thalesgroup.com

THALES

Secure Pivotal Platform Credentials and Secrets

Using Luna HSM with Pivotal Credhub

Enterprises adopt Pivotal Platform to accelerate their application and infrastructure transformation so they can bring their value to market faster, cheaper, and at a lower risk than ever before. Pivotal gives companies the speed, simplicity, and control they need to maintain a competitive advantage in the market.

Though organizations are iterating and developing software at faster and faster speeds, security remains a fundamental concern. Applications require certificates and secrets, and they often collect and process an organization's most valuable data. Pivotal makes this certificate management easy for DevOps and security administrations through its Credhub.

Managing those certificates and secrets is only part of the challenge. Enterprises collecting highly sensitive data, especially within regulated industries, face compliance obligations that often dictate how these secrets are managed. And, cryptography protects data wherever it exists for only as long as the corresponding cryptographic keys are held safe.

Fortunately, Thales works with Pivotal to address these compliance and security obstacles to ensure that DevOps can continue to accelerate their development, create new and exciting applications, and compete in dynamic ways.

Thales Luna Hardware Security Modules (HSMs) integrate with Pivotal Platform to isolate and secure secrets stored and managed in Pivotal Credhub. Organizations use Luna HSMs to attain the high assurance, hardware security needed to protect their cloud services and applications running on Pivotal Platform.

Highlights

Superior Performance

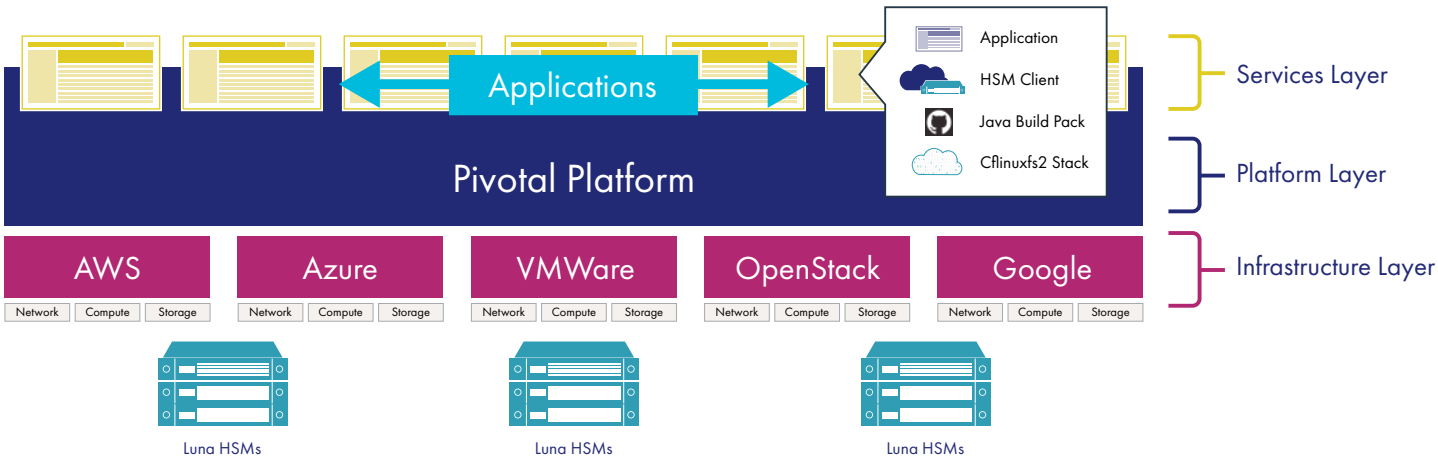
- Over 20,000 ECC and 10,000 RSA operations per second
- Lower latency for improved efficiency

Security at a Glance

- FIPS 140-2 Level 3-validated, tamper-evident hardware key storage
- Multiple roles for strong separation of duties
- Multi-person MofN with multi-factor authentication
- Address compliance needs for GDPR, HIPAA, PCI-DSS, eIDAS, Common Criteria and more
- Secure audit logging

Features

- Partitioning and strong cryptographic separation
- High availability, load balancing and scalability



Using Luna HSM in Cloud Foundry to Provide High Assurance Key Security and Industry Compliance

Approach to Security in Cloud Foundry: Making it Easy for Applications

Luna HSMs provide high assurance protection for cryptographic keys used by applications on Pivotal Platform. With Luna HSMs, organizations can centrally protect entire key and certificate-lifecycles, and leverage a single cryptographic key audit point to facilitate compliance reporting.

With Pivotal's Java Build pack, developers can seamlessly add Luna HSM services to the application, much like how external databases can be added. Through its keys-in-hardware approach, Luna HSMs maintain keys within the FIPS 140-2 validated confines of a dedicated purpose-built hardware appliance. This method ensures that keys always benefit from both the physical and logical protections of the HSM appliance, irrespective of their environment, to prevent unauthorized access; even by platform operators or third-party cloud infrastructure providers.

Secure Application Portability

Enterprises innovate and construct on Pivotal Platform in order to deploy seamlessly across a variety of cloud infrastructures. Luna HSMs work the same way by supporting many deployment scenarios including on-premises data centers, and private, hybrid, public and multi-cloud environments. Irrespective of where the HSM is located or where the application is running, Luna HSMs maintain a secure cryptographic foundation to ensure that data is safe wherever it is traveling. Together, the Pivotal Platform and Luna HSMs' deployment flexibility cost-effectively enables application portability and multi-cloud use of high-assurance cryptographic key protection.

Compliance Through Customer Control

Luna HSMs allow for central key storage and administration, enabling organizations to demonstrate that only they can access the encryption keys that keep their data safe. This is important as data and applications span cloud Infrastructures, some of which may not be fully in the organization's direct control. Being able to demonstrate cryptographic key and secret ownership and control in any environment is essential for demonstrating regulatory compliance and meeting audit needs.

Applications bound and secured by the Luna HSM enable you to comply with industry standards compliance certifications such as FIPS 140-2 and Common Criteria.

Luna HSM and Breadth of Integrations

Luna HSMs benefit from one of the broadest partnership ecosystems available on the market, integrating with over 400 of the most commonly used enterprise applications for PKI, big data, code signing, TLS, web servers, application servers, databases, and more. Standard applications can be quickly secured with Luna HSMs documented, out-of-the-box integrations.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> thalesgroup.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com