Integrated solution enables containerized applications to easily and efficiently access cryptographic services

- Deliver higher level security for the hybrid cloud with Red Hat OpenShift and nCipher
- Provide secure controlled access to nShield hardware security module (HSM) services
- Enable security and key management to run transparently
- Allow dynamic, rapid application deployment
- Utilize powerful platform to deploy and orchestrate containers protected by FIPS 140-2 and Common Criteria certified nShield HSMs

Red Hat

nCipher nShield and Red Hat OpenShift deliver enhanced security to containarized application deployments

THE PROBLEM: ENSURING APPLICATIONS RUN RELIABLY AND SECURELY NO MATTER THE USER ENVIRONMENT

As modern application development and deployment have evolved to meet demands for flexibility and scalability, development teams are increasingly relying on containers and Kubernetes. Kubernetes is an open-source container platform that meets the dynamic needs of today's development teams, helping them to deploy applications that run reliably no matter the user environment. When applications require an enhanced level of protection, developers need the ability to incorporate cryptographic operations. Adequately protecting these cryptographic operations is also vital to ensure the integrity of the applications and data.

THE CHALLENGE: ENABLING DEVELOPERS USING CONTAINERS TO HAVE EASY ACCESS TO CRYPTOGRAPHIC SERVICES

Applications requiring cryptographic capabilities including key generation, digital signing, and data encryption need an easy and efficient way to access robust cryptographic services to facilitate security auditing and regulatory compliance. This includes access to HSMs to protect critical keys. But integrating with HSMs in a way that is compatible with containerized workflows is complex and unfamiliar to many application developers.

nCipher nShield and Red Hat OpenShift deliver enhanced security to containarized application deployments

THE SOLUTION: RED HAT OPENSHIFT CONTAINER PLATFORM AND NSHIELD HSMs

Red Hat OpenShift is a container orchestration cloud platform that includes everything needed for containerized Kubernetes application development and deployment in hybrid cloud environments. OpenShift enables development, test, staging, and production teams to work in a common environment to deliver a write once, run anywhere capability so software can run reliably when moved across computing environments.

Red Hat OpenShift provides:

- Integrated platform including container host, Kubernetes, and application life-cycle management using your choice of infrastructure
- Greater value from operations and development teams throughout the application life-cycle
- More secure, validated container content and services from a wide partner ecosystem
- Faster application development cycles and more frequent software deployments with simpler installations and upgrades, even in air-gapped environments
- Lower IT operations costs and application portability across hybrid cloud and multi-cloud footprints

Red Hat OpenShift integrates with nCipher nShield HSMs and the nShield Container Option Pack to enhance the security of containerized applications that use cryptographic services.

WHY USE NSHIELD WITH RED HAT OPENSHIFT?

nShield HSMs are specifically designed to safeguard and manage cryptographic keys and processes within a certified hardware environment to establish a root of trust. nShield HSMs protect critical assets such as payment card details, personal information, applications, and business critical data. Critical keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attacks that can lead to disclosure of confidential information. nShield HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management.

nShield Container Option Pack provides a set of scripts to enable the seamless development and deployment of containerized applications or processes underpinned by a high-assurance HSM.

For DevOps and DevSecOps, nShield Container Option Pack provides the tools and proven architecture to deploy containers at scale as part of a continuous improvement/continuous development (CI/CD) process. When the time from development to deployment is tight, nCipher Container Option Pack accelerates the development of container images with cryptography provisioned by an nShield HSM root of trust.
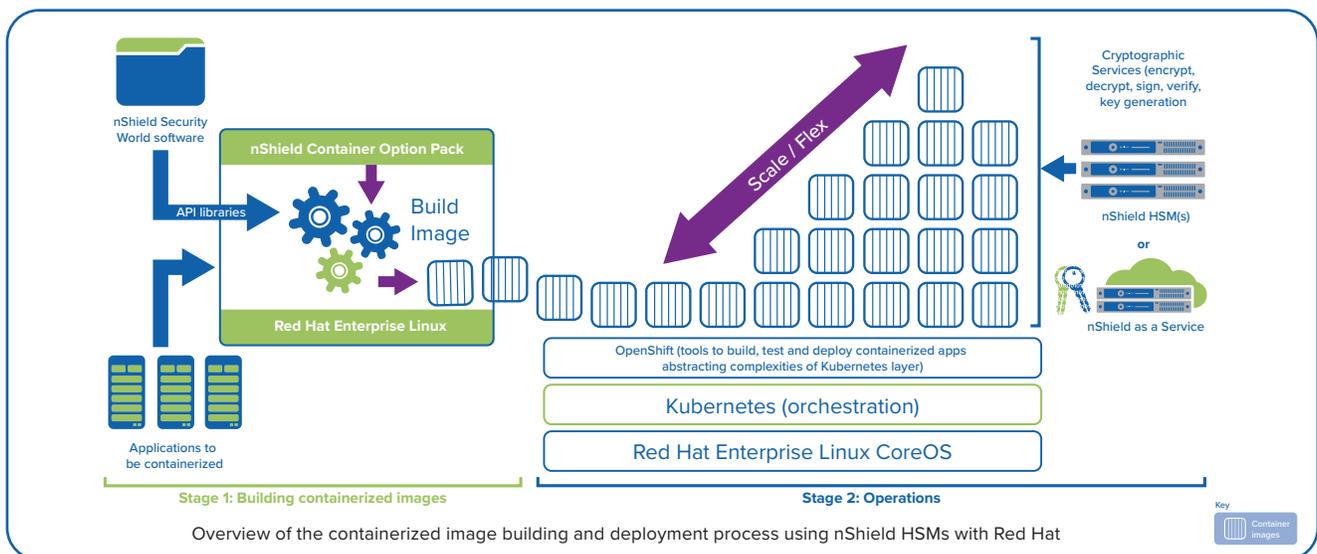
NCIPHER

nCipher Security, an Entrust Datacard company, is a leader in the general purpose HSM market, empowering world-leading organizations by delivering trust, integrity and control to their business critical information and applications. By using the same proven technology our customers depend on today to protect against threats and meet compliance, we underpin the trust of tomorrow.

RED HAT

Red Hat is the world's leading provider of open source solutions for the enterprise. In addition to RedHat OpenShift, solutions include Red Hat Enterprise Linux, Red Hat Certificate System, and Red Hat OpenStack platform, among a broad range of management and services. nShield HSMs support Red Hat OpenShift container platform, enhancing security and providing a root of trust.

LEARN MORE

For more information visit **www.ncipher.com** and **www.redhat.com**

Overview of the containerized image building and deployment process using nShield HSMs with Red Hat