ProtectServer Gold

Hardware Security Module

ProtectServer Gold is a tamper-protected PCI Hardware Security Module (HSM) that provides high-performance, secure cryptographic processing in server systems, and supports applications requiring high-performance symmetric and asymmetric cryptographic operations.

Benefits

Performance
Specialized cryptographic electronics offload processing from the host system

Security
FIPS 140-2 level 3 validated
Tamper-protected environment

Easy Management
Graphic User Interface
Command Line Interface
In-field secure firmware upgrade
Remote management on network HSMs

Wide Range of Cryptographic Processing

ProtectServer Gold HSM incorporates 64 bit PCI interface, 4Mb secure storage capacity and a dedicated cryptographic processor to deliver high-speed cryptographic processing for cryptographic operations and fast transaction speeds. It provides a wide range of cryptographic services including encryption, user and data authentication, message integrity, secure key storage and key management for e-Commerce, PKI, document management, Electronic Bill Presentation and Payment (EBPP), database encryption, financial EFT transactions, plus many others.

Keys Remain in Hardware

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 organization.

Extensive APIs/Toolkits and Customization

A wide range of Application Programming Interfaces (APIs) are available to assist adherence of your 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 provider implementation, plus seamless integration with Open SSL. The software development kit functionality allows an unsurpassed level of flexibility and extensibility. It provides the ability to produce your own custom cryptographic application (including completely new algorithms) and allow it to be securely downloaded and executed within the secure confines of the HSM. This is in addition to an EFT/payment processing command set and a customization module to facilitate customized cryptographic applications operating on a HSM.

Strong Security

The ultimate level of protection is afforded to sensitive cryptographic processing that often operates within the less secure environment of servers. The FIPS 140-2 level 3 validated, 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. Further, cryptographic keys are never exposed outside the HSM in clear form.

Easy Management

Easy interaction and key management are achieved via an intuitive Graphic User Interface (GUI). GUI simplifies HSM device administration and key management using intuitive 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.

Convenience

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 expense of returning the product to the service location

Regulatory Standards Certification

- FCC Part 15 - Class B
- RoHS Compliant
- BAC and EAC ePassport Certification
- ISO– 9002 Certification
- FIPS 140-2 Level 3 Certificate 739
- 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

Technical Specifications

Operating Systems

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

Connectivity

- *PCI 2.2 compliant interface (32 bit or 64 bit, 33 MHz or 66 MHz)*
- *Supports both 3.3v and 5v signaling*

Cryptographic Processing

Asymmetric Key Encryption

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

Symmetric Algorithms

- *AES, DES, 3DES, CAST-128, RC2, RC4, SEED, 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, 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*

Power Requirements

- *+3.3 volts at 655 mA, +5 volts at 645 mA, +12 volts at 27 mA*

Dimensions

231mm x 18.7mm x 105.5mm (9.1" x .73" x 4.15")

SafeNet
The Foundation of Information Security

www.safenet-inc.com

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

PB-HSM PCI 3.32-06.10.08