密钥管理服务

什么是密钥管理服务

产品文档

腾讯云

文档目录

什么是密钥管理服务
- 产品简介
- 使用场景
- 产品优势

什么是密钥管理服务
产品简介

最近更新时间：2017-12-21 17:37:40

密钥管理服务（Key Management Service），简称 KMS，是一项安全相关的管理服务，通过密钥管理服务，您可以更安全、便捷的管理密钥类敏感信息，腾讯云为您保障相关的可用性和安全性。基于密钥管理服务，您还可以实现面向海量数据或文件的高效加密保护方案。

目前 腾讯云KMS服务提供两种主密钥类型，一种普通密钥类型，另一种为量子密钥类型。
1.普通密钥是基于软件实现的一种真随机密钥，提供可靠，安全，低成本的主密钥，适用于有加密需求的各类场合。
2.量子密钥狭义上是指通过量子密钥分发技术产生的安全性由量子力学基本原理保障的信息论可证安全的密钥；广义上,采用一种或多种理论论证安全的量子技术进行安全增强的密钥均可以称为“量子密钥”。量子密钥的随机源来自量子现象本质的不确定性，通过对物理源的信号采集和数字化技术输出随机数序列。采用“量子熵源”等量子安全增强技术的量子密钥管理系统，以其安全性、易用性、易维护性等特点，适用于有加密需求的各类场合。

适用开发者

开发者身份	受保护数据	保护目的	解决方案
网站或应用开发	证书、密钥	网站和应用会使用HTTPS证书来保证通信协议的安全，也会使用密钥来给文件打上自己企业的签名，但是这些常见的安全解决方案非常依赖证书和密钥本身的安全	KMS文件加密
后台服务开发	密码、登录密钥、配置	数据库密码、登录密钥、后台服务的配置信息可能会被黑客利用为掌控整个系统的跳板信息，明文放在硬盘上非常危险	KMS文件加密
内容、社交网站或应用	用户原创内容、有价值的知识产权	企业依赖核心的UGC内容或独特的知识产权来建立在行业的竞争优势，一定不能发生『拖库』这样的事故	KMS信封加密
政府、金融机构	协议通信内容、重要文件和资料	政府和金融机构任何的通信和存储数据都具有高价值性和高保密性，需要在建立业务系统时就考虑好合规性和安全性	KMS信封加密

使用场景

最近更新时间：2018-04-10 18:10:13

场景	安全风险点	KMS解决方案
证书、密钥保护	网页或应用开发商，在提供HTTPS 和前面之类服务时需要使用到证书、密钥，密钥若以明文保存本地，攻击者可以轻易获取	通过KMS 服务接口或在线工具对密钥加密，本地保存密钥的密文文件，使用时通过接口解密且不保存本地，攻击者难以获取
核心知识产权保护	通过核心知识产权建立业界竞争优势的开发商，需要对核心知识产权做严格保护，一旦泄露对公司打击难以估算。部分开发商有将敏感数据加密后保存，但是无法保证数据密钥的安全	所有核心数据通过数据密钥加密后才保存在对应的存储容器内，而数据密钥通过KMS 加密，缺乏有效权限，即使拿到密文的数据密钥和数据，也无法解开内容
协议和通信保护	政府，金融机构日常工作通信中难以避免会涉及高敏感性的信息，需要对不同终端和不同服务器之间的协议进行加密处理，但是用于加密协议包的密钥本身安全保证是个问题	密钥管理服务提供对应密钥加密保护和权限管理

产品优势

最近更新时间：2017-11-29 20:44:41

腾讯云 密钥管理服务与传统密钥管理方案对比

腾讯云 密钥管理服务 相比 传统密钥管理方案有诸多优势：

优势	腾讯云 密钥管理服务 KMS	传统 密钥管理 解决方案
成本	**无预支费用，按需付费** • 无需预支任何费用，仅需要为使用部分付费； • 无需考虑部署和维护成本。	• 需要购买昂贵的密码服务器硬件； • 启用后还有高额后续维护成本。
易用	**化繁为简，统一易用** • 满足安全访问权限即可随时随地使用； • 将繁杂的密码机接口统一成腾讯云简单易用的HTTPS接口； • 为多个主流开发平台提供SDK。	• 密码服务器业界无统一标准，需要培养专业人员； • 除了调试和部署密码服务器需要耗费大量精力，处理晦涩的密码服务器接口也很困难。
可靠	**集群管理，安全可靠** • 由腾讯云提供高可用性的密码服务器和专业开发及运维人员； • 服务涉及各个流程均采用高安全性协议通信； • 提供分布式集群管理和热备份保证高可靠性。	• 通常通过离线备份的方式来实现可靠性，过程纯手工操作繁琐易错，出错时，服务恢复时长也不可控； • 依赖熟悉密码服务器的运维人员，人员请假或离职将带来安全风险。