Thales Network HSMs Provide High Assurance Key Security for the VMware Tanzu Application Service

After facing an initial cloud migration push, large enterprises are increasingly revisiting their cloud strategies. Gone are the ideas of simply rejiggering legacy applications to work in cloud infrastructure. These enterprises are now imagining how they would build their products, and ultimately their businesses, in ways that are native to the cloud – both in terms of technology and customer interaction. This shift in thinking has meant a greater emphasis on DevOps, automation, and cloud native technologies such as containers and kubernetes. These shifts are letting businesses bring their products and services to market faster, cheaper, and with lower risk than ever before.

Many large enterprises look to VMware Tanzu as their platform of choice for their cloud native business transformation. Yet, while the cloud offers exciting new possibilities, the same old security risks and challenges remain. In the risky and highly-regulated world in which enterprises operate, there is an increasing need for high assurance security when developing for the cloud. This is especially true when applications handle sensitive information or run in infrastructure that is outside of the organizations' direct control.

Cryptography provides a means for protecting and controlling data wherever it exists. However, when cryptography is used, the risk is transferred from the content of the data, to the cryptographic keys used to protect that data. For years organizations have turned to Hardware Security Modules (HSM) to isolate and secure their most sensitive cryptographic keys for a variety of uses.

By leveraging the Tanzu Application Service (TAS) Java Buildpack, organizations can easily deploy Thales Luna Network HSMs to attain the high assurance security needed to protect their cloud services and applications running on the VMware Tanzu Platform.

Approach to Security in VMware Tanzu

Making it Easy for Applications

Luna Network HSMs provide high assurance cryptographic key protection for applications in VMware Tanzu environments – wherever they are located. With Luna Network HSMs, organizations: protect the entire key-lifecycle externally on a centralized platform, accelerate cryptographic operations, and benefit from a single audit point for all cryptographic keys.

Developers use the TAS Java Buildpack to seamlessly deploy Luna Network HSMs, leaving only configuration to the application as the final step, ultimately making the addition of security straightforward and painless. Thales' keys-in-hardware approach keeps keys within the FIPS 140-2 validated, tamper-resistant confines of the hardware appliance so they always benefit from both the appliance's physical and logical protections. Ease-of-use aside, fundamentally, Luna HSMs prevent unwanted access to cryptographic keys - even by third-party cloud infrastructure providers - irrespective of where applications are deployed.

Secure Application Portability

VMware Tanzu Application Service attracts organizations looking to innovate and build on a platform that lets them work across a variety of cloud infrastructures and optimize investments without the need to customize applications for each cloud. Luna Network HSMs work in similar fashion by supporting many deployment scenarios, from on-premises data centers to private, hybrid, public, and multi-cloud environments. Luna Network HSMs' tremendous flexibility allows customers to move cryptographic keys in and out of cloud environments to support applications and workloads wherever customers choose to deploy them. Luna Network HSMs' service binding (built into the Java Buildpack) operates in a multi-cloud fashion on services such as VMware Tanzu Application Service, Cloud Foundry or Microsoft Azure, IBM Cloud, as well as in private PaaS deployments.

Together, VMware and Thales' deployment flexibility enables true application portability and multi-cloud high-assurance cryptographic key protection without the need for costly customization.

Compliance through Customer Control

Luna Network HSMs empower organizations to demonstrate that only they can access the encryption keys that secure their data. This carries significant value 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.

Luna Network HSM service binding, which enables stateless Java applications to leverage the Luna Network HSM's security validations, such as FIPS 140-2 and Common Criteria, facilitate regulatory compliance with a wide range of common mandates, such as PCI DSS, HIPAA, CCPA, NYDFS eIDAS and GDPR.

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, code signing, TLS, web servers, application servers, databases, and many more. As organizations secure their TAS applications, they can also derive greater value from their investment by addressing other cryptographic use cases in their enterprise.

Scale Security for Virtual and Cloud Environments

Luna Network HSMs can divide into 100 cryptographically isolated partitions, each acting as if it were an independent HSM. A single HSM can serve as the root of trust that protects the cryptographic key lifecycle of hundreds of independent Tanzu applications allowing for tremendous scalability and flexibility. Keys and partitions are cryptographically separated from each other to allow organizations to leverage the same hardware for multiple tenants, business units or applications.

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.

> cpl.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: apacsales.cpl@thalesgroup.com
Europe, Middle East, Africa – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com