gemalto
security to be free

PRODUCT BRIEF

Gemalto SafeNet
PS HSM (Hardware Security Module)

PS HSM (Hardware Security Module) is a security hardened network crypto server designed to protect cryptographic keys against compromise, while providing encryption, signing and authentication services to security sensitive applications.

Highly Secure

Gemalto SafeNet PS HSM includes a cryptographic module performing secure cryptographic processing in a high assurance fashion. The appliance features a heavy-duty steel case with tamper-protected security that safeguards against physical attacks and delivers the highest level 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 Hardware Security Module (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

SafeNet PS 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 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 PS HSM. When ready, a developer simply installs the HSM and redirects communication to the hardware — no software changes are necessary.

Benefits

Security
- Physical tamper protection
- True Random Number Generation
- Smartcard backup of key material
- 4 MB Secure Memory (All key in Memory)
- Key encryption Key (KEK Mode) for External Key

Performance
- Dual LAN
- WLD (Work Load Distribution)
- Multi-threaded APIs

Easy Management
- PSM(ProtectServer Monitor) /chinese version
- GUI HSM interface (CMD line interface)
- Redundant power supply

Extensive API support
Available in 25, 220, and 1500 performance models.

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.

High Performance and Scalability

SafeNet PS HSM (Hardware Security Module) performs rapid processing of cryptographic commands. Specialized cryptographic electronics — including a dedicated data cipher micro-processor, memory, and a true Random Number Generator (RNG) — offloads the cryptographic processing from the host system, freeing it to respond to more requests.

SafeNet PS HSM is 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 1500 RSA signature operations per second. The included dual-network interface optionally enables the HSM 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 infield location, avoiding the expense of returning the product to the service location.

About Gemalto' s SafeNet Identity and Data Protection Solutions

Gemalto' s portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions–from the edge to the core. Gemalto' s SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Technical Specifications

Operating Systems
- WIN 2008 R2 (64-bits),WIN 2012 R2 (64-bits), WIN 7(32-bits,64-bits),Solaris 10,11 SPARC (64-bits), Linux SuSE 12(64-bits),AIX 6.1(64-bits), RedHat Enterprise Linux 6 (32-bits,64-bits)

Cryptographic APIs
- PKCS#11, CAPI/CNG, JCA/JCE, JCProv, 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

Power Consumption
- 220/110 Volts Switchable

Security Certifications
- FIPS 140-2 Level 3 -Tamper protected physical (PCI) HSM Security

Safety and Environmental Compliance
- UL, CSA, CE
- FCC, KC Mark, VCCI, CE
- RoHS, WEEE

license charges
- Unlimited license (for free)

GEMALTO.COM

gemalto
security to be free