CRYPTOMAThIC

Solution Brief

CKMS: A BYOK Solution for Lifecycle Management of Cloud Keys

Manage and migrate critical keys between on-prem and cloud applications

BYOK for Multi-Cloud

Today's Financial Institutions (FIs) are moving their applications to cloud providers, like AWS, GCP and Azure. Cloud providers now offer the possibility to import cryptographic keys into their infrastructure to be used by their different services. This process is called BYOK (Bring Your Own Key) and requires the support of specific key formats, depending on the cloud provider of choice. FIs face conflicting requirements to efficiently manage and control a key's lifecycle but also deliver it to an external environment for use. At the same time, FIs might want to maintain the freedom to change provider without having to re-architect their entire key management ecosystem, or to 'dual source' cloud services for resilience and business continuity. A final and related challenge is to securely migrate high-value keys between on-prem and cloud application instances.

CKMS for Cloud-Agnostic Key Management

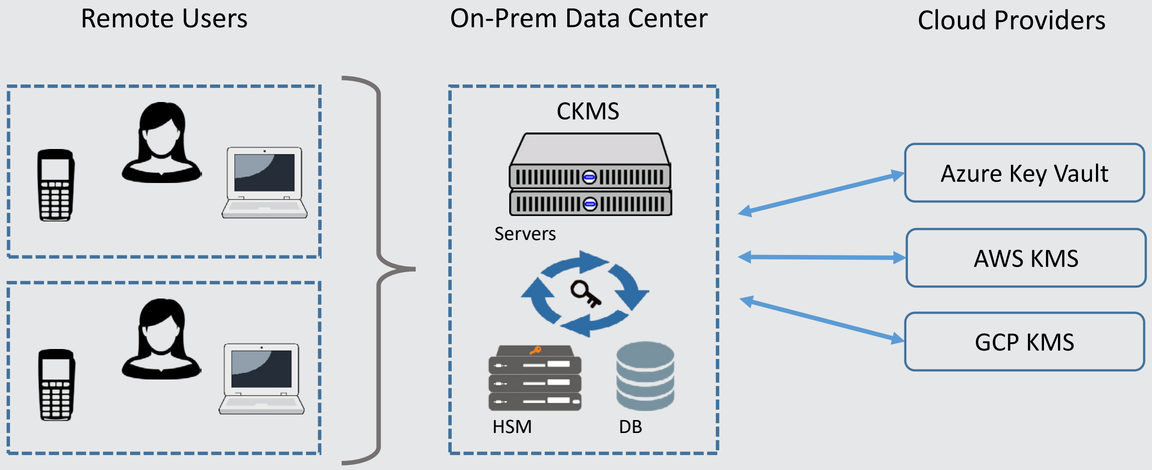
Cryptomathic's Crypto Key Management System (CKMS) directly addresses the above challenges by providing a centralized, on-premise KMS that enables multi-cloud key management and on-prem-to-cloud migration. Cryptographic keys are managed for all the regions of the different cloud providers. E.g. one key can be used in multiple regions in multiple clouds and, if required, can be shared between on-prem and cloud applications. Keys are securely backed-up on-premise and rotated when required. Furthermore, keys can be distributed manually or automatically to the key vault of a cloud provider. It allows FIs to follow security best practice by strongly segregating keys from data to be encrypted or signed. CKMS provides dual-control of critical operations and gives operational insights on usage with signed logs, reports and administration dashboards. By enabling control of key lifecycles across on-prem and cloud environments, CKMS moves beyond 'BYOK' and delivers enhanced "Manage Your Own Key" (MYOK) capabilities for the cloud.

Solution Benefits

- ✓ **Support any service delivery model:** Today, some of your most sensitive systems might still run in an on-prem model. Driven by requirements from your business units, IT department and not least the promise of cost savings, migration to a cloud-based architecture is certainly on the near-term horizon. In the CKMS-model, you can smoothly migrate between different cloud providers, on-prem or private cloud scenarios to cater for the needs of your organization – whilst maintaining the centralized management of the lifecycle of all your keys.
- ✓ **Streamline security operations:** CKMS' one-stop-shop approach to key management, lightens the burden of working with many discrete applications and security hardware day-in-day-out,while unlocking the full potential of multi-cloud and hybrid environments.
- ✓ **Centralize lifecycle management of "good" keys for proof of compliance:** Centralized generation of strong keys, dual control for the most sensitive operations, secure storage and management of the lifecycle of your entire key estate gives you a strong foundation in managing the risk of a data breach. Likewise, with signed log files and usage reporting, the workload for your internal and external audits will become less cumbersome and time consuming.

High Level Architecture

CKMS is built on a resilient client-server architecture. Administrators securely access the remote key management server via the easy-to-use CKMS client GUI - supported by secure PIN entry devices (PEDs) and ICCs for strong authentication. CKMS uses Hardware Security Modules (HSMs) to ensure high quality key material and strong protection of encrypted keys that are stored in a database. High availability is ensured through clustering of the server, database and HSMs. The PEDs also support remote key import/export and key share printing. Keys are distributed to applications and HSMs in a wide range of formats (key-blocks).



MYOK - Control the Key Lifecycle

With CKMS, the Manage Your Own Key (MYOK) capability enables users to generate, store, deploy, retrieve, back-up, revoke and retire keys regardless of cloud model (public, private or hybrid) and cloud provider. By enabling users to control and manage the entire lifecycle of their own, unique portfolio of keys, Cryptomathic is answering the call for a new level of end-user security control in cloud services. As a banking-grade key management system, CKMS provides a flexible and secure solution to the challenges of cloud migration, including:

- Control of the lifecycle of keys – independent of cloud provider
- Supporting banking cryptography, e.g. key blocks and integration with payment HSMs
- Sharing keys between cloud and on-prem applications for parallel operations and secure migration from on-prem to cloud
- Moving keys from one cloud provider to another to avoid vendor lock-in

Banking-Grade Key Management for Multi-Cloud Environments

Banking-grade key management for multi-cloud environments CKMS allows managing the lifecycle of cryptographic keys from generation, import, export and renewal. It integrates securely with FIPS140-2 level 3 approved HSMs. All cryptographic operations are executed inside the secure boundary of the HSM.

CKMS supports multiple ways to import and export keys in a variety of formats such as TR-31 key block, Atalla Key block, PKCS#8 cryptograms and others. BYOK wrapping methods used by the cloud providers, including PKCS#1 v1.5, OAEP SHA1 and OAEP SHA256 are supported.

Automated key distribution is ensured via the different REST APIs made available by the cloud-providers.

Learn more at cryptomathic.com/CKMS

About Cryptomathic

Contact us: Sales_enquiry@Cryptomathic.com

Cryptomathic is a global provider of secure server solutions to businesses across a wide range of industry sectors, including banking, government, technology manufacturing, cloud and mobile. With over 30 years' experience, we provide systems for Authentication & Signing, EMV, Mobile App Security and Crypto & Key Management through best-of-breed security solutions and services.

We pride ourselves on strong technical expertise and unique market knowledge, with two-thirds of employees working in R&D, including an international team of security experts and a number of world-renowned cryptographers. At the leading edge of security provision within its key markets, Cryptomathic closely supports its global customer base with many multinationals as longstanding clients.