

Red Hat and Thales Ensure the Integrity of Containerized Applications: Thales Luna HSM for Red Hat OpenShift



Key Benefits:

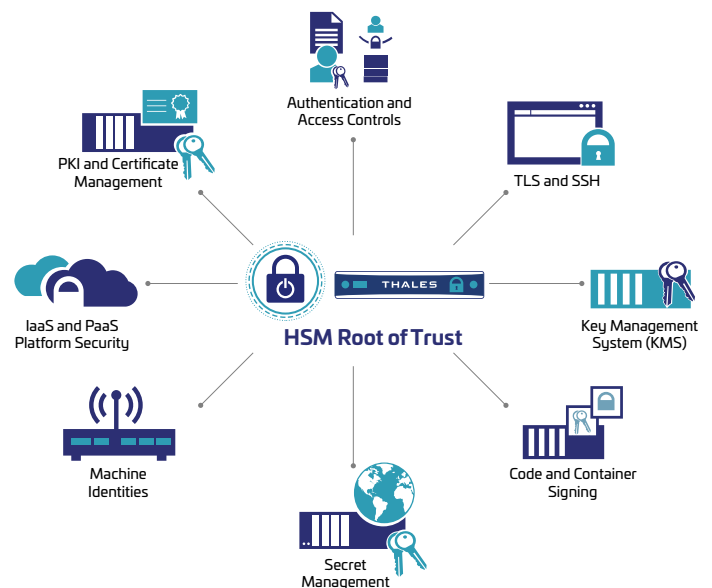
- Secure encryption, signing, key generation and storage
- Compliance with government and industry data security regulations
- Security designed for cloud native development

The problem: Cloud native development happens quickly but legacy application security is slow

Cloud native technologies and DevOps methodologies are designed to move more quickly and to iterate regularly with the intent that continuous improvement will allow organizations to bring their value to market faster, more cheaply, and vitally, more securely.

Red Hat OpenShift and Kubernetes are fundamental for many organizations making this shift to cloud native development. Applications designed using these tools and processes are dynamic. They change regularly, are broken into component parts, and may run for only a matter of minutes at a time. Traditional ways of doing application security must adapt to this new dynamism because applications continue to be a primary target for anyone looking to steal sensitive data, and organizations continue to be subject to a range of data security regulations.

Fortunately, Thales partners with Red Hat to bring trust to containerized applications running on OpenShift.



The Solution

Red Hat OpenShift is an application development platform that allows organizations to use Docker container technology orchestrated by Kubernetes. OpenShift allows organizations to develop their applications quickly and to seamlessly deploy and update their applications continuously.

Thales Luna Network Hardware Security Modules (HSM) provide high assurance security for cryptographic keys. Luna Network HSMs store cryptographic keys within the logical and physical confines of an appliance externally from the application server with the sole purpose of providing dedicated protection to those keys. With a client deployed in a container on OpenShift, organizations can ensure that containerized applications can continue to benefit from HSM protection in an automated way even if they exist for only a matter of minutes. Using Luna Network HSMs, organizations protect the entire key-lifecycle, accelerate cryptographic operations, and benefit from FIPS 140-2 Level 3 security in accordance with industry and government regulations.

Why use Thales Luna Network HSM with Red Hat OpenShift?

Combining Thales Luna Network HSM with Red Hat OpenShift allows organizations to securely develop and deploy their containerized applications. Securely storing cryptographic keys in an HSM allows organizations to create a trusted foundation upon which they can build their applications and data workflow. Organizations can store application encryption keys and certificates in an HSM to securely encrypt data or assure an application's identity. Additionally, organizations can use an HSM to securely sign a container image to assure that it is trusted and hasn't been tampered with. Given the dynamism of the cloud native world, Luna Network HSMs give organizations the peace of mind that their applications are secure and trusted, so they can focus their attention elsewhere.





Securely Generate and Store Cryptographic Keys

Protect cryptographic keys across their entire lifecycle within the FIPS 140-2 Level 3 validated confines of a tamper-proof appliance. Thales' unique approach to securing keys in hardware ensures that only authorized users of the appliance can access the keys. Such restricted access allows organizations to securely generate and store encryption keys which allows for trust wherever those keys are used. Unlike other methods of key storage which move keys outside of the HSM into a "trusted layer," the keys-in-hardware approach ensures that your keys always benefit from both physical and logical protections of the Thales Luna Network HSM.

Achieve Regulatory Compliance

With Luna Network HSMs, organizations can demonstrate that only they have access to the encryption keys that secure their data and applications. This is valuable when running applications in third-party cloud infrastructure outside of the customer's direct control. Being able to demonstrate that organizations own and control their cryptographic keys, irrespective of the environment, is essential for compliance.

Additionally, Luna Network HSMs are FIPS 140-2 Level 3 and Common Criteria EAL4+ certified which facilitates regulatory compliance with a wide range of common mandates, such as PCI DSS, HIPAA, CCPA, NYDFS, eIDAS and more.

> cpl.thalesgroup.com <    

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us

HSM Audit Trail

Centrally storing keys within an HSM allows for close oversight and logging the result of which is a detailed audit trail. These audit trails can be used to enhance security oversight or to demonstrate to auditors that customers are in sole control of their encryption keys.

Luna Network HSM and Breadth of Integrations

Luna Network HSMs benefit from one of the broadest ecosystems available on the market and integrate with over 400 of the most commonly used enterprise applications for big data, PKI, privileged access management, secrets, code signing, TLS, web servers, application servers, databases, and more. As organizations secure their OpenShift applications, they can also derive greater value from their investment by addressing other cryptographic use cases in their enterprise.

For more detailed technical specifications, please visit <https://cpl.thalesgroup.com/> or <https://www.openshift.com/>

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and highperforming Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.



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.