

# Thales ProtectServer PCIe HSM 2



**Thales ProtectServer PCIe Hardware Security Module (HSM) 2 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 1500 RSA 1024-bit 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.



## Sample user applications

- Encryption, including database
- User and data authentication
- Message integrity
- Secure key storage
- Key management for eCommerce
- Key management for PKIs
- Electronic document management
- Electronic Bill Presentation and Payment (EBPP)
- EFT transactions

## Benefits

### Performance

- Specialized cryptographic electronics offload processing from the host system

### Security

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

### Easy Management

- Intuitive GUI
- Command Line Interface
- In-field secure firmware upgrade
- Remote management on network HSMs

## 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, JCEP, 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.

## Technical specifications

### Operating Systems

- Windows and Linux

### Cryptographic APIs

- PKCS#11, CAPI/CNG, JCA/JCE, JCEP, 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: Full Height, Half Length 4.16" x 6.6" (106.7mm x 167.65mm)
- Power Consumption: 12W maximum, 8W typical
- Temperature: operating 0°C – 50°C

#### Security Certifications

- FIPS 140-2 Level 3
- BAC & EAC ePassport Support

#### Safety and Environmental Compliance

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

#### Host Interface

- PCI-Express X4, PCI CEM 1.0a

#### Reliability

- MTBF 216,204 hrs

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

## 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.

## 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.