



# ProtectServer External Hardware Security Module

## PRODUCT BRIEF

### Benefits

#### Security

- Includes a FIPS 140-2 L3 certified cryptographic module
- Tamper protection physical
- HSM security
- True RNG
- Smartcard backup of key material
- Hardened Linux Platform

#### Performance

- Dual LAN
- Up to 600 RSA signings/sec
- WLD (Work Load Distribution)
- Multi-threaded APIs

#### Easy Management

- GUI HSM admin interface
- CMD line interface
- Infield upgrade
- Remote HSM Management

#### Extensive API support

ProtectServer External provides a cost-effective, high assurance HSM solution for protecting cryptographic keys against compromise and providing encryption, signing and authentication services to security sensitive applications.

### Most Secure

SafeNet ProtectServer External includes a FIPS 140-2 Level 3 cryptographic module performing secure cryptographic processing in a high assurance fashion. In addition, SafeNet ProtectServer External provides a tamper-protected environment that delivers 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.

### Ease of Management

SafeNet ProtectServer External 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 administrative 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 infield location avoiding the cost of returning the product to the service location.

### Ease of Integration

SafeNet ProtectServer External offers a wide range of Application Programming Interfaces (APIs) to assist adherence of cryptographic applications to industrystandard 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. Additionally, a customization module facilitates customized cryptographic applications operating on an 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.

## Technical Specifications

### Operating Systems

- Win NT (32-bit)
- Win 2003 (32 & 64-bit)
- Win 2008 (64-bit)
- Solaris 9, 10 (32 & 64-bit)
- Linux E4K 2.6 (32 & 64-bit)
- Linux E5K 2.6 (32 & 64-bit)
- Linux SuSE 10 (32-bit)
- Linux RH8K 2.4 (32-bit)
- AIX 5.3 (32 & 64-bit)
- HP-UX 11i (32 & 64-bit)

### Client API and Toolkit Support

- PKCS#11
- Java JCA/JCE
- Microsoft CryptoAPI (CAPI)
- Microsoft CNG
- Open SSL
- Customizable Software Development (SDK)

### Host Platforms

- ProtectToolkit C
- ProtectToolkit J
- ProtectToolkit M
- ProtectProcessing

### Cryptographic Processing

#### Asymmetric Key Encryption and Key Exchange

- RSA (up to 4096 bits), DSA, ECDSA (up to 512 bits), Diffie Hellman (DH), plus others upon request

#### Symmetric Algorithms

- AES, DES, 3DES, CAST-128, RC2, RC4, SEED, plus others upon request

#### Modes Supported

- ECB, CBC, OFB64, CFB-8 (BCF)

### Physical Characteristics

#### Host Connectivity

- TCP/IP over Ethernet
- Dual LAN Support

#### Dimensions

- 12 7/8" x 11 3/4" x 3"
- Weight 8.8lbs

#### Power Requirements

- 220/110 Volts Switchable

#### Operating Environment

- 0° to 40°C
- 5% to 95% Relative Humidity

### Compliance

- Cryptographic module: FIPS 140-2 Level 3
- Certificate# 739

### Regulatory Standards Certifications

- UL 1950 (EN60950) & CSA C22.2 Safety Compliant
- FCC Part 15 — Class B
- RoHS Compliant

## High Performance and Scalability

SafeNet ProtectServer 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. ProtectServer External is available in a broad range of symmetric and asymmetric cryptographic performance levels to meet a wide variety of security application processing requirements, with speeds up to 600 RSA signature operations/sec. The included dual-network interface optionally 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. In addition, 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.

## Migrating Keys from SafeNet ProtectServer Orange-External to SafeNet ProtectServer External

For migrating keys from a PSO-e appliance (legacy) to a ProtectServer External appliance, all of the keys you wish to migrate must be set as exportable. If a key is not exportable it cannot be removed from the HSM. Your pre-existing keys can be exported using a graphical environment with the Java utility “kmu”, or via the command line with the “ctkmu” tool. For the graphical tool the task is as simple as selecting your keys and then selecting “Export”. In the export dialog, leave the wrapping key as “Random”; the wrapping key is generated and transported along with the wrapped/exported keys. If you select an explicit wrapping key, that same wrapping key must be present on the destination HSM. On the destination HSM you select the destination slot and then choose the “Import” command.

## Enterprise Data Protection

SafeNet ProtectServer External is a key component of SafeNet’s comprehensive enterprise data protection solution to reduce the cost and complexity of regulatory compliance, data privacy, and information risk management. SafeNet Enterprise Data Protection (EDP) is the only solution that secures data across the connected enterprise, from core to edge, with protection of data at rest, data in transit, and data in use. Unlike disparate, multi-vendor point solutions that can create limited “islands” of security, SafeNet EDP provides an integrated security platform with centralized policy management and reporting for seamless, cost-efficient management of encrypted data across databases, applications, networks, and endpoint devices. For more information, visit [www.safenet-inc.com/EDP](http://www.safenet-inc.com/EDP)

**Contact Us:** For all office locations and contact information, please visit [www.safenet-inc.com](http://www.safenet-inc.com)

**Follow Us:** [www.safenet-inc.com/connected](http://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)-09.28.10