thalestct.com

THALES

AppViewX and Thales Trusted Cyber Technologies Luna Network HSM

The SSL/TLS protocol is used to facilitate secure communication over a network; relying heavily on digital certificates to authenticate entities and encrypt exchanged information. Digital certificates provide support for public key cryptography because they contain the public key of the entity identified in the certificate. Public key cryptography uses public and private keys to encrypt and decrypt data – keys generated and paired together but not identical (asymmetric). The digital certificate matches a public key to a particular entity, and that certificate's authenticity is guaranteed by the certificate issuer (a certification authority).

Traditionally, asymmetric keys are created and stored locally on the devices handling SSL/TLS communication. Having the keys stored locally exposes them to an attack on the device. If the device is compromised then the attacker also has access to the keys, which could then be used to masquerade as the owner of the device.

To mitigate the exposure of keys an external device is used for key generation, safe storage, and the off-loading of cryptographic processing. In the USA, the requirements for government security are regulated by Federal Information Processing Standards (FIPS) publications. FIPS 140-2 specifically deals with the asymmetric keys used in SSL/TLS communication and how to secure them. Organizations can prevent attackers from gaining access to sensitive key material by storing their keys in a FIPS-compliant hardware device, such as a hardware security module (HSM). A HSM is a FIPS-validated, dedicated cryptographic processor that is specifically designed for the protection of the cryptographic key lifecycle.

AppViewX CERT

AppViewX CERT+ provides a one-stop solution for automated discovery, expiry alerting, renewal, provisioning and revoking of SSL/TLS certificates across networks including servers, clients, and ADC devices. It arms Security Operations and Public Key Infrastructure (PKI) teams with critical insights that can be used to avoid unwanted outages and other issues associated with non-compliant certificates.

AppViewX stores the private keys discovered in a secure part of the database, which is encrypted using AES-256 algorithm. It encrypts each private key with independent keys and stores the encrypted independent keys in the database with a randomly generated key. Thus, even if the hackers gets the database, they will not be able to get to the private keys.

Thales Trusted Cyber Technologies Luna Network HSM

For an added level of security, organizations can integrate Thales Trusted Cyber Technologies' (TCT) Luna Network Hardware Security Module (HSM) with AppViewX CERT+ to store keys in a FIPS-compliant* environment.

Centralized Management and Operations

Luna Network HSM can be clustered into high-availability configurations that can be managed as one unit. In addition, Luna Network HSM can perform multiple operations – such as key generation, digital signatures, and encryption/decryption functions – where enterprises would normally require multiple appliances or solutions.

Logging and Auditability Features

Luna Network HSM combines proven hardware key management with rigorous logging features to provide non-reputable audit records of access and cryptographic key usage. Separated administrative roles and flexible security policy management allows security teams to maintain tight control over the management of cryptographic keys. Knowing who is accessing the private keys and being able to easily demonstrate detailed log records makes reporting for audits easier on security teams.

Partition to Easily Scale

Luna Network HSM can be separated into 20 cryptographically isolated partitions, with each partition acting as if it were an independent HSM. Partitions provide a tremendous amount of scalability and flexibility, as a single HSM can act as the root of trust that protects the cryptographic key lifecycle of twenty independent AppViewX installations. What's more, the partitions are designed to protect key material from other tenants on the appliance, meaning different lines of business, can leverage the same appliance without fear of losing their keys to another tenants. Enterprises with largescale AppViewX deployments can use Luna Network HSM as a cost-effective solution to hardware key storage.

High-Performance Processing

Luna Network HSM are capable of processing up to 7,000 RSA and 1,000 ECC transactions per second. High processing speeds allow administrators to offload cryptographic functions to improve server and datacenter performance.

Robust Security that Meets Compliance Standards

Luna Network HSM offers the highest level of tamper-resistant security and are validated to be compliant with FIPS 140-2 Level 2 and 3*.

Multi-Level Access Control

Luna Network HSM offer partitioning for signing/key management. Backup features allow administrators to securely move copies of their sensitive cryptographic material to the Luna Network HSM.

Luna Network HSM Advantages

Market Leadership

- Strong partnerships and participation in standardization bodies.
- Proven track record of security in the Federal Government.

Operational Cost Savings

- Secure remote management and remote backup.
- Secure transport mode.

High Availability (HA) and High Performance

- Can be separated into 20 partitions and can be clustered into HA configurations for easy linear scaling as the number of transactions grows.
- Are capable of processing up to 7,000 RSA and 1,000 ECC transactions per second.

Vendor Interoperability

- Works with multiple endpoints in the infrastructure.

Highly Secure/Easily Auditable

- FIPS 140-2 Levels 2 & 3 and Common Criteria certified.
- Maintain keys in hardware throughout the key lifecycle.
- Customers always know where keys reside. Demonstrating compliance is easier.

Cloud Ready

- Luna Network HSM powers AWS CloudHSM.
- Customers can enjoy FIPS level hardware key storage for deployments run through AWS.

Integration Benefits

- Stores, in hardware, the certificates and master encryption key (MEK) to AppViewX transactions.
- Hardware storage keeps keys protected from unauthorized users. Knowing the master key is safe ensures the integrity of the entire encryption infrastructure.
- Provides a secure, high-performance, scalable solution.
- Provides FIPS 140-2 Level 3 protection of encryption/decryption keys.
- Provides a key generator and safe key storage facility.
- Serves as a tool for securely encrypting sensitive data for storage in a relatively non-secure location such as, a database.
- Serves as a tool for verifying the integrity of data stored in a database.

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

*FIPS Validation Pending

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