Key Management Service

Product Introduction

Product Documentation

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

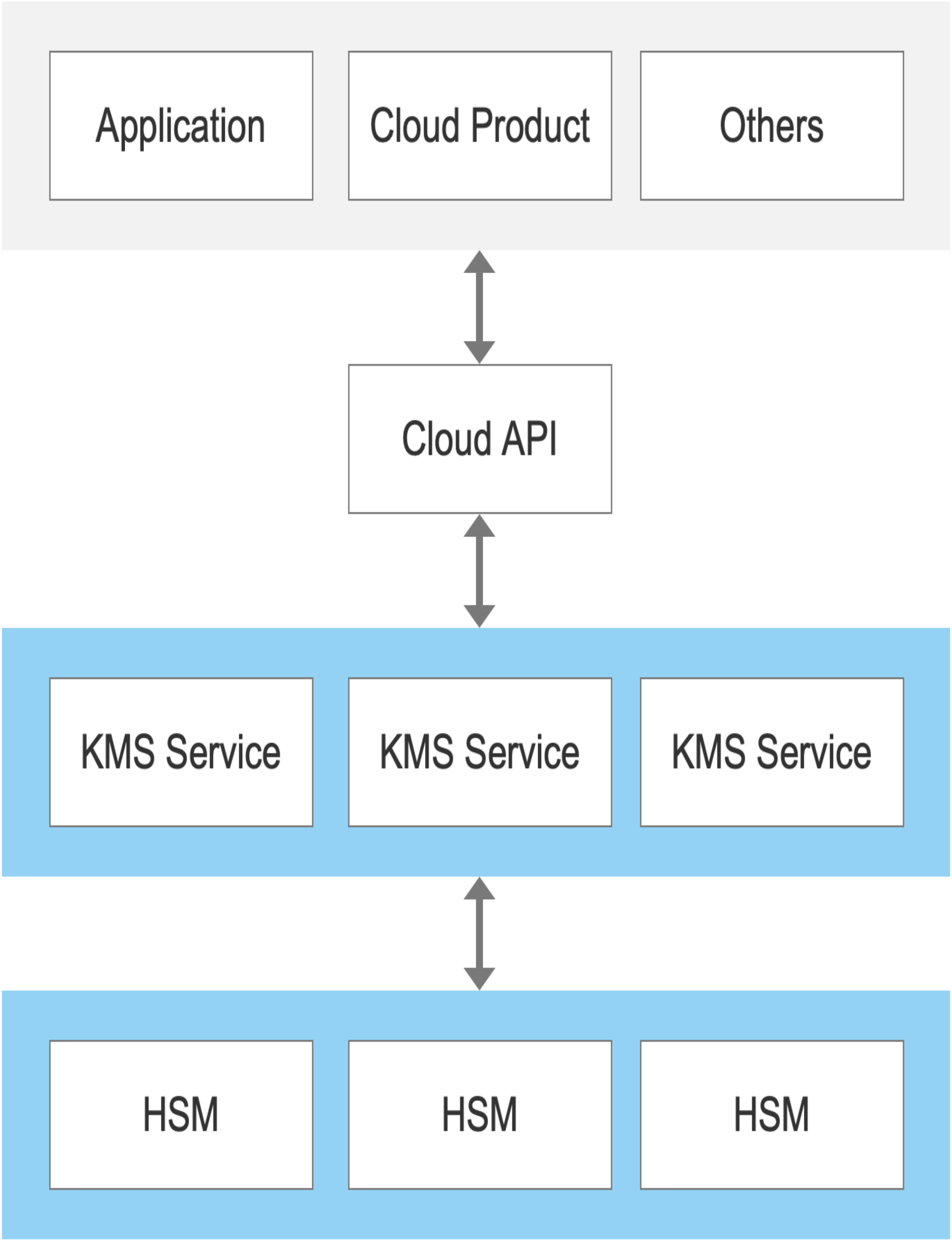
Product Introduction

Overview

Last updated：2023-08-24 11:21:51

Key Management Service (KMS) is a security management service that utilizes third-party certified Hardware Security Modules (HSM) to generate and safeguard keys. It assists users in effortlessly creating and managing keys, fulfilling key management requirements for various applications and services, and facilitating compliance implementation.

The following diagram illustrates the Key Management Service (KMS) product architecture:



Strengths

Last updated：2023-08-24 11:30:54

Security and Compliance

KMS employs third-party certified hardware security modules (HSM) to generate and safeguard keys, ensuring security and quality control through various compliance programs. The creation and management of your primary keys will be conducted within the encryption device, preventing anyone, including Tencent Cloud, from accessing your plaintext primary keys.

High Availability

At the architectural level, KMS service ensures reliability through multi-data center deployment within a single region. The underlying HSM devices also employ multi-data center clustered deployment and provide dual-data center cold backup equipment to guarantee high availability. At the access level, KMS offers external access services through Cloud API 3.0. Deployed across regions, Cloud API 3.0 provides both unified domain names and region-independent domain names to ensure high availability for service access.

Centralized key management

You can access Tencent Cloud KMS service through APIs, SDKs, and connected cloud products, using KMS to centrally manage key policies for your business applications, regardless of whether they are deployed within or outside Tencent Cloud.

Instant Activation

Pay-as-you-go KMS can be deployed quickly at the click of a button. Tencent Cloud covers all backend maintenance, eliminating your need to purchase any dedicated hardware encryption devices.

Simplified encryption service

KMS utilizes envelope encryption, allowing you to encrypt and decrypt massive local data by simply calling encryption and decryption APIs and managing CMK permissions.

Dedicated Key Resources

KMS Exclusive Edition is a cloud-based key management service with dedicated physical encryption devices. Encryption operations are performed within the exclusive physical encryption devices, which possess a dedicated cryptographic resource pool.

Scenarios

Last updated：2023-08-24 11:31:08

Tencent Cloud Key Management System (KMS) is suitable for all users within and outside Tencent Cloud, addressing their sensitive data encryption needs and meeting compliance requirements while assisting various industries in solving data encryption pain points.

Protection of sensitive data in industries such as finance

Pain point: In industries such as finance, all communication and stored data have high value and confidentiality, requiring consideration of encryption security and compliance.

Solution: Envelope encryption provides encryption services for communication content, important documents, and materials, as well as key protection and access management, meeting security and compliance requirements.

Protection of Configuration Information in Backend Service Development

Challenge: Configuration files for application development need to be encrypted to protect program data.
Solution: KMS can encrypt and protect the integrity of sensitive configuration information such as database connection information, database passwords, login keys, and backend service configurations.

Protection of Enterprise Core Data

Challenge: Core private data such as intellectual properties, mobile numbers, ID numbers, and bank account numbers of end users, and passwords must be strictly protected. Although sensitive data can be stored after encryption, it is difficult to ensure the security of the data encryption keys.
Solution: KMS can encrypt all core data using data encryption keys in envelope encryption mode and then encrypt the keys too to provide another layer of security protection for the data.

Website or Application Development Security

Challenge: If certificates and keys required for HTTPS services are stored in plaintext in the local file system, they can be easily obtained by hackers.
Solution: KMS can encrypt and decrypt keys. After encryption, the key files in ciphertext will be stored locally to be decrypted as needed. The key files will not be stored locally after

decryption, making it impossible for hackers to obtain them, thereby ensuring the security of webpages and applications.

Centralized Management of Password Policies

Challenge: A unified key management policy needs to be applied to decentralized business systems.
Solution: KMS can be called through APIs, SDKs, and Tencent Cloud products and services to achieve centralized key management for cloud-based and local application data.

Concepts

Last updated：2023-08-24 11:32:15

This guide describes basic concepts in Key Management Service (KMS).

Key lifecycle

Key lifecycle refers to a set of operations including generating, saving, distributing, importing, exporting, applying, restoring, archiving and terminating keys. KMS provides a full lifecycle management to manage keys in a safe manner and prevent key leaks.

Symmetric encryption and decryption

Symmetric encryption and decryption is a data encryption technique where the same key is used to both encrypt and decrypt the data.

> **Note**
> Key Management Service (KMS) offers symmetric encryption and decryption solutions. For more details, see **Symmetric Encryption and Decryption**.

Asymmetric encryption and decryption

Asymmetric encryption and decryption requires two keys: a public key and a private key. The public and private keys are a pair, where the sender uses the public key to encrypt data, and the recipient can only decrypt it using the corresponding private key. On the other hand, the sender can sign confidential information using the private key, and the recipient can verify the received data using the corresponding public key.

> **Note**
> KMS also supports asymmetric encryption and decryption. For more details, see **Asymmetric Encryption and Decryption**.

Customer Master Key (CMK)

Customer Master Keys (CMKs) are used to protect sensitive data and Data Encryption Keys (DEKs) of Key Management Service (KMS) users. They are generated by hardware security modules and protected by Domain Keys. CMKs can only be encrypted and decrypted through encryption devices.

Data Encryption Key (DEK)

In envelope encryption scenarios, DEK is used to directly encrypt and decrypt user data. It is generated by the key management system using a hardware security module (HSM) and returned to the application system in both ciphertext and plaintext forms after being encrypted by the customer master key (CMK). The business side performs high-performance local encryption and decryption using the plaintext DEK in memory.

White-box Key

White-box keys are secured using white-box cryptography techniques and are designed to protect sensitive root key information on the client side, such as API SecretKey, authentication keys or tokens used by internal systems, and other local sensitive root key information.

> **Note**
> Key Management Service (KMS) offers a solution for white-box key management. For more details, see White-box Key Management.

Sensitive data

Sensitive data refers to sensitive and private information, such as keys, certificates, configuration files, bank account numbers, and identification numbers.

HSM

Hardware Security Module (HSM) is a computer hardware device designed to protect and manage keys used in strong authentication systems while providing cryptographic operations. KMS utilizes commercial or FIPS-140-2 certified HSMs to ensure the confidentiality, integrity, and availability of keys.

BYOK

Bring Your Own Key (BYOK) allows users to import their own key material into their master key. For more information, please refer to External Key Import.