cpl.thalesgroup.com

THALES
Building a future we can all trust

Thales ProtectServer 3 PCIe HSM

Thales ProtectServer 3 PCIe Hardware Security Module (HSM) provides tamper-protected hardware security for server systems and applications that require high-performance symmetric and asymmetric cryptographic operations.

Varied performance levels

ProtectServer PCIe HSM is a PCI Express x4-compliant card available in different performance levels to meet varied system requirements: 25, 220, or 3500 RSA-1024 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. The HSM provides 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.

Benefits

Performance

- Up to 3500 RSA-1024 signatures / sec
- Specialized cryptographic electronics offload processing from the host system

Security

- FIPS 140-2 Level 3 validated*
- Tamper-protected environment

Reliability:

- High quality components

Easy Management

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

Interoperability

- ANSI X9 TR-31 Key Block Support

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 PCIe HSM is FIPS 140-2 Level 3-validated*, and features tamper-protected security that safeguards against physical attacks on the HSM 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 HSM 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, JCProv, 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.

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. 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.

Multiple slots

ProtectServer PCIe HSM supports multiple cryptographic key storage slots. Storage slots function similarly to a smart card reader with multiple card slots, but without the need for a physical card reader. These virtual slots are effectively secure folders for keys, with each folder secured by a unique user and security officer password. This allows a single ProtectServer HSM to be used by multiple applications, for greater cost savings and flexibility.

Technical specifications

Available models:

- ProtectServer 3 PCIe HSM - PL25, PL220 and PL3500 performance models

Operating Systems

- Windows and 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, AES-GMAC, 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
- ANSI X9 TR-31 Key Block Support for interoperability

Physical Characteristics

- Low profile PCIe card
- Dimensions: 2.74" x 6.57" x .074" (69.6mm x 167mm x 187mm)
- Power Consumption: 18W maximum, 14W typical
- Heat Dissipation: 61.4 BTU/hr maximum, 47.8 BTU/hr typical
- Temperature: operating 0°C to 50°C, storage -20°C to 60°C
- Relative Humidity: 5% to 95% (38°C) non-condensing

Host Interface

- PCI-Express CEM 3.0, PCI, PCI Express Base 2.0

Security Certifications

- FIPS 140-2 Level 3*

Safety, Export and Environmental Compliance

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

Reliability

- Mean Time Between Failure (MTBF) 997,508 hours
- High Availability (HA) / Work Load Distribution (WLD)
- Backup/Restore

* in progress

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.