



## PRODUCT BRIEF

# SafeNet PCIe HSM (Formerly SafeNet Luna PCI-E)

The SafeNet Network HSM from Gemalto is the choice for enterprises requiring strong security for digital signatures, cryptographic key storage, transactional acceleration, certificate signing, code signing, bulk key generation, data encryption, DNSSEC, and more.

The SafeNet PCIe HSM from Gemalto is the most widely deployed general purpose embedded hardware security module in the market. With dedicated performance and the ability to build completely integrated solutions, SafeNet PCIe HSM is ideally suited for authentication, signing and key issuance.

### Secure Hardware Key Management

The high assurance design of SafeNet PCIe HSM offers dedicated hardware key management to protect sensitive cryptographic keys throughout the key lifecycle. The internal security architecture of SafeNet PCIe HSM provides an unprecedented level of security for the keys and sensitive data generated, utilized, and stored within the HSM.

### Embed the SafeNet General Purpose HSM Feature Set for Operational Cost Savings

SafeNet PCIe HSM benefits from a robust and forward thinking feature set. These features, including remote management, secure transport, and remote backup, will greatly reduce the management and operational costs of a solution that utilizes SafeNet PCIe HSM.

### High Availability and Scalable Performance

Multiple SafeNet PCIe HSM cards can be grouped together in the same server to provide high availability, load balancing and scalable performance. The HA Group technology shares the transaction load, synchronizes data among members of the group, and redistributes the processing capacity in the event of failure in a member card to maintain uninterrupted service. The HA capability also enables easy recovery when a unit returns to service. SafeNet PCIe HSM also includes API support for synchronization of keys between cards in different servers. Using this API, organizations can create their own high-availability setup.

## Benefits & Features

### Most Secure

- > Keys in hardware
- > Remote Management
- > Secure transport mode for high-assurance delivery
- > Multi-level access control
- > Multi-part splits for all access control keys
- > Intrusion-resistant, tamper-evident hardware
- > Secure Audit Logging
- > Strongest cryptographic algorithms
- > Suite B algorithm support
- > Secure decommission

### Sample Applications

- > PKI key generation & key
- > Storage (online CA keys & offline CA keys)
- > Certificate validation & signing
- > Document signing
- > Transaction processing
- > Database encryption
- > Smart card issuance
- > Root of Trust for the Internet of Things

## Flexible Backup and Disaster Recovery Options

SafeNet PCIe HSM provides secure, auditable and flexible options to simplify backup, duplication, and disaster recovery. Key backups can be performed locally or remotely to the SafeNet Backup HSM, small form factor eTokens or other SafeNet HSMs.

## Achieve FIPS 140-2 and Common Criteria Validation without Investing in Costly Certifications

Achieving FIPS and Common Criteria certification can be a time consuming and costly process. As Gemalto's sole focus is security, we make third-party certifications a priority. Our team has years of experience in designing products that adhere to FIPS 140-2 and Common Criteria. Leveraging a SafeNet PCIe HSM in your appliance or service represents a cost effective way to bring FIPS 140-2 and Common Criteria validated solutions to market.

## Develop Solutions for Resource Constrained Environments with ECC Support

As the need to provide security for resource constrained devices (smart phones, tablets, smart meters) grows, vendors must be able to provide solutions that leverage ECC algorithms. ECC offers high key strength, at a greatly reduced key length when compared to RSA keys. SafeNet PCIe HSM offers hardware accelerated ECC algorithms that can be used in the development of solutions without the need to purchase additional licenses.

## Common Architecture

All SafeNet general purpose HSMs benefit from a common architecture where the supported client, APIs, algorithms, and authentication methods are consistent across the entire general purpose HSM product line. This eliminates the need to design applications around a specific HSM, and provides the flexibility to move keys from form factor to form factor.

## Available in Two Performance Models

SafeNet PCIe HSM is available in two performance models; SafeNet PCIe HSM 7000 and SafeNet PCIe HSM 1700. SafeNet PCIe HSM 7000 is a high performance HSM capable of best in class performance across a breadth of algorithms including ECC, RSA, and symmetric transactions. The standard performance variant, SafeNet PCIe HSM 1700, is capable of 1700 RSA 1024-bit transactions per second.

Algorithm	Model	
	PCIe HSM 1700	PCIe HSM 7000
RSA-1024	1,800	7,300
RSA-2048	360	1,200
ECC P256	580	2,000
ECIES	200	310
AES-GCM	3,600	3,600

## Technical Specifications

### Operating System Support

- > Windows, Linux, Solaris

### API Support:

- > PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL, Ruby, Python

### Cryptography

- > PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL

### Cryptography

- > Full Suite B support
- > Asymmetric: RSA (1024-8192), DSA (1024-3072), Diffie-Hellman, KCDSA, Elliptic Curve Cryptography (ECDSA, ECDH, ECIES) with named, user-defined and Brainpool curves
- > Symmetric: AES, RC2, RC4, RC5, CAST, DES, Triple DES, ARIA, SEED
- > Hash/Message Digest/HMAC: SHA-1, SHA-2 (224-512), SSL3-MD5-MAC, SSL3-SHA-1-MAC
- > Random Number Generation: FIPS 140-2 approved DRBG (SP 800-90 CTR mode)

### 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 2 and Level 3
- > Common Criteria EAL4+ (in process)
- > 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

**Contact Us:** For all office locations and contact information, please visit [www.safenet-inc.com](http://www.safenet-inc.com)

**Follow Us:** [data-protection.safenet-inc.com](https://twitter.com/data-protection.safenet-inc.com)

 GEMALTO.COM

 **gemalto**  
security to be free