密钥管理服务

产品简介

产品简介

密钥管理服务（Key Management Service，简称：KMS）是阿里云提供的一款安全、易用的管理类服务。用户无需花费大量成本来保护密钥的保密性、完整性和可用性，借助密钥管理服务，用户可以安全、便捷的使用密钥，专注于开发加解密功能场景。

KMS要解决的主要需求

角色	问题	KMS如何解决
应用/网站开发者	我的程序需要使用密钥、证书用于加密或者签名，我希望密钥管理的功能是安全且独立的。不论我的应用部署在哪里，都能安全的访问到密钥。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，主密钥存放在KMS服务中，只部署加密后的数据密钥，仅在需要使用时调用KMS服务解密数据密钥
服务开发者	我不想承担客户密钥、数据的安全责任。我希望用户自己管理他的密钥；在拥有授权的情况下，我会使用用户指定的密钥加密他的数据。这样，我就能专注于服务功能的开发	基于信封加密技术以及KMS开放的API，服务能够集成KMS，使用用户指定的主密钥完成数据密钥的加解密，能够轻松的实现**明文不落盘**的要求，也不用为管理用户的密钥而犯愁
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的授权，任何使用密钥的情况都必须被审计	KMS服务接入RAM服务实现统一的授权管理

密钥管理服务（KMS）是一个区域化的服务，对于每个用户，在不同的地区的KMS资源与使用限制是相对独立的。目前已经支持的地区共有五个：新加坡、华东1、华东2、华北2、华南1。

用户主密钥(Customer Master Key)数量限制

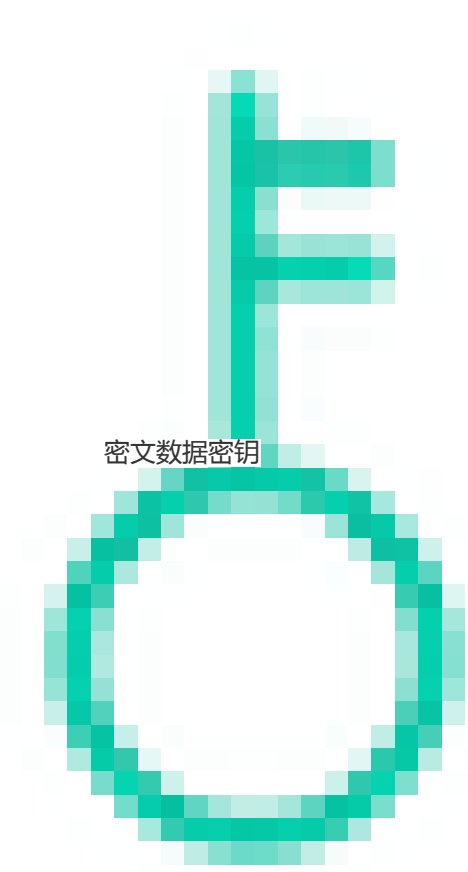
每个用户，在每个地区，最多可以创建200个用户主密钥。

如果用户有提高数量限制的需求，可以通过工单系统向我们提交申请。

优势	传统密钥管理方案	使用密钥管理服务

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。

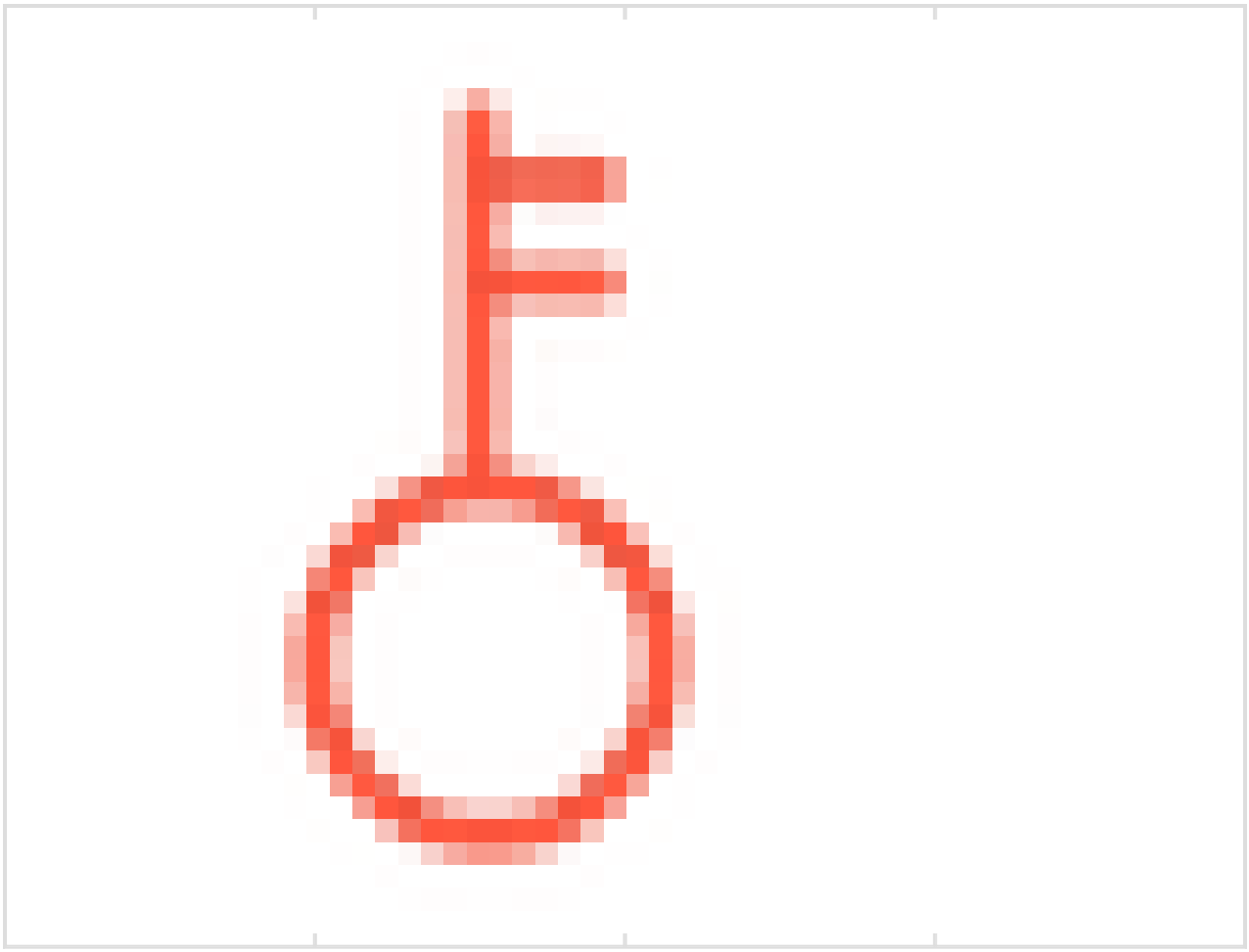
图例说明

图例	含义	图例	含义
 用户主密钥（CMK）	 密文数据密钥		
	明文证书		明文文件

密文证书

密文文件

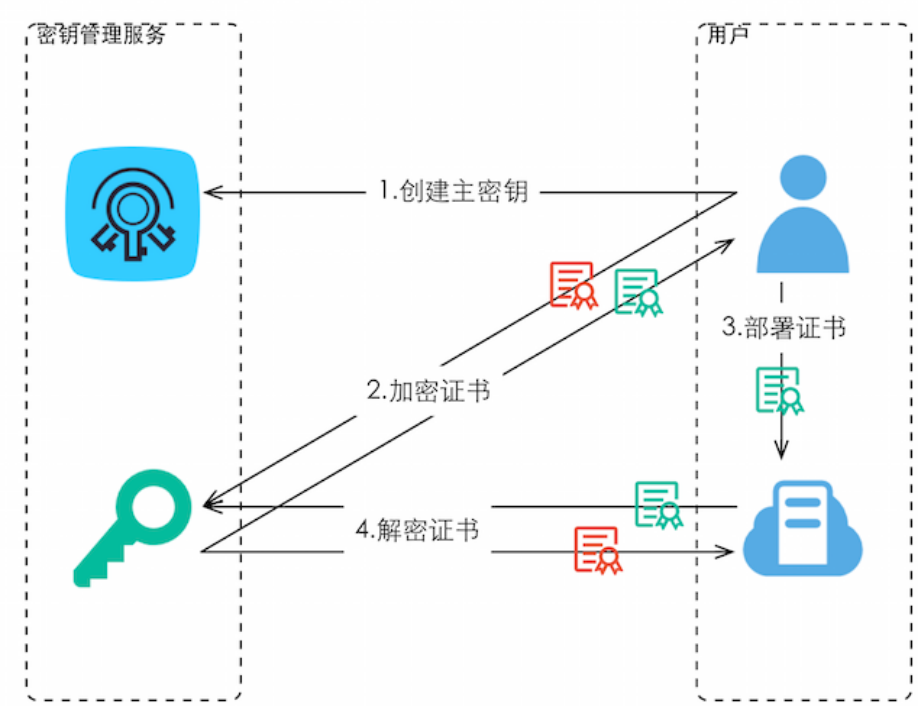
明文数据密钥



直接使用KMS加密、解密

用户可以直接调用KMS的API，使用指定的CMK来加密、解密数据。这种场景适用于少量（少于4KB）数据的加解密，用户的数据会通过安全信道传递到KMS服务端，对应的结果将在服务端完成加密、解密后通过安全信道返回给用户。

场景举例：保护服务器HTTPS证书



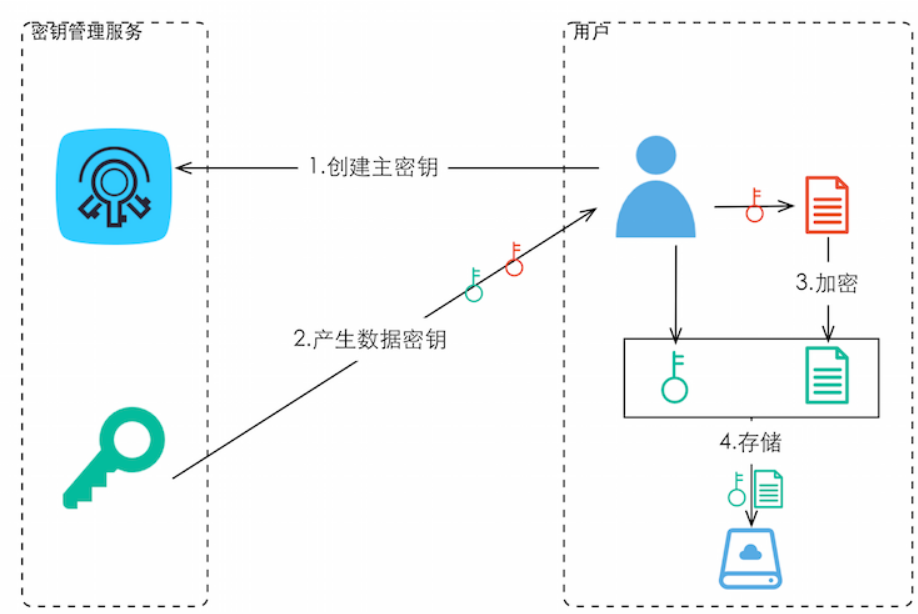
流程：

1. 首先用户需要创建一个主密钥。
2. 调用KMS服务的Encrypt接口将明文证书加密为密文证书。
3. 用户在服务器上部署密文证书。
4. 当服务器启动需要使用证书时，调用KMS服务的Decrypt接口，将密文证书解密为明文证书。

使用信封加密在本地加密、解密

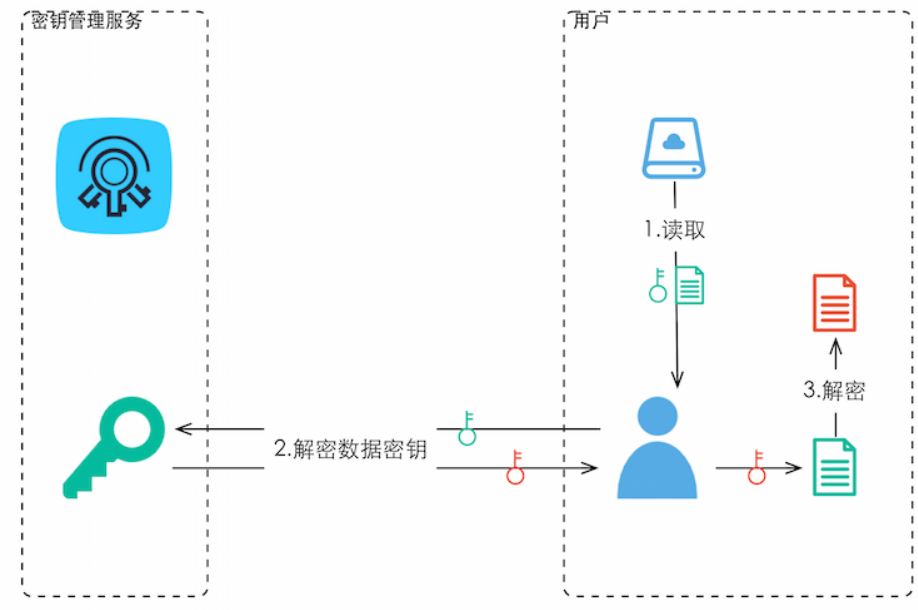
用户可以直接调用KMS的API，使用指定的CMK来产生、解密数据密钥，自行使用数据密钥在本地加解密数据。这种场景适用于大量数据的加解密，用户的数据无需通过网络传输大量数据，可以低成本的实现大量数据的加解密。

场景举例：加密本地文件



加密流程：

1. 首先用户需要创建一个主密钥。
2. 调用KMS服务的GenerateDataKey接口，产生数据密钥。这里用户能够得到一个明文的数据密钥和一个密文的数据密钥。
3. 用户使用明文的数据密钥，加密文件，产生密文文件。
4. 用户将密文数据密钥和密文文件一同存储到持久化存储设备或服务中。



解密流程：

1. 用户从持久化存储设备或服务中读取密文数据密钥和密文文件。
2. 调用KMS服务的Decrypt接口，解密数据密钥，取得明文数据密钥。

3. 使用明文数据密钥解密文件。

注意事项：

1. 验证阿里云服务端的HTTPS证书，防止钓鱼者窃取您的信息。
2. 推荐使用RAM服务子账号功能，实现最小权限原则。

发布时间	发布版本	发布内容
2016年4月6日	1.0	密钥管理服务公测
2016年5月19日	1.1	增加三个地域支持（华北2、华东2、华南1）
2016年6月22日	1.2	支持密钥禁用、启用功能
2016年8月10日	1.3	性能优化，部分错误返回修改；加解密API支持Encryption Context
2016年9月20日	1.4	性能优化；增加密钥删除有关的API： ScheduleKeyDeletion 和 CancelKeyDeletion
2016年11月29日	1.5	性能优化；增加四个地域支持：亚太东北(日本)、欧洲中部(法兰克福)、中东东部(迪拜)、 亚太东南(悉尼)
2017年1月22日	1.6	性能优化；增加地域支持：香港
2017年3月1日	1.7	性能优化
2017年5月10日	1.8	4月25日中文站正式商业化；增加地域支持：华北3；性能优化
2017年6月5日	1.9	增加API: DescribeRegions；SDK更新至2.4.0

这些名词是密钥管理服务的关键概念。

术语	全称	中文	概念
KMS	Key Management Service	密钥管理服务	阿里云计算提供的密钥管理服务
envelope encryption	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	Customer Master Key	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	EnvelopedDataKey / DataKey	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