ALIBABA CLOUD

Alibaba Cloud

Key Management Service

FAQ

Document Version: 20211008

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
⚠ Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	⚠ Danger: Resetting will result in the loss of user configuration data.
🔔 Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	🔔 Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
📢 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	📢 Notice: If the weight is set to 0, the server no longer receives new requests.
? Note	A note indicates supplemental instructions, best practices, tips, and other content.	? Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.What is envelope encryption? 05

2.Why is the error Forbidden.KeyNotFound reported during decry... 08

3.Why am I unable to access the KMS endpoint? 09

1.What is envelope encryption?

Envelope encryption is an encryption mechanism similar to the digital envelope technology. Envelope encryption allows you to encrypt data by using data keys and encapsulate data keys in an envelope to ensure security during the storage, transfer, and use of data keys. Customer master keys (CMKs) are not used to directly encrypt or decrypt data.

Benefits

You may encounter the following issues when you use data keys:

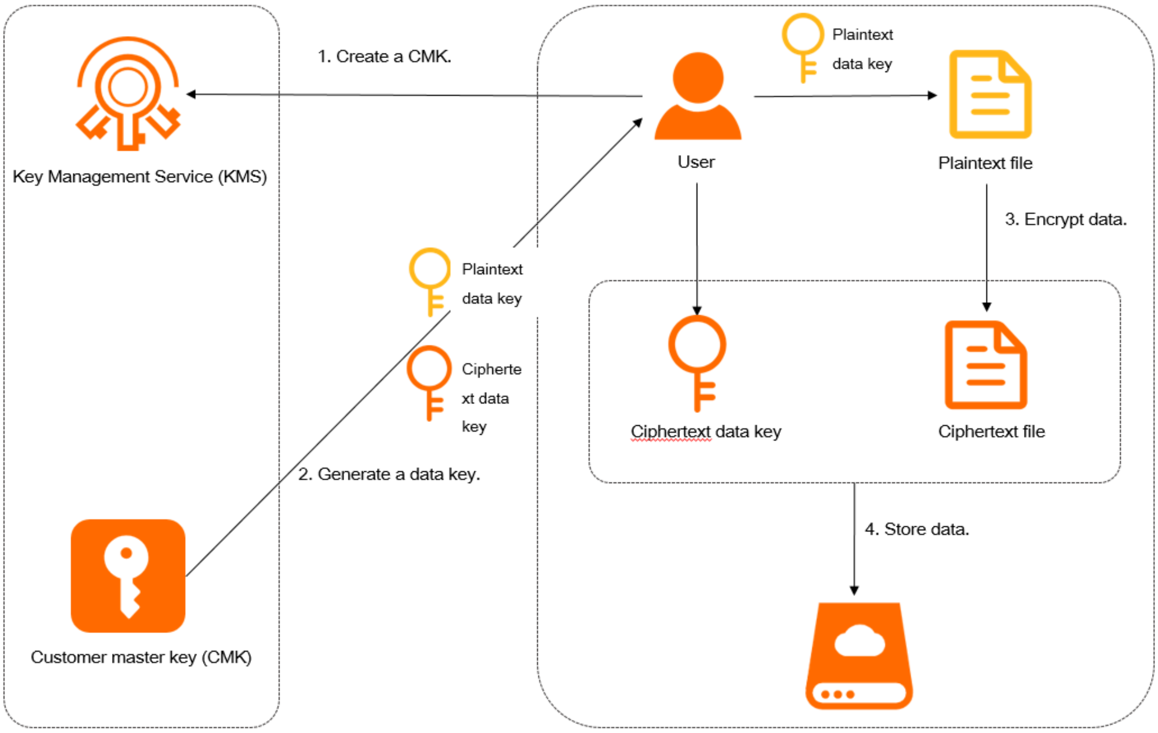
- Security risks: Security risks such as eavesdropping and phishing may occur during the process of transferring your sensitive data to Alibaba Cloud over the network.
- Absence of mutual trust and reliable certificates: You may not trust Alibaba Cloud and may not want to upload your sensitive data to Alibaba Cloud. In addition, Alibaba Cloud cannot prove that it will never misuse or leak the received sensitive data.
- Poor performance and high costs: If you have a large amount of sensitive data, a secure channel is required to transfer the data to an Alibaba Cloud server and the processed data must be encrypted before the server transfers the data to you. Such a process has a great impact on the service performance of Alibaba Cloud. In addition, high costs are required to transfer a large amount of data.

Envelope encryption has the following benefits:

- Protection for data keys: When data is encrypted by envelope encryption, data keys are also encrypted. Encrypted data and encrypted data keys can be safely stored together.
- Provision of trust and reliable certificates: Key Management Service (KMS) implements access control on and generates trackable logs for all operations on data keys. KMS also provides records of all data keys to meet your auditing and compliance requirements.
- High performance and cost-effectiveness: KMS calls key-related API operations to generate online data keys and uses offline data keys to encrypt a large number of local files.

Encrypt and decrypt local files

- **Encryption process**



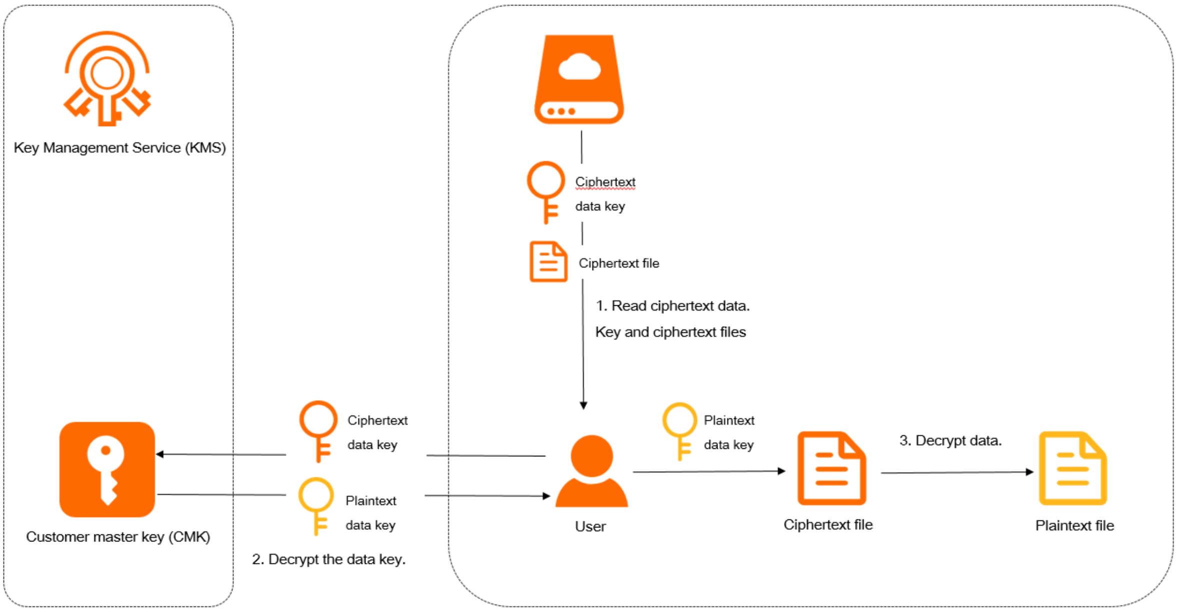
i. Create a CMK.

ii. Call the GenerateDataKey operation to generate a data key. KMS returns the plaintext and ciphertext of the data key.

iii. Use the plaintext data key to encrypt the local files.

iv. Store the ciphertext data key and encrypted files on a persistent storage device or service.

- **Decryption process**



i. Retrieve the ciphertext data key and encrypted files from the persistent storage device or service.

ii. Call the Decrypt operation to decrypt the ciphertext data key. The plaintext data key is returned.

iii. Use the plaintext data key to decrypt the files.

Examples

You can use one of the following SDKs to implement envelope encryption:

- KMS SDK

  Use KMS SDK to call the GenerateDataKey operation to generate a data key. Then, use a third-party encryption library and the data key to encrypt your data. After the encryption process is complete, encapsulate the ciphertext data key and encrypted data in an envelope.

  For more information about the sample code of KMS SDK, see Encrypt and decrypt local files.

- Encryption SDK

  Encryption SDK provides the best practices of envelope encryption. You can implement encryption and decryption with ease by using Encryption SDK.

  For more information about the sample code of Encryption SDK, see Quick start of Encryption SDK for Java.

2.Why is the error Forbidden.KeyNotFound reported during decryption?

The error is reported because you decrypt data in the wrong region.

Key Management Service (KMS) is independent in each region. Make sure that you decrypt data in the same region as the encrypted data.

3.Why am I unable to access the KMS endpoint?

The Key Management Service (KMS) endpoint cannot be accessed because HTTPS is not enabled when you use the SDK for access.

To ensure your data security, KMS **supports only** HTTPS. Make sure that HTTPS is enabled when you use the SDK for access.

```
req.setProtocol(ProtocolType.HTTPS);
```