Key Management Service

FAQs

Contents

FAQs
General Questions

Last updated：2023-08-24 11:48:07

What can Tencent Cloud KMS do?

Tencent Cloud KMS provides full lifecycle management of symmetric and asymmetric keys during the encryption process, including generation, storage, enabling/disabling, distribution, rotation, auditing, and destruction. This meets the key management needs of users with multiple applications and services while complying with regulatory requirements. Additionally, KMS offers encryption capabilities such as sensitive data encryption, envelope encryption, and cloud product integration, allowing users to focus on business development.

Which cloud services support data encryption using Key Management System?

KMS seamlessly integrates with Tencent Cloud products such as TencentDB, COS, and CBS, encrypting cloud product data using envelope encryption provided by KMS.

What is the difference between Customer Master Keys and Tencent Cloud Managed CMKs in the Key Management System console?

- **Customer Master Keys (CMKs)** are created by users through the console or API. You can perform operations such as creating, enabling, disabling, rotating, and controlling access to these keys.
- **Cloud Product Keys** are CMKs automatically created for users by Tencent Cloud products/services (such as CBS, COS, TDSQL, etc.) when invoking the Key Management System. You can query and enable key rotation for cloud product keys, but disabling and scheduled deletion operations are not supported.

How can massive data be encrypted?

For larger data encryption, it is recommended to use the envelope encryption scheme for high-performance local data encryption and decryption.

Does KMS impose access rate limitations on users?

KMS imposes limits on the frequency of user access.
- For the same primary account (accessing KMS services under its own account), the maximum access frequency to a single KMS service interface is 15,000 times per second.
- For a role-authorized master account (after granting permission, the master account can

access other accounts' KMS services), the maximum access frequency for a single KMS interface is 3,000 times per second.

If the frequency of accessing KMS service exceeds the corresponding value, please submit a ticket to contact us for adjustments.

Development Access Questions

Last updated：2023-08-24 16:26:46

How do I get my secret ID and secret key from the SDK?

You must use your primary account to log in to the API Key Management Console to obtain your SecretID and SecretKey. **Please ensure to securely store your SecretID and SecretKey to prevent any unauthorized disclosure.**

How do I create a Customer Master Key (CMK)?

There are three methods to create a Customer Master Key (CMK): through the Key Management System Console, using the Tencent Cloud Command Line Tool (TCCLII, and via API requests.

Is there a limit to the number of CMKs I can create?

Yes, there is a limit of 200 CMKs per account per region, excluding those in the scheduled deletion status. This does not include cloud product keys. If you need to create more CMKs, please submit a ticket or contact Tencent Cloud sales.

When creating a key, you can choose the key material source to be external. "External" refers to using your own key material. The BYOK (Bring Your Own Key) solution allows you to use your own key material for encryption and decryption services within Tencent Cloud.

- **External** refers to using the user's own key material.
- **BYOK** (Bring Your Own Key) is a solution that allows users to utilize their own key material. This is achieved by generating a CMK with no key material through the KMS service, then importing the user's own key material into this master key, forming an External CMK (EXTERNAL CMK). The distribution and management of this external key is then handled by the KMS service.

How long does it take to effect after I modify the CMK alias or description information via API calls?

The changes will **take effect immediately** after a successful API request.

Does Tencent Cloud support rotating Customer Master Keys (CMKs)? How can I enable it?

Key rotation is supported. You can enable it through the **Key Management System Console**, **Command Line Tool**, or **API interface**.

> ⚠ **Note**
>
> CMKs not supported for rotation include:
> - Asymmetric CMKs
> - CMKs made from external key materials

Do I need to change my application after enabling rotation?

- Key rotation only changes the CMK's key material. Its attributes (key ID, alias, description, permission) remain.
- After you enable key rotation, KMS will automatically rotate keys based on the specified rotation period (365 days by default). Each rotation will generate a new version of CMK. The rotated keys can be encrypted and decrypted as follows:
  - In encryption, KMS will automatically use the latest version of CMK.
  - In decryption, KMS will automatically use the CMK that is applied in encryption.

How do I choose an encryption algorithm?

- **Symmetric Encryption/Decryption**: Symmetric encryption algorithms include SM4 and AES256. The algorithm is automatically assigned by the system based on the region selected when creating the master key. If the selected region is "China Mainland," the system will choose the SM4 algorithm; if the selected region is "Outside China Mainland," the system will choose the AES256 algorithm.
- **Asymmetric Encryption/Decryption**: Asymmetric encryption algorithms include RSA keys with a 2048-bit modulus and SM2. The choice of algorithm is determined by the region and KeyUsage you select when creating the master key.

> ⚠ **Note**
>
> When creating a CMK through the API, it is recommended to first query the **encryption methods** supported in the current region to ensure the correctness of the creation.