密钥管理系统

常见问题

产品文档

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

文档目录

常见问题
一般性问题
开发接入相关问题

版权所有：腾讯云计算（北京）有限责任公司

常见问题
一般性问题

最近更新时间：2024-01-11 16:31:55

在密钥管理系统中创建的用户主密钥的个数是否有限制？

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。

哪些云服务可以使用密钥管理系统加密数据？

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

如何使用 KMS 服务加密数据？

您可以使用以下三种方式调用腾讯云 KMS 服务：
通过 KMS API 调用 KMS 服务。此种场景下，您的业务应用程序在腾讯云内或腾讯云外均可。
通过腾讯云 KMS SDK 集成到您自己的业务应用程序中调用 KMS 服务。此种场景下，您的业务应用程序在腾讯云内或腾讯云外均可。
通过已经与 KMS 对接的腾讯云产品调用 KMS 服务，对该腾讯云云产品的数据进行加解密操作。

如何开启密钥轮换功能？

您可以在控制台配置让腾讯云 KMS 每年自动轮换 CMK。
CMK 轮换后，用户无需重新加密数据，腾讯云会自动保留原 CMK，使用原 CMK 加密的旧的密文依然可以解密，新的数据加密则使用新的 CMK。

关于量子密钥服务？

根据产品发布计划，密钥管理系统已经停止提供量子密钥管理服务，已经使用量子密钥的用户可在 密钥管理系统 控制台继续使用。

版权所有：腾讯云计算（北京）有限责任公司

开发接入相关问题

最近更新时间：2024-01-11 16:31:55

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，这个是外部是指什么？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。

版权所有：腾讯云计算（北京）有限责任公司

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 AES，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，例如地区选择的是“中国区”，即系统会选择 SM4 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。