

Key Management Service

Product Introduction

Product Introduction

Key Management Service (KMS)

Key Management Service (KMS) is a secure and easy-to-use management service provided by Alibaba Cloud. Through KMS, you no longer have to spend a great deal to protect the confidentiality, integrity, and availability of keys. You can use keys securely and conveniently, and focus on developing encryption/decryption function scenarios.

Major problems to resolve using KMS

Role	Problem	How to resolve the problem using KMS
Application/Website developer	My program needs to use a key for encryption or a certificate for signature, and I hope the key is managed in a secure and independent manner. I hope I can safely access the key no matter where my application is deployed. I would never allow deploying the plaintext key randomly, which is too risky.	Through the envelop encryption technology, users can store the Customer Master Key (CMK) in KMS and deploy only the encrypted data key, and users can call KMS to decrypt the data key only when they need to use it.
Service developer	I do not want to be responsible for the security of users' keys and data. I hope users can manage their keys by themselves and I can use specified keys to encrypt their data with their authorization. In this way, I can devote all energy to developing service functions.	Based on the envelop encryption technology and the open APIs of KMS, service developers can use specified CMKs to encrypt and decrypt data keys, easily satisfying the requirement of not storing the plaintext directly in a storage device ; therefore, service developers do not need to worry about how to manage users' keys.
Chief Security Officer (CSO)	I hope the key management of my company can meet compliance requirements. I need to ensure that keys are reasonably authorized and	KMS can be associated with RAM for unified authorization management.

	any use of keys must be audited.	
--	----------------------------------	--

Limits of use

KMS is a region-based service. KMS resources and limits of use are relatively independent for each user in different regions. Currently, KMS is supported in five regions, that is, Singapore, China East 1, China East 2, China North 2, and China South 1.

CMK quota

Each user can create up to 200 CMKs in each region.

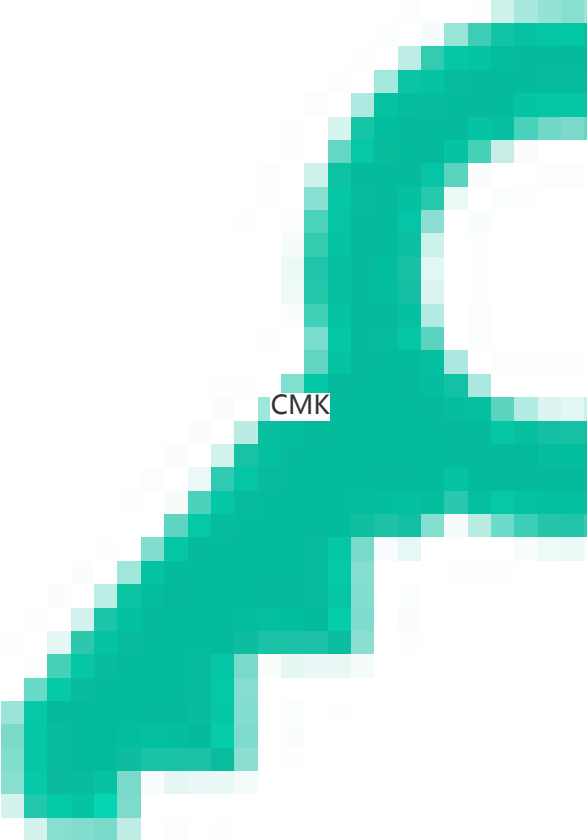
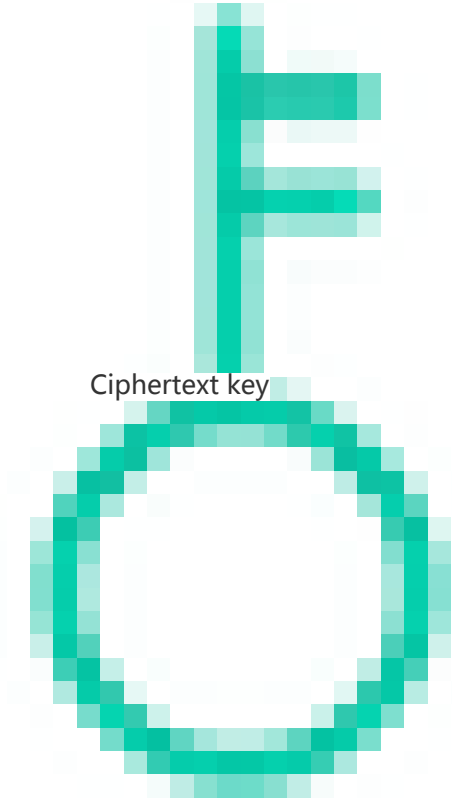
Any user requiring to create more than 200 CMKs can apply to Alibaba Cloud through the ticket system.

Product strengths

Advantage	Traditional key management solution	KMS
Cost effectiveness	Buying secure key management equipment to construct a secure physical environment results in high hardware costs. Designing and executing secure key management specifications involve high software costs.	With KMS, you pay only for what you need and the price is low.
Easy to use	Hardware equipment APIs lack standards, making them confusing and difficult to use. Solutions and configurations of communication channel security are cumbersome.	Unified and easy-to-use APIs. Standard HTTPS protocol.
Reliability	Generally, you need to use an offline backup solution to ensure high reliability.	KMS combines a distributed system and cryptographic hardware to achieve high reliability.

Application scenarios

Example

Example	Meaning	Example	Meaning
			
	Plaintext certificate		Plaintext file

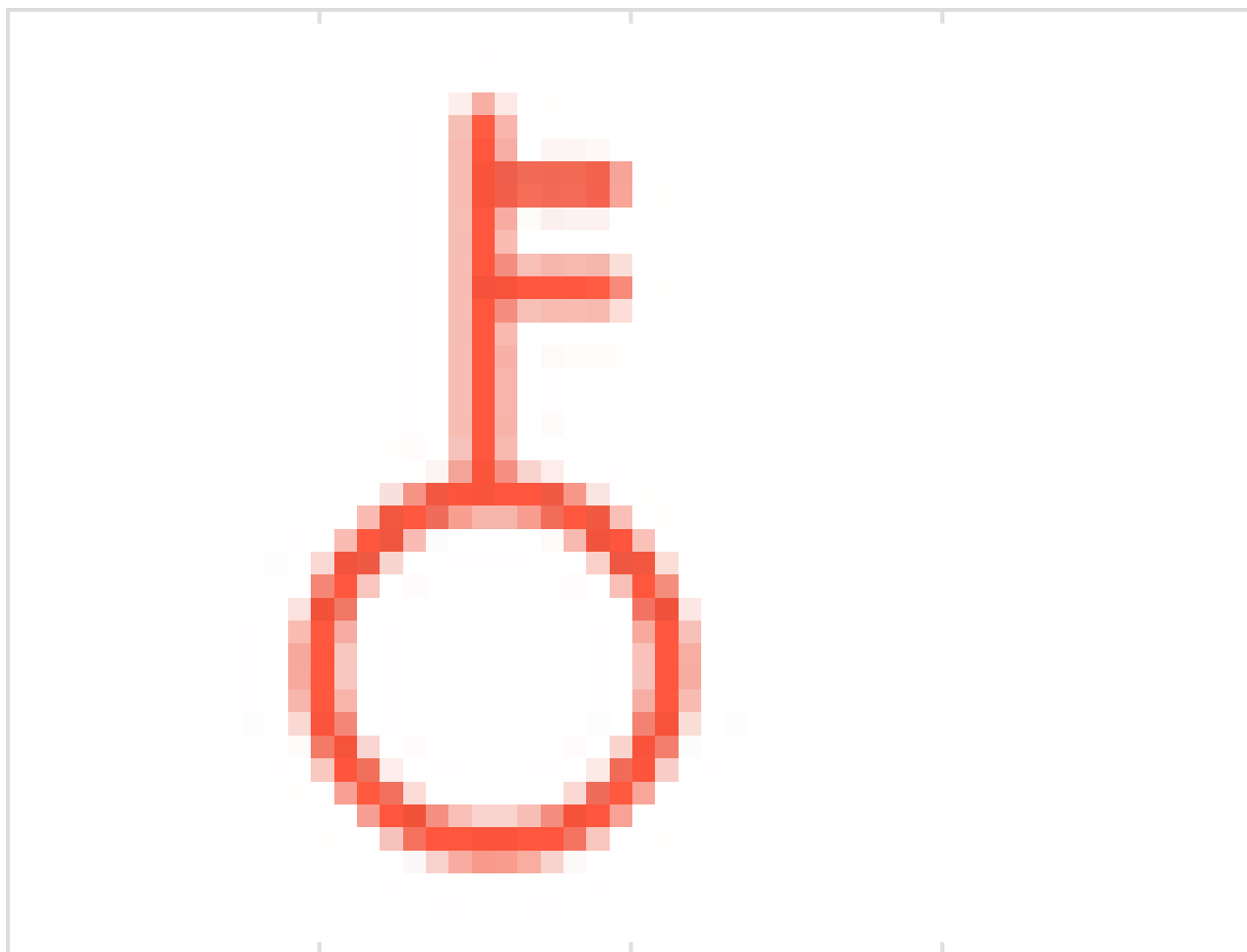


Ciphertext certificate

Ciphertext file



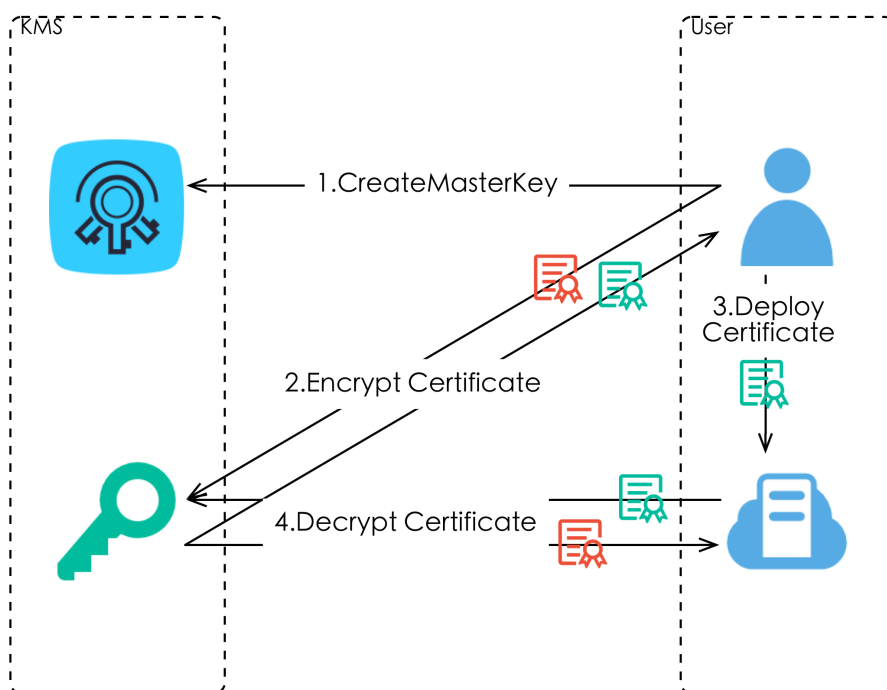
Plaintext key



Directly use the KMS for encryption and decryption

You can directly call the KMS API and use the specified CMK to encrypt and decrypt data. This scenario applies to encryption and decryption of a small amount of data (less than 4 KB). Data is transmitted to the KMS server through secure channels, encrypted or decrypted at the server, and returned through secure channels.

Scenario example: Protect the HTTPS certificate on the server

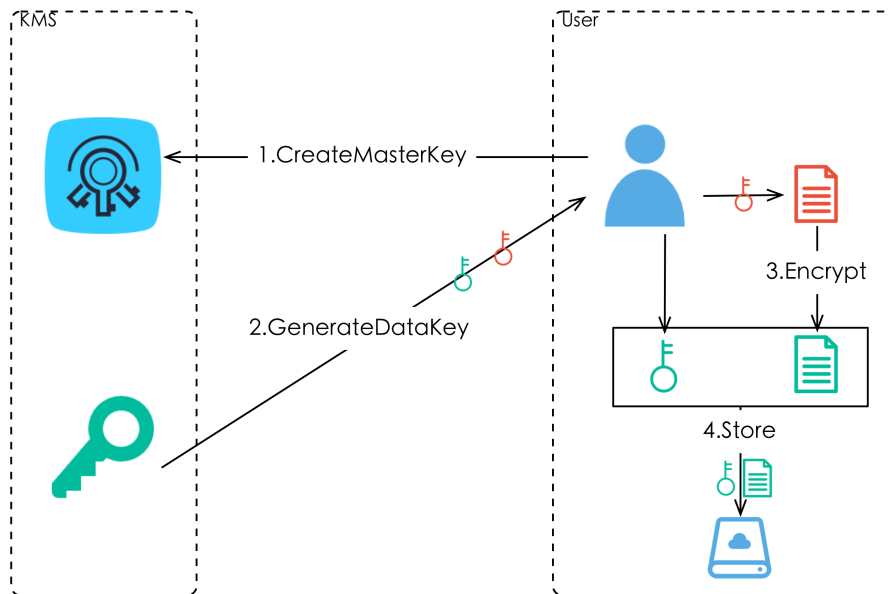
**Steps:**

1. Create a CMK.
2. Call the Encrypt interface of the KMS to encrypt the plaintext certificate to a ciphertext certificate.
3. Deploy the ciphertext certificate on the server.
4. Call the Decrypt interface of the KMS to decrypt the ciphertext certificate to a plaintext certificate when the server starts and needs to use the certificate.

Use envelop encryption to perform local encryption and decryption

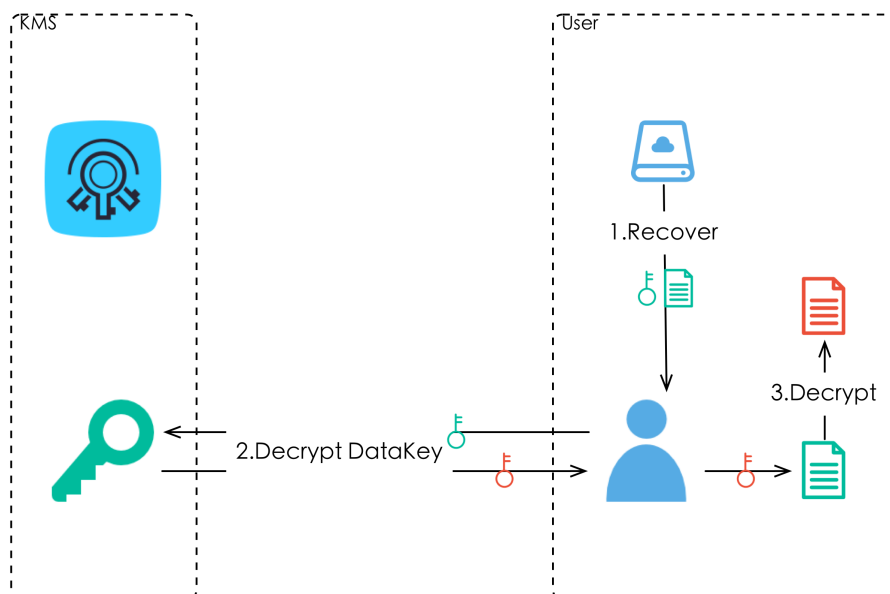
You can directly call the KMS API, use the specified CMK to generate and decrypt the data key, and use the data key for local data encryption and decryption. This scenario applies to mass data encryption and decryption, and you do not need to transmit mass data through the network, realizing mass data encryption and decryption at low cost.

Scenario example: Encrypt a local file



Encryption steps:

1. Create a CMK.
2. Call the GenerateDataKey interface of the KMS to generate data keys. You can obtain a plaintext data key and a ciphertext data key.
3. Use the plaintext data key to encrypt the file and generate a ciphertext file.
4. Save the ciphertext data key and the ciphertext file to a persistent storage device or service.



Decryption steps:

1. Read the ciphertext data key and the ciphertext file from the persistent storage device or service.
2. Call the Decrypt interface of the KMS to decrypt the ciphertext data key to obtain the

plaintext data key.

3. Use the plaintext data key to decrypt the file.

NOTE:

1. You must authenticate the HTTPS certificate on the Alibaba Cloud server to prevent phishers from stealing your information.
2. You are recommended to use the sub-account function of RAM service to implement the principle of least privilege.

Release date	Version	Content
2016-04-06	1.0	KMS OBT
2016-05-19	1.1	Three additional regions (China North 2 (Beijing), China East 2 (Shanghai), and China South 1 (Shenzhen)) are supported.
2016-06-22	1.2	Keys can be enabled and disabled.
2016-08-10	1.3	The performance is optimized, some errors are corrected, and the encryption and decryption APIs support Encryption Context.
2016-09-20	1.4	The performance is optimized, keys are added, and relevant APIs are deleted: ScheduleKeyDeletion and CancelKeyDeletion
2016-11-02	1.5	The performance is optimized, and four additional regions are supported: Asia Pacific NE 1 (Japan), Germany 1 (Frankfurt), Middle East 1 (Dubai), Asia Pacific SE 2 (Sydney)
2017-01-22	1.6	The performance is optimized, one additional regions is supported: Hong Kong
2017-03-01	1.7	Regular upgrade

Glossary

The following terminologies are key concepts in KMS.

Terminology	Full name	Description
KMS	Key Management Service	KMS provided by Alibaba Cloud Computing.
envelope encryption	envelope encryption	A symmetric key is generated each time for data to be encrypted. You can use a specific CMK to encrypt this symmetric key to make it "enveloped" . The "enveloped key" is directly transferred in unsafe communication process such as data transmission and storage. You can take the symmetric key out from the envelope only when you use it.
CMK	Customer Master Key	CMK is the master key created by a user in Alibaba Cloud KMS, which is mainly used to encrypt data keys and generate envelopes. It can also be directly used to encrypt a small amount of data.
EDK/DK	EnvelopedDataKey / DataKey	DK is the plaintext key for data encryption, and EDK is the ciphertext key obtained after envelope encryption.