cpl.thalesgroup.com

THALES

Thales ProtectServer 2 Network HSM

ProtectServer External 2 and ProtectServer External 2+

Thales ProtectServer Network 2 Hardware Security Modules (HSMs) are security hardened network crypto servers designed to protect cryptographic keys against compromise, while providing encryption, signing and authentication services to security sensitive applications.

ProtectServer External 2 HSM

ProtectServer 2+ HSM

Highly secure

ProtectServer Network HSMs include a cryptographic module performing secure cryptographic processing in a high assurance fashion. The appliances feature heavy-duty steel cases with tamper-protected security that safeguard against physical attacks and 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. Secure storage and processing means cryptographic keys are never exposed outside the HSM 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.

ProtectServer 2+ HSM

In addition to the features and functionality provided by ProtectServer 2 HSM, ProtectServer 2+ HSM employs dual swappable AC power supplies to help high-availability data centers protect against power failures, and enables business continuity by providing the ability to connect the appliance to two separate power sources to safeguard against the possible malfunction of one of the sources. This provides the necessary flexibility to perform maintenance on or replace a failed power supply or power feed with the assurance that your device will continue to operate.

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

- PSE2 available in 25, 220, and 1500 performance models
- PSE2+ available in 1500 performance model only

High performance and scalability

ProtectServer Network HSMs perform rapid processing of cryptographic commands. Specialized cryptographic electronics — including a dedicated data cipher micro-processor, memory, and a true Random Number Generator (RNG) — offloads the cryptographic processing from the host system, freeing it to respond to more requests.

ProtectServer Network HSMs are 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 HSMs 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.

Technical specifications

Operating Systems

- Windows, Linux, AIX, HP_UX, Solaris

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, BIP32 and SECP256k1, Milenage, 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) (PSE2 model)
- 482.6mm (W) x 533.4mm (D) x 43.815mm (H) (PSE2+ model)

Power Consumption

- 220/110 Volts switchable (PSE2 model)
- Dual swappable AC power supplies (PSE2+ model)

Temperature

- Operating 0°C - 35°C

Security Certifications

- FIPS 140-2 Level 3

Safety and Environmental Compliance

- UL, CSA, CE
- FCC, KC Mark, VCCI, CE
- RoHS, WEEE