CRYPTOMATHIC

Solution Brief

AWS External Key Store (XKS)

Powered by Cryptomathic Crypto Service Gateway (CSG)

AWS KMS, BYOK & XKS

AWS KMS has long offered cryptographic services to protect your AWS resources. In the most basic configuration, keys are generated and maintained by the KMS. This typically works well for mainstream applications that do not deal with regulated workloads.

AWS introduced the ability to Bring Your Own Key (BYOK) to allow KMS-integrated AWS services and custom applications to have more control of the lifecycle of keys - from creation to expiration. BYOK is a great addition to the KMS portfolio, but it does come with several manual workflows for configuring, maintaining, and renewing keys. Furthermore, BYOK only affords you the ability to enhance the encryption of the actual data keys.

The latest feature is AWS External Key Store (XKS), which gives more flexibility and complete control of your cryptographic keys outside of AWS KMS. In essence it introduces the concept of Hold Your Own Key (HYOK) also known as BYOE – Bring Your Own Encryption, effectively providing an entire encryption life-cycle management platform.

Crypto Service Gateway (CSG)

Cryptomathic's CSG is designed to simplify the management and use of HSMs and can offer a streamlined and secure cryptographic engine to AWS KMS as an external key manager through the XKS feature.

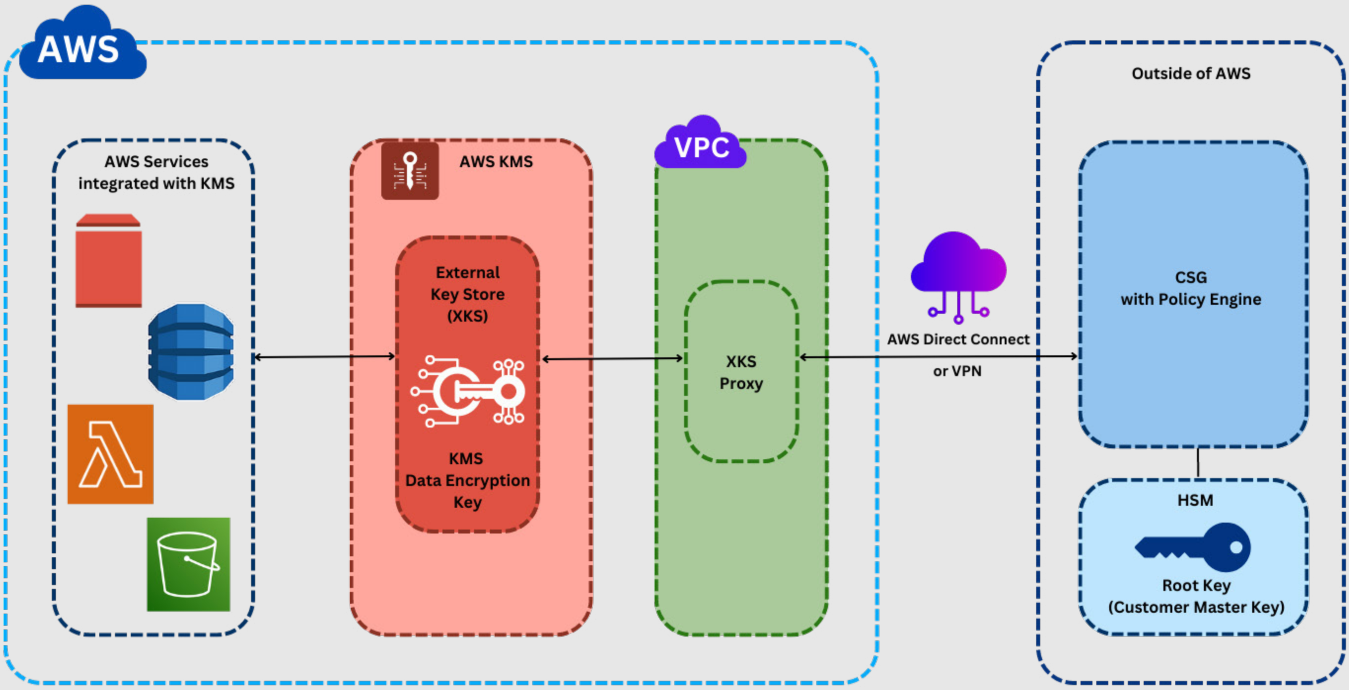
AWS XKS with CSG

CSG offers straightforward integration with XKS, adds streamlined key management processes and policy-controlled usage of your keys for cryptographic operations. With CSG, as an external key manager, organizations will have full control of their keys, including usage of these in a multi-region/multi-cloud environment, on-premise or in a hybrid deployment of applications and services.

Client benefits

- ✓ **Faster and more reliable than anything else:** a key requirement by AWS XKS is that the security proxy is available with a response within 250 milliseconds (ms). This can be a tall order during peak performance in a cloud—based infrastructure. With the Cryptomathic XKS proxy, we can guarantee scale to any level, without sacrificing performance, and without breaking the budget!
- ✓ **Privacy Law Compliance:** Whether demonstrating compliance to the CCPA, GDPR, or the Privacy Act, or something else, there is a jungle of compliance to navigate, and many companies are worried about compliance. Cryptomathic XKS gets you on top of your compliance game.
- ✓ **Centralized Policy Control:** CSG's policy enforcement allows security teams to rigorously control who can use keys and the specific parameter choices for all operations from a central service.
- ✓ **Logging:** CSG produces extensive tamper-evident logs for auditing and regulatory purposes. These logs record who used a key, when they used it, and what cryptographic operation was performed.

High-level architecture



How it works

The connection from AWS KMS to an external key manager is facilitated through a bespoken XKS Proxy. The proxy receives the encryption/decryption requests from an AWS resource through KMS and translates them into operations that are picked up by CSG's interface. CSG, as external key manager, executes the encryption/decryption commands it receives using a pool of FIPS 140-2 level 3 HSMs holding the Root Keys (AWS Customer Master Keys) and returns the responses back to the AWS resources through the XKS proxy and KMS.

To the AWS resource requiring data encryption/decryption, it is completely transparent that an external key manager was in fact handling the request. AWS KMS never interacts directly with the external key manager, and hence has no knowledge about its deployment details and physical location. This also allows CSG to be a central kill-switch should that be required in a scenario where organizations would want to halt data encryption or decryption at AWS resources.

CSG - a unified platform for multiple regions

Since CSG offers a scalable infrastructure, a single CSG environment can easily act as an external key manager for multiple AWS regions and unique KMS instances. This can be useful for organizations wanting to have their keys, and their data encryption operations, completely segregated between application teams and services, but still manage their external keys centrally - namely in CSG.

Learn more www.cryptomathic.com

About Cryptomathic

Contact us: 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 Identification & Signing, Payments, 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.