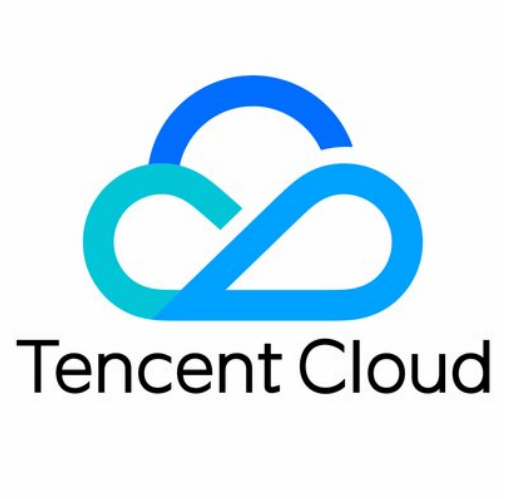
Key Management Service

Product Introduction

Product Documentation



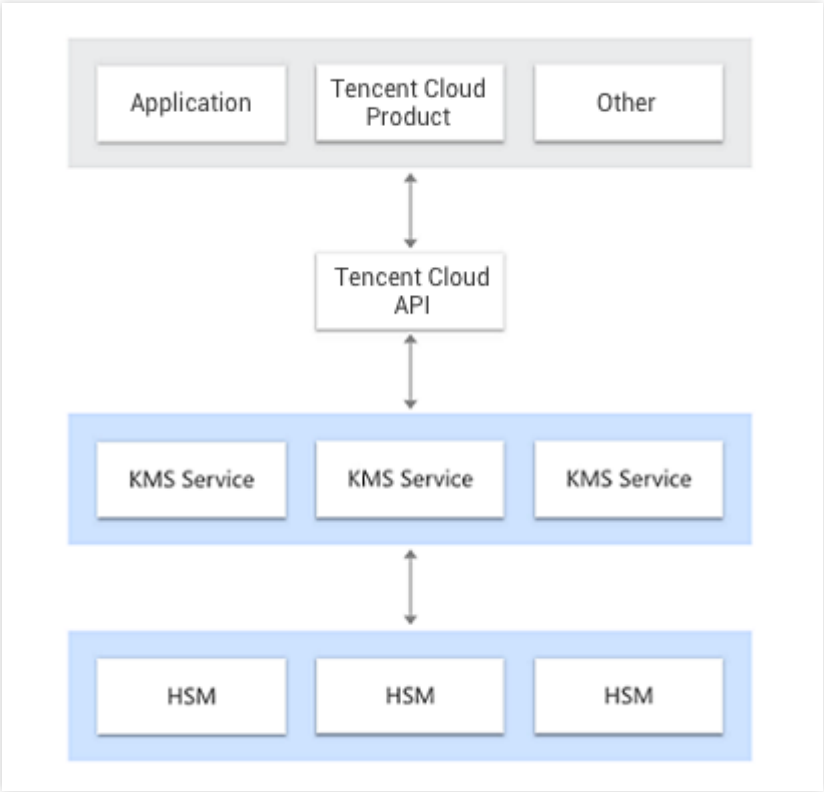
Contents

Product Introduction

Product Overview

Last updated：2024-01-11 16:28:53

Tencent Cloud Key Management Service (KMS) is a security management solution that leverages a third-party certified hardware security module (HSM) to generate and protect keys so you can easily create and manage keys, helping you to meet your key management and compliance needs in multi-application and multi-business scenarios. Below is the architecture of KMS:



Features

Last updated：2024-01-11 16:28:53

Security and Compliance

KMS leverages a State Cryptography Administration of China or FIPS-140-2 certified hardware security module (HSM) to protect keys, thereby ensuring their confidentiality, integrity, and availability.

Managed Key Services

KMS provides a wealth of management features, including key creation, enabling, disabling, rotation settings, alias settings, key details viewing, and related information modification, which help you create and protect keys and implement key management policies with ease.

Encryption Algorithms

KMS supports symmetric encryption algorithms (SM4 and AES256) and asymmetric encryption algorithms (RSA and SM2). You can choose an appropriate algorithm based on your actual business needs.

Key Import

For symmetric keys, KMS allows you to use your own key material to encrypt and decrypt sensitive data by implementing a Bring Your Own Key (BYOK) solution in Tencent Cloud.

Key Rotation

For symmetric keys, KMS has a customer master key (CMK) rotation feature which is disabled by default and can be enabled as needed. After this feature is enabled, a CMK will be rotated once every year. Managed by KMS, key rotation is imperceptible to the upper-layer businesses, and existing ciphertexts encrypted by the old CMK can still be decrypted, while only new encryption tasks use the new CMK.

Permission Control

Fully integrated with CAM, KMS can control which accounts and roles can access or manage your sensitive keys through identity and policy management.

Built-in Audit

KMS is integrated with CloudAudit to record all API requests for detailed statistics of key management activities and key usage.

Stability and Reliability

KMS is deployed in a distributed and clustered manner across multiple data centers with hot backup enabled, and its underlying HSM devices are deployed in two data centers with cold backup enabled, guaranteeing high availability

around the clock.

Seamless Integration

Seamlessly integrated with Tencent Cloud services such as COS, TDSQL for MySQL, and CBS, KMS enables you to encrypt data stored in such services with ease.

Centralized Key Management

KMS can be called and integrated through APIs, SDKs, and Tencent Cloud products and services to achieve centralized management of keys from various applications, no matter whether they are in or off Tencent Cloud.

Sensitive Data Encryption

Sensitive information encryption is a core capability of KMS, which is mainly used to protect sensitive data (less than 4 KB) on the server disks such as keys, certificates, and configuration files.

Envelope Encryption

Envelope encryption is a high-performance encryption and decryption solution for massive amounts of data. With the aid of envelope encryption in KMS, only the data encryption keys (DEKs) need to be transferred to the KMS server to be encrypted or decrypted with the CMK, and all business data is processed with efficient local symmetric encryption which has little impact on the business access experience.

Product Strengths

Last updated：2024-01-11 16:28:53

Security and Compliance

KMS leverages the third-party certified hardware security module (HSM) to generate and protect keys. The security and quality control practices adopted by KMS are accredited by multiple compliance schemes. The creation, management, and other operations of your master keys are performed in the compliant HSM, and no one (including Tencent Cloud) will be able to obtain your plaintext master keys.

High availability

At the service architecture level, the reliability of KMS is guaranteed through a single-region multi-data center deployment. The HSM used in the underlying system is also deployed in a clustered manner across data centers with cold backup enabled to ensure high availability of the service. At the access level, KMS can be accessed through TencentCloud API 3.0 deployed in different regions with both unified and region-specific access domain names provided to ensure high accessibility.

Centralized key management

KMS can be called and integrated through APIs, SDKs, and connected Tencent Cloud products to centrally manage the key policies of your business applications in and outside Tencent Cloud.

Low costs

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.

Encryption SDK

The KMS Ultimate Edition supports different encryption requirements with its Encryption SDK, a certified commercial encryption product conforming to Chinese encryption standards.

Simplified encryption service

The KMS Ultimate Edition protect keys by envelope encryption and encapsulates them using the Encryption SDK for complex management. To encrypt/decrypt massive data, you only need to call encryption/decryption APIs and ensure your permission control of the CMK.

Use Cases

Last updated：2024-01-11 16:28:53

KMS can be used by Tencent Cloud and non-Tencent Cloud resources for sensitive data encryption to meet security and compliance requirements and help resolve data encryption challenges in various industries.

Protection of sensitive industry data

Challenge: Communications and data of any industry such as financial institutions are highly confidential. The security and compliance of encryption must be well executed.
Solution: KMS provides encryption, key protection, and permission management services through envelope encryption for important data such as various agreements, documents, and materials to meet 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, bank account numbers of end users, and passwords must be strictly protected. Although sensitive data can be encrypted, 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 also 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 and can be decrypted as needed. The decrypted key files will not be stored locally so that hackers cannot 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, making it possible for users to achieve centralized key management for cloud-based and local application data.

Concepts

Last updated：2024-01-11 16:28:53

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:

KMS supports symmetric encryption and decryption. For more details, see **Symmetrical Encryption and Decryption**.

Asymmetric encryption and decryption

Asymmetric encryption and decryption is a type of encryption that uses a pair of keys (public key and private key) to encrypt and decrypt data. The public key is used by a sender to encrypt data and only the receiver can decrypt the data with the matched private key. On the other hand, the sender can use the private key to sign a confidential message, while the receiver can verify the message using the matched public key.

Note:

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

Sensitive data

Sensitive data refers to sensitive and private user information such as keys, certificates, bank accounts and ID numbers.

HSM

Hardware Security Module (HSM) is a computer hardware device that protects and manages keys in the strong authentication system as well as supports cryptographic operations. With the State Cryptography Administration or FIPS-140-2 approved HSM, Tencent Cloud KMS secures keys in terms of confidentiality, integrity and availability.

BYOK

Bring Your Own Key (BYOK) refers to the ability of a user to import key material to a Customer Master Key (CMK). For details, see **Importing External Key**.