SafeNet

THE DATA PROTECTION COMPANY

ProtectServer External 2

PRODUCT BRIEF

Benefits

Security
- Physical tamper protection
- True Random Number Generation
- Smartcard backup of key material

Performance
- Dual LAN
- Up to 1500 RSA signings/sec
- WLD (Work Load Distribution)
- Multi-threaded APIs

Easy Management
- Infield upgrade
- GUI HSM interface
- Remote HSM Management

Extensive API support

Available in 25, 220, and 1500 performance models.

ProtectServer External 2 is a security hardened network crypto server designed to protect cryptographic keys against compromise, while providing encryption, signing and authentication services to security sensitive applications.

Highly Secure

SafeNet ProtectServer External 2 includes a cryptographic module performing secure cryptographic processing in a high assurance fashion. The appliance features a heavy-duty steel case with tamper-protected security that safeguards against physical attacks and 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. Secure storage and processing means cryptographic keys are never exposed outside the HSMs in clear form, offering customers a level of security unavailable from software alternatives, while providing a certified level of confidentiality and integrity that meets the security demands of industry organizations.

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.

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.

Technical Specifications

Operating Systems
- Windows and Linux

Cryptographic APIs
- PKCS#11, CAPI/CNG, JCA/JCE, JCProv, OpenSSL

Cryptographic Processing
Asymmetric Algorithms
- RSA (up to 4096 bit), DSA, ECDSA Diffie Hellman (DH), ECC Brainpool Curves (named and user-defined), 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

Physical Characteristics
Dimensions
- 437 mm(W) x 270 mm (D) x 44 mm (H)

Power Consumption
- 220/110 Volts Switchable

Temperature
- Operating 0°C - 40°C

Security Certifications
- FIPS 140-2 Level 3**

**Under evaluation

Safety and Environmental Compliance
- UL, CSA, CE
- FCC, KC Mark, VCCI, CE
- RoHS, WEEE

High Performance and Scalability

SafeNet ProtectServer External 2 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 2 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 1500 RSA signature operations per second. The included dual-network interface optionally enables the HSM to be integrated on the same or different subnets, and to 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.

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 infield location, avoiding the expense of returning the product to the service location.

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