

密钥管理服务

产品简介

产品文档



腾讯云

【版权声明】

©2013-2019 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模式的承诺或保证。

文档目录

产品简介

产品概述

产品功能

产品优势

应用场景

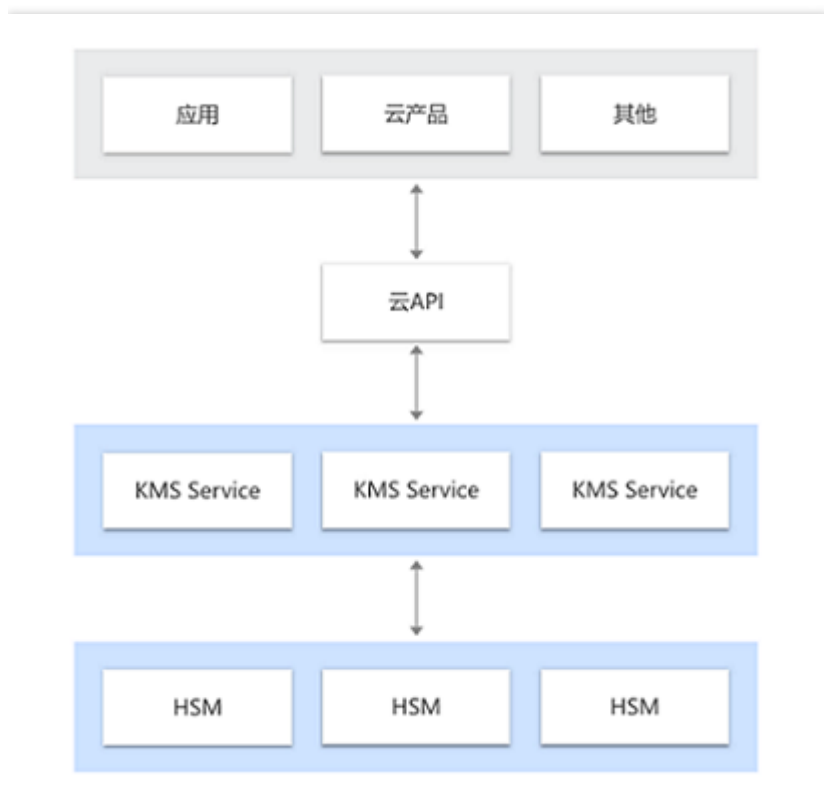
产品简介

产品概述

最近更新时间：2019-04-30 16:01:59

密钥管理服务（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，符合监管和合规要求。

下图所示为密钥管理服务（KMS）产品架构图：



产品功能

最近更新时间：2019-07-05 15:18:39

安全合规

密钥管理服务底层使用国家密码局或 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。

托管式密钥管理

密钥管理服务为您提供了丰富的管理功能，包括密钥创建、启用、禁用、轮换设置、别名设置、查看密钥详情、修改相关信息等功能。您可以依托腾讯云密钥管理服务轻松的创建、保护以及执行您的各项密钥管理策略。

密钥轮换

提供 CMK 密钥交换能力，默认关闭，由用户设置是否打开，开启后 CMK 会一年交换一次，密钥交换由密钥管理服务系统管理，对上透明，交换后使用该 CMK 加密的旧的密文依然可以解密。新的加密则使用新的 CMK。

权限控制

与腾讯云访问管理集成，通过身份管理和策略管理控制哪些账户，哪些角色可以访问或管理您的敏感密钥。

内置审计

与腾讯云审计集成，可记录所有 API 请求，包括密钥管理操作和密钥使用情况。

稳定可靠

采用多机房分布式集群化的业务部署和热备份，底层 HSM 设备采用双机房冷备份部署，确保密钥管理服务的高可用性。

无缝集成服务

密钥管理服务与对象存储、分布式数据库、云硬盘等服务的加密特性无缝集成，您可以轻松地应用密钥管理服务来管理这些服务内所存储数据的加密。

集中化密钥管理

您可以通过 API、SDK、云产品等多种方式调用并集成密钥管理服务，实现对各类应用程序的密钥的集中管理，无论这些业务应用在腾讯云内或是腾讯云外。

敏感数据加密

敏感信息加密是密钥管理服务核心的能力，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。

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。在密钥管理服务信封加密场景中，只需要传输数据加密密钥 DEK 到密钥管理服务服务端 (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。

产品优势

最近更新时间：2019-07-05 15:18:32

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。您的主密钥的创建、管理等操作都将在合规的 HSM 硬件中进行，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

在服务架构方层面，KMS 服务通过单地域多机房提供可靠性，其底层使用的 HSM 设备也采用多机房集群化部署，并提供双机房冷备份设备，确保服务的高可用性。在接入层面，KMS 通过云 API3.0 提供对外接入服务。云 API3.0 分地域部署，接入域名提供统一域名和地域独立域名两种方式，确保服务接入的高可用性。

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在腾讯云或是腾讯云外。

成本低廉

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。

应用场景

最近更新时间：2019-07-05 15:18:25

腾讯云密钥管理服务 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，满足安全合规，同时帮助不同行业数据加密痛点问题。

金融/政府敏感数据保护

痛点：金融和政府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。