Samsung Cloud Platform

Security

Key Management Service

Easily Creates and Securely Protects Encryption Keys

Key Management Service(KMS) is a secure, easy-to-use service that enables users to create, store and manage encryption keys, thereby securely protecting critical data in applications. The encryption key is used to encrypt/decrypt data and is managed securely in a centralized manner.

Hierarchical Key Management

KMS uses hierarchical encryption for data key, master key and root key, thereby ensuring secure key management. The master key is created through the root key stored in the FIPS 140-2 Level 3 certified Hardware Security Module(HSM) and distributed and stored in the KMS for secure protection. Using the mater key, users create a data key for data encryption.

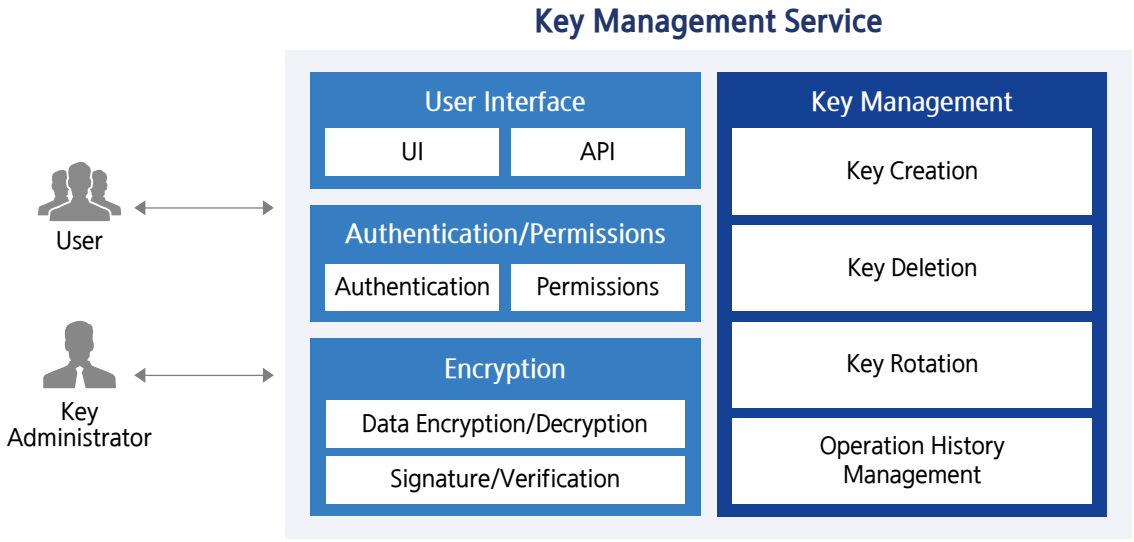
Key Lifecycle Management

Key rotation enables the creation of new encrypted data for a given master key and allows users to define the frequency of key rotation based on user policy. In addition, managing usage logs become easy with KMS monitoring. By administrating the lifecycle of encryption keys, one can also delete or reactivate disabled keys to protect data against cryptographic threats.

High Availability Infrastructure

Using a high availability infrastructure, KMS delivers a reliable service. KMS provides high availability with multiplexing configurations such as the KMS engine that creates master key and the HSM that stores root key.

Service Architecture



Key Features

- **Key types**
  - Encryption/Decryption(AES256) : Use the AES256 key(symmetric key) for data encryption operation of up to 32KB
  - Encryption/Decryption or Signature/Verification(RSA-2048) : Use the RSA key(asymmetric key, 2048 bit) for data encryption of up to 190B or 8KB signature
  - Creation/Verification(HMAC) : Use to create and verify hash-based message authentication code(HMAC)
  - Signature/Verification(ECDSA) : Use the ECDSA key(asymmetric key) for data signature of up to 8KB

  ※ Korea's Public Authentication Encryption Algorithm, ARIA can be used for SCP Sovereign
- **Managing key permissions**
  - Select an account that will be granted access to the master key(within the same account)
  - Assignment of key roles : Key manager, Encryptor/Decryptor, Encryptor, Decryptor, Key reviewer
- **Managing key lifecycle**
  - Key rotation : Create a new key version. Define automatic key rotation, anywhere from 1 day to 730 days
  - Key deletion : Upon request, a key will immediately be disabled and be permanently deleted after 72 hours
  - View operational logs : Date of operation, operation details and results, account used for operation

SAMSUNG SDS

www.samsungsds.com / cloud.samsungsds.com
contact.sds@samsung.com / scp_sales@samsung.com
youtube.com/samsungsds