SAFENET® PROTECTSERVER HARDWARE SECURITY MODULES (HSMS)

Benefits

Security

- *FIPS 140-2 level 3 validated*
- *Tamper-protected environment*
- *True Random Number Generation*
- *Meets Visa and Mastercard security requirements*

Performance

- *Specialized cryptographic electronics offload processing from the host system*
- *Up to either 25 or 600 RSA 1024-bit signatures per second*

Management

- *Intuitive GUI*
- *Remote management on network HSMs*

Internal and External Hardware Security Modules

Datacard Group has partnered with SafeNet Inc., a global leader in information security and HSM technology, to support Datacard® Affina® issuance platform software and Datacard® CardWizard® issuance software functions that require high-performance symmetric and asymmetric cryptographic operations.

Four SafeNet HSM Options

- HSM ProtectServer PL25 (External Rack Mountable)
- HSM ProtectServer PL600 (External Rack Mountable)
- HSM ProtectServer PL25 (Internal PCIe Card)
- HSM ProtectServer PL600 (Internal PCIe Card)

To improve security, functionality, and efficiency, Datacard Group combines the HSM offerings with Affina PKCS #11 firmware. This firmware is developed specifically for magnetic stripe data calculations, chip data preparation and personalization, and PIN functions.

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 HSMs provide a wide range of services, including encryption, user and data authentication, message integrity, and secure key storage.

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. The ProtectServer HSMs have tamper-protected security that safeguards against physical attack; the internal key storage memory is completely erased. Further, cryptographic keys are never exposed outside the HSMs 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 the industry standards such as Federal Information Processing Standard (FIPS) and EMV® standards.

Performance

The ProtectServer HSMs are available in two symmetric and asymmetric cryptographic performance levels to meet specific security application processing requirements, with speeds up to either 25 or 600 RSA 1024-bit signature operations per second.

DatacardGroup

SAFENET PROTECTSERVER HARDWARE SECURITY MODULES (HSMS)

Affina PKCS #11 Firmware and Key Management Features

PKCS #11 Firmware

- *Improves security, functionality, and efficiency for cryptographic operations required by the personalization process*
- *Supports magnetic stripe data calculations and chip data preparation and personalization as well as validation*
- *Supports PIN encryption and calculations*

KMS

- *Enhances user authentication*
- *Simplifies key management tasks*
- *Supports certificate handling for major payment applications*

Physical Characteristics and Bus Interface

The ProtectServer Internal is a PCI-Express x4-compliant card. The ProtectServer External appliance features a heavy-duty rack mount 1U steel case with tamper-protected security that safeguards against physical attacks.

The ProtectServer External includes a dual-network interface which optionally enables the HSM to be integrated on the same or different subnets. It can be shared between different networks in order to protect multiple business domains or provide redundancy within a single network.

Centralized Management

The Affina software KMS component includes an intuitive graphic user interface (GUI) that simplifies HSM device administration and key management. 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.

Convenience

Upgrades can be cost-effectively performed on location, avoiding the expense of returning the product to the service location.

Supported Configurations

Internal PCIe card

- Microsoft® Windows® XP 32 bit (for local applications only)
- Microsoft® Windows® 7 32/64 bit (for both local and remote applications)
- Microsoft® Windows® 2003 32/64 bit (for both local and remote applications)
- Microsoft® Windows® 2008R2 64 bit (for both local and remote applications)

External Rack Mountable

- Windows XP 32 bit
- Windows 7 32/64 bit
- Windows 2003 32/64 bit
- Windows 2008R2 64 bit

Internal PCI Express (PCIe) Card Characteristics

Connectivity
PCI Express Base Specification, revision 1.1, PCI Express Card Electromechanical Specification, revision 1.1x4 link

Dimensions
Full height 6.63" length
Weight 3.1 kg

Power requirements
+5V at 3A max; +12V at 0.2A max

Operating environment
0 degrees to 40 degrees C
5% to 95% Relative Humidity

Regulatory standards certifications
Cryptographic module: FIPS 140-2 Level 3
FCC Part 15 – Class B
RoHS Compliant
BAC and EC ePassport Certification
FCC Part 15 Class B Unintentional Radiators
ANSI C63.4-2003
EN 55022:1998 Amendment 1:2000, Amendment 2:2003
EN 55024: 1988 Amendment 1:2001

Seucre storage
Up to 4MB

External Rack Mountable Characteristics

Connectivity
Dual LAN Support
TCP/IP over Ethernet

Dimensions
437 mm (W) x 270 mm (D) x 44 mm (H)
Weight 3.1 kg

Power requirements
220/110 Volts Switchable

Operating environment
0 degrees to 40 degrees C
5% to 95% Relative Humidity

Regulatory standards certifications
Cryptographic module: FIPS 140-2 Level 3
UL 1950 (EN60950) & CSA C22.2 safety compliant
FCC Part 15 --- Class B
RoHS Compliant

Seucre storage
Up to 4MB

DatacardGroup

CORPORATE HEADQUARTERS
11111 Bren Road West
Minnetonka, Minnesota 55343-9015
Phone: +1 952 933 1223
www.datacard.com
info@datacard.com

FS12-3113