Entrust nShield HSMs Deliver Robust Cryptographic Functionality to VMware Tanzu Kubernetes Grid

The integrated solution enables key generation, signing, and encryption for containerized application development

HIGHLIGHTS

- Simplify Kubernetes management and operations

- Run Kubernetes on the infrastructure of your choice

- Protect sensitive container data and transactions

- Establish a FIPS 140-2 and Common Criteria certified root of trust

- Facilitate auditing and compliance with data security regulations

PARTNER
READY

VMWARE
TANZU

THE PROBLEM
Securing sensitive applications developed using containers

As enterprises increasingly shift application development to multi-cloud environments using DevOps, the use of containers has dramatically increased. The containerized approach provides easy building blocks of predefined functionality that enabled businesses to accelerate the application development.

Containerization not only increases performance, but also reduces costs by ensuring that applications can run reliably no matter the end user environment. However, adding security to sensitive applications build in this manner has been difficult, as cryptographic services have not been readily available to integrate to the process.

THE CHALLENGE

Ensuring applications designed using containerized environments have easy access to robust cryptographic functions

When containerized applications incorporate the use of digital signing and encryption to control access and protect sensitive data, the underpinning signing and encryption keys must also be protected and managed to ensure the security of the process. Doing this at the scale and speed of DevOps environments requires trusted predefined scripts. Establishing high assurance security is critical to ensuring a trusted application development process in a fast-paced continuous improvement and continuous development model.

THE SOLUTION

VMware® Tanzu Kubernetes Grid and Entrust nShield® hardware security modules (HSMs) deliver robust cryptographic services for containerized application development

VMware Tanzu Kubernetes Grid is an industry-leading, enterprise-ready container runtime platform that streamlines operations across multi-cloud infrastructures. The solution enables developers to run Kubernetes on their infrastructure of choice – in private clouds, public clouds, or at the edge of their networks. With more applications developed using containerized methods, security must be seamlessly integrated into development processes.
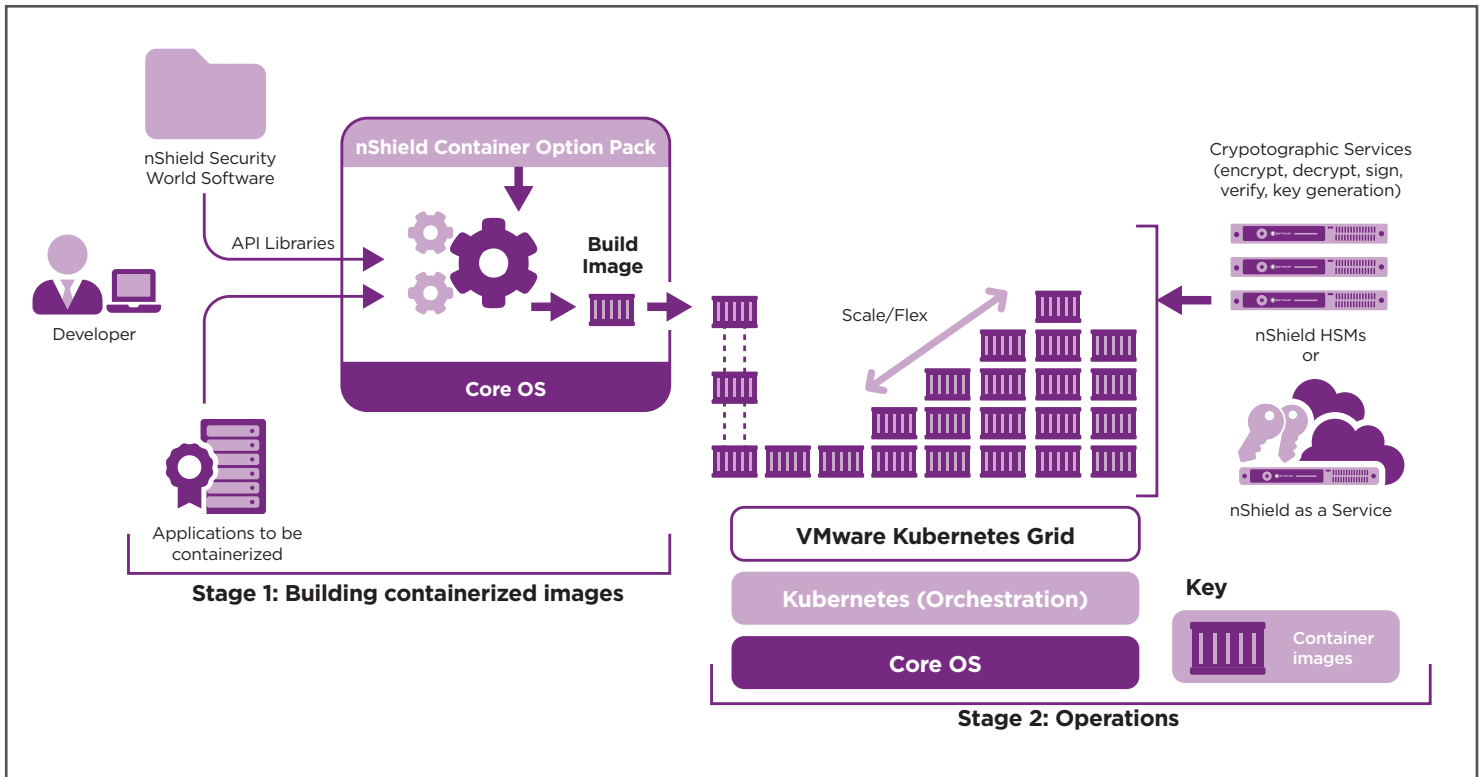
The integration of VMware Tanzu Kubernetes Grid with Entrust nShield HSMs and the nShield Container Option Pack enables developers to build, launch, and scale container-based applications. Using the customers' existing VMware vSphere environments, the integration provides easy access to the robust cryptographic functionality of the nShield HSM to deliver secure Kubernetes clusters at a rapid pace.

The purpose-built nShield HSMs are designed to generate, safeguard, and manage cryptographic keys on behalf of applications. The unique nShield Security World key management architecture enforces important separation of duties with dual controls that segregate security functions from administrative responsibilities.

With containerization becoming the standard for software development, it is critical to have a proven model to enforce security with scripts to help reduce the overall deployment cycle. Integrating nShield HSMs with Tanzu Kubernetes Grid enables developers to build containerized images using the nShield Security World software and the nShield Container Option Pack. Tanzu Kubernetes Grid provides the tools to test and deploy containerized applications, while encryption, decryption, signing, verification, and key generation are enabled using nShield HSMs on premises or nShield as a Service.

Entrust and VMware Integrated Solution

Stage 1: Building containerized images

nShield Security World Software

API Libraries

Developer

Applications to be containerized

nShield Container Option Pack

Build Image

Core OS

Scale/Flex

Crypotographic Services (encrypt, decrypt, sign, verify, key generation)

nShield HSMs or

nShield as a Service

VMware Kubernetes Grid

Kubernetes (Orchestration)

Core OS

Stage 2: Operations

Key

Container images

A CLOSER LOOK

Why use nShield HSMs with Tanzu Kubernetes Engine?

Attackers trying to hack your systems can easily find cryptographic keys maintained in software. Critical keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attacks that can compromise confidential information. When using HSMs to protect these keys, you add a robust layer of security, preventing attackers from finding them. nShield HSMs are specially designed to establish a root of trust, safeguarding and managing cryptographic keys and processes within a certified hardware environment. nShield HSMs, offered as an appliance deployed at an on-premises data center or leased through an as-a-service subscription, provide enhanced key generation, signing, and encryption to protect sensitive container data and transactions.

About Entrust nShield HSMs

Entrust nShield HSMs are among the highest-performing, most secure, and easiest-to-integrate HSMs available. They help facilitate regulatory compliance and deliver the highest levels of data and application security for enterprise, financial, and government organizations. Our unique Security World key management architecture provides strong, granular controls over access and usage of keys. For more information visit entrust.com/HSM

About VMware

VMware streamlines the journey for organizations to become digital businesses that deliver better experiences to their customers and empower employees to do their best work. The company's software spans application modernization, cloud, networking and security, and the digital workspace. For more information visit vmware.com

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223

info@entrust.com   **entrust.com/contact**