

目录

目录	1
产品概述	2
产品优势	2
核心优势:	2
产品功能:	2
应用场景	2
使用场景	2
使用场景	2
术语说明	2

# 产品概述

本文档提供了密钥管理服务（Kingsoft Key Management Service，简称：KKMS）产品的相关说明和操作指南。

金山云密钥管理服务（Kingsoft Key Management Service，简称：KKMS），是一款安全易用的管理类服务。您无需花费大量成本来保护密钥的保密性、完整性和可用性，借助密钥管理服务，您可以安全、便捷的使用密钥，专注于开发您需要的加解密功能场景

本文档能够帮助您了解密钥管理产品的功能特点，指导您使购买并使用KKMS。

# 产品优势

金山云密钥管理服务（Kingsoft Key Management Service，简称：KKMS），是一款安全易用的管理类服务。您无需花费大量成本来保护密钥的保密性、完整性和可用性，借助密钥管理服务，您可以安全、便捷的使用密钥，专注于开发您需要的加解密功能场景

## 核心优势：

- 可靠：金山云使用由国家认证的第三方密码硬件，与分布式系统结合，实现高可靠。
- 易用：金山云开放统一、易用的 API，方便的完成您本地数据的加密。
- 低成本：按照您的业务发展动态调整创建的密钥个数、按实际使用情况收费，并且每月2万次的免费API调用。

## 产品功能：

- 密钥生成；描述：可以通过控制台或API产生主密钥；用于加密数据密钥或密码、证书、配置文件等小包数据（最多4KB）；
- 密钥管理；描述：随时禁用与开启密钥、查看密钥详情、修改相关信息；
- 数据加解密；描述：可以通过控制台或API进行敏感信息加解密；
- 信封加密；描述：通过信封加密技术实现海量数据的本地加解密；

## 应用场景

场景	问题	KKMS如何解决
网站或应用开发	开发过程中需要使用密钥、证书，用于加密或者签名，希望密钥管理的功能安全且独立的	通过KKMS 控制台，生成安全密钥；通过在线工具对明文证书加密
核心知识产权保护	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	采用信封加密的方式，将加密数据的数据密钥封入信封中储存、传递和使用。缺乏有效权限，即使拿到密文数据密钥和数据，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

# 使用场景

## 使用场景

场景	问题	KKMS如何解决
网站或应用开发	开发过程中需要使用密钥、证书，用于加密或者签名，希望密钥管理的功能安全且独立的	通过KKMS 控制台，生成安全密钥；通过在线工具对明文证书加密
核心知识产权保护	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	采用信封加密的方式，将加密数据的数据密钥封入信封中储存、传递和使用。缺乏有效权限，即使拿到密文数据密钥和数据，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

# 术语说明

术语	概念
KKMS（密钥管理服务）	金山云提供的密钥管理服务

用户主密钥	用户在金山云控制台或使用API直接创建的主密钥，主要用于产生数据密钥，产生信封。也可直接用于加密少量的数据（小于4K）
数据密钥	加密数据时使用的明文数据密钥
信封加密	使用KMS为要加密的数据产生数据密钥，用户使用数据密钥