阿里云
密钥管理服务

产品简介

文档版本：20190916

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
	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。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能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，恢复业务所需时间约10分钟。
	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。	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。	单击 确定。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	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。	`swich` *`{stand | slave}`*

目录

1 什么是密钥管理服务

密钥管理服务（Key Management Service，简称KMS）提供密钥的安全托管、密码运算等服务。它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。

使用场景

角色	场景	KMS的解决方案
应用/网站开发者	作为应用/网站开发者，我的程序需要使用密钥、证书用于加密或签名。我希望密钥管理功能是安全且独立的，无论我的应用部署在哪里，都能安全访问到密钥。我绝不接受把明文的密钥到处部署，这太危险了。	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。仅在需要使用解密数据密钥时，调用KMS服务。
服务提供商	作为服务提供商，用户要求我们加密保护服务中的用户数据。一方面，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；另一方面，用户也希望我们提供的数据加密保护能力是可控、可信的。	· 用户的管理员：在KMS中生成密钥，并且管理密钥的生命周期；在访问控制服务（RAM）中管理密钥使用的权限。 · 服务提供商：通过集成KMS的API，允许用户使用自选密钥，对服务中的数据进行加密保护。 · 用户的审计员：通过操作审计服务（ActionTrail），对服务提供商每次访问KMS使用密钥的行为进行事后审计。

角色	场景	KMS的解决方案
首席安全官（CSO）	作为首席安全官（CSO），我希望公司的密钥管理能满足合规需求。我需要确保密钥都被合理地授权，任何使用密钥的情况都必须被审计。	· KMS服务提供了托管密码机。托管密码机使用通过监管机构认证的第三方硬件设备，运行在许可的安全模式下。用户可以使用托管密码机创建密钥，或将密钥导入到托管密码机中，保证密钥的安全性。 · KMS通过接入RAM服务，实现统一的认证和授权管理。

产品优势

优势	传统密钥管理方案	KMS
低成本	采购安全的密钥管理设备、建设安全的物理环境都需要很高的硬件成本，设计和执行安全的密钥管理规范需要很高的软件成本。	按需收费，且价格低廉。
易用	· 硬件设备API缺乏标准，晦涩难用。 · 信道安全的方案和配置繁琐。	· 统一、易用的API 。 · 标准的HTTPS协议。
可靠	通常使用离线备份方案实现高可靠。	分布式系统与密码硬件设备结合，实现高可靠。

2 使用限制

本文为您介绍密钥管理服务（KMS）的使用限制。

KMS是一个区域化的服务。KMS在不同地域的使用限制是相对独立的。关于KMS的开服地域详情，请参见#unique_5。

用户主密钥（Customer Master Key）数量限制

每个用户在每个地区最多可以创建200个用户主密钥。

如果用户有提高数量限制的需求，可以提交工单申请。

用户别名（Alias）数量限制

每个用户在每个地区最多可以创建300个别名。

如果用户有提高数量限制的需求，可以提交工单申请。

3 基本概念

本文为您介绍密钥管理服务（KMS）的基本概念。

术语	全称	概念
KMS	密钥管理服务	阿里云提供的密钥管理服务
Envelope Encryption	信封加密	为要加密的数据产生一次一密的对称密钥。使用特定的主密钥加密该对称密钥，使这个对称密钥处于一种被密封的信封保护的状态。在传输、存储等非安全的通信过程中，直接传递被密封保护的密钥。当且仅当要使用该对称密钥时，打开信封取出密钥。
CMK	用户主密钥	用户在阿里云密钥管理服务中创建的主密钥。主要用于加密保护数据密钥，产生信封，也可直接用于加密少量的数据。
EDK/DK	信封数据密钥/数据密钥	DK为加密数据使用的明文数据密钥。EDK为通过信封加密技术保密后的密文数据密钥。