密钥管理系统

产品简介

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【商标声明】

腾讯云

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。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。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。

【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。

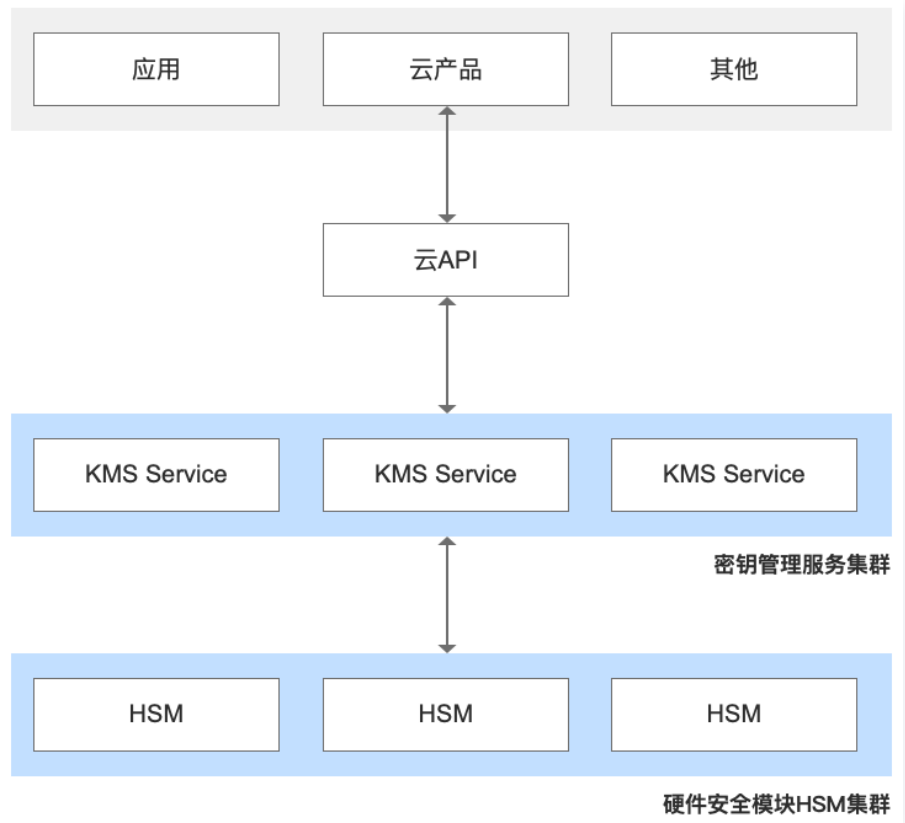
文档目录

产品简介
- 产品概述
- 产品优势
- 应用场景
- 基本概念

产品简介
产品概述

最近更新时间：2025-07-04 18:15:02

密钥管理系统（Key Management Service，KMS）是一款安全管理类服务，使用经过第三方认证的硬件安全模块 HSM（Hardware Security Module）来生成和保护密钥。帮助用户轻松创建和管理密钥，满足用户多应用多业务的密钥管理需求，助力用户落实合规要求。
下图所示为密钥管理系统（KMS）产品架构图：



核心功能

密钥全生命周期管理

- 支持密钥生成、存储、轮换、归档、销毁等全流程管理，可通过控制台或 API 灵活配置策略。
- 计划删除缓冲：支持密钥的计划删除（7-30 天缓冲期），并支持本地备份导入的外部密钥材料。

加密能力

- 敏感数据加密：直接加密小于4KB 的敏感信息（如 API 密钥、证书），确保数据明文不落盘。
- 信封加密：通过数据密钥（DEK）与根密钥（CMK）结合，实现本地高性能加密，减少对业务性能的影响，适合海量数据场景。

- 非对称加密：支持 RSA 等非对称密钥管理，适用于数字签名、加密通信场景需求。

BYOK（Bring Your Own Key）方案

自主控制：允许用户导入自有密钥材料生成外部密钥 CMK，实现对密钥的完全自主管理。

云服务集成

- 透明加密：与对象存储（COS）、云硬盘（CBS）、数据库（TencentDB/CDB）等腾讯云产品无缝集成，用户只需选择 KMS 托管的密钥，无需关心加密的细节，即可实现透明的云上数据加解密。
- 凭据管理：与凭据管理系统（SSM）结合，实现数据库密码、Token 等敏感凭据的集中托管与加密存储。

权限控制与审计

- 细粒度权限：与访问管理（CAM）集成，支持资源级授权，精确控制用户 / 角色对密钥的访问权限。
- 操作审计：集成操作审计，记录所有密钥操作与 API 调用日志，支持自定义日志留存时间以落实合规审计需求。

版权所有：腾讯云计算（北京）有限责任公司

产品优势

最近更新时间：2025-07-11 15:13:21

安全合规

KMS 使用经过第三方认证的硬件安全模块 HSM 来生成和保护密钥，安全和质量控制已通过多种合规性计划认证。您主密钥的创建、管理等操作都将在加密机中进行，腾讯云在内的任何人都无法获取到您的明文主密钥。

高可用

保障关键密钥的持续可用性，是业务连续性的基石。腾讯云 KMS 通过三层架构设计，分别在密钥存储、加密运算和服务访问层面实现跨可用区（AZ）高可用，降低单点故障带来的风险：

- 密钥数据跨 AZ 冗余： 您的密钥及其关键信息，均以加密形态自动备份到多个不同物理位置的可用区（AZ）。即使单个 AZ 故障，其他备份点可确保密钥安全可用，不影响业务加解密操作。
- 加密机集群跨 AZ 部署： 进行加密运算的底层硬件加密机（HSM），采用多机房分布式部署。单一 AZ 故障时，系统能快速将加密运算任务切换至其他 AZ 的健康加密机，保持加密服务稳定运行。
- 服务接入点跨 AZ 高可用： KMS 的云 API 接入点和控制节点同样部署于多个 AZ。若某个 AZ 出现问题，客户端请求将自动切换到其他 AZ 的服务节点，保障管理界面和 API 的持续访问。

集中化密钥管理

您可以通过 API、SDK 及已经对接的云产品接入腾讯云 KMS 服务，并使用 KMS 集中管理您业务应用的密钥策略，无论这些业务应用是部署在腾讯云内或是腾讯云外。

即开即用

无须购买专门的硬件加密设备，一键部署，按量付费，腾讯云将提供所有后端服务维护。

极简加解密服务

KMS 采用信封加密，仅需调用加解密接口和关注 CMK 的权限控制即可实现本地海量数据加解密。

专属密钥资源

KMS 独享版是物理密码机独享的云上密钥管理服务。加密运算在独享的物理密码机中进行，并拥有独享的密码资源池。

版权所有：腾讯云计算（北京）有限责任公司

应用场景

最近更新时间：2023-03-15 10:47:03

腾讯云密钥管理系统 KMS 可适用于腾讯云内及云外所有用户，解决用户敏感数据加密需求，落实合规要求，同时帮助不同行业解决数据加密痛点问题。

金融等行业敏感数据保护

痛点：金融等行业机构任何的通信和存储数据都具有高价值性和高保密性，需要考虑加密的安全性及合规性。
方案：通过信封加密对协议通信内容、重要文件和资料提供加密服务及密钥保护和权限管理，满足安全性及合规性要求。

后台服务开发配置信息保护

痛点：应用开发配置文件需要进行加密以保护程序数据安全。
方案：通过 KMS 对敏感配置信息、数据库连接信息、数据库密码、登录密钥、后台服务的配置信息进行加密及完整性保护。

企业核心数据保护

痛点：核心知识产权、用户手机号、身份证号、银行账号、口令等隐私数据做严格保护，将敏感数据加密后保存，但是无法保证数据密钥的安全。
方案：以信封加密方式，将所有核心数据通过数据密钥加密，数据密钥再经过 KMS 加密，为核心数据提供双重保护。

网站或应用开发安全

痛点：提供 HTTPS 等服务时需要使用到证书、密钥，这些信息若以明文保存本地，攻击者可以轻易获取。
方案：通过 KMS 对密钥进行加解密，加密后本地保存密钥的密文文件，使用时解密且不保存本地，使得攻击者难以获取，从而保证网页和应用的安全性。

集中管理密码策略

痛点：应用统一的密钥管理策略至分散的业务系统。
方案：通过 SDK、云产品或 API 调用 KMS 服务，对云上及本地应用系统数据应用统一的密钥管理策略。

版权所有：腾讯云计算（北京）有限责任公司

基本概念

最近更新时间：2025-07-04 18:15:02

本文主要罗列了密钥管理系统（KMS）的基本概念。

密钥生命周期

密钥生命周期指密钥的生成、存储、分发、导入、导出、使用、恢复、归档与销毁等一系列环节，其中密钥管理系统 KMS 提供密钥全生命周期管理，确保密钥以安全的方式完成该系列操作，防止密钥被泄露。

对称加解密

对称加解密指采用单钥密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密。

> **说明：**
> 密钥管理系统（KMS）提供了对称加解密方案，详细请参见 **对称加解密** 。

非对称加解密

非对称加解密需要两个密钥：公开密钥和私有密钥。公钥和私钥是一对密钥，信息传送者使用公钥对数据进行加密，信息接收者只有用对应的私钥才能解密。另一方面，信息传送者可使用私钥对机密信息进行签名，信息接收者使用对应的公钥对接收的数据进行验签。

> **说明：**
> 密钥管理系统（KMS） 也提供了非对称加解密方案，详情请参见 **非对称加解密** 。

根密钥（CMK）

用于保护密钥管理系统（KMS）用户敏感数据和数据密钥（DEK），由密钥管理系统调用硬件密码机产生，并且被 Domain Key 加密保护。CMK 仅能通过加密机进行加解密操作。

数据密钥（DEK）

信封加密场景中，DEK 用于直接加密解密用户数据，由密钥管理系统调用硬件密码机产生，并且被根密钥（CMK）加密后以密文及明文的形式返回给应用系统，业务侧通过在内存中的 DEK 明文进行本地高性能加解密。

白盒密钥

指通过白盒密码技术保障安全性下的密钥，白盒密钥用于保护端上的敏感根密钥信息，例如 API SecretKey，用户内部系统使用的鉴权密钥或 token，其它本地敏感根密钥信息等。

> **说明：**

> 密钥管理系统（KMS）提供了白盒密钥管理的解决方案，详情请参见 白盒密钥管理 。

敏感数据

敏感数据是指敏感、隐私的信息内容，例如密钥、证书、配置文件、银行账号、身份证号码等。

硬件安全模块

硬件安全模块（Hardware Security Module，HSM） 是一种用于保护和管理强认证系统所使用的密钥，并同时提供相关密码学操作的计算机硬件设备 。KMS 底层使用商用密码认证或 FIPS-140-2 认证的硬件安全模块 HSM 来保护密钥的安全，确保密钥的保密性、完整性和可用性。

BYOK

BYOK（Bring Your Own Key）是指用户可以自行导入密钥材料至用户主密钥中，详情请参见 外部密钥导入 。