TEEware

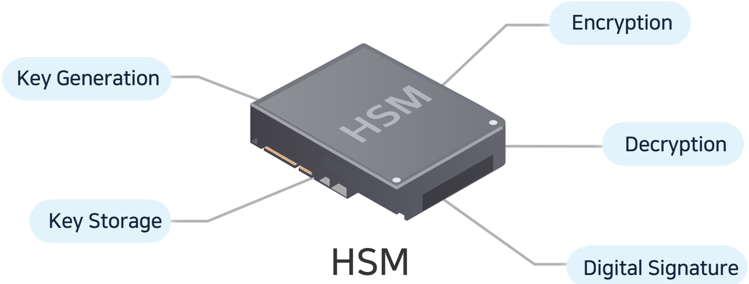
KangaLock
vHSM

Large-scale Key Management
in a Cloud Environment

The Importance of Cryptographic Key Management

When you encrypt data using cryptographic keys, the data is randomized at the bit level and secured. But here is the problem: where do you store the key? The keys are still exposed and, if compromised, adversaries now have the means to decrypt the data and the data is no longer safe. Thus cryptography by itself, does not relieve us from having to manage and protect sensitive data. Therefore, we need a safe place, the ultimate vault (Root of Trust), to store the keys.

The Best Way to Manage Keys



HSM
(Hardware Security Module)

The tried-and-true way to safely store keys is to use a hardware appliance called a Hardware Security Module (HSM). An HSM safeguards cryptographic keys, and it supports the lifecycle of key management and various cryptographic operations such as encryption, digital signature, and more.

The Need for New HSM

Traditionally, companies installed HSMs in an isolated location and limited both the physical and network access as much as possible. However, the advent of cloud computing has changed the role HSMs must play. And traditional HSMs are no longer suitable to meet the new requirements emerging from the cloud environment and cloud-scale applications.

- HSMs need to be deployed in the cloud. This means that companies don't own hardware and don't have control over physical access to them.
- Cloud-scale applications and millions of devices connected to the cloud require rapid horizontal scalability of HSMs.

The Need for New HSM

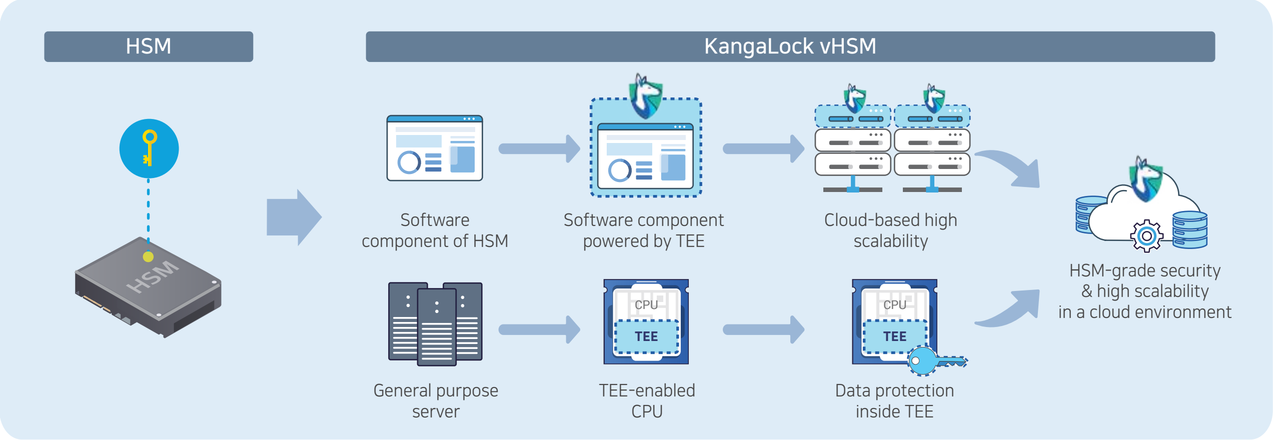
KangaLock vHSM

KangaLock vHSM is a paradigm-shifting key management solution. We completely redesigned the traditional HSM from the ground up to overcome its limitations to support new requirements emerging in the era of cloud computing.

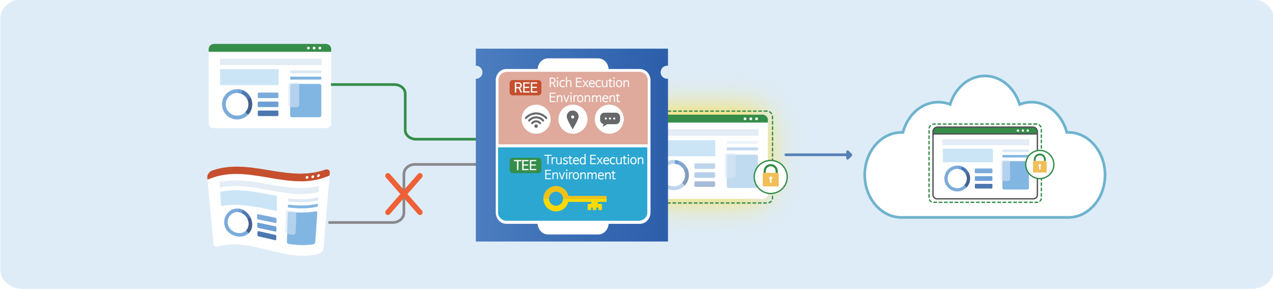
- ✓ Unparalleled security and reliability in a cloud environment. KangaLock protects sensitive data even in the face of infrastructure, virtual machine, and OS compromise.
- ✓ Massive scalability. KangaLock can manage millions to billions of keys and perform cryptographic operations at a high rate. It's a perfect solution to optimize HSM workloads to respond to change in demand. It can scale out according to the surge and decline in demand.
- ✓ Fast and easy deployment and configuration. No need to own special-purpose hardware or hire skilled HSM engineers.

KangaLock
vHSM

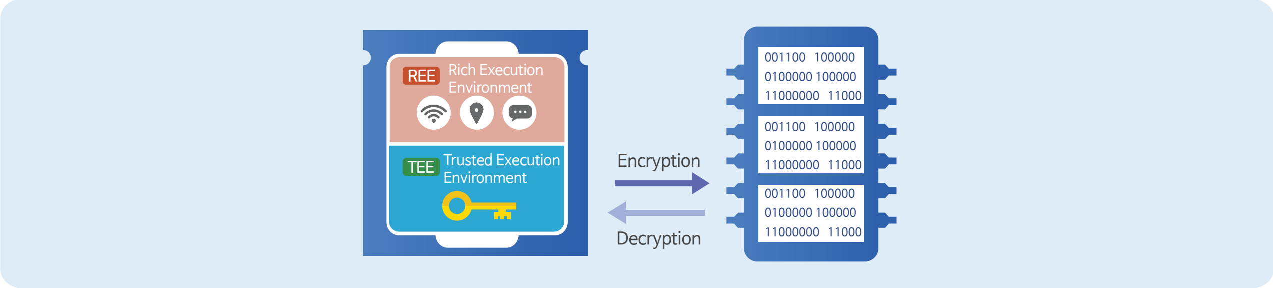
What is the Trusted Execution Environment (TEE)?


HSM
KangaLock vHSM
HSM
Software component of HSM
Software component powered by TEE
Cloud-based high scalability
HSM-grade security & high scalability in a cloud environment
General purpose server
CPU
TEE
TEE-enabled CPU
Data protection inside TEE

KangaLock virtual HSM features strong security powered by the Trusted Execution Environment. TEE is a cutting-edge security technology that dramatically reduces the attack surface down to the CPU. It is resistant against a variety of attacks, including malicious insiders, zero-day exploits, OS vulnerabilities, and even compromised cloud providers or government oversight.



TEE creates a secure area inside the main processor, isolated from the Regular Execution Environment (REE). In the trusted area, only authorized programs can run and access sensitive information.



Any data leaving the TEE will be automatically encrypted by the sealing key hidden inside the CPU. TEE, by design, blocks unwanted data leaks and allows secure execution of critical applications.

TEE & Confidential Computing

As companies rely more on cloud computing services, companies require greater assurances that their data in the cloud remains confidential. This has been a difficult-to-fulfill requirement, and many companies and organizations have declined to migrate their sensitive operations to the cloud due to potential data exposure.

Confidential Computing Consortium (CCC) is an effort to establish IT-industry-wide standards for Confidential Computing and facilitate the adoption of and migration to cloud computing platforms. Many industry giants participate in this movement, notably Microsoft, Google, Intel, and others.

intel Google Microsoft arm ORACLE HUAWEI Red Hat

Key Features

Strong Security Powered by TEE

Guaranteed HSM-grade security and reliability in a cloud environment using the advanced runtime security provided by TEE technology.

Limitless & Flexible Scalability

Built to scale horizontally and support large-scale key management. Flexibly scale up or down according to changes in operational workload.

Instant Deployment & Easy Configuration

KangaLock runs on cloud infrastructure thanks to its software-like quality. Fast time to value (TTV) is possible with minimal configuration.

Compatibility With Existing Interface

Provides a variety of standard interfaces such as PKCS#11, REST APIs, and etc., as well as support for NSA Suite B algorithms.

KangaLock vHSM Applications

KangaLock vHSM serves as a Root of Trust (RoT) and helps you achieve a variety of goals in critical applications, from traditional use cases to emerging applications such as IoT, Blockchain, and V2X.

Finance Database DRM Digital Signature Cloud IoT Blockchain V2X

Usecase

01 Blockchain

Private keys represent the identity and security credentials of participants in Blockchain applications. And it is common to expect tens of millions of potential users. This requires a large number of private keys to be secured and managed. KangaLock vHSM's capacity for security and scalability makes it indispensable to Blockchain applications.

02 Key Management in the Cloud

Container encryption and Big Data encryption are becoming increasingly common for companies and organizations to build an IT infrastructure in the cloud. KangaLock vHSM's scalability and ease of deployment can support large volume encryption and decryption services in a cost-effective manner.

03 Cryptographic Infrastructure

Encryption is essential to safely store and exchange customer information and intellectual property. KangaLock vHSM supports standard interfaces and a broad set of algorithms required for database encryption, SSL/TLS processing, document signing, as well as secrets management solutions. such as Vault by HashiCorp and AWS Secrets Manager.

04 Public Key Infrastructure (PKI)

IoT applications such as connected vehicles or smart meters may utilize many millions of devices. To support secure communication among the devices, a PKI must issue large numbers of certificates and perform cryptographic operations at a high rate. KangaLock vHSM serves as the Root of Trust to offload such cryptographic operations.

Specifications

Operating System	Linux (Ubuntu, Debian, RHEL, CentOS), Windows
Interface	PKCS#11 (Supports C, C++, Go, Python, Node.js, OpenSSL)
Algorithm	RSA, ECDSA, EdDSA, HMAC, SHA-2, AES, Triple DES, ARIA, SEED
Application	NGINX, Apache HTTP Server, Oracle Database
Certification	FIPS 140-2 Compliant Algorithm

Product Inquiry

contact@teeware.io website | http://www.teeware.io

US I 8609 Westwood Center Dr #110, Vienna, VA 22182, USA
KR I E19 9F, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon, Rep. of Korea

TEEware