

Alibaba Cloud KeyManagementService

Product Introduction

Issue: 20190916

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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid <i>Instance_ID</i></code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 What is KMS.....	1
2 Terms.....	4

1 What is KMS

Key Management Service (KMS) supports secure key creation and key management. KMS provides security practices such as key rotation. Other cloud services can be integrated into KMS to encrypt the user data that KMS manages. With KMS, you can focus on developing services such as data encryption, data decryption, and digital signature verification. It helps you save costs in maintaining the security, integrity, and availability of your keys.

Scenarios

User role	Scenario	KMS solution
Application and website developers	Application and website developers need to use keys and certificates to encrypt data and sign signatures. They need a secure and independent key management service which can enable their applications to securely access keys at any place . They want to keep plaintext keys confidential.	KMS uses the envelope encryption mechanism. Customer master keys (CMKs) are stored in KMS . Only ciphertext data keys are installed on user servers. When a server wants to decrypt a data key , it only needs to call the KMS service.
Service providers	Service providers need to encrypt and protect user data used in their services . Service providers want to focus on developing business functions. They do not want to spend additional time and costs in developing key management and distribution functions. In addition, customers want the data encryption and protection functions provided by service providers to be manageable and reliable.	<ul style="list-style-type: none"> · Administrators (users): use KMS to generate keys and manage the lifecycle of keys, and use Resource Access Management (RAM) to manage access permissions to keys. · Service providers: integrate the KMS API into their services and use user-specified keys to encrypt data. · Auditors (users): use ActionTrail to audit activities of accessing keys managed in KMS.

User role	Scenario	KMS solution
Chief security officers (CSOs)	CSOs want their key management services to comply with the security requirements and regulations of their enterprises. They want to implement key usage authorization. All key usage activities must be audited.	<ul style="list-style-type: none"> • KMS provides managed Hardware Security Modules (HSMs). Managed HSMs are authority-certified third-party devices running in an approved security mode. You can use managed HSMs to generate keys, or import keys to managed HSMs to protect the keys. • KMS is integrated with Resource Access Management (RAM) to implement unified authentication and authorization.

Benefits

Benefit	Traditional key management solution	KMS solution
Cost-effectiveness	The hardware and software costs for key management are high. For hardware, you have to purchase key management devices and build a physical environment. For software, you have to create and maintain key management regulations.	KMS is billed based on the actual usage with a customer favored price.
Easy to use	<ul style="list-style-type: none"> • No standard connector is provided for calling the functions of key management devices. • It is complex to establish and maintain encrypted connections. 	<ul style="list-style-type: none"> • KMS provides a unified and easy-to-use API for you to call all the functions. • KMS uses the standard HTTPS protocol.

Benefit	Traditional key management solution	KMS solution
Reliability	Typically, data is backed up on local devices to guarantee high reliability.	KMS uses distributed systems and HSMs to guarantee high reliability.

2 Terms

This topic describes the terms used in KMS.

Term	Full name	Definition
KMS	Key Management Service	The key management service provided by Alibaba Cloud.
Envelope encryption	-	The practice of encrypting plaintext by using a unique DK, which is then encrypted with CMK. The EDK is stored and transferred directly over unsecured communication processes. You need to retrieve the EDK only when you need it.
CMK	Customer Master Key	The master key created by a user in KMS. It is used to encrypt DKs and generate EDKs, as well as to encrypt a small amount of data.
EDK and DK	Enveloped Data Key and Data Key	DK is the plaintext key used to encrypt data. EDK is the ciphertext key generated by using envelope encryption.