ALIBABA CLOUD

阿里云

密钥管理服务

产品简介

文档版本：20201228

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。

产品架构

KMS主要包含密钥服务和凭据管家两种业务组件。

业务组件	说明	参考文档
密钥服务	密钥服务提供密钥的全托管和保护，支撑基于云原生接口的极简数据加密和数字签名。	密钥服务概述
凭据管家	凭据管家为凭据提供托管加密、定期轮转、安全分发、中心化管理的能力，降低传统IT设施配置静态凭据带来的安全风险。	凭据管家概述

产品优势

选用KMS，您将具有数据加密和凭据保护相关优势。

功能	优势	说明	参考文档
数据加密	领先的安全合规能力	支持业界领先的密码安全基础设施，满足国内外对密码安全的等级和合规要求。	合规
	完全托管	您无需投资采购密码硬件、软件，无需投入密码设施的运维和研发，即可敏捷使用密码功能，并进行功能扩展。	使用托管密码机
	云原生优势	基于云原生极简设计的接口，支持广泛的云产品集成，支持一键配置服务端加密数据。	支持服务端集成加密的云服务
	极简应用接入	支持KMS SDK、加密SDK等多种方式，帮助您使用KMS加密API，快速满足数据加密解密、数字签名验签业务的多样性需求。	• Java SDK示例 • 加密SDK快速入门
	中心化规模化管理	支持自动开通KMS服务，支持ROS、Terraform等产品，帮助您在多账号登录时自动化实施默认加密策略，对云服务器ECS（云盘）、对象存储OSS 、关系型数据库RDS、大数据计算MaxCompute等产品自动开启服务端加密。	通过API开通
	云原生优势	原生集成支持RDS动态凭据，帮助您有效应对数据库安全面临的主要威胁。	动态RDS凭据概述

功能	优势	说明	参考文档
凭据保护	极简应用接入	支持KMS SDK、凭据管家客户端、Kubernetes插件等多种方式，帮助您使用动态凭据。	应用程序接入凭据管家
	中心化规模化管理	支持自动开通KMS服务，支持ROS、Terraform等产品。帮助您实现数据库、OSS Bucket等云资源的运维编排和凭据安全托管的自动化管理，从而实现中心化的凭据管理。	通过API开通

相关文档

- 产品优势
- 应用场景
- 基本概念
- 使用限制
- 计费说明
- 入门概述

2.产品优势

密钥管理服务（KMS）与传统密钥管理设施（KMI）相比具有多集成、易使用、高可靠以及低成本等优势。

多集成

- 身份认证与访问控制

  KMS借助于身份认证机制（AccessKey）来鉴别请求的合法性，KMS还通过与访问控制（RAM）集成，允许您配置多样化的自定义策略，满足不同的授权场景。任何请求仅由合法用户发起且满足RAM对权限的动态检测（基于属性的访问控制，简称ABAC），才能被KMS接受。详情请参见使用RAM实现对资源的访问控制。

- 审计密钥的使用

  KMS通过与操作审计（ActionTrail）集成，可以查看近期KMS的使用状况，也可以将KMS使用情况存储到OSS等其他云服务中，满足更长周期的审计需求。详情请参见使用操作审计查询密钥管理服务的操作事件。

- 控制云产品集成加密

  KMS和阿里云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，而您只需要付出密钥的管理成本，无需实现复杂的加密能力。同时集成加密解决了其他云产品中原生数据的加密保护问题。详情请参见服务端集成加密概述和支持服务端集成加密的云服务。

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：生成一个数据密钥，并将主密钥（CMK）用作密钥加密密钥（Key Encryption Key，简称KEK）来保护数据密钥。详情请参见什么是信封加密？

- 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。

  - 您可以随时创建新的用户主密钥，并通过访问控制（RAM）轻松管理谁可以访问该密钥
  - 您可以通过操作审计（ActionTrail）审核密钥的使用情况。
  - 您可以从线下密钥管理基础设施（KMI）或在阿里云加密服务中创建的HSM里将密钥导入到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）

  MS支持自带密钥（Bring Your Own Key，简称BYOK）。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（Key Management Infrastructure，简称KMI）里的密钥
  - 在阿里云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。详情请参见导入密钥材料和保持对密钥的控制。

- 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。详情请参见自动轮转密钥。

高可靠、高可用、可伸缩

作为全托管的分布式服务，KMS在每个地域构建了多可用区冗余的密码计算能力，保证阿里云上各个产品和您的自定义应用向KMS发起的请求可以得到低延迟处理。您可以根据需要，在不同地域的KMS创建足够的密钥，而不必担心底层设施的扩容或缩容。

安全与合规能力

KMS经过严格的安全设计和审核，保证您的密钥在阿里云得到最严格的保护。

- KMS仅提供基于TLS的安全访问通道，并且仅使用安全的传输加密算法套件，符合PCI DSS等安全规范。
- KMS提供了监管机构许可和认证的密码设施。根据地域分布，分别提供了经国家密码管理局检测和认证的硬件密码设备，取得了FIPS 140-2第三级认证和运行在FIPS许可的第三级模式下的密码设备。详情请参见合规。
- KMS使用硬件安全模块来托管密钥，从而达到更高的安全标准，详情请参见托管密码机概述。

低成本

使用KMS，您可以按需使用和付费。

- 您无需支付采购硬件密码设备的初始成本以及对硬件系统进行运维、修补、老旧替换的持续开销。
- KMS为您节省了搭建具有可用性和可靠性密码设备集群，以及自建密钥管理设施的研发成本和维护开销。
- KMS与其他产品的集成为您节省了研发数据加密系统的开销，仅需通过管理密钥而获得可控的云上数据加密的能力。

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常见的应用场景。

典型场景

用户角色	诉求	典型场景	解决方案
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的业务数据和运行数据。我希望敏感数据被加密保护，而加密密钥则通过KMS来保护。	敏感数据加密保护
IT运维人员	为部署在云上的IT设施提供安全的环境。	云上的IT设施与其他租户共享，我无法像传统自建机房那样，在云上建立物理的安全边界。但是我仍然需要为云上的计算与存储托管环境构建一套可信、可见及可控的安全机制。	控制云上计算与存储环境
首席安全官	保证信息系统的安全与合规。	作为首席安全官（CSO），我既需要满足一些合规标准中对密钥管理的直接要求，也需要利用密码技术去满足更多针对应用和信息系统安全的要求。	信息系统满足合规要求
服务提供商	使用第三方加密作为服务的安全能力。	作为ISV服务提供商，用户要求我们加密保护ISV服务中的用户数据。 • 我们专注于服务的业务功能开发，不希望重复实现密钥的管理和分发功能。 • 用户希望我们提供的数据加密保护能力是可控、可信的。	ISV的第三方加密方案

敏感数据加密保护

您可以通过数据加密，保护云上产生或存储的敏感数据。阿里云支持您通过多种方式实现对敏感数据的加密保护。

加密保护方式	说明	参考文档
信封加密	使用信封加密技术将主密钥存放在KMS中，只部署加密后的数据密钥。仅在需要使用数据密钥时，使用KMS获取数据密钥的明文，用于本地加解密业务数据。 您也可以使用封装了信封加密的加密SDK进行加密保护。	• 什么是信封加密？ • 使用KMS信封加密在本地加密或解密数据 • 加密SDK快速入门
直接加密	调用KMS的加密API，使用主密钥直接加密敏感数据。	使用KMS主密钥在线加密和解密数据
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，更有效地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。	支持服务端集成加密的云服务

加密保护方式	说明	参考文档
使用凭据管家	您可以将口令、Token、SSH Key、AK等敏感数据托管到凭据管家，通过安全的接入方式进行管理。您也可以动态轮转凭据，避免数据泄露风险。	• 凭据轮转 • 动态RDS凭据概述

控制云上计算与存储环境

通过云产品集成KMS加密（服务端集成加密）的方式，阿里云为您提供了控制云上计算与存储环境的能力，在分布式多租户系统中隔离保护您的计算与存储资源。您可以通过控制KMS主密钥的生命周期、使用状态或访问控制的权限策略，控制分布式计算环境或存储环境。您也可以配合操作审计服务，检查与审计KMS密钥的使用情况。控制云上计算与存储环境有以下几种常见应用场景：

应用场景	说明	参考文档
云服务器ECS场景	通过授权ECS使用KMS密钥，帮助ECS加密保护系统盘、数据盘、快照及镜像。例如：启动ECS实例需要同时解密系统盘和数据盘，从加密盘制作的快照也需要被加密。增加的这些限制措施，使ECS实例和存储资源的使用，都通过KMS得到了安全加固。	加密概述
持久化存储场景	阿里云提供的持久化存储类服务（例如：RDS、OSS或NAS等），通过分布式多冗余的方式，保证数据存储的可靠性。这些服务通过集成KMS对数据进行落盘前的加密，让您获得对分布式系统中数据冗余的可控与可见性，即任何读取的请求都需要首先经过KMS对数据进行解密。	无
其他计算与存储场景	多种云服务均支持服务端集成加密。	支持服务端集成加密的云服务

信息系统满足合规要求

企业或者组织在评估合规标准对密码技术的要求时，可能会遇到以下两种情况：

- 合规规范要求使用密码技术对信息系统进行保护，并且所使用的密码技术必须满足特定的技术标准和安全规范。
- 合规规范对密码技术并不强制要求使用，但使用密码技术会对加快满足合规的过程。例如：在打分制的规范中获得更多的得分点。

KMS提供以下方面的能力，帮助企业满足合规要求：

功能	说明	参考文档
密码合规	KMS支持托管密码机。托管密码机使用了通过监管机构认证的第三方硬件设备，在许可的安全模式下运行。针对不同市场，托管密码机分别获得了国密局的检测和认证，以及FIPS 140-2第三级的检测认证。	• 托管密码机概述 • 使用托管密码机
密钥轮转	KMS内置了加密密钥的自动轮转功能，企业可以自定义轮转策略，快速满足数据安全规范和最佳实践。	• 密钥轮转概述 • 自动轮转密钥
凭据轮转	通过使用凭据管家，轻松满足对口令、访问密钥等凭据的轮转要求，同时带来高效而可靠的数据泄露应急处理能力。	凭据轮转

功能	说明	参考文档
数据保密性	通过KMS对个人隐私进行加密保护，防止个人隐私在攻击场景下泄露，满足数据保护相关法律法规要求。	无
数据完整性	通过和日志服务、操作审计服务的集成，对云上日志进行防止篡改的加密保护，同时满足对日志数据的保密性和完整性保护。	无
身份认证和访问控制	KMS通过接入访问控制（RAM），实现统一的认证和授权管理。	使用RAM实现对资源的访问控制
审计密钥的使用	KMS将所有的API调用记录存储到操作审计（ActionTrail），操作审计可以对密钥的使用情况进行合规性审计。	使用操作审计查询密钥管理服务的操作事件

ISV的第三方加密方案

如果您是ISV服务提供商，您可以集成KMS，将KMS作为第三方的数据安全解决方案，保护您提供的服务中的用户数据。通过允许用户在KMS中管理密钥，并授权ISV服务使用这些密钥，KMS充当了ISV服务和用户中间的第三方安全保护机制，用户和ISV服务可以各司其职，共同保证系统的安全性。

用户角色	说明	参考文档
用户的管理员	在KMS中生成密钥并管理密钥的生命周期。在访问控制（RAM）中管理密钥使用的权限，通过跨阿里云账号的资源授权等方式，允许ISV服务使用KMS中的指定密钥。	跨阿里云账号的资源授权
ISV服务	通过集成KMS的API使用用户指定的密钥，对ISV服务中的数据进行加密保护。	API概览
用户的审计员	通过操作审计（ActionTrail），对ISV服务每次访问KMS使用密钥的行为进行事后审计。	使用操作审计查询密钥管理服务的操作事件

4.基本概念

本文罗列了密钥管理服务（KMS）的基本概念。

密钥管理服务（Key Management Service，简称KMS）

阿里云提供的密钥管理服务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（Customer Master Key，简称CMK）

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API CreateKey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API GenerateDataKey或GenerateDataKeyWithoutPlaintext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。详情请参见什么是信封加密？

数据密钥（Data Key，简称DK）

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API GenerateDataKey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（Enveloped Data Key/Encrypted Data Key，简称EDK）

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API GenerateDataKeyWithoutPlaintext仅返回数据密钥密文。

硬件安全模块（Hardware Security Module，简称HSM）

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。详情请参见托管密码机概述。

加密上下文（Encryption Context）

加密上下文是KMS对可认证加密（Authenticated Encryption with Associated Data，简称AEAD）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（Additional Authenticated Data，简称AAD）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。详情请请见EncryptionContext说明。

5.使用限制

本文为您介绍密钥管理服务KMS（Key Management Service）的使用限制。

KMS是一个区域化的服务，在不同地域的使用限制相对独立。KMS支持的地域详情，请参见请求结构。

资源配额

KMS设置了资源配额，为您提供快速而具有弹性的服务。某些资源配额只适用于您创建的资源，而不适用于阿里云产品为您创建的资源。如果您使用的资源不属于您的云账户，那么这些资源不会计入相应配额。

如果已达到资源限制，那么创建该资源类型的其他请求会生成 `Rejected.LimitExceeded` 错误消息。

下表列出了每个阿里云账户和地域中的KMS资源配额。如果您有提高数量限制的需求，可以提交工单申请。

资源类型	默认配额	配额说明
用户主密钥（CMK）	200	同一地域内创建的CMK总数
别名	300	同一地域内创建的别名总数
CMK的密钥版本	10000	同一地域内创建的所有CMK中的密钥版本总数

请求配额

KMS对每秒请求的API操作数量设置了配额。超过API请求配额后，KMS会限制请求（即拒绝本来有效的请求），并返回类似以下的错误响应。针对此类可通过重试解决的错误类型，可以在应用中引入请求的退避和重试策略，详情请参见使用指数退避方法对请求错误进行重试。

```
{
 "HttpStatus": 429
 "Code": "Rejected.Throttling"
 "Message": "QPS Limit Exceeded"
 "RequestId": "e85db688-a2d3-44ca-9790-4259********"
}
```

下表列出了每个阿里云账户和地域中的KMS请求配额。如果您有提高数量限制的需求，可以提交工单申请。

密钥每秒默认请求配额

CMK的规格	创建操作	密码运算操作	只读操作	写操作
`Aliyun_AES_256` `Aliyun_SM4`	10	750	20	10
`RSA_2048`	10	200	20	10

CMK的规格	创建操作	密码运算操作	只读操作	写操作
EC_P256 EC_P256K EC_SM2	10	200	20	10

说明 密钥的默认请求配额按照操作类型分组，每一个分组内的所有接口共享这一分组的请求配额。每个分组定义如下：

- 创建操作：包含CreateKey接口，请参见CreateKey。
- 密码运算操作：包含对应密钥规格支持的密码运算接口，请参见API概览。
- 只读操作：包含与CMK、别名、CMK标签相关，不改变资源元数据、属性或状态的操作。
- 写操作：包含与CMK、别名、CMK标签相关，改变资源元数据、属性或状态的操作。