cpl.thalesgroup.com

THALES
Building a future we can all trust

Thales ProtectServer 3 Network HSMs

ProtectServer 3 External
ProtectServer 3+ External

Thales ProtectServer 3 Network 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 secure sensitive applications.

ProtectServer 3 External HSM

ProtectServer 3+ External 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 levels 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

Benefits

Performance

- 3500 RSA-1024 signatures / sec

Security

- FIPS 140-2 Level 3 validated
- Physical tamper protection
- True Random Number Generation
- Smartcard backup of key material

Reliability

- High quality components

Easy Management

- Intuitive GUI
- In-field secure upgrade
- Remote management

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 3+ HSM

In addition to the features and functionality provided by ProtectServer 3 HSM, ProtectServer 3+ 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.

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) — offload 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 3500 RSA-1024 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 in-field location, avoiding the expense of returning the product to the service location. ProtectServer HSMs also support key component entry via a compatible PIN pad.

Multi-factor authentication

ProtectServer HSMs support multi-factor authentication. This authentication scheme adds another layer of security by requiring both the memorized token PIN and a 6-digit number randomly generated by the 110 OTP Token.

Technical specifications

Available models:

- PSE 3 available in PL25, PL220, and PL3500 performance models
- PSE 3+ available in PL3500 performance model only

Operating Systems

- Windows, Linux

Cryptographic APIs

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

Cryptography

- Asymmetric: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519) with named, userdefined and Brainpool curves, and more
- Symmetric: AES, AES-GCM, AES-CCM, Triple DES, DES, CAST 128, RC2, RC4, SEED, ARIA plus others
- Hashing: SHA-1, SHA-2, SHA-3, MD5, MD2, RIPEMD 128, RIPEMD 160, DES MDC2 PAD1 and more
- Message Authentication Codes: SHA-1, SHA-2, SHA-3, 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
- Digital Wallet Encryption: BIP32
- 5G Cryptographic Mechanisms for Subscriber Authentication: MILENAGE and TUAK

Physical Characteristics

- Rack Mountable
  - Standard 1U 19" rack mount appliance
- Dimensions
  - 17.20" x 9.84" x 1.73" (437 mm x 270 mm x 44 mm) (PSE 3)
  - 19" x 21" x 1.725" (482.6mm x 533.4mm x 43.815mm) (PSE 3+)
- Weight
  - 6.83lb (3.1 kg) (PSE 3)
  - 28lb (12.7kg) (PSE 3+)
- Input Voltage
  - 100-240V, 50-60Hz (PSE 3)
  - 100-240V, 50-60Hz (PSE 3+)
- Power Consumption
  - 90W maximum, 58W typical (PSE 3)
  - 100W maximum, 84W typical (PSE 3+)
- Temperature
  - Operating 0°C to 35°C, storage -20° to 60°C
- Relative Humidity
  - 5% to 85% (38°C) non-condensing (PSE 3)
  - 5% to 95% (38°C) non-condensing (PSE 3+)

Host Interface

- 2 Gigabit Ethernet ports with Port Bonding (PSE 3)
- 4 Gigabit Ethernet ports with Port Bonding (PSE 3+)
- IPv4 and IPv6

Security Certifications

- FIPS 140-2 Level 3

Management and Monitoring

- High Availability (HA) / Work Load Distribution (WLD)
- SNMP, Syslog
- Backup/Restore

Safety and Environmental Compliance

- UL, CSA, CE
- FCC, KC Mark, VCCI, CE
- RoHS, WEEE
- India BIS [IS 13252 (Part 1)/IEC 60950-1]

Reliability

- Dual hot-swap power supplies (PSE 3+)
- Mean Time Between Failure (MTBF) 165637 hours (PSE 3)
- Mean Time Between Failure (MTBF) 171,308 hours (PSE 3+)

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us