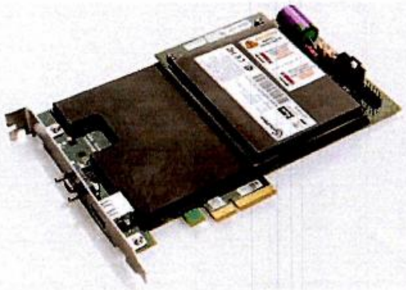
gemalto
security to be free



PRODUCT BRIEF

SafeNet PrtSrv Internal2, Toolkit PL25

The SafeNet ProtectServer PCIe HSM from Gemalto provides tamper-protected hardware for server systems and applications that require high-performance symmetric and asymmetric cryptographic operations.

Varied Performance Levels

SafeNet 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

SafeNet 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.

Strong - 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. SafeNet ProtectServer PCIe HSM is FIPS 140-2 Level 3-validated, and features tamper-protected 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 unavailable from software alternatives, while providing a certified level of confidentiality and integrity that meets customer expectations and the 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 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.

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
- FIPS 140-2 Level 3 validated (in process)
- Tamper-protected environment

Easy Management

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

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.