ALIBABA CLOUD

阿里云

专有云企业版

密钥管理服务

产品简介

产品版本：V3.15.0

文档版本：20210726

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.什么是密钥管理服务

密钥管理服务KMS（Key Management Service）是您的一站式密钥管理和数据加密服务平台，提供简单、可靠、安全、合规的数据加密保护能力。KMS帮助您极大的降低在密码基础设施和数据加解密产品上的采购、运维、研发开销，帮助您更好的关注业务的发展。

KMS支持的功能如下：

- 加密密钥的托管

  KMS为您提供加密密钥的托管功能，KMS托管的加密密钥叫做用户主密钥CMK（Customer Master Key）。您可以对CMK进行生命周期管理（启用或禁用CMK）。

- 自带密钥（BYOK）

  KMS支持自带密钥BYOK（Bring Your Own Key）。您可以将密钥租借给KMS用作云上数据的加密保护，从而更好的管理密钥。可租借的密钥包括以下两种：

  - 线下密钥管理基础设施KMI（Key Management Infrastructure）中的密钥
  - 在加密服务中自主管理的HSM中的密钥

  > **说明** 通过安全合规的密钥交换算法，导入到KMS的托管密码机中的密钥不会被任何机制所导出，密钥明文不会被操作者或任何第三者查看。

- 自动轮转加密密钥

  KMS支持同一个CMK有多个密钥版本，每个版本为一个独立的密钥，各个版本互不相关。在多版本的基础上，KMS内建了加密密钥的自动轮转能力，帮助您实现安全最佳实践并满足合规审计要求。详情请参见 *用户指南* 手册 *密钥的轮转* 章节中的 *密钥轮转概述* 和 *自动轮转密钥* 。

- 全托管密码机

  KMS提供了全托管的密码机，您可以将密钥托管在密码机中，密码运算仅在密码机内部进行，从而保证密钥的安全性。

  > **说明** 全托管密码机需要额外购买硬件安全模块（HSM），并且购买KMS高级版本的License。

- 简化的密码运算API
  - KMS提供了简化的密码运算API，相比于传统密码模块或密码软件库的API更简单易用。
  - KMS的加密密钥支持可认证的加密，通过传入额外认证数据AAD（Additional Authenticated Data）保护数据的完整性。详情请参见 *用户指南* 手册 *使用对称密钥* 章节中的 *EncryptionContext说明* 。

- 主密钥别名

  KMS支持为主密钥创建别名，通过别名可以更方便的使用主密钥。详情请参见 *用户指南* 手册中的 *别名使用说明* 。例如：您可以通过主密钥别名在特定场景下实现人工轮转主密钥。

- 资源标签

  KMS支持资源标签，通过资源标签您可以更方便的管理KMS中的密钥资源。

2.产品优势

密钥管理服务KMS（Key Management Service）与传统密钥管理设施（KMI）相比具有多集成、易使用等优势。

多集成

KMS和ECS、RDS、OSS等多个产品无缝集成。通过一方集成，您可以很容易的使用KMS主密钥加密和控制您存储在这些服务中的数据，帮助您保持对云上计算和存储环境的控制。

易使用

- 轻松实现加密

  KMS提供简单的密码运算API，简化和抽象了密码学概念，让您可以轻松的使用API完成数据的加解密。对于需要密钥层次结构的应用，KMS提供了方便的信封加密能力，快速实现密钥层次结构。例如：生成一个数据密钥，并将主密钥（CMK）用作密钥加密密钥KEK（Key Encryption Key）来保护数据密钥。详情请参见 *技术白皮书* 手册中 *功能原理* 章节的 *信封加密技术* 。

- 集中的密钥托管

  密钥管理服务为您提供对密钥的集中化托管与控制。

  您可以从线下密钥管理基础设施（KMI）或在加密服务中创建的HSM中将密钥导入到KMS。无论在KMS内创建的密钥还是外部导入的密钥，密钥中的机密信息或者敏感数据都会被阿里云上的其他云产品用于加密保护。

- 支持自带密钥（BYOK）

  KMS支持自带密钥BYOK（Bring Your Own Key）。您可以将密钥租借给KMS用作云上数据的加密保护，从而更好的管理密钥。可租借的密钥包括以下两种：

  - 线下密钥管理基础设施KMI（Key Management Infrastructure）中的密钥
  - 在加密服务中自主管理的HSM中的密钥

  > **说明** 通过安全合规的密钥交换算法，导入到KMS的托管密码机中的密钥不会被任何机制所导出，密钥明文不会被操作者或任何第三者查看。

- 自定义密钥轮转策略

  KMS允许您根据所需的安全策略来自动轮转对称加密密钥。您只需要为主密钥（CMK）配置一个自定义的轮转周期，KMS会自动为您生成新的加密密钥版本。一个主密钥可以有多个密钥版本，其中每个版本可以被用来解密对应的密文数据，而最新的密钥版本（称为主版本）是活跃加密密钥，用于加密当前传入的数据。详情请参见 *用户指南* 手册 *密钥的轮转* 章节中的 *自动轮转密钥* 。

3.应用场景

密钥管理服务KMS（Key Management Service）具有广泛的应用场景，本文为您介绍KMS的应用场景。

典型场景

用户角色	诉求	典型场景
应用开发者	保证应用系统中敏感数据的安全。	作为开发者，我的程序需要使用一些敏感数据。我希望敏感数据被加密保护，而加密密钥则通过KMS来保护。

解决方案

- 信封加密

  使用信封加密技术将主密钥存放在KMS服务中，只部署加密后的数据密钥。仅在需要使用数据密钥时，调用KMS服务获取数据密钥的明文，用于本地加解密业务数据。

  信封加密详情，请参见 *技术白皮书* 手册中 *功能原理* 章节的 *信封加密技术* 。

- 直接加密

  您也可以直接调用KMS的加解密API，使用主密钥直接加密或解密敏感数据。

- 服务端加密

  如果您使用阿里云产品来保存数据，您可以使用云产品的服务端加密功能，更简单有效的对数据进行加密保护。例如：通过对象存储服务端加密，保护存储敏感数据的OSS桶或通过数据库透明数据加密（TDE），保护存储敏感数据的表。

4.基本概念

本文解释了密钥管理服务KMS（Key Management Service）的基本概念，帮助您正确理解和使用KMS。

> **说明** API接口详情，请参见 *开发指南* 手册中的 *API参考* 章节。

密钥管理服务KMS（Key Management Service）

KMS可以提供密钥的安全托管及密码运算等服务。KMS内置密钥轮转等安全实践，支持其它云产品通过一方集成的方式对其管理的用户数据进行加密保护。借助KMS，您可以专注于数据加解密、电子签名验签等业务功能，无需花费大量成本来保障密钥的保密性、完整性和可用性。

用户主密钥CMK（Customer Master Key）

用户主密钥主要用于加密保护数据密钥并产生信封，也可直接用于加密少量的数据。您可以调用KMS的CreateKey接口创建一个用户主密钥。

信封加密（Envelope Encryption）

当您需要加密业务数据时，您可以调用KMS的GenerateDataKey接口或GenerateDataKeyWithoutPlaintext接口生成一个对称密钥，同时使用指定的用户主密钥加密该对称密钥（被密封的信封保护）。在传输或存储等非安全的通信过程中，直接传递被信封保护的对称密钥。当您需要使用该对称密钥时，打开信封取出密钥即可。

信封加密详情，请参见 *技术白皮书* 手册中 *功能原理* 章节的 *信封加密技术* 。

数据密钥DK（Data Key）

数据密钥为加密数据使用的明文数据密钥。

> **说明** 您可以调用KMS的GenerateDataKey接口生成一个数据密钥，同时使用指定用户主密钥加密该数据密钥，返回数据密钥的明文（DK）和密文（EDK）。

信封数据密钥EDK（Enveloped Data Key/Encrypted Data Key）

信封数据密钥为通过信封加密技术保密后的密文数据密钥。

> **说明** 如果暂时不需要数据密钥的明文，您可以调用KMS的GenerateDataKeyWithoutPlaintext接口仅返回数据密钥密文。

硬件安全模块HSM（Hardware Security Module）

硬件安全模块也称为密码机，是一种执行密码运算、安全生成和存储密钥的硬件设备。KMS提供的托管密码机可以满足监管机构的检测认证要求，为用户在KMS托管的密钥提供更高的安全等级保证。

加密上下文（Encryption Context）

加密上下文是KMS对可认证加密AEAD（Authenticated Encryption with Associated Data）的封装。KMS将传入的加密上下文作为对称加密算法的额外认证数据AAD（Additional Authenticated Data）进行密码运算，从而为加密数据额外提供完整性（Integrity）和可认证性（Authenticity）的支持。详情请参见 *用户指南* 手册 *使用对称密钥* 章节中的 *EncryptionContext说明* 。