密钥管理服务

最佳实践

产品文档

腾讯云

文档目录

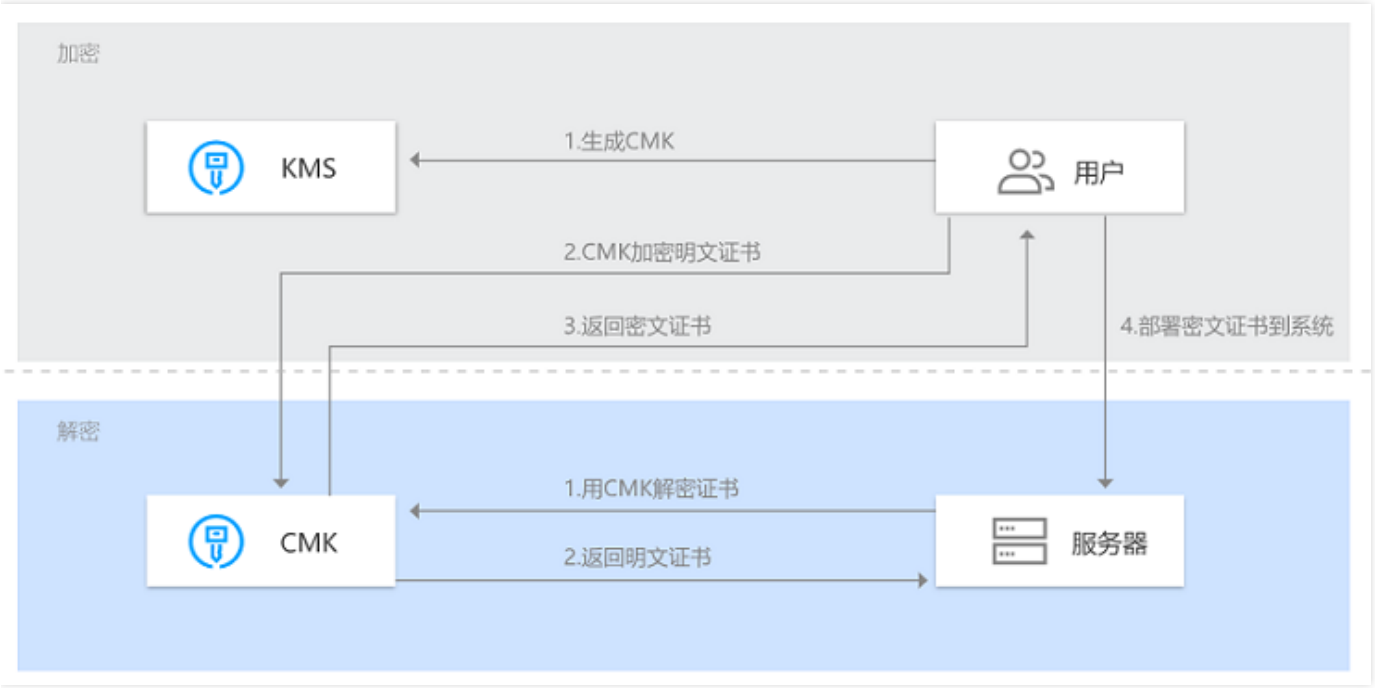
最佳实践
敏感信息加密

最近更新时间：2019-04-30 16:07:00

简介

敏感信息加密是密钥管理服务（KMS）核心的能力，实际应用中主要用来保护服务器硬盘上敏感数据的安全（小于4KB），如密钥、证书、配置文件等。
使用 CMK 加密敏感数据信息，而非直接将明文放置到云服务器上。使用时，再将密钥解密到内存，保证明文不落盘。这样，即使云服务器因为个人疏忽而遭受不明人员访问，这些数据信息也不会泄漏。

示意图



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。

操作步骤

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。

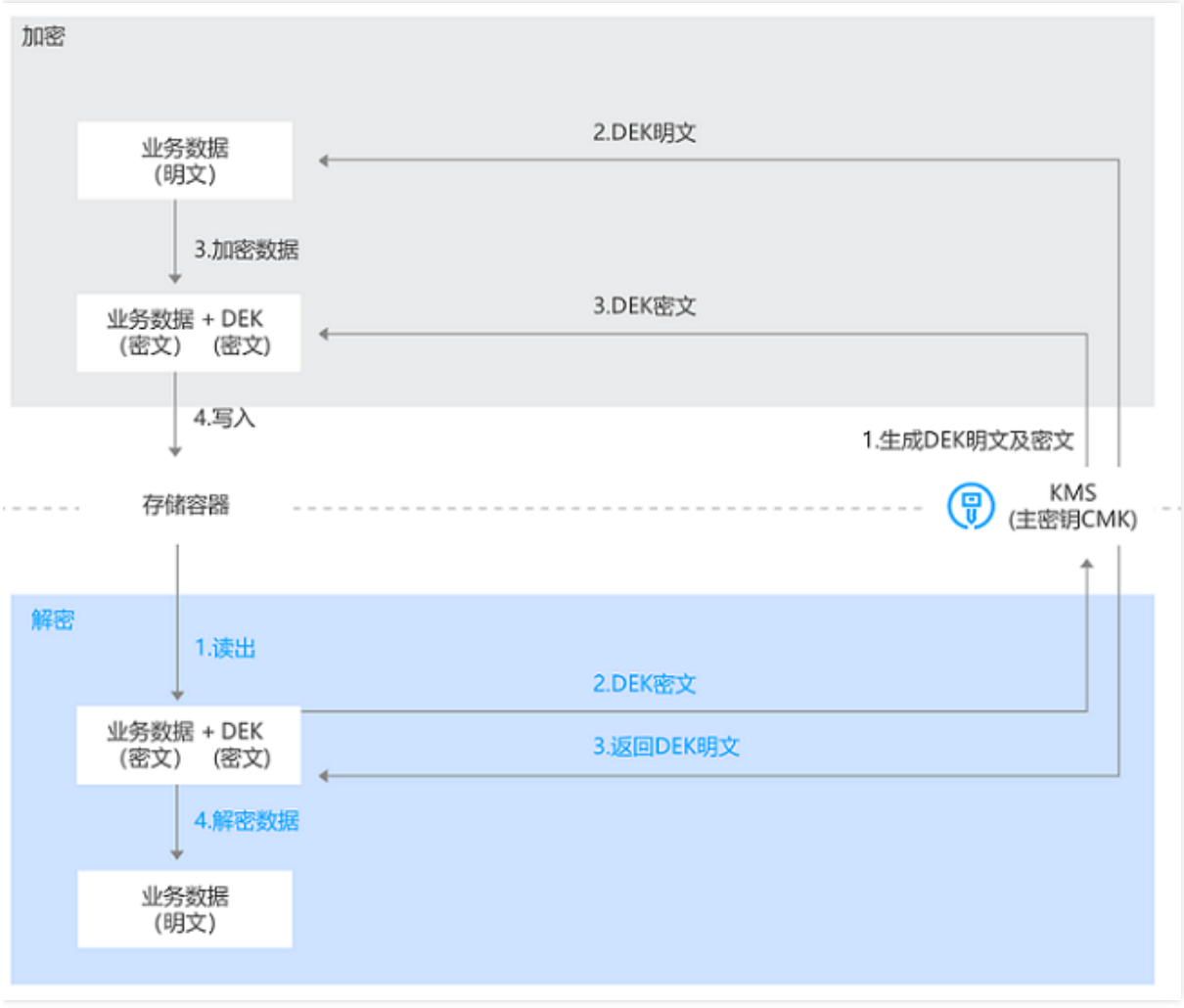
信封加密

最近更新时间：2019-04-30 16:07:38

简介

信封加密（Envelope Encryption）是一种应对海量数据的高性能加解密方案。对于较大的文件或者对性能敏感的数据加密，使用 GenerateDataKey 接口生成 AES 数据加密密钥 DEK，只需要传输数据加密密钥 DEK 到 KMS 服务端（通过CMK 进行加解密），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。

示意图



操作步骤

创建明文 DEK

1. 通过 KMS 云 API 来创建一个 AES 256 规格的数据密钥，详细操作步骤请参阅 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）。

创建和保存密文 DEK

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，详细操作步骤请参阅 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4KB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

访问控制
概述

最近更新时间：2019-04-30 16:09:36

如果您使用到了密钥管理服务（KMS）、私有网络（VPC）、云服务器、数据库等服务，这些服务由不同的人管理，但都共享您的云账号密钥，将存在以下问题：

- 您的密钥由多人共享，泄密风险高。
- 您无法限制其它人的访问权限，易产生误操作造成安全风险。

访问控制（CAM）用于管理腾讯云账户下资源访问权限，通过 CAM，您可以通过身份管理和策略管理控制哪些子账号有哪些资源的操作权限。

例如，您的根账户下有个主密钥，您只想让子帐号 A 使用该主密钥，而让子账号 B 不能使用，就可以通过在 CAM 中配置策略，对子账号的权限进行控制。

如果您不需要对子账户进行 KMS 相关资源的访问控制，您可以跳过此章节。跳过这些部分并不影响您对文档中其余部分的理解和使用。

CAM 基本概念

根账户通过给子账户绑定策略实现授权，策略设置可精确到**（API，资源，用户/用户组，允许/拒绝，条件）**维度。

- **账户**
  - **根账号**：腾讯云资源归属、资源使用计量计费的基本主体，可登录腾讯云服务。
  - **子账号**：由根账号创建账号，有确定的身份 ID 和身份凭证，且能登录到腾讯云控制台。根账号可以创建多个子账号(用户)。**子账号默认不拥有资源，必须由所属根账号进行授权。**
  - **身份凭证**：包括登录凭证和访问证书两种，**登录凭证**是指用户登录名和密码，**访问证书**是指云 API 密钥（SecretId 和 SecretKey）。
- **资源与权限**
  - **资源**：资源是云服务中被操作的对象，如一个 KMS 的一个主密钥，云服务器实例，COS 存储桶，VPC 实例等。
  - **权限**：权限是指允许或拒绝某些用户执行某些操作。默认情况下，**根账号拥有其名下所有资源的访问权限**，而**子账号没有根账号下任何资源的访问权限。**
  - **策略**：策略是定义和描述一条或多条权限的语法规范。**根账号**通过将**策略关联**到用户/用户组完成授权。

了解更多请参阅 CAM 产品文档。

相关文档

目标	链接
了解策略和用户之间关系	策略管理
了解策略的基本结构	策略语法

目标	链接
了解还有哪些产品支持 CAM	支持 CAM 的产品

KMS 访问控制策略示例

最近更新时间：2019-04-30 16:09:41

KMS 的全读写策略

以下策略允许子账号有所有操作的权限。Action 元素指定所有 KMS 相关 API。

```
{
"version": "2.0",
"statement": [
{
"action": [
"name/kms:*"
],
"resource": "*",
"effect": "allow"
}
]
}
```

KMS 的只读策略

以下策略允许子账号查询您的 KMS 资源。但子账号无法创建、更新或删除它们。
在控制台，操作一个资源的前提是可以查看该资源，所以建议您为用户开通 KMS 全读权限。

```
{
"version": "2.0",
"statement": [
{
"action": [
"name/kms:ListKey",
"name/kms:GetKeyAttributes"
],
"resource": "*",
"effect": "allow"
}
]
}
```

允许子账号做管理类操作

```
{
"version": "2.0",
"statement": [
{
"action": [
```

```
"name/kms:CreateKey",
"name/kms:ListKey",
"name/kms:GetKeyAttributes",
"name/kms:SetKeyAttributes"
],
"resource": "*",
"effect": "allow"
}
]
}
```

允许子账号做数据类操作，但不允许其做管理类操作

```
{
"version": "2.0",
"statement": [
{
"action": [
"name/kms:*"
],
"resource": "*",
"effect": "allow"
},
{
"action": [
"name/kms:CreateKey",
"name/kms:ListKey",
"name/kms:GetKeyAttributes",
"name/kms:SetKeyAttributes"
],
"resource": "*",
"effect": "deny"
}
]
}
```

KMS API 操作支持的资源级权限

最近更新时间：2019-04-30 16:09:45

在 CAM 中，可对主密钥资源进行以下 API 操作的授权， 具体 API 支持的资源和条件的对应关系如下：

API 操作	资源	备注
kms:CreateKey	qcs::kms:$region:$account:key/*	creatorUin 表示资源创建者的 uin，资源创建者可为根帐号或子账号。
kms:ListKey	qcs::kms:$region:$account:key/*	
kms:ListKeys	qcs::kms:$region:$account:key/*	
kms:ListKeyDetail	qcs::kms:$region:$account:key/*	
kms:GetServiceStatus	qcs::kms:$region:$account:key/*	
kms:Encrypt	qcs::kms:$region:$account:key/creatorUin/$creatorUin/$keyid（授权单个资源） qcs::kms:$region:$account:key/creatorUin/$creatorUin/*（授权某个创建者的所有资源） qcs::kms:$region:$account:key/*（授权某个根帐号的所有资源）	
kms:Decrypt	qcs::kms:$region:$account:key/creatorUin/$creatorUin/$keyid（授权单个资源） qcs::kms:$region:$account:key/creatorUin/$creatorUin/*（授权某个创建者的所有资源） qcs::kms:$region:$account:key/*（授权某个根帐号的所有资源）	
kms::GenerateDataKey	qcs::kms:$region:$account:key/creatorUin/$creatorUin/$keyid（授权单个资源） qcs::kms:$region:$account:key/creatorUin/$creatorUin/*（授权某个创建者的所有资源） qcs::kms:$region:$account:key/*（授权某个根帐号的所有资源）	
kms::EnableKey	qcs::kms:$region:$account:key/creatorUin/$creatorUin/$keyid（授权单个资源） qcs::kms:$region:$account:key/creatorUin/$creatorUin/*（授权某个创建者的所有资源） qcs::kms:$region:$account:key/*（授权某个根帐号的所有资源）	
kms::DisableKey	qcs::kms:$region:$account:key/creatorUin/$creatorUin/$keyid（授权单个资源） qcs::kms:$region:$account:key/creatorUin/$creatorUin/*（授权某个创建者的所有资源） qcs::kms:$region:$account:key/*（授权某个根帐号的所有资源）	
kms::GetKeyAttributes	qcs::kms:$region:$account:key/creatorUin/$creatorUin/$keyid（授权单个资源）	

	qcs::kms:$region:$account:key/creatorUin/$creatorUin/*（授权某个创建者的所有资源） qcs::kms:$region:$account:key/*（授权某个根帐号的所有资源）
kms::SetKeyAttributes	qcs::kms:$region:$account:key/creatorUin/$creatorUin/$keyid（授权单个资源） qcs::kms:$region:$account:key/creatorUin/$creatorUin/*（授权某个创建者的所有资源） qcs::kms:$region:$account:key/*（授权某个根帐号的所有资源）
kms:GetKeyRotationStatus	qcs::kms:$region:$account:key/creatorUin/$creatorUin/$keyid（授权单个资源） qcs::kms:$region:$account:key/creatorUin/$creatorUin/*（授权某个创建者的所有资源） qcs::kms:$region:$account:key/*（授权某个根帐号的所有资源）
kms:ReEncrypt	qcs::kms:$region:$account:key/creatorUin/$creatorUin/$keyid（授权单个资源） qcs::kms:$region:$account:key/creatorUin/$creatorUin/*（授权某个创建者的所有资源） qcs::kms:$region:$account:key/*（授权某个根帐号的所有资源）
kms:DescribeKey	qcs::kms:$region:$account:key/creatorUin/$creatorUin/$keyid（授权单个资源） qcs::kms:$region:$account:key/creatorUin/$creatorUin/*（授权某个创建者的所有资源） qcs::kms:$region:$account:key/*（授权某个根帐号的所有资源）
kms:UpdateKeyDescription	qcs::kms:$region:$account:key/creatorUin/$creatorUin/$keyid（授权单个资源） qcs::kms:$region:$account:key/creatorUin/$creatorUin/*（授权某个创建者的所有资源） qcs::kms:$region:$account:key/*（授权某个根帐号的所有资源）
kms:UpdateAlias	qcs::kms:$region:$account:key/creatorUin/$creatorUin/$keyid（授权单个资源） qcs::kms:$region:$account:key/creatorUin/$creatorUin/*（授权某个创建者的所有资源） qcs::kms:$region:$account:key/*（授权某个根帐号的所有资源）
kms:DisableKeyRotation	qcs::kms:$region:$account:key/creatorUin/$creatorUin/$keyid（授权单个资源） qcs::kms:$region:$account:key/creatorUin/$creatorUin/*（授权某个创建者的所有资源） qcs::kms:$region:$account:key/*（授权某个根帐号的所有资源）
kms:EnableKeyRotation	qcs::kms:$region:$account:key/creatorUin/$creatorUin/$keyid（授权单个资源） qcs::kms:$region:$account:key/creatorUin/$creatorUin/*（授权某个创建者的所有资源） qcs::kms:$region:$account:key/*（授权某个根帐号的所有资源）

kms:EnableKeys	qcs::kms:$region:$account:key/creatorUin/$creatorUin/$keyid（授权单个资源） qcs::kms:$region:$account:key/creatorUin/$creatorUin/*（授权某个创建者的所有资源） qcs::kms:$region:$account:key/*（授权某个根帐号的所有资源）
kms:DisableKeys	qcs::kms:$region:$account:key/creatorUin/$creatorUin/$keyid（授权单个资源） qcs::kms:$region:$account:key/creatorUin/$creatorUin/*（授权某个创建者的所有资源） qcs::kms:$region:$account:key/*（授权某个根帐号的所有资源）
kms:DescribeKeys	qcs::kms:$region:$account:key/creatorUin/$creatorUin/$keyid（授权单个资源） qcs::kms:$region:$account:key/creatorUin/$creatorUin/*（授权某个创建者的所有资源） qcs::kms:$region:$account:key/*（授权某个根帐号的所有资源）