ALIBABA CLOUD

阿里云

密钥管理服务

常见问题

文档版本：20200929

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

1.什么是信封加密？

信封加密是类似数字信封技术的一种加密手段。这种技术将加密数据的数据密钥封入信封中存储、传递、和使用，不再使用主密钥直接加解密数据。

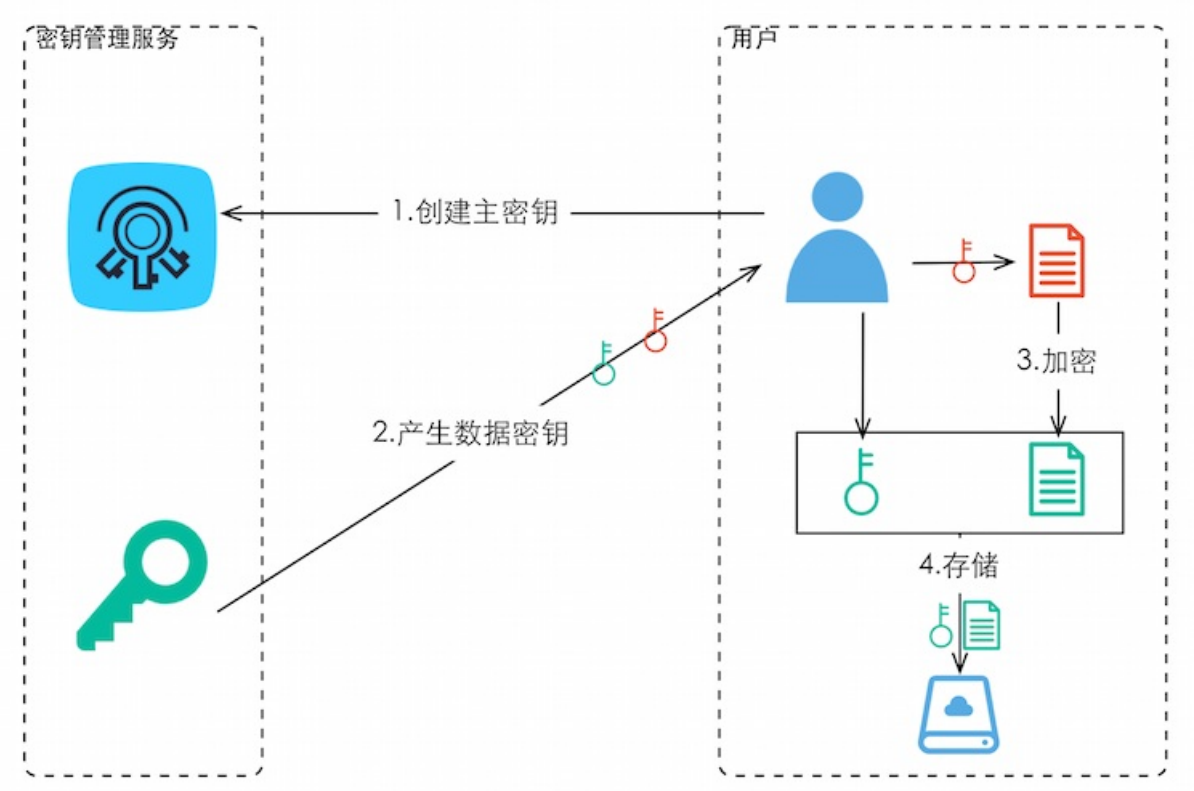
直接的加解密服务不适合云场景

由云服务直接为用户加解密数据存在以下问题：

- 安全性隐患
  - 通过因特网将敏感信息从客户手中传递到服务的过程中会存在诸多风险，例如：窃听、钓鱼。
- 信任和可信证明难做
  - 用户不一定信任云服务，愿意上传如此敏感的数据。
  - 云服务也难以证明自己不会误用和泄露这些数据。
- 性能差、成本高
  - 大量数据需要通过安全信道传递到服务端，加密后再返回给用户。对用户服务的性能影响很大。
  - 我们都知道，在分布式系统中，我们应该尽可能的移动计算而不是移动数据，大量的移动数据会带来巨大的成本。

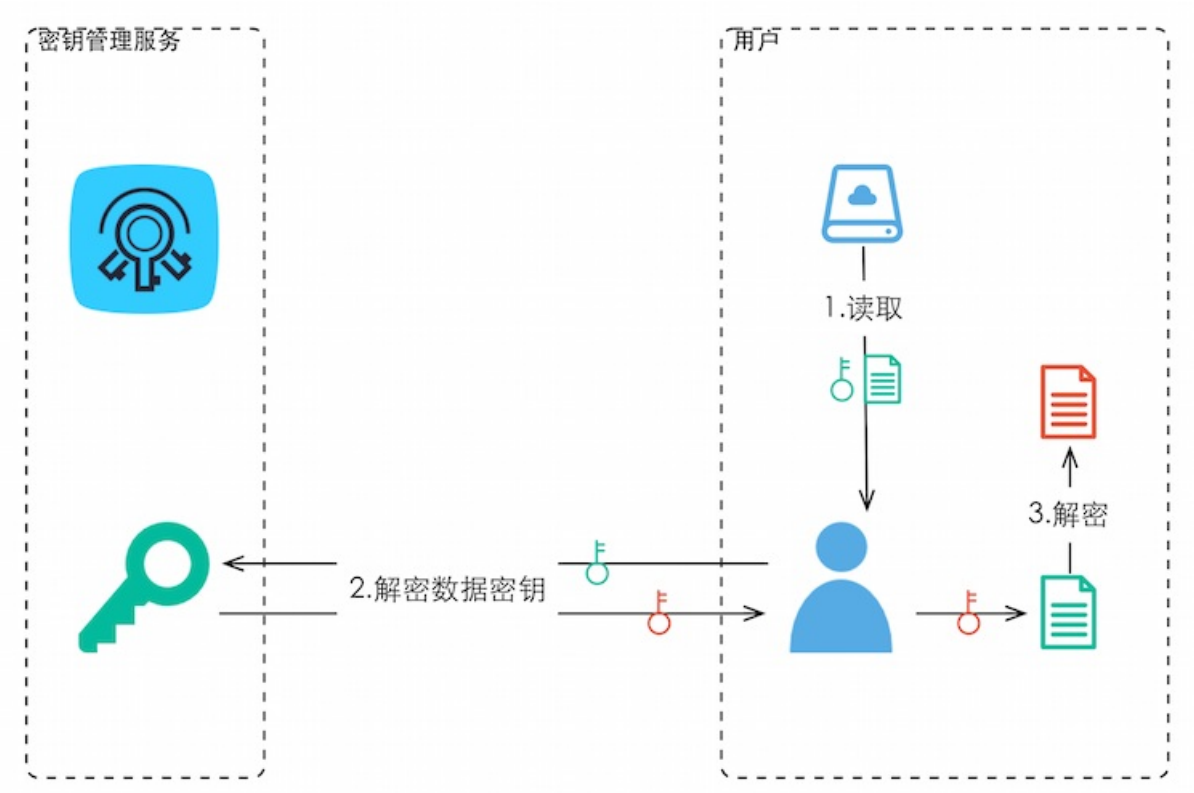
信封加密场景：加密本地文件

图例	含义
	用户主密钥
	明文数据密钥
	密文数据密钥
	明文文件
	密文文件



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。

2.解密时为何出现 Forbidden.KeyNotFound 的错误？

解密时出现上述错误提示，通常是因为您解密时访问了错误的地域。

由于各个地域的密钥管理服务是完全独立的，请您确保解密时访问的地域与加密时一致。

3.密钥管理服务的端点为何无法访问？

密钥管理服务的端点无法访问，通常是因为在使用 SDK 访问密钥管理服务时，未启用 HTTPS 协议。

为了确保您的数据安全，密钥管理服务**仅支持** HTTPS 协议。因此在使用 SDK 访问密钥管理服务时，确保启用 HTTPS 协议。

```
req.setProtocol(ProtocolType.HTTPS);
```