server are processed within the HSM — ensuring sensitive keys are always protected from compromise.**

**ProtectServer Orange External** is typically employed to provide cryptographic services such as high-speed encryption, user and data authentication, message integrity, secure cryptographic key storage and key management for e-Commerce, PKI, document management, Electronic Bill Presentation and Payment (EBPP), database encryption, plus many other applications.

The HSM provides a secure, easy-to-perform local and remote management facility plus in-field servicing. Easy interaction and key management are delivered via an intuitive Graphic User Interface (GUI), plus remote network access to the HSM facilitates increased administration convenience and reduced cost and time. Smart cards provide the highest security and administrative convenience for secure back-up, recovery and transfer of cryptographic keys. Upgrades can be cost-effectively performed at the in-field location avoiding the cost of returning the product to the service location.

A wide range of Application Programming Interfaces (APIs) are available to assist adherence of your cryptographic application to industry-standard security applications and platform environments. This includes the broadest suite of PKCS#11 function sets available on the market, a Java JCA/JCE and Microsoft CryptoAPI provider implementation, plus seamless integration with OpenSSL. This is in addition to a customization module to facilitate customized cryptographic applications operating on a HSM.

These APIs are interoperable across many of SafeNet's PCI adapter and network-attached HSMs, enabling a wide choice of hardware configurations to suit specific needs.

### BENEFITS AT A GLANCE

#### STRONG SECURITY

- FIPS 140-1 level 3 validation independently certifies the secure management and storage of secret keys and sensitive data
- Tamper-protected security safeguards against physical attacks on the HSM to obtain sensitive information. Upon detection of a physical attack, the complete internal key storage memory is erased
- Cryptographic keys are never exposed outside of the HSM in clear form

#### EASY MANAGEMENT

- An easy to use Graphic User Interface (GUI) simplifies HSM device administration and key management via intuitive navigation and user interaction
- Time-critical management tasks, such as key modification, addition and deletion, can be securely performed from remote locations reducing management costs, resource constraints and response times

#### EXTENSIVE APIs/ TOOLKITS

- Adhere to a wide range of industry-standard security applications and platform environments. SafeNet delivers the most extensive suite of cryptographic APIs/developer toolkits available on the market
- Seamlessly integrate SafeNet HSMs into PKCS#11, Java JCA/JCE, Microsoft and OpenSSL applications
- Easily develop customized cryptographic applications, or extend SafeNet's cryptographic APIs with a customization Software Development Kit (SDK)

PRODUCT DATA SHEET

# ProtectServer Orange External

## Hardware Security Module



### 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

#### Security Benefits

**FIPS 140-1 level 3 certification**

The FIPS 140-1 level 3 certification of the core processor and memory confirms that the **ProtectServer Orange External** HSM is uniquely qualified to detect attempted physical attacks and perform secure cryptographic processing including correct implementations of several commercially significant and approved cryptographic algorithms.

**Tamper-protected physical security**

Tamper-protected physical security incorporating tamper-responsive circuitry ensures that all information stored within the secure memory is cleared in the event of a break-in attempt to the device.

**Secure, battery-backed memory for key storage**

1Mb of battery-backed secure key storage is available to store and maintain the integrity of symmetric cipher keys (DES, 3DES, AES etc), asymmetric keys (RSA, DSA, ECC, Diffie Hellman etc), certificates, and sensitive data. A battery provides 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 key memory erasure.

**True Random Number Generator (RNG)**

**ProtectServer Orange External** allows the generation of truly random cryptographic keys that ensure the required level of entropy essential for the highest levels of security. This is achieved using a true Random Number Generator meeting ANSI X9.31 requirements and certified to the requirements of FIPS 140.

**Smart card key transfer**

Storage of cryptographic keys on smart cards minimizes human error when needing to enter keys into multiple HSMs and significantly speeds up the process of configuring a pool of identically-keyed HSMs in a high-availability production environment. 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.

**Direct connection of smart card reader and PIN pad**

Secure PIN pad entry devices can be connected to the HSM for direct entry of PINs and key components. This eliminates insecure data entry paths via keyboards, operating system processes and memory.

**Hardened Linux platform**

Services that could possibly threaten the cryptographic security and reliability of the **ProtectServer Orange External** have been removed or restricted. This includes restricting incoming ports to a single net-server port plus utilizing a customized small footprint Linux operating system.



### Performance

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

#### Performance Features

#### Performance Benefits

**Broad range of performance levels**

**ProtectServer Orange External** is available in a broad range of symmetric and asymmetric cryptographic performance levels to meet a wide variety of security application processing requirements. Processing speeds up to 450 RSA signatures (1024 bit) operations/sec (PL 450) are available.

To confirm your performance needs and options, please contact your SafeNet representative.

**Dual LAN support**

An optional dual-network interface variant of **ProtectServer Orange External** enables the HSM to be integrated on the same or different sub-nets and be shared between different networks in order to protect multiple business domains or provide redundancy within a single network.

**Multiple HSM scalability and Workload Distribution (WLD)**

High levels of scalability, reliability, redundancy 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.

**Multi-threading**

SafeNet's cryptographic APIs are fully thread-safe allowing the use of multi-threaded applications to achieve greater HSM throughput.



## Easy Management

Easy management is critical to a competent security system. The **ProtectServer Orange External** Hardware Security Module (HSM) enables trouble-free configuration, operation and key management.

### Management Features

### Management Benefits

#### Graphic User Interface (GUI)

Simple to use Graphic User Interface (GUI) eases HSM administration and key management via intuitive navigation and user interaction. The use of Java-based GUI technology provides a consistent look and feel across all supported operating platform environments.

#### Command Line Interface

A Command Line Interface for key management and certificate tools allow easy script-based integration into automated systems administration facilities.

#### 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.

Additionally, internal certificate-based security mechanisms ensure that only authentic, digitally signed software can be installed, eliminating the possibility of non-proprietary software downgrading the security of the device.

#### Remote management (device & key management) on network HSMs

Convenient remote network access to the HSM reduces administrative overheads by enabling device administration and key management operations to be remotely performed on network-based HSMs.



## Extensive API/Toolkit Support for ProtectServer Orange External

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

### Toolkit Solution

### Toolkit

#### PKCS#11 API implementation

**ProtectToolkit C** is a cryptographic provider that enables secure applications to be constructed using the industry-standard PKCS#11 API.

#### Java JCA/JCE provider implementation

**ProtectToolkit J** is a Java-based Cryptographic Provider that allows JCA/JCE security programs to access hardware-based, high-strength cryptographic services.

#### Cryptographic Service Provider (CSP) for Microsoft CryptoAPI

**ProtectToolkit M** is SafeNet's implementation of a Microsoft Cryptographic Service Provider (CSP) for Microsoft's CryptoAPI.

#### OpenSSL engine integration

**ProtectServer Orange External** integrates with OpenSSL to operate as both a HSM and SSL Accelerator, increasing the cryptographic processing for the SSL protocol and protecting sensitive cryptographic keys.

#### Customization Software Development Kit (SDK)

The Software Development Kit (SDK) functionality within **ProtectProcessing** provides the ability to produce your own custom cryptographic application (including completely new algorithms), or modify SafeNet's existing cryptographic applications, and allow them to be securely downloaded and executed within the secure confines of a HSM.



## TECHNICAL SPECIFICATIONS

### CRYPTOGRAPHIC ALGORITHMS

- **Symmetric** - AES, DES, 3DES, CAST-128, RC2, RC4, SEED, plus others on request; Modes supported include ECB, CBC, OFB64, CFB-8 (BCF), plus others on request
- **Asymmetric** - RSA (up to 4096 bits), DSA, ECDSA (up to 512 bits) Diffie Hellman (DH), plus others on request

For full details of all supported algorithms, digital signature and message authentication schemes, key operations, message digests, certificate support etc; please refer to the cryptographic API relevant to your interest.

### HOST PLATFORMS

**ProtectServer Orange External** can operate in conjunction with the host-based cryptographic APIs **ProtectToolkit C**, **ProtectToolkit J**, **ProtectToolkit M** and **ProtectProcessing**.

### HOST CONNECTIVITY

- TCP/IP over Ethernet
- Dual LAN Support (optional)

### STANDARD COMPLIANCE

Please refer to the cryptographic API relevant to your interest

### DIMENSIONS

- 379mm x 76mm x 300mm or 15" x 3" x 11.8" (w/h/d)
- Optional 19" rack mounting assembly of height 2U for EIA-310-D-compliant mounting rails
- Weight - 5kg (11lb)

### POWER REQUIREMENTS

- Voltage - 220/110 Volts switchable

### OPERATING ENVIRONMENT

- Temperature - 0° to 40°C (32 to 104 °F)
- Relative Humidity - 5 to 95%

## ABOUT SAFENET

SafeNet (SFNT:Nasdaq) is a global leader in information security. Founded more than 20 years ago, the company provides complete security utilizing its encryption technologies to protect communications, digital identities and intellectual property, and offers a full spectrum of products including hardware, software, and chips. ARM, Bank of America, Cisco Systems, the Departments of Defense, and Homeland Security, Microsoft, Samsung, Texas Instruments, the U.S. Internal Revenue Service, and scores of other customers entrust their security needs to SafeNet. For more information, visit [www.safenet-inc.com](http://www.safenet-inc.com).

#### Corporate:

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

#### Sales Offices:

**Australia** +61 3 9882 8322  
**Brazil** +55 11 3392 4600  
**Canada** +1 613 723 5077  
**China** +86 10 8266 3936  
**Finland** +358 20 500 7800  
**France** +33 1 47 55 74 70  
**Germany** +49 18 03 72 46 26 9  
**Hong Kong** +852 3157 7111  
**India** +91 11 2691 7538  
**Japan (Tokyo)** +81 45 640 5733  
**Korea** +82 31 705 8212  
**Mexico** +52 55 5575 1441  
**Netherlands** +31 73 658 1900  
**Singapore** +65 6297 6196  
**Taiwan** +886 2 2735 3736  
**U.K.** +44 1276 608 000  
**U.S. (Massachusetts)** +1 978 539 4800  
**U.S. (New Jersey)** +1 201 333 3400  
**U.S. (Virginia)** +1 703 279 4500  
**U.S. (Irvine, California)** +1 949 450 7300  
**U.S. (Santa Clara, California)** +1 408 855 6000  
**U.S. (Torrance, California)** +1 310 533 8100

**Australia** +61 2 9906 2988  
**Brazil** +55 21 2215 5765  
**Czech Republic** +420 2 2423 6833  
**Germany** +49 2151 3630 20  
**India** +91 80 5110 0600  
**Italy** +39 02 7729 7599  
**Netherlands** +31 20 311 6540  
**Singapore** +65 6559 3449  
**Switzerland** +41 61 462 2010  
**U.S. (Roseville, California)** +1 916 677 2450

Distributors and resellers located worldwide

[www.safenet-inc.com](http://www.safenet-inc.com)