



ProtectServer Gold and ProtectServer Internal-Express

PRODUCT BRIEF

Sample User Applications

- Encryption, including database
- User and data authentication
- Message integrity
- Secure key storage
- Key management for eCommerce
- Key management for PKIs
- Electronic document management
- Electronic Bill Presentation and Payment (EBPP)
- EFT transactions

Benefits

Performance

- Specialized cryptographic electronics offload processing from the host system

Security

- ProtectServer Gold: FIPS 140-2 Level 3 validated
- PSI-E: FIPS 140-2 Level 3 validated
- Tamper-protected environment

Easy Management

- Intuitive GUI
- Command Line Interface
- In-field secure firmware upgrade
- Remote management on network HSMs

For server systems and support applications that require high-performance symmetric and asymmetric cryptographic operations, ProtectServer Gold and ProtectServer Internal-Express provide tamper-protected hardware security.

Varied Performance and Bus Interface

SafeNet ProtectServer Gold is a PCI-X-compliant expansion card, while SafeNet ProtectServer Internal-Express is a PCI Express x4-compliant card. Both HSMs offer different performance levels to meet varied system requirements: 25, 220, or 600 RSA 1024-bit signatures per second.

Wide Range of Cryptographic Processing

ProtectServer HSMs provide secure storage and a dedicated cryptographic processor to deliver high-speed processing for cryptographic operations and fast transaction speeds. ProtectServer Gold offers 4MB of secure storage, while ProtectServer Internal-Express offers double this amount. The HSMs provide a wide range of cryptographic services, including encryption, user and data authentication, message integrity, secure key storage, and key management for eCommerce, PKI, document management, Electronic Bill Presentation and Payment (EBPP), database encryption, financial EFT transactions, plus many others.

Strong Security - Keys Remain in Hardware

The ultimate level of protection is afforded to sensitive cryptographic processing that often operates within the less secure environment of servers. ProtectServer Gold and ProtectServer Internal-Express are FIPS 140-2 Level 3-validated, and feature tamper-protected security that safeguards against physical attacks on the HSMs to obtain sensitive information. Upon detection of a physical attack, the internal key storage memory is completely erased. Further, cryptographic keys are never exposed outside the HSMs in clear form.

Secure storage and processing offers customers a level of security unavailable from software alternatives, while providing a certified level of confidentiality and integrity that meets customer expectations and the security demands of industry organizations.

Extensive APIs/Toolkits and Customization

A wide range of application programming interfaces (APIs) are available to assist in adherence of the cryptographic application to industry security standards and platform environments. This includes the broadest suite of PKCS#11 function sets available on the market, a Java JCA/JCE and Microsoft CryptoAPI/CNG provider implementation, and seamless integration with Open SSL. The software development kit allows an unsurpassed level of flexibility and extensibility—providing the ability to produce custom cryptographic applications – including completely new algorithms – and to be securely downloaded and executed within the protected confines of the HSM. This capability is in addition to an EFT/payment processing command set and a customization module to facilitate tailored cryptographic applications operating on an HSM.

Technical Specifications

Operating Systems

- Windows Server 2003 (32- & 64-bit)
- Windows Server 2008 (32- & 64-bit)
- Solaris 9, 10 SPARC (32- & 64-bit)
- Solaris 10 x86 (32- & 64-bit)
- Linux E4K 2.6 (32- & 64-bit)
- Linux E5K 2.6 (32- & 64-bit)
- Linux SuSE 9, 10 (32- & 64-bit)
- AIX 5.3 (32- & 64-bit)
(ProtectServer Gold)
- HP-UX 11i (32- & 64-bit)
(ProtectServer Gold)

Connectivity

- ProtectServer Gold: PCI 2.2-compliant interface (32-bit or 64-bit, 33 MHz or 66 MHz); supports both 3.3v and 5v signaling
- ProtectServer Internal-Express: PCI Express Base Specification, revision 1.1, PCI Express Card Electromechanical Specification, revision 1.1 x4 link

Cryptographic Processing

Asymmetric Algorithms

- RSA (up to 4096 bit) , DSA, ECDSA Diffie Hellman (DH), plus others

Symmetric Algorithms

- AES, DES, 3DES, CAST-128, RC2, RC4, SEED, ARIA, plus others
- Modes supported include ECB, CBC, OFB64, CFB-8 (BCF) plus others

Hashing Algorithms

- MD5, SHA-1, SHA-256, SHA- 384, SHA-512, MD2, RIPEMD128, RIPEMD160, DES MDC-2 PAD1

Message Authentication Codes

- SHA-1, SHA-256, SHA-384, SHA-512, MD2, RIPEMD128, RIPEMD160, DES MDC-2 PAD1, SSL3 MD5 MAC, AES MAC, CAST-128 MAC, DES MAC, DES3 MAC, DES3 Retail CFB MAC, DES30x9.19 MAC, IDEA MAC, RC-2 MAC, SEED MAC, ARIA MAC, VISA CVV
- ECC Brainpool Curves (named and user-defined)

Random Number Generation

- Digital Signing
- DSA (512-1024), ECDSA, RSA, PKCS#11v1.5, 9796, X509, Timestamp

Physical Characteristics

Operating Temperature

- 0°C to 40°C

Storage Temperature

- -20°C to +65°C

Power Requirements

- ProtectServer Gold: +3.3 volts at 655 mA, +5 volts at 645 mA, +12 volts at 27 mA
- ProtectServer Internal-Express: +5V@3A max; +12V@0.2A max

Dimensions

- ProtectServer Gold: 231mm x 18.7mm x 105.5mm (9.1" x .73" x 4.15")
- ProtectServer Internal-Express: Full height 6.63" length

Easy Management

The intuitive graphic user interface (GUI) simplifies HSM device administration and key management using easy-to-understand navigation and user interaction. Urgent and time-critical management tasks—such as key modification, addition, and deletion—can be securely performed from remote locations, reducing management costs and response times.

Flexible Programming

ProtectServer HSMs offer a unique level of flexibility for application developers to create their own firmware and execute it within the secure confines of the HSM. Known as functionality modules, the toolkits provide a comprehensive facility to develop and deploy custom firmware. A full-featured software emulator rounds out the flexible development tools, enabling developers to test and debug custom firmware from the convenience of a desktop computer. This emulator also serves as an invaluable tool to test applications without the need to install a ProtectServer HSM. When ready, a developer simply installs the HSM and redirects communication to the hardware. No software changes are necessary.

Convenience

Smart cards provide the highest security and administrative convenience for secure backup, recovery, and transfer of cryptographic keys. Upgrades can be cost-effectively performed at the in-field location, avoiding the expense of returning the product to the service location.

Regulatory Standards Certification

- FCC Part 15 - Class B
- RoHS Compliant
- BAC and EAC ePassport Certification
- ProtectServer Gold: FIPS 140-2 Level 3 Certificate #739 and #1137
- ProtectServer Internal Express: FIPS 140-2 Level 3 Certificate #1550
- FCC Part 15 Class B Unintentional Radiators ANSI C63.4-2003
- EN 55022:1998 Amendment 1:2000, Amendment 2:2003
- EN 55024:1998 Amendment 1:2001

About SafeNet

Founded in 1983, SafeNet is a global leader in information security. SafeNet protects its customers' most valuable assets, including identities, transactions, communications, data, and software licensing, throughout the data lifecycle. More than 25,000 customers across both commercial enterprises and government agencies, and in over 100 countries, trust their information security needs to SafeNet.



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

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

©2011 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)-07.26.11