thalestct.com

THALES

Luna PCI-E for Government
Hardware Security Module

Luna PCI-E for Government is the fastest and most secure cryptographic accelerator card in the industry. Designed for authentication, signing and key Issuance, Luna PCI-E for Government is ideal for use as an embedded HSM in servers or appliances. Derived from industry leading technology, the Luna PCI-E for Government is manufactured, sold, and supported exclusively by Thales Trusted Cyber Technologies (TCT).

Secure Hardware Key Management

The high assurance design of Luna PCI-E for Government offers dedicated hardware key management to protect sensitive cryptographic keys throughout the key lifecycle. The internal security architecture of Luna PCI-E for Government provides an unprecedented level of security for the keys and sensitive data generated, utilized, and stored within the HSM. At the core of Luna PCI-E for Government is the SafeXcel 3120, a robust, fail-safe security system on a chip used to protect internal keys and sensitive data. This defense-in-depth architecture isolates plaintext key material from the HSM's primary firmware by further encrypting internal keys with a key that exists only in the SafeXcel hardware.

Embed the TCT Luna General Purpose HSM Feature Set for Operational Cost Savings

Luna PCI-E for Government 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 Luna PCI-E for Government .

High-Availability and Scalability

Multiple Luna PCI-E for Government 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. Luna PCI-E for Government also includes API support for synchronization of keys between cards in different servers. Using this API, organizations can create their own high-availability setup.

Flexible Backup and Disaster Recovery Options

Luna PCI-E for Government provides secure, auditable and flexible options to simplify backup, duplication, and disaster recovery. Key backups can be performed locally or remotely to the Luna Backup HSM, Small Form Factor eTokens or other Luna HSMs.

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. Luna PCI-E for Government offers hardware accelerated ECC algorithms that can be used in the development of solutions without the need to purchase additional licenses.

Security Certification

The Luna PCI-E for Government has received FIPS 140-2 Level 2 and 3 validation from the National Institution of Standards and Technology (NIST). This validation signifies that TCT's Luna HSMs for Government comply with these stringent standards.

Common Luna Domain

All Luna HSMs benefit from a Common Luna Architecture where the supported client, APIs, algorithms, and authentication methods are consistent across the entire Luna 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

Luna PCI-E for Government is available in two performance models; Luna PCI-E for Government 7000 and Luna PCI-E for Government 1700. Luna PCI-E for Government 7000 is a high performance HSM capable of best in class performance across a breadth of algorithms including ECC, RSA, and symmetric transactions. The low performance variant, Luna PCI-E for Government 1700, is capable of 1700 RSA 1024-bit transactions per second.

Luna PCI-E for Gov 1700	Luna PCI-E for Gov 7000
• RSA-1024 1,700 tps • RSA-2048 360 tps • ECC P256 580 tps • ECIES 200 tps • AES-GCM 3,600 tps	• RSA-1024 7,000 tps • RSA-2048 1,200 tps • ECC P256 2,000 tps • ECIES 300 tps • AES-GCM 3,600 tps

Benefits

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
- Suite B algorithm support
- Secure decommission
- Secure audit logging
- Strongest cryptographic algorithms

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

Technical Specifications

Operating System

- Windows, RedHat Linux

Cryptographic APIs

- 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

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 Validated

Safety and Environmental Compliance

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

Host Interface

- PCI-Express X4, PCI CEM 1.0a

Reliability

- Mean Time Between Failure (MTBF) 204 hrs

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

Contact Us: For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com