nCipher
AN ENTRUST DATACARD COMPANY

www.ncipher.com

Red Hat Openstack Barbican secures your secrets and keys in the cloud with nCipher nShield HSMs

- Offer consistent secure storage, provisioning, and management of secrets and keys used by OpenStack cloud applications
- Enable fine-grained and uniform control and scalability
- Ensure sensitive materials are never visible to applications
- Segment cryptographic components by OpenStack projects
- Deliver FIPS 140-2 and Common Criteria EAL 4+ HSM root of trust

redhat.

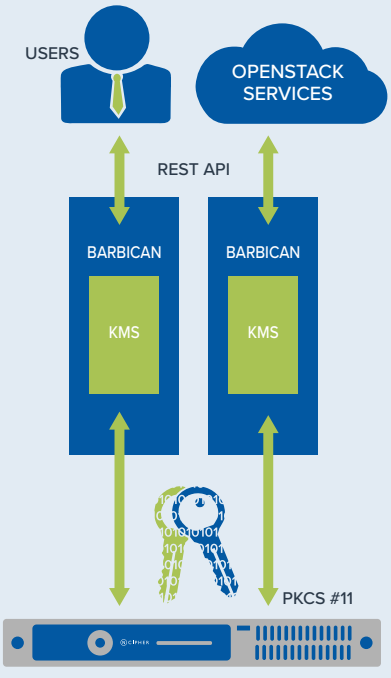
nCipher and Red Hat delivers security and trust in the cloud

THE PROBLEM: SECURING SECRETS AND KEYS USED BY OPENSTACK APPLICATIONS IN THE CLOUD

Applications using cryptography to control access and to protect the confidentiality and integrity of the data they process need secure storage, provisioning, and management of secrets and keys. Without a common key management system (KMS), individual applications rely on custom built key stores in various locations, with no demarcation between storage and execution space. Making the system only as strong as the weakest KMS implementation, this weakens the overall security of the applications.

THE CHALLENGE: MAINTAINING SECRETS AND KEYS IN A CENTRALIZED AND SECURED CLOUD ENVIRONMENT

OpenStack cloud services provide convenience, quick deployment, and scalability. However, lack of separation between storage and application space create scenarios where cryptographic material used by applications can be scattered in software, creating a high risk of compromise. Ensuring that these materials are stored and managed centrally, securely, and in a uniform manner is essential for the robustness and trustworthiness of service.



nCipher nShield Connect hardware security module (HSM) protects the storage, transport, and secure keys used by the Red Hat Barbican OpenStack common KMS. nCipher nShield can be deployed on-premises or as a service.

nCipher and Red Hat delivers security

THE SOLUTION: BARBICAN OPENSTACK SERVICE FOR MANAGING SECRETS AND KEYS IN THE CLOUD

With the release of Red Hat OpenStack Platform 15, Red Hat is shipping Barbican, OpenStack's common KMS. Barbican is a REST API service designed to address the cryptographic material management needs of users and OpenStack services. Barbican facilitates secure storage, provisioning, and management of secrets and keys used by applications, including key generation, lifecycle management, and revocation. As a component of OpenStack, Barbican supports symmetric and asymmetric key types. Barbican's availability allows encrypted volume support (via Cinder), signed image verification support in Glance, and the use of logical, secure compartments in which to store tenant secrets and keys for individual applications.

Red Hat OpenStack Platform 15 is a Red Hat long life release, and integrates with the nCipher nShield Connect HSMs to provide enhanced security and compliance, as well as a certified source of entropy for generating keys. nShield protects the master key used to secure the storage, transport, and service keys managed by Barbican, providing a robust FIPS 140-2 Level 3 and Common Criteria EAL 4+ root of trust for OpenStack. As a robust certification management system, Barbican integrated with nShield Connect, provides a foundation for large public key infrastructure (PKI) deployments, and offers the scalability and reliability needed for such environments. Coupled with the most widely deployed HSMs, the combined solution provides the powerful security needed for growing cloud deployments.

WHY USE NCIPHER NSHIELD AND BARBICAN IN RED HAT OPENSTACK PLATFORM 15?

Cryptographic keys handled outside the secure boundary of a certified nShield HSM are significantly more vulnerable to attack, which can lead to the compromise of critical data. nShield provides a proven and auditable means to secure valuable key materials, and to perform cryptographic processes. nCipher nShield integration with Barbican delivers comprehensive logical and physical protection of the master key protecting critical operational keys.

The combination delivers an auditable method for managing secrets and keys used by OpenStack end points and for enforcing security policies. By providing a mechanism to enforce security policies and a secure tamper resistant environment to safeguard master keys, end users can trust the security of OpenStack services.

nCipher nShield Connect HSMs enables users and OpenStack services to:

- Secure master keys within a carefully designed cryptographic boundary that uses robust access control mechanisms, so keys are only used for their authorized purpose
- Ensure key availability by using sophisticated management, storage, and redundancy features to guarantee key is always accessible when needed by the Barbican OpenStack service
- Segregate application and key management functions

NCIPHER - AN ENTRUST DATACARD COMPANY

nCipher nShield Connect HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. nCipher HSMs:

- Provide a tightly controlled tamper resistant environment for safekeeping and managing cryptographic keys
- Enforce key use policies, separating security functions from administrative tasks
- Interface with applications using industry-standard APIs (PKCS#11, OpenSSL, JCE, CAPI, CNG, nCore, and nShield Web Services Crypto API)

nCipher nShield is available in several form-factors: as an appliance, PCIe, USB, and and as a service.

RED HAT

Red Hat is the world's leading provider of open source solutions for the enterprise. Solutions include Red Hat Enterprise Linux, Red Hat OpenStack Platform, and Red Hat Certificate System as well as a broad range of management and services. nCipher nShield HSMs are certified with the Red Hat Certificate System.

For more information, please visit www.ncipher.com or www.redhat.com