密钥管理系统

常见问题

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

常见问题
一般性问题

最近更新时间：2023-03-02 17:41:56

腾讯云 KMS 可以做什么?

腾讯云 KMS 提供加密过程中的对称密钥与非对称密钥的全生命周期管理，包括生成、存储、启用/禁用、分发、轮换、审计、销毁等，满足用户多应用多业务的密钥管理需求，符合监管和合规要求。同时，KMS 提供敏感数据加密、信封加密、云产品集成等加密能力，方便用户专注于业务开发。

哪些云服务支持密钥管理系统加密数据?

KMS 服务无缝对接腾讯云 TencentDB、COS 和 CBS 等云产品，通过 KMS 提供信封加密的方式对云产品数据进行加密。

密钥管理系统控制台中用户主密钥与云产品密钥有什么区别吗?

- **用户主密钥**是用户通过控制台或 API 来创建的用户主密钥。您可以对用户密钥进行创建/启用/禁用/轮换/权限控制等操作。
- **云产品密钥**是腾讯云产品/服务（例如 CBS、COS、TDSQL 等）在调用密钥管理系统时，自动为用户创建的 CMK。您可以对云产品密钥进行查询及开启密钥轮换操作，不支持禁用、计划删除操作。

海量数据如何进行加密?

对于较大的数据加密，建议采用 信封加密 方案，实现本地高性能数据加解密。

KMS 会限制用户访问频率吗?

KMS 会对用户访问的频率进行限制。

- 对于同一个主账号（主账号访问自己账号下的 KMS 服务），访问 KMS 服务单一接口的最高频率为15000次/每秒。
- 对于角色授权服务主账号（经过授权同意后，主账号访问其他账号的 KMS 服务），访问 KMS 单一接口的最高频率为3000次/每秒。

如果正常访问 KMS 服务频率超过对应值，请 提交工单 联系我们进行修改

开发接入相关问题

最近更新时间：2024-01-12 14:34:31

SDK 中的 SecretID 和 SecretKey 在哪里获取?

您需使用主账号登录 **API 密钥管理控制台** 获取您的 SecretID 和 SecretKey。**请您务必保存好您的 SecretID 和 SecretKey 不被泄露。**

如何创建用户主密钥 CMK？

创建用户主密钥有三种方式，分别是通过 **密钥管理系统控制台**、**腾讯云命令行工具 TCCLI** 及 **API 接口请求**。

创建用户主密钥 CMK 是否有个数限制?

是。每账户每区域下限制创建200个 CMK，计划删除状态下的除外。不包含云产品密钥。如需创建更多的 CMK，请 **提交工单** 或联系腾讯云商务。

创建密钥时，密钥材料来源可以选择外部，外部是指什么？BYOK 方案是指什么?

- **外部**是指使用用户自己的密钥材料。
- **BYOK**（Bring Your Own Key）是实现用户使用自己密钥材料的一个方案，其方式是通过 KMS 服务生成一个密钥材料为空的 CMK，并将自己的密钥材料导入到该用户主密钥中，形成一个外部密钥 CMK（EXTERNAL CMK），再由 KMS 服务进行该外部密钥的分发管理。

修改用户主密钥的别名或描述信息，通过接口请求的方式，需要多久才能生效?

接口成功请求后会**立即生效**。

是否支持轮换用户主密钥 CMK？如何开启?

支持轮换。可以通过 **密钥管理系统控制台**、**命令行工具** 或 **API 接口** 三种方式进行开启操作。

> ⚠ **注意：**
> 不支持轮换的用户主密钥：
> - 非对称的用户主密钥 CMK
> - 使用外部密钥材料的用户主密钥 CMK

开启轮换后，业务是否需要做更改?

- 密钥轮换只会更改用户主密钥的密钥材料，用户主密钥的属性（密钥 ID、别名、描述、权限）不会发生变化。
- 开启密钥轮换后，密钥管理服务会根据设置的轮换周期（默认365天）自动轮换密钥，每次轮换都会生成一个新版本的用户主密钥，轮换的密钥加解密数据的方式如下所示：

- 加密数据时，KMS 会自动使用当前最新版本的用户主密钥来执行加密操作。
- 解密数据时，KMS 会自动使用加密时所使用的用户主密钥来执行解密操作。

如何选择数据加密算法?

- **对称加解密**：对称加解密算法包括 SM4和 AES256，其算法的选择是系统根据创建主密钥时上传的地区自动分配。如地区选择的是“中国国内站”，即系统会选择 SM4算法；当选择的是“非中国国内站”，则系统会选择AES256算法。
- **非对称加解密**：非对称加解密算法包括模长为2048比特的 RSA 密钥和 SM2，其算法的选择由您创建主密钥时选择的地区和 KeyUsage 共同决定。

> **注意：**
> 通过 API 接口方式创建用户主密钥，建议在创建之前先查询当前地区支持的 **加密方式**，从而确保创建的正确性。