CRYPTOMATHIC

Solution Brief

The Enclave Security Module (ESM)

Addressing confidential computing for key management in the cloud

Trusting the cloud to protect your assets

When organizations decide to move their applications and infrastructure to the cloud, several challenges need to be addressed to ensure the confidentiality, authenticity, and integrity of their digital assets. Some of these challenges are:

- **Compliance with privacy laws:** CCPA, GDPR, the Privacy Act, etc. – it's a complex topic and many companies are worried about compliance.
- **Lack of control:** Organizations may have limited control over their data and keys when they are stored in the cloud.
- **Shared infrastructure:** Cloud service providers (CSPs) often use a shared infrastructure, including HSMs, which increases the risk of data leakages and unauthorized access.
- **Insider threats:** Insider threats, such as a rogue employee or contractor can pose a significant risk to critical data.

Addressing all these challenges requires a thorough approach to cloud security, which includes implementing appropriate security controls. When it comes to the protection of your keys, it is critical that organizations are in control and that the keys cannot be compromised. "But how do we keep keys secure when we don't necessarily trust the cloud?"

Client benefits

- ✓ **Speed and operational scalability -** many third-party systems, such as e.g., AWS XKS demand high availability in less than 250 milliseconds. Only few HSM based implementation can promise this at peak levels, but with the ESM you get that as a central feature.
- ✓ **Demonstrate Compliance -** with so many laws and court cases abounding around privacy you need a system with a migration path towards the ultimate goal: Full encryption life-cycle management.
- ✓ **Economical, secure, and scalable solution -** that can be easily extended to fit future needs. Saves cost as traditional hardware units are not required.
- ✓ **Full control of your keys within the cloud -** as no master keys or data is shared with CSPs. No risk of insiders compromising your keys.

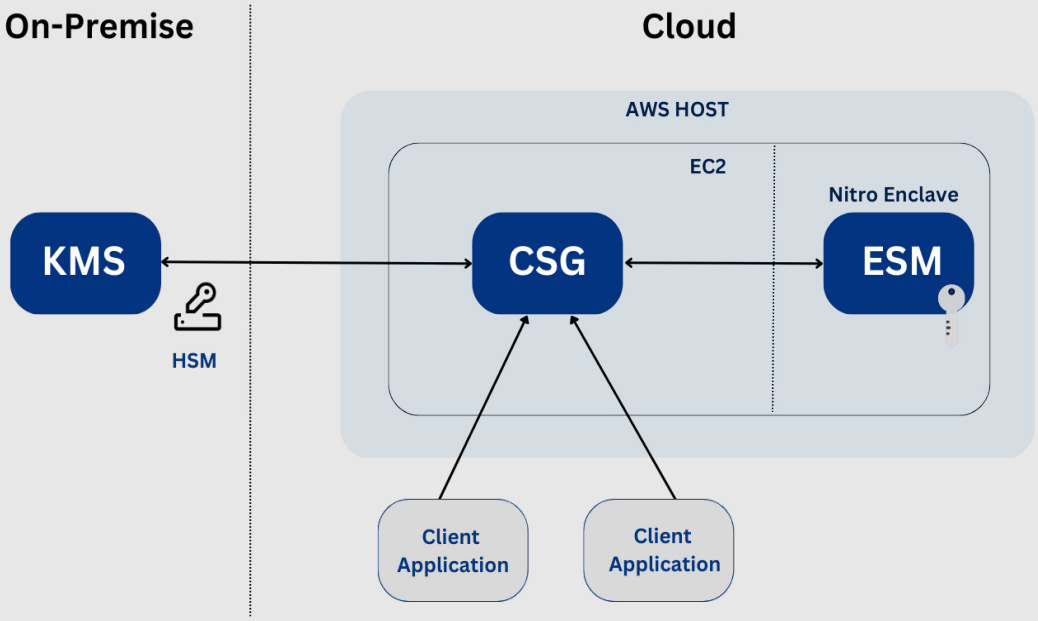
ESM - your own secure partition in the cloud

A solution to confidential computing in the cloud is the enclave technology that is now provided by CSPs. These enclaves provide a secure and isolated computing environment, which is isolated from other processes on the system, solving parts of the challenges around shared infrastructure.

Cryptomathic has specifically developed an enclave security module to be operated within the AWS Nitro Enclave, as an alternative to traditional HSMs. The ESM specifically focuses on the protection of your keys and provides a unique solution for securely transferring keys from your highly secure key management system to the ESM. Additionally, the ESM ensures that you are in full control of your keys for their entire lifecycle, even when used in the cloud.

How it works

The ESM is deployed as a crypto resource available to the Crypto Service Gateway (CSG) platform in the same manner as traditional HSMs. The CSG nodes are deployed within an EC2 instance of the AWS environment and act as a gateway to the ESM loaded into the AWS Nitro Enclave. The key management system responsible for the keys can be deployed on-premises or in the cloud depending on compliance and security requirements.



ESM for additional control and certainty

The The ESM builds on the Cryptomathic Crypto Service Gateway platform, which facilitates the key exchange between the KMS and ESMs. Authenticity and Integrity Protection are ensured by building trust inside the ESM and by utilizing the enclave attestation features. This ensures that the keys can be securely transferred between the KMS and the ESM without any risk of compromise by man-in-the-middle attacks or similar.

The ESM provides support for general purpose as well as custom cryptographic operations, which are made available to applications on the CSG platform – The cryptographic module within the ESM is FIPS 140-2 level compliant. With the ESM an organization doesn't just get a high degree of flexibility in terms of deployment and availability, but also gets full control of its keys within the cloud.

Cryptomathic's Crypto Service Gateway (CSG)

Cryptomathic's CSG provides a highly-available and scalable infrastructure for using ESM/HSM crypto services.

A CSG server cluster sits between ESMs/HSMs and the applications, distributing load to the appropriate HSMs, enforcing crypto policy and centralized key management. Application-specific crypto parameters are all managed centrally through an easy-to-read policy language. The policy simplifies internal and external compliance audits and empowers your security team with true crypto agility.

With ESM and CSG combined, we get not only the security level we aspire to, but also convenience, speed and cost control, which were the initial drivers for moving to the cloud!

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.

v1.0