密钥管理系统

词汇表

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。

词汇表

最近更新时间：2025-08-12 11:09:21

辅助校验数据

辅助校验数据（Encryption Context）是 JSON 格式的一段数据，如果在调用加密接口时传入这段数据，解密时必须提供等价的 JSON 数据，否则解密失败，您可以通过定时更新 Encryption Context 来提高业务安全性，也可以在不禁用主密钥的情况下，快速阻止非法访问。

数据加密密钥

数据加密密钥（Data Encryption Keys，DEK）用于加密业务数据的密钥，受主密钥保护，可以自定义，也可以通过 KMS 的 API 来创建新的数据密钥。

信封加密

信封加密（Envelope Encryption）是一种应对海量数据的高性能加解密方案，加解密业务数据时使用数据密钥，并采取性能较高的对称加密方法，再通过密钥管理服务来保证数据密钥的使用安全，特点是在保证数据安全的同时保持较高的数据读写性能。

根密钥

用户主密钥（Customer Master Keys，CMK）是由腾讯云为您保管的主密钥，这些主密钥受到经过第三方认证硬件安全模块（HSM）的保护，通过它来加解密业务使用到的密码、证书、数据密钥等敏感数据，可以通过控制台和 API 来创建和管理主密钥。
用户主密钥（CMK）包括用户密钥（CMK）和云产品密钥（CMK）两种类型。

数据密钥

数据密钥（DEK）是基于 CMK 生成的二级密钥，可用于用户本地数据加密解密。
您可以使用密钥管理系统 CMK 生成 DEK，但是，密钥管理系统不会存储、管理或跟踪您的 DEK，也不会用 DEK 执行加密操作。您必须在密钥管理系统之外使用和管理 DEK。
一般 DEK 在信封加密流程中使用，通过 DEK 进行本地业务数据的加密。DEK 受 CMK 保护，可以自定义，也可以通过 GenerateDataKey 接口来创建 DEK。

云产品密钥

云产品密钥是腾讯云产品/服务（如 COS、TDSQL）在调用密钥管理服务时，自动为用户创建的用户主密钥。
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。