密钥管理服务

常用方案

产品文档

腾讯云

文档目录

常用方案
敏感信息加密

最近更新时间：2018-06-13 15:29:44

简介

数据加密是密钥管理服务最核心的能力，实际应用中主要用来保护服务器硬盘上的敏感信息的安全，比如密钥、证书、配置文件。

敏感信息举例

	密钥，证书	后台配置文件
用途	加密业务数据，通信通道，数字签名	保存系统架构和其他业务信息，比如数据库IP、密码
丢失风险	保密信息被盗、加密通道遭监听、签名被伪造	业务数据被拖库、成为攻击其他系统的跳板

提前规划安全性

敏感信息是访问企业更高机密以及安全通道的钥匙，它本身的安全性尤为重要，所以在公司业务发展的阶段就应该规划其安全性。一个最基本的保护方法就是不要在云服务器硬盘上**明文放置敏感信息**，而是通过密钥管理服务将它们加密后放置，使用时再解密到内存，保证**明文不落盘**。
这样的好处是即使云服务器因为个人疏忽而遭受不明人员访问，也无法被直接获取明文敏感信息。对于攻击者来说，获取密文信息后还需要再推测密文文件用途、获取解密访问权限以及编写解密程序，这些将大大提高获取明文信息的难度和被发现的可能性。

为什么腾讯云不直接保存您的敏感信息？

安全性提升一个很重要的举措就是权限分离，比如信息的持有权和信息的加密权限分离，将持有权握在自己手上，而腾讯云负责加密相关操作和权限控制，是一种实现简单但有效的安全性提升方法。

举例：保护后台应用配置文件

简要步骤如下

1. 准备工作
   - 一台云服务器（CVM）
   - 一个您熟悉的后台服务框架并部署到云服务器（比如Python）
   - 业务使用到的后台应用配置文件，比如一个配置了数据库IP 和密码的文件
   - 创建一个KMS 主密钥，保持启用状态并注意所在地域，可以通过控制台或云API 来完成

2. 生成密文配置文件

   方法1：通过在线工具生成

   方法2：使用KMS SDK 生成

   将生成好的密文配置文件放置到您的后台应用可以访问的位置。

3. 在应用中解密文件并使用

在您的后台应用中编写代码，读取密文配置文件并通过KMS SDK 将其解密后使用，示例代码见 SDK 示例代码。

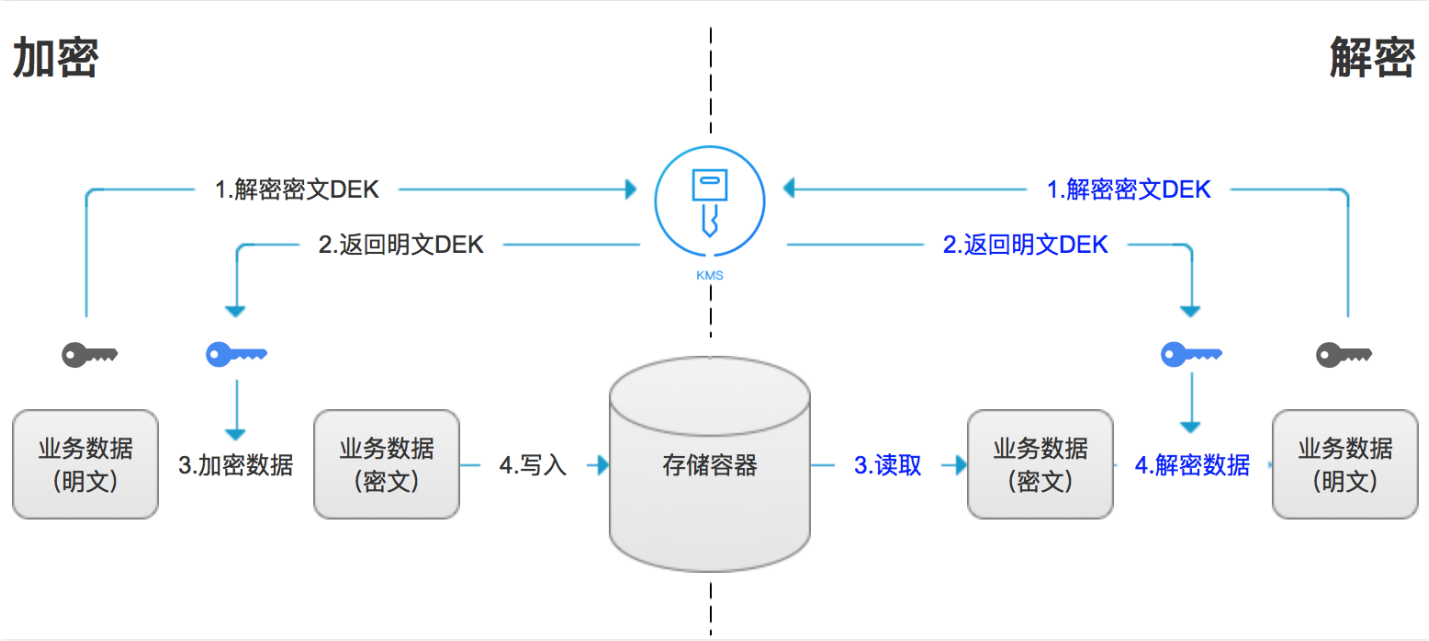
信封加密

最近更新时间：2018-06-13 15:30:50

简介

信封加密也被称为数字信封技术，它是一种综合利用对称加密和非对称加密技术的加密方案，目的是利用**对称加密的高性能**和**非对称加密的易管理**。在信封加密方案中，海量的业务数据在存储或通信的过程中使用**数据密钥（DEK）**以**对称加密**的方式加密，而DEK 又通过**主密钥（CMK）**采用**非对称加密**方式加密保护，而解密时，以通信场景为例，发送方将数据密文和DEK 密文一起传输，接收方先解密出DEK 明文，然后通过DEK解密出数据明文。

示意图



加密步骤3【加密数据】和解密步骤4【解密数据】是用户在云服务器上的**本地服务**使用DEK 对业务数据以**对称加密**方式进行加解密。

明文DEK 如何创建？

1. 通过KMS云API 来创建一个AES 256规格的数据密钥，见 生成数据密钥。
2. 用户通过第三方工具或者开发库创建（比如OpenSSL）。

密文DEK 如何创建和保存？

1. 密文DEK可以通过KMS云API 对明文加密生成，也可以通过在线工具来处理，见 加密解密。

2. 密文DEK由用户自行保存，常见的实现方案中，密文DEK 会和密文业务数据保存在一起，比如存储场景下保存在一个或类似访问途径的存储容器，通信场景下与密文DEK 和密文业务数据共同组成一个报文。

优势

高效

所有的业务数据都是采用高效的本地对称加密处理，对业务的访问体验影响很小。而对于DEK 的创建和加解密开销，除了非常极端的情况下，您需要采用"一次一钥"的方案，大部分场景下可以在一段时间内复用一个DEK 的明文和密文，所以大多数情况下这部分开销非常小。

安全易用

信封加密的安全性类似于常见公钥体系，DEK 保护业务数据，而腾讯云KMS 则保护DEK 并提供更好的可用性，您的主密钥无论如何都不会被泄露，只有有用密钥访问权限的对象才有能力操作CMK。

何时在云上使用信封加密？

1. **较大体积**：目前KMS API 支持4 KB以下数据加解密。
2. **海量数据，低延迟**：想对业务数据加解密，但是又比较在乎访问延迟。腾讯云 KMS后台虽然拥有非常高的性能，但是是远程调用且采用非对称加密，而信封加密方案大多数操作使用高性能的本地对称加密。

常见方案对比

	敏感信息加密	信封加密
相关密钥	CMK	CMK、DEK
性能	非对称加密，远程调用	少量远程非对称加密，海量本地对称加密
主要场景	密钥、证书、小型数据	海量大型数据