# 密钥管理

# 目录

# 目录



## 最佳实践



## 常见问题

# 产品公告

## 【产品公告】 关于天翼云密钥管理包周期版本上线的通知

尊敬的天翼云客户：

您好！

天翼云密钥管理服务于9月13日升级上线包周期版本，订购可选规格包含基础版、企业版。当前支持在上海33资源池售卖，其他资源池陆续上线，敬请期待！

更多产品介绍及资费信息，请参见产品帮助文档：https://www.ctyun.cn/document/10014047。

感谢您对天翼云的信赖与支持，如您有任何问题，可随时通过工单或者服务热线（400-810-9889）与我们联系。

感谢您对天翼云一如既往的支持与理解！

天翼云服务团队

## 【产品公告】 关于天翼云密钥管理按需版本停止新购的通知

尊敬的天翼云客户：

您好！

因业务调整，自2024年9月13日起，密钥管理按需版不再支持新购。

调整影响范围：

-新增客户：2024年9月13日起，无法订购按需版本，可选择开通包周期版本，规格说明：https://www.ctyun.cn/document/10014047/10032155。

-存量客户：2024年9月13日前已开通过按需版的用户，可继续使用按需版本，并按照按需版资费计费。

给您带来不便，敬请谅解！感谢您对天翼云的信赖与支持，如您有任何问题，可随时通过工单或者服务热线（400-810-9889）与我们联系。

感谢您对天翼云一如既往的支持与理解！

天翼云服务团队

## 【产品公告】天翼云密钥管理KMS产品旧版openapi下线

尊敬的天翼云用户：

您好！

天翼云计划于2023年9月28日00:00（北京时间）将密钥管理（KMS）旧版openAPI下线，后续将不再提供服务，为了避免影响您的业务，请您在2023年9月28日00:00（北京时间）前切换调用新版openAPI接口。新版openAPI接口文档详见：API参考。

如需要技术支持，可随时通过在线工单、客服热线（400-810-9889）联系我们，也可联系您的客户经理获取帮助，天翼密钥管理服务团队将全程配合您完成接口调用切换工作，为您的业务保驾护航。

感谢您对天翼云一如既往的支持与理解。

# 产品介绍

## 产品定义

密钥管理服务（Key Management Service，KMS）是一站式密钥管理和数据加密服务平台，提供安全合规、可靠易用的资源托管及密码运算服务。同时与天翼云云硬盘、对象存储、弹性文件、关系型数据库MYSQL等云产品无缝集成，实现云上原生数据的加密保护。

### 产品架构


### 业务组件

| 业务组件 | 说明 | 参考文档 |
| --- | --- | --- |
| 密钥管理 | 密钥管理组件提供密钥安全托管存储、生命周期管理以及密码运算能力。您可以在自建应用程序中，通过KMS提供的云原生接口实现数据加解密、签名验签等运算，同时KMS已对接天翼云云硬盘、对象存储、弹性文件、关系数据库MySQL版，为云服务提供服务端加密能力。 | 密钥管理概述 |
| 证书管理 | 证书管理组件提供高可用、高安全的密钥和证书托管能力，您可以通过KMS提供的云原生接口实现签名验签运算。 | 证书管理概述 |

# 产品介绍

## 产品优势

密钥管理服务（KMS）与传统的密钥管理设施相比具有安全合规、弹性高效、广泛集成以及稳定可用等优势。

### 安全合规

- 通过国家密码管理局安全性审查，符合国家密码行业标准（GM/T）相关技术规范要求，获得由国家密码管理局商用密码检测中心颁发的《商用密码产品认证证书》。
- 采用由国家密码管理局批准的硬件密码设备，通过更高安全的保护机制确保密钥的保密性、完整性和可用性。

#### 集中托管

- 支持自动化开通，按需扩容，弹性灵活。
- 提供密码基础设施的完全托管，可轻松创建密钥等资源，并通过极简API/SDK实现应用的快速集成。

#### 广泛集成

- 与云硬盘、对象存储、弹性文件、数据库等天翼云产品无缝集成，实现云上资源原生数据的加密保护。
- 云产品服务端加密功能可一键开启，加密过程透明无感知，用户体验极好。

#### 稳定可靠

- 采用分布式部署，在每个资源池构建了冗余的密码计算能力，有效保证服务可靠性。
- 支持VPC内应用通过私密的连接通道访问KMS服务，保证数据安全性的同时，大幅度提高了访问效率，减少延时。

## 功能特性

### 密钥生命周期管理

提供密钥全生命周期管理，包括密钥创建、自带密钥导入（BYOK）、启用/禁用、别名设置、轮转策略设置、版本设置、计划删除、取消删除等。

#### 密钥算法

- 支持对称密钥算法类型为AES_256、SM4。
- 支持非对称密钥算法类型为RSA_2048、SM2。

#### 硬件保护

通过部署托管密码机，采用由国家密码管理局批准的密码设备硬件，满足监管合规需求。

提供更高安全等级的硬件保护机制保护密钥，确保密钥的保密性、完整性和可用性。

#### 密钥轮转

支持通过定期自动轮转或手动创建密钥版本，以加强密钥使用的安全性。

- 对于对称密钥，密钥版本可通过设置轮转策略，由系统根据轮转周期自动生成。
- 对于非对称密钥，可人工创建新的密钥版本。

密钥轮转或人工创建产生新的主版本后，KMS不会删除或禁用非主版本，使得经非主版本加密的密文仍可以正常解密。

#### 自带密钥导入

支持导入用户自带密钥。当用户希望使用自己的密钥材料时，可通过KMS管理控制台的导入密钥功能创建密钥材料为空的用户主密钥，并将自己的密钥材料导入该用户主密钥中。

#### 别名管理

别名是用户主密钥的可选标识，同一个用户在一个地域中的别名具有唯一性。每个别名只能指向同地域的一个用户主密钥，但是每个用户主密钥可以绑定多个别名。

用户可通过控制台创建别名、删除别名，还可以通过API进行别名的创建、更新、删除等。

#### 在线加密

在线加密是对称密钥加密的场景，适用于保护小型敏感数据（小于6KB），如口令、证书、身份信息、后台配置文件等。通过密钥管理服务KMS的在线加密API，使用用户主密钥（CMK）直接加密敏感数据信息，而非直接将明文存储，确保敏感数据安全。

#### 信封加密

信封加密是对称密钥加密的场景，是一种应对海量数据的高性能加解密方案。这种技术不再使用用户主密钥（CMK）直接加密和解密数据，而是通过生成加密数据的数据密钥（DEK），将其封入信封中（即通过CMK加密）存储、传递和使用，由KMS确保数据密钥的随机性和安全性。

实际使用时，用户无需将大量业务数据上传至KMS服务端，直接通过离线的数据密钥在本地实现加解密，有效避免安全隐患，保证了业务加密性能的要求。

#### 签名验签

数字签名技术是非对称加密算法的另一种典型应用。用户可在KMS中创建非对称用户主密钥（CMK），其由一对关联的公钥和私钥构成。公钥可以被分发给任何人，而私钥由KMS确保安全性，不提供任何接口导出非对称密钥的私钥。 使用者仅能通过接口调用私钥进行签名运算。

实际使用时，签名者将验签公钥分发给消息接收者，签名者使用签名私钥，对数据产生签名，签名者将数据以及签名传递给消息接收者，消息接收者获得数据和签名后，使用公钥针对数据验证签名的合法性。

#### 非对称数据加解密

非对称密钥加密通信的过程类似于对称加密，区别在于需要使用公钥进行数据加密，使用私钥进行数据解密。由于KMS中用户私钥不支持导出，使用者仅能通过接口调用私钥进行数据解密。

实际使用时，信息接收者将加密公钥分发给信息传送者，信息传送者使用公钥对敏感信息进行加密保护，信息传送者将敏感信息的密文传递给信息接收者，信息接收者使用私钥将敏感信息的密文解密。

#### 云产品服务端加密

与天翼云产品联动，提供对云硬盘、对象存储、弹性文件、数据库等产品中的数据进行服务端加密，保证云上数据的安全性。用户只需通过云产品控制台一键勾选KMS加密功能，加解密过程透明无感知。

#### 完整性保护

提供基于国密算法的完整性保护能力，通过SM3算法计算HMAC值以进行对比验证，实现完整性校验。

## 相关术语解释

### 对称密钥加密

又称私钥加密，即信息的发送方和接收方用一个密钥去加密和解密数据。

### 非对称密钥加密

非对称密钥由一对互相关联的公钥和私钥组成，其中的公钥可以被分发给任何人，而私钥必须被安全保护起来，只有受信任者可以使用。非对称密钥通常用于在信任程度不对等的系统之间，实现数字签名验签或者加密传递敏感信息。

### 用户主密钥（Customer Master Key，CMK）

用户主密钥包括对称密钥及非对称密钥，主要用于加密保护数据密钥，也可直接用于加密少量的数据。用户可以调用KMS的产品控制台或CreateKey接口创建一个用户主密钥。

### 默认主密钥（Default CMK）

用户使用云产品加密功能时，由云产品触发KMS系统自动生成的并托管在用户账号下的服务密钥。

### 信封加密（Envelope Encryption）

信封加密是类似数字信封技术的一种加密手段。这种技术将加密数据的数据密钥封入信封中存储、传递和使用，不再使用用户主密钥（CMK）直接加密和解密数据。当需要加密业务数据时，可以调用KMS的GenerateDataKey或GenerateDataKeyWithoutPlaintext接口生成一个对称密钥，同时使用指定的用户主密钥加密该对称密钥（被密封的信封保护）。

### 数据加密密钥（Data Encryption Key，DEK）

信封加密技术中用于加密业务数据的密钥，受用户主密钥CMK加密保护。

### 硬件安全模块（Hardware Security Module，HSM）

硬件安全模块也称为密码机，是一种执行密码运算、安全生成和存储密钥的硬件设备。KMS提供的托管密码机可以满足监管机构的检测认证要求，为用户在KMS托管的密钥提供更高的安全等级保证。

### 密钥导入（Bring Your Own Key，BYOK）

指用户可以自行导入密钥材料至用户主密钥中，KMS不会为创建的用户主密钥（CMK）生成密钥材料。

### 应用接入点

是一种身份验证和访问控制机制，当用户VPC内的自建应用需要访问KMS服务时，需要创建应用接入点实现私网通道打通，同时在应用接入点内完成访问权限策略配置以及身份凭证的生成。

## 应用场景

密钥管理服务KMS（Key Management Service）具有广泛的应用场景。

### 场景介绍

| 应用场景 | 开发者身份 | 受保护数据 | 保护目的 | 解决方案 |
| --- | --- | --- | --- | --- |
| 敏感信息加密保护 | 网站或应用开发 | 证书、密钥 | 网站和应用使用HTTPS证书来保证通信协议的安全性，同时使用密钥对文件进行数据签名。这些安全解决方案非常依赖证书和密钥本身的安全性。 | 敏感数据在线加密 |
| | 后台服务开发 | 密码、登录密钥、配置信息 | 数据库密码、登录密钥以及后台服务的配置信息可能会被黑客利用，明文存储在硬盘上非常危险。 | 敏感数据在线加密 |

| 应用场景 | 开发者身份 | 受保护数据 | 保护目的 | 解决方案 |
| --- | --- | --- | --- | --- |
| 重要文件加密保护 | 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行业竞争优势，务必防范“拖库”事故的发生。 | 信封加密 |
| | 政府、金融机构 | 协议通信内容、重要文件和资料 | 政府和金融机构的通信和存储数据具有高价值性和高保密性，需要在建立业务系统时就充分考虑安全性和合规性。 | 敏感数据在线加密、信封加密 |
| 云上数据安全保护 | 云服务 | 云上数据 | 企业上云过程中，需要在云上存储并处理大量数据，云上数据的安全性及便捷性成为企业安全用云的核心诉求。 | 云产品透明加密 |

### 数据加密方案

为满足各类场景下的数据加密需求，KMS提供标准化的接口能力，支持多种加密方案。

## 敏感数据在线加密

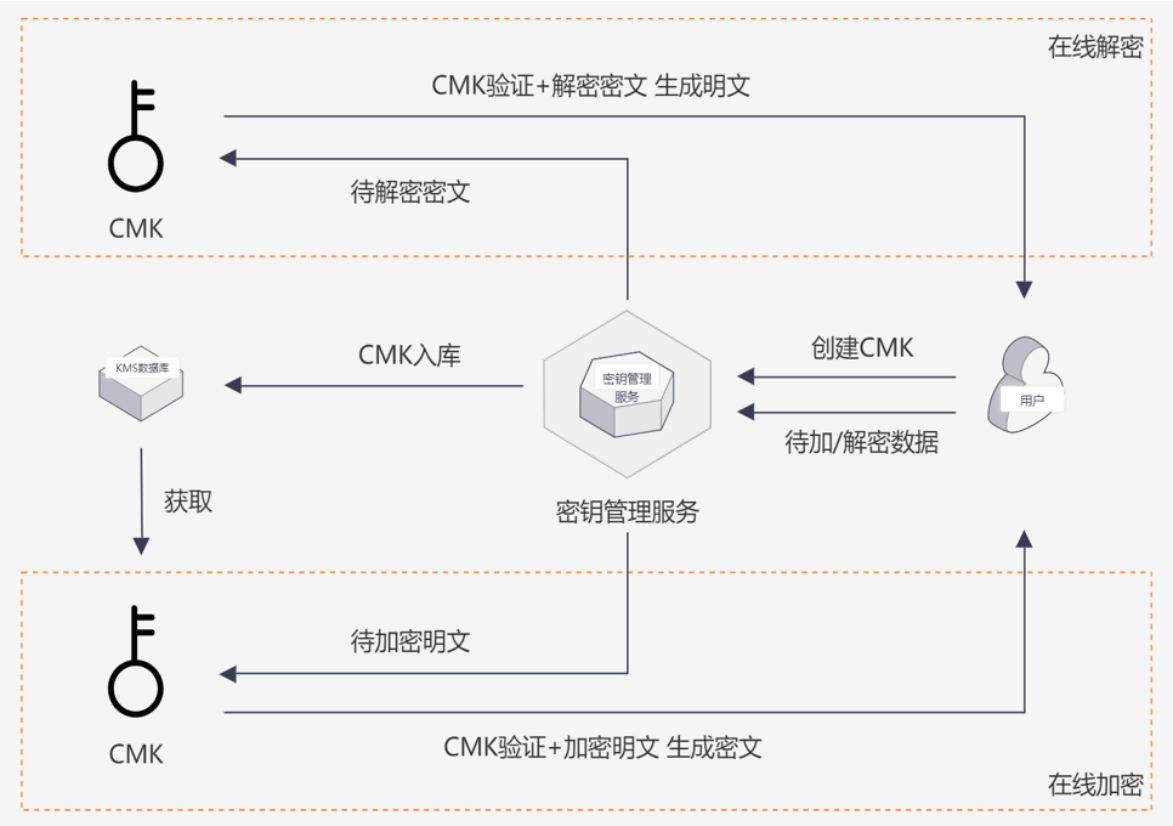
通过调用密钥管理服务（KMS）的密码运算API实现数据的在线运算，直接使用用户主密钥进行数据的加解密。

场景特点：用于少量数据（例如：口令、证书、配置文件等）的加密保护，有效避免敏感信息泄露。

### 优势

- 轻松加密：通过密钥管理服务的密码运算API，在线对数据直接加解密。
- 安全可靠：直接通过主密钥进行数据加解密保护，保证明文数据不落盘。

### 场景示意图




## 信封加密

通过调用密钥管理服务（KMS）的密码运算API在线生成数据密钥，数据密钥通过用户主密钥加密并支持安全导出，通过导出的数据密钥在本地进行大规模数据的加解密。

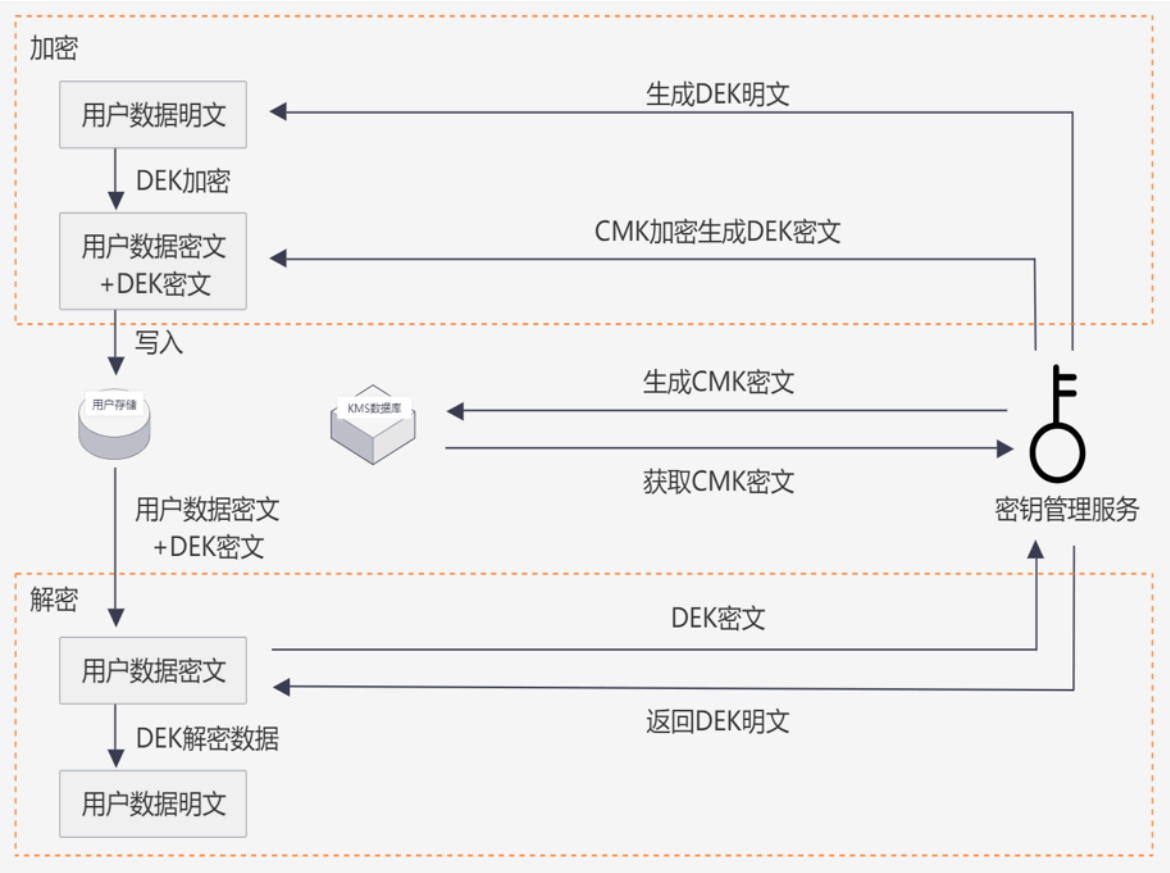
### 场景特点

用于海量大型数据或对性能敏感数据的加密保护，保证业务访问体验。

### 优势

- 高效易用：通过创建数据密钥，实现本地数据的离线加密，避免移动大量数据产生安全隐患。
- 双重加密：通过主密钥和数据密钥两级密钥结构，确保数据密钥的随机性和安全性，保证数据加密性能。

### 场景示意图




## 云产品透明加密

密钥管理服务（KMS）与多种云产品集成，提供服务端加密能能力，加密功能一键开启，加密过程透明无感知。

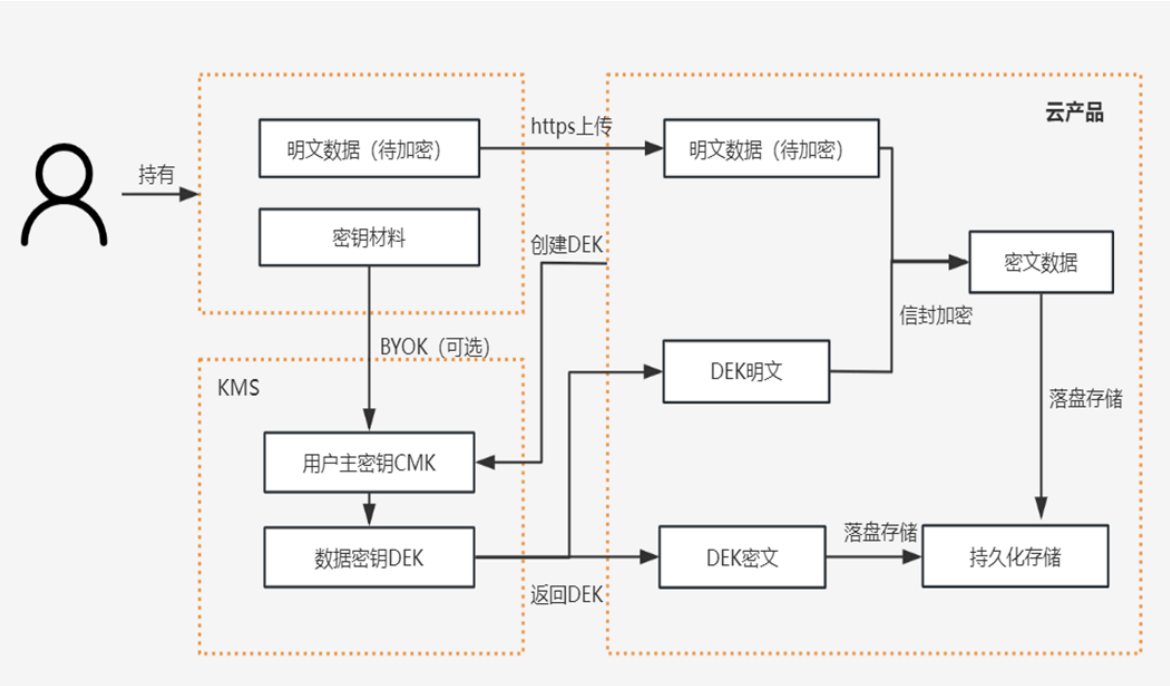
### 场景特点

为云上IT设施数据安全环境提供基础保障。

### 优势

- 服务端自动加密：无需用户自行实现复杂的加密能力，免改造。
- 安全保障：加密密钥通过KMS主密钥加密保护，满足安全合规要求。

场景示意图




# 产品规格

注意

自2024年9月13日起，KMS全新升级上线包周期版，升级后不再支持按需版本的开通，新用户需购买包周期版KMS（基础版、企业版），原已开通按需版KMS的用户仍可继续使用按需密钥，并依据按需版计费标准计费。

## 包周期服务

KMS服务提供两种版本，分别为基础版、企业版，您可以根据本章节列出的版本对比信息，选择合适的服务版本，同时，KMS包周期服务提供免费的默认密钥，支持用于云产品加密功能。具体配额数据请参见下方表格。

同一账号支持开通多套KMS服务，服务之间资源隔离。单套KMS服务规模取决于基础实例数量，您可根据业务需求选择开通数量，支持扩容，扩容后可提升服务整体性能及可用性。服务性能（单基础实例）请参见性能数据。

说明

当前仅华南2资源池支持开通多套KMS服务，其他资源池陆续上线，敬请关注。

√表示支持，×表示不支持。

| 对比项 | 子项 | 默认密钥 | 基础版 | 企业版 |
| --- | --- | --- | --- | --- |
| 计费模式 | - | 免费 | 包周期 | 包周期 |

| 对比项 | 子项 | 默认密钥 | 基础版 | 企业版 |
| --- | --- | --- | --- | --- |
| 应用场景 | 云产品透明加密 | √ | √ | √ |
| | 用户自建应用加密 | - | √ | √ |
| | 密评合规 | - | × | √ |
| | 证书管理 | - | √ | √ |
| 配额 | 默认计算性能（以对称加密为例） | 1000QPS（所有云产品的默认密钥共享加密接口的性能） | • 单基础实例专享：2000QPS（通过应用接入点在VPC间调用）<br>• 共享网关：750QPS（通过openapi调用） | • 单基础实例专享：2000QPS（通过应用接入点在VPC间调用）<br>• 共享网关：750QPS（通过openapi调用） |
| | 密钥数量 | 每个天翼云账号在每个资源池，可为每个云产品创建1个默认密钥 | 单基础实例：0-2000个 | 单基础实例：0-2000个 |
| | 证书数量 | - | 单基础实例：0-1000个 | 单基础实例：0-1000个 |
| | 应用接入点 | - | 单基础实例：3个 | 单基础实例：3个 |
| 接入网络类型 | - | 内部网络 | • openapi（公网）<br>• VPC间调用（私网） | • openapi（公网）<br>• VPC间调用（私网） |
| 密钥管理 | 密钥规格 | AES_256 | • 对称密钥：AES_256<br>• 非对称密钥：RSA_2048 | • 对称密钥：<br>  • AES_256<br>  • SM4<br>• 非对称密钥：<br>  • RSA_2048<br>  • SM2 |
| | 导入外部密钥材料（BYOK） | × | √<br>对称密钥支持 | √<br>对称密钥支持 |
| | 密钥自动轮转 | × | √<br>对称密钥支持 | √<br>对称密钥支持 |
| | 计划删除密钥 | × | √ | √ |
| | 密钥删除保护 | × | √ | √ |
| | 密钥别名管理 | √（系统默认别名） | √ | √ |
| | 密钥标签管理 | √ | √ | √ |
| 密码运算 | 数据加解密 | √（云产品） | √ | √ |
| | 签名验签 | × | √ | √ |
| | 完整性校验 | × | √ | √ |
| 证书管理 | 创建证书 | × | √ | √ |

| 对比项 | 子项 | 默认密钥 | 基础版 | 企业版 |
| --- | --- | --- | --- | --- |
| | 导入证书 | × | √ | √ |
| | 吊销证书 | × | √ | √ |
| | 删除证书 | × | √ | √ |

### 按需服务

对于前期已开通按需版本的客户，仍可继续使用按需服务。按需服务无产品规格上的区分，根据业务情况创建所需的密钥或证书资源即可。

KMS服务会根据所创建的密钥类型及个数、API调用次数进行统计并计费。

## 按需版支持密钥类型

| 密钥类型 | 算法类型 | 保护级别 | 是否支持加解密 | 是否支持签名验签 |
| --- | --- | --- | --- | --- |
| 对称密钥 | AES_256 | Software<br>HSM | √ | × |
| | SM4 | HSM | √ | × |
| 非对称密钥 | RSA_2048 | Software<br>HSM | √ | √ |
| | SM2 | HSM | √ | √ |

## 按需版资源配额

- 默认主密钥：同一云产品在同一资源池仅有一个默认主密钥。
- 用户主密钥-对称密钥：暂不限制创建个数。
- 用户主密钥-非对称密钥：限制密钥的版本数量，同一用户在同一资源池最多创建50个版本。

# 性能数据

## 概述

KMS支持通过SDK或OpenAPI方式调用：

- SDK：应用接入点，内网调用
- OpenAPI：共享网关，公网调用

两种访问方式的接口请求的QPS配额不同，应用接入点的QPS是针对每个KMS服务（基础实例）进行限制，需要更高的QPS时，您可以通过扩展KMS实例的计算性能配额来实现；OpenAPI共享网关的QPS是针对每个天翼云账号进行限制，QPS为固定值不支持升配。

### 应用接入点

应用接入点访问方式的SDK主要包含密码运算类接口，对比OpenAPI调用方式侧重计算性能的提升，即密码运算类的接口QPS，而密钥管理类接口与OpenAPI的QPS一致。

下表列出通过应用接入点访问KMS服务的密码运算类接口限制QPS，数据为单基础实例的参考值。

| 操作类型 | API | QPS（每秒请求数） |
| --- | --- | --- |
| 处理对称密钥算法 | encrypt<br>exportDataKey<br>generateAndExportDataKey<br>generateDataKeyWithoutPlaintext<br>reEncrypt<br>generateDataKey<br>decrypt | 2000 |
| 处理非对称密钥算法 | asymmetricEncrypt<br>asymmetricDecrypt<br>asymmetricSign<br>asymmetricVerify<br>getPublicKey | 300 |
| 完整性校验算法 | hmaccompute | 2000 |
| 处理证书运算 | certificatePrivateKeySign<br>certificatePrivateKeyDecrypt<br>certificatePublicKeyEncrypt<br>certificatePublicKeyVerify | 300 |
| 生成随机数 | getRandom | 2000 |

OpenAPI

| 操作类型 | API | QPS（每秒请求数） |
| --- | --- | --- |
| 创建密钥 | createKey | 10 |
| 查询密钥等读操作 | describeKey<br>listAliasKeys<br>listAlias<br>listAliasByUuid<br>listKeyVersions<br>describeKeyVersion<br>getParametersForImport | 50 |

| 操作类型 | API | QPS（每秒请求数） |
| --- | --- | --- |
| 更新密钥属性等写操作 | disableKey<br>enableKey<br>deleteKeyMaterial<br>deleteProtect<br>cancelDeleteProtect<br>updateKeyDescription<br>importKeyMaterial<br>scheduleKeyDeletion<br>updateAlias<br>updateRotationPolicy<br>cancelKeyDeletion<br>createAlias<br>createKeyVersion<br>deleteAlias | 30 |
| 创建、导入证书 | importCertificate<br>createCertificate<br>importCertificateByPKCS12 | 10 |
| 证书查询等读操作 | listCertificate<br>describeCertificate<br>getCertificate<br>exportCertifiicatePrivatkey<br>describeCertificateForUk<br>istCertificateForUk | 50 |
| 证书更新等写操作 | updateCertificateStatus<br>deleteCertificate<br>updateCertificateStatusForUk<br>deleteCertificateForUk | 30 |
| 处理对称密钥算法 | encrypt<br>exportDataKey<br>generateAndExportDataKey<br>generateDataKeyWithoutPlaintext<br>reEncrypt<br>generateDataKey<br>decrypt | 750 |
| 处理非对称密钥算法 | asymmetricEncrypt<br>asymmetricDecrypt<br>asymmetricSign<br>asymmetricVerify<br>getPublicKey | 200 |
| 完整性校验算法 | hmaccompute | 750 |

| 操作类型 | API | QPS（每秒请求数） |
| --- | --- | --- |
| 处理证书运算 | certificatePrivateKeySign<br>certificatePrivateKeyDecrypt<br>certificatePublicKeyEncrypt<br>certificatePublicKeyVerify | 200 |
| 生成随机数 | getRandom | 750 |

# 与其他云服务关系

## KMS与其他云服务的加密关系

KMS集成天翼云产品提供服务端加密能力，实现云上原生数据提供加密保护，有效提升默认安全能力。在创建云产品资源时开启加密功能，您可以自定义加密密钥，支持选择默认密钥和您在KMS中自行创建的用户主密钥。

## 服务端加密优势

- 提升云产品内生安全性

  加密过程中使用的密钥由用户自定义选择，集中托管在KMS服务中，KMS已通过国家密码管理局审查，获得商用密码产品认证，合规性得到有效保障。
- 降低研发成本

  使用云产品服务端加密能力，您无需自行构建和维护密钥管理基础设施，无需考虑自研数据加密能力所涉及的密钥管理安全及合理性、加密算法的研发等一系列复杂的工程，大幅度降低开发成本。
- 加密过程透明无感知

  服务端加密为您提供内嵌至云服务中的加密方案，您无需关注底层数据加密的细节，只需一键开启加密功能，即可实现数据加密。

## 支持服务端加密的云产品

- 云硬盘
- 对象存储
- 弹性文件
- 关系型数据库MySQL版
- 关系型数据库PostgreSQL版
- 文档数据库服务

功能详情详见云产品服务端加密。

### KMS与云审计服务的关系

已对接天翼云云审计服务，可通过云审计服务查看资源操作的记录，用于支撑合规审计、安全分析、操作追踪和问题定位等场景，同时提供事件跟踪功能，将操作日志转储至日志审计等产品实现永久保存。

### KMS与云监控服务的关系

已对接天翼云云监控服务，可通过云监控服务查看实例节点的相关监控指标，并可以设置相关指标的告警规则及通知策略。

# 计费说明

## 计费概述

注意

自2024年9月10日起，KMS全新升级上线包周期版，升级后不再支持按需版本的开通，新用户需购买包周期版KMS（基础版、企业版）。

### 计费模式

KMS产品当前支持包周期版本及按需版本，对应两种计费模式：

- 包年/包月计费：一种预付费模式，即先付费再使用。您可根据业务需要，选择合适的包周期服务版本（基础版、企业版），一次性支付一个月/多个月/一年/多年的费用，支付成功后，KMS服务资源将被系统分配给用户使用，直到超过保留期后被系统回收。
- 按使用量计费：一种后付费模式，即先使用再付费。在结算时会按照您在按需版本中，实际资源使用量收取费用，如密钥数量、API调用量等。

注意

KMS包周期版本上线后，则不再允许新增用户开通按需版本，存量用户可继续使用已有按需资源，已上线包周期服务的资源池不再支持新增按需密钥。

若需长期使用存量按需资源，请注意保证账户余额充足，避免因账号欠费导致服务冻结、资源释放。

#### 优惠政策

KMS包周期版支持包年优惠政策，若您按年购买，可享受8.5折优惠。

#### 账单和用量查询

您可以在天翼云管理中心-账单管理中的流水账单、账单详情页面查看计费详情，支持导出账单明细。

## 计费项

### 密钥管理-包周期版

### 主版本基础实例服务费

| 计费项 | 说明 | 标准资费（包月） | 计费周期 |
| --- | --- | --- | --- |
| 基础版 | 提供软件保护等级服务，支持客户构建专属的密钥库，具备高度可扩展性；同时提供极简的密码运算接口能力，满足应用的安全快速集成。 | 3099元 | 1~11个月、1年、2年、3年 |
| 企业版 | 提供硬件保护等级服务，底层对接使用经国家密码管理局认证的密码机硬件，提供更高安全与合规等级保证的资源管理及密码运算服务，满足监管机构的检测认证要求。 | 9699元 | 1~11个月、1年、2年、3年 |

关于不同服务版本的规格参数，请参见产品规格。

# 计费说明

针对一次性包年付费，可享8.5折优惠，如一次性支付2年，费用=包月标准价格x24x85%。

## 扩展资源服务费

| 计费项 | 说明 | 标准资费（包月） | 计费周期 |
| --- | --- | --- | --- |
| 计算性能扩展包 | 服务基础实例中默认提供计算性能配额，若用户需求超过KMS服务默认提供的QPS限制时，可以通过叠加计算性能扩展包提升上限。 | 600元/个 | 1~11个月、1年、2年、3年 |
| 应用接入点 | 通过应用接入点可以实现用户VPC内的应用内网访问KMS服务，同时实现权限管控，用户可根据业务需求创建多个应用接入点，实现不同应用访问控制。 | 600元/个 | 1~11个月、1年、2年、3年 |
| 密钥数量 | 服务基础实例中默认包含一定的配额，若用户需求超过KMS服务默认提供的数量限制时，可以按需额外购买。 | 30元/10个 | 1~11个月、1年、2年、3年 |

针对一次性包年付费，可享8.5折优惠。

说明

资源扩展项基于包周期版本服务叠加购买、续订、退订，到期时间与主版本服务一致，不支持单独购买、续订、退订。

### 密钥管理-按需版

## 密钥托管费

密钥创建后托管在KMS服务产生的费用，按照密钥类型、密钥个数以天为周期进行计费。

| 计费项 | 说明 | 标准资费（元/天） | 计费周期 |
| --- | --- | --- | --- |
| 默认主密钥 | 在使用云产品加密功能时，由云产品为用户自动创建的主密钥，同时托管在用户主账号下。 | 免费 | —— |
| 用户主密钥-软件密钥 | 由用户自主创建且保护级别为Software的主密钥。 | 0.014 | 天 |
| 用户主密钥-硬件密钥 | 由用户自主创建且保护级别为Hsm的主密钥。 | 0.237 | 天 |

说明

计划删除状态的密钥不收费。

# 计费说明

## API调用费

密钥创建后通过接口调用产生的请求费用，按照API请求次数计费，每个账户每月有20000次的免费请求次数，超过20000次后开始计费。

| 计费项 | 含义 | 标准资费（万次/月） | 计费周期 |
| --- | --- | --- | --- |
| API调用 | 用户通过云原生接口调用密钥实现密码运算操作产生的调用量。 | 0.6 | 月 |

说明

仅密码及证书运算类接口调用收费。

### 客户端加密模块

通过在客户端服务器集成客户端加密模块，实现数据加解密、文件流加解密等功能，帮助客户在本地完成大型文件数据的加解密。

| 计费项 | 计费方式 | 标准资费 |
| --- | --- | --- |
| 基础版 | 免费 | 免费 |
| 企业版 | 一次性计费（按License个数计费） | 10000元/个 |

# 续订说明

若您购买了包周期版KMS服务，为避免KMS服务到期后停服导致您的业务无法使用密钥等资源，需要在服务到期前为实例手动续订，或设置到期自动续订策略。

## 到期说明

- 服务即将到期前，系统会以短信或邮件的形式提醒服务即将到期，并提醒用户续订。
- 服务到期后，如果没有按时续订，平台会冻结服务，但用户的资源及配置信息会提供15天的保留期。

说明

保留期内，平台会冻结KMS服务，用户购买包周期版本后所创建的密钥等资源不可用，即无法正常进行加解密等运算操作。保留期满，用户若仍未续订，平台会清除服务资源，用户所创建的密钥等资源及其所有配置将会被删除且不可恢复。 如果您仍需继续使用KMS服务中的密钥等资源，请提前进行续订。

### 续订说明

- 服务支持手动续订，需要在服务到期前进入KMS产品控制台或天翼云续订管理页面操作。续订规则可参考续订规则说明。
- 在购买KMS服务时，支持勾选并同意“自动续订”，则在服务到期前，系统会自动按照默认的续订周期生成续费订单并进行续费，无须用户手动续订。自动续订规则可参考自动续订。

# 计费说明

说明

若购买KMS服务时勾选了“自动续订”，系统将会默认设置续费周期：

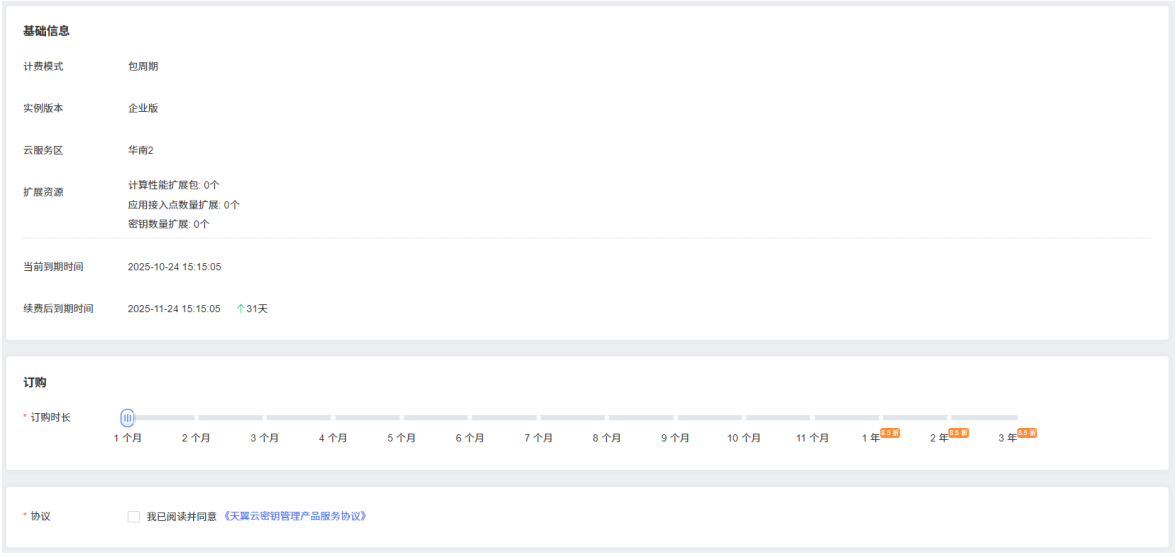
- 按月购买，自动续订周期默认为1个月。
- 按年购买，自动续订周期默认为1年。

如需要修改自动续费周期，可进入天翼云“费用中心 > 订单管理 > 续订管理”页面，在资源页面找到待修改自动续订的资源，单击操作列的“修改自动续订”，拖动“续订周期”可修改自动续订周期，当自动续订周期达1年或以上时，将可享受包年折扣。

**操作步骤**

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > 密钥管理”。
4. 在左侧导航栏，选择“信息概览”，进入信息概览页面，在页面上方选择目标服务。


5. 切换至目标服务后，在当前服务信息展示页面，点击“续订”。
6. 进入续订页面，选择订购时长，确认无误后，勾选“我已阅读并同意《天翼云密钥管理产品服务协议》”后，点击“确认”后进入支付页面。



7. 完成订单支付，可在订单详情页查看订单状态，状态更新为“已完成”后代表续订成功。

# 退订说明

KMS服务支持退订，可通过KMS服务控制台界面、天翼云费用中心发起并完成退订操作。

## 退订说明

您可根据需要，在符合天翼云退订规则的前提下，灵活退订KMS服务。目前退订包含七天无理由全额退订和非七天无理由退订以及其他退订，退订规则详情见退订规则说明。

退订完成后，退款金额会退回账户余额，客户可根据需要进行提现。提现操作详情见余额提现。

说明

KMS基础版、企业版服务支持退订；默认密钥由天翼云云服务创建，为免费资源，无须退订。

成功发起退订后，KMS将转入冻结状态，冻结期15天。冻结期间，密钥等资源及配置会保留15天，15天后资源被释放，释放后无法恢复。

### 操作步骤

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > 密钥管理”。
4. 在左侧导航栏，选择“信息概览”，进入信息概览页面，在页面上方选择目标服务。


5. 在当前服务信息展示页面，点击“退订”。
6. 进入退订申请页面，确认退订信息，信息确认无误后选择退订原因，勾选“我已确认本次退订金额和相关费用”后，点击“退订”后即可进行退订。
7. 系统提示退订申请提交成功，可前往订单详情查看退订进度。

# 到期与欠费说明

KMS目前存在包周期、按需两种付费方式，关于到期、欠费后对KMS服务会进入冻结状态，期间服务将不可用。如需继续使用服务，您需要进行包周期服务续订、账户充值。

# 计费说明

注意若您使用了云硬盘、对象存储、弹性文件、关系数据库Mysql版，并开启了KMS服务端加密功能，请特别注意KMS服务的到期或欠费状态。若KMS服务到期未及时续订、欠费未及时充值而进入冻结，云产品加密所使用的密钥将无法正常使用，加密、解密等调用请求将被拒绝，云产品将会出现异常。

## 包周期到期说明

若您购买了包周期版KMS服务，为避免KMS服务到期后停服导致您的业务无法使用密钥等资源，需要在服务到期前为实例手动续订，或设置到期自动续订策略。

- 服务即将到期前，系统会以短信或邮件的形式提醒服务即将到期，并提醒用户续订。
- 服务到期后，如果没有按时续订，平台会冻结服务，但用户的资源及配置信息会提供15天的保留期。

说明保留期内，平台会冻结KMS服务，用户购买包周期版本后所创建的密钥等资源不可用，即无法正常进行加解密等运算操作。保留期满，用户若仍未续订，KMS服务将被释放，用户所创建的密钥等资源及其所有配置将会被删除且不可恢复。 如果您仍需继续使用KMS服务中的密钥等资源，请提前进行续订。

### 按需欠费说明

当您已开通KMS按需版服务，若账户进入欠费状态，平台会冻结KMS按需版服务，服务将不可用，同时按需资源会进入保留期。

- KMS按需版服务资源保留期为15天，保留期内KMS按需服务停止服务，用户对密钥管理系统的访问将被拒绝。
- 欠费期间，KMS将不会再收取密钥托管费用，但当月进入冻结状态前所产生的API调用费，在本月底仍会生成账单，累计欠费。
- 若您在保留期内充值，充值后系统会自动扣减欠费金额。
- 若保留期到期您仍未充值，KMS服务中的密钥等资源会被释放且不可恢复。
- 结清账单后，已欠费冻结的KMS按需服务会自动启动并进入可用状态。

## 注册天翼云账号

在创建和使用密钥管理服务之前，您需要先注册天翼云门户的账号。本节将介绍如何进行账号注册，如果您拥有天翼云的账号，请跳转到开通密钥管理服务。

1. 登录天翼云门户，单击“免费注册”；


2. 在注册页面，请填写“邮箱地址”、“登录密码”、“手机号码”，并点击 **同意协议并提交**，如1分钟内手机未收到验证码，请再次点击 **免费获取短信验证码**；


3. 注册成功后，可到邮箱激活您的账号或立即体验天翼云。

## 购买密钥管理服务

密钥管理服务（KMS）包周期版提供基础版、企业版两个规格，本章为您介绍如何购买KMS服务。

## 前提条件

已经注册天翼云账号并完成实名认证。

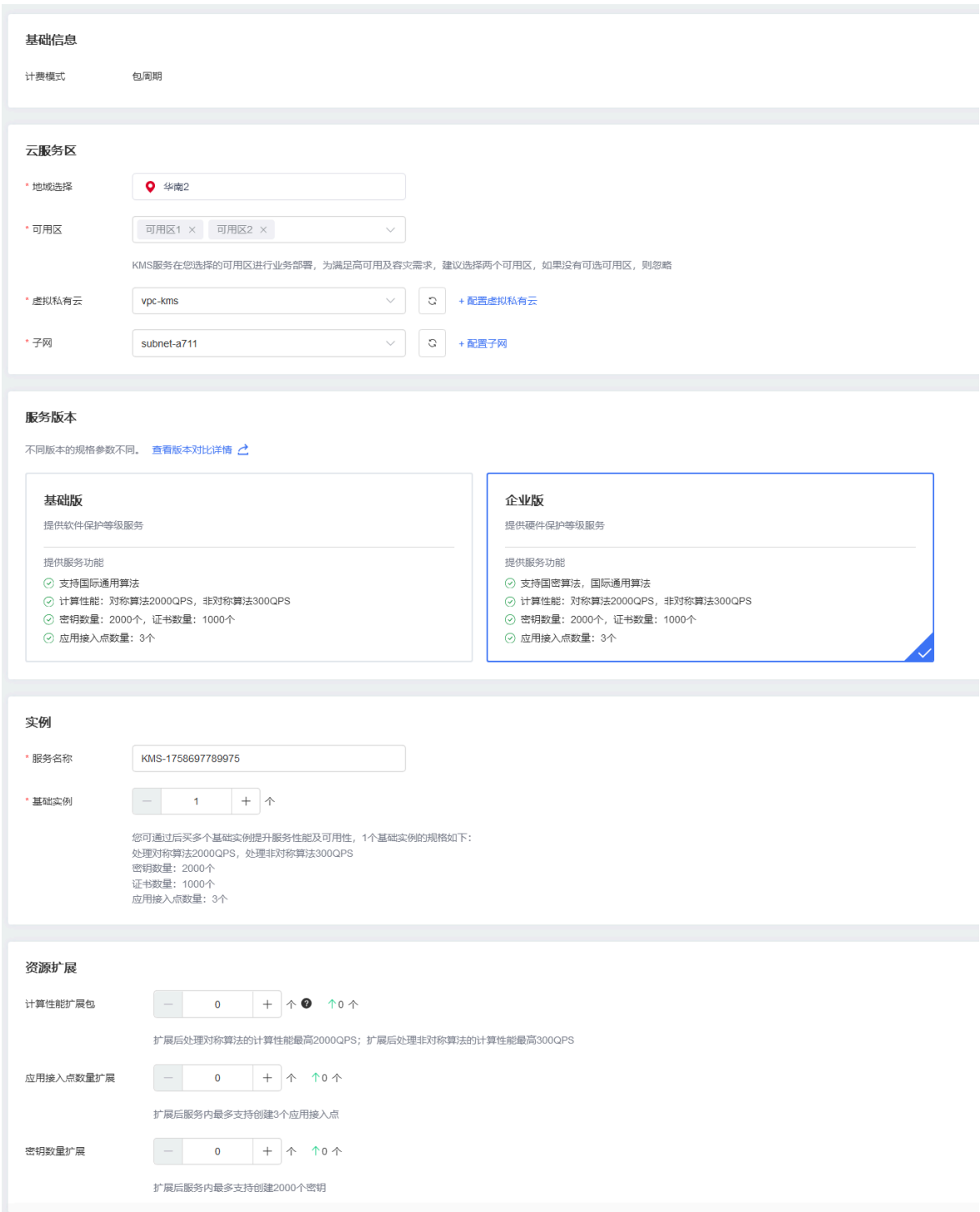
### 规格限制

- 基础版提供软件保护等级服务，支持客户构建专属的密钥库，具备高度可扩展性；同时提供极简的密码运算接口能力，满足应用的安全快速集成。
- 企业版提供硬件保护等级服务，底层对接使用经国家密码管理局认证的密码机硬件，提供更高安全与合规等级保证的资源管理及密码运算服务，满足监管机构的检测认证要求。
- 基础版、企业版单基础实例计算性能（应用接入点）默认为2000QPS。
- 基础版、企业版单基础实例最多可创建2000个密钥、1000个证书。

## 操作步骤

1. 进入天翼云门户并登录，在产品导航栏，定位到“安全与管理”分类，找到密钥管理，点击进入。
2. 进入密钥管理产品详情页，单击“立即开通”。

3. 进入到**密钥管理服务订购**页面，选择云服务区、服务版本、实例数量、扩展资源数量，设置订购时长，确认参数配置后，阅读《天翼云密钥管理服务协议》，并勾选“我已阅读并同意《天翼云密钥管理服务协议》”，点击“立即购买”。

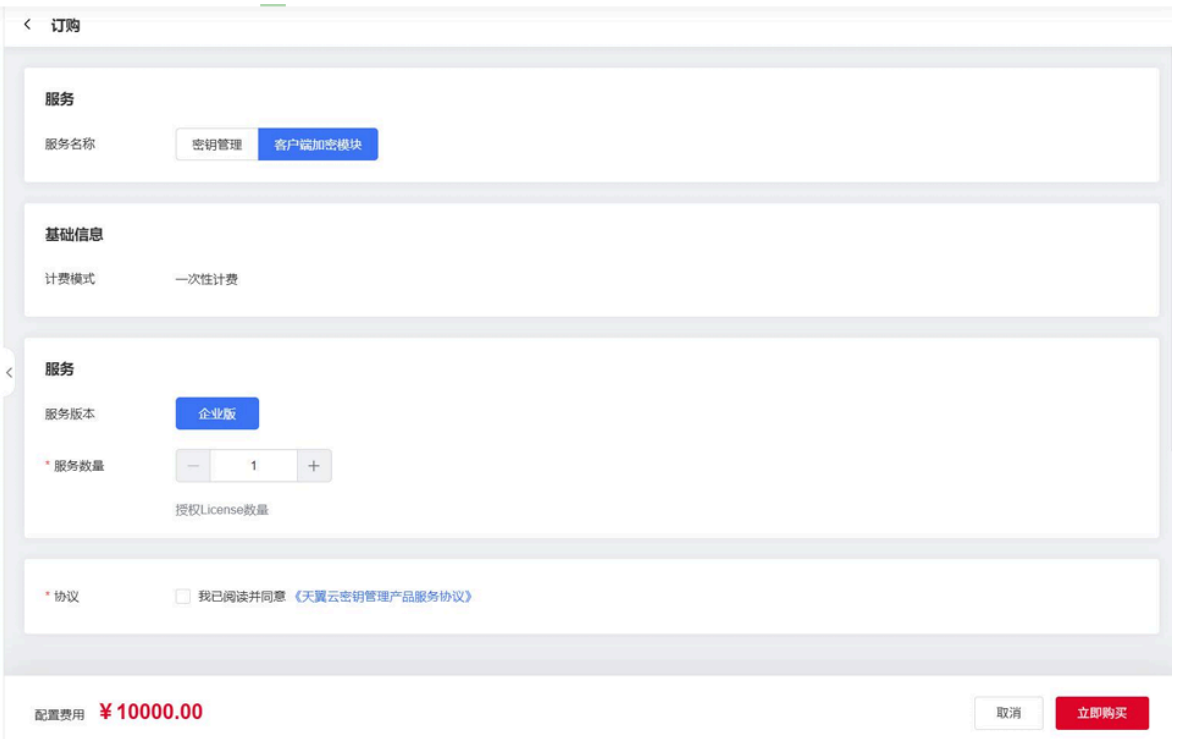


4. 进入**订单详情**页面，确认支付金额，点击 **立即支付** 。
5. 完成订单支付，可在**订单详情页**查看订单状态，状态更新为“已完成”后代表服务已开通。
6. 服务开通后，您可进入密钥管理服务控制台创建资源。

## 购买客户端加密模块

1. 进入天翼云门户并登录，在产品导航栏，定位到“安全与管理”分类，找到密钥管理，点击进入。
2. 进入密钥管理产品详情页，点击“立即开通”。

3. 进入到密钥管理服务订购页面，服务名称选择“客户端加密模块”，选择服务数量（单次最多可购买 1000 个License）。




4. 阅读《天翼云密钥管理服务协议》，并勾选“我已阅读并同意《天翼云密钥管理服务协议》”，点击 “立即购买”。
5. 进入“订单详情”页面，确认支付金额，点击“立即支付”。
6. 完成订单支付，可在“订单详情”页查看订单状态，状态更新为“已完成”后代表服务已开通。
7. 服务开通后，您可在官网帮助文档下载SDK安装包并配置使用。

# 快速接入服务

开通密钥管理服务后，您可以在控制台轻松地创建不同类型的密钥，以满足各类业务场景的需求。同时密钥集中托管在KMS服务中，便于统一管理，满足安全与合规要求。

## 前提条件

已开通密钥管理服务。

### 步骤一：创建应用接入点

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏选择服务所在的区域。

3. 进入“应用接入点”页面，点击创建应用接入点。

4. 在弹出的创建对话框，根据页面提示进行配置。

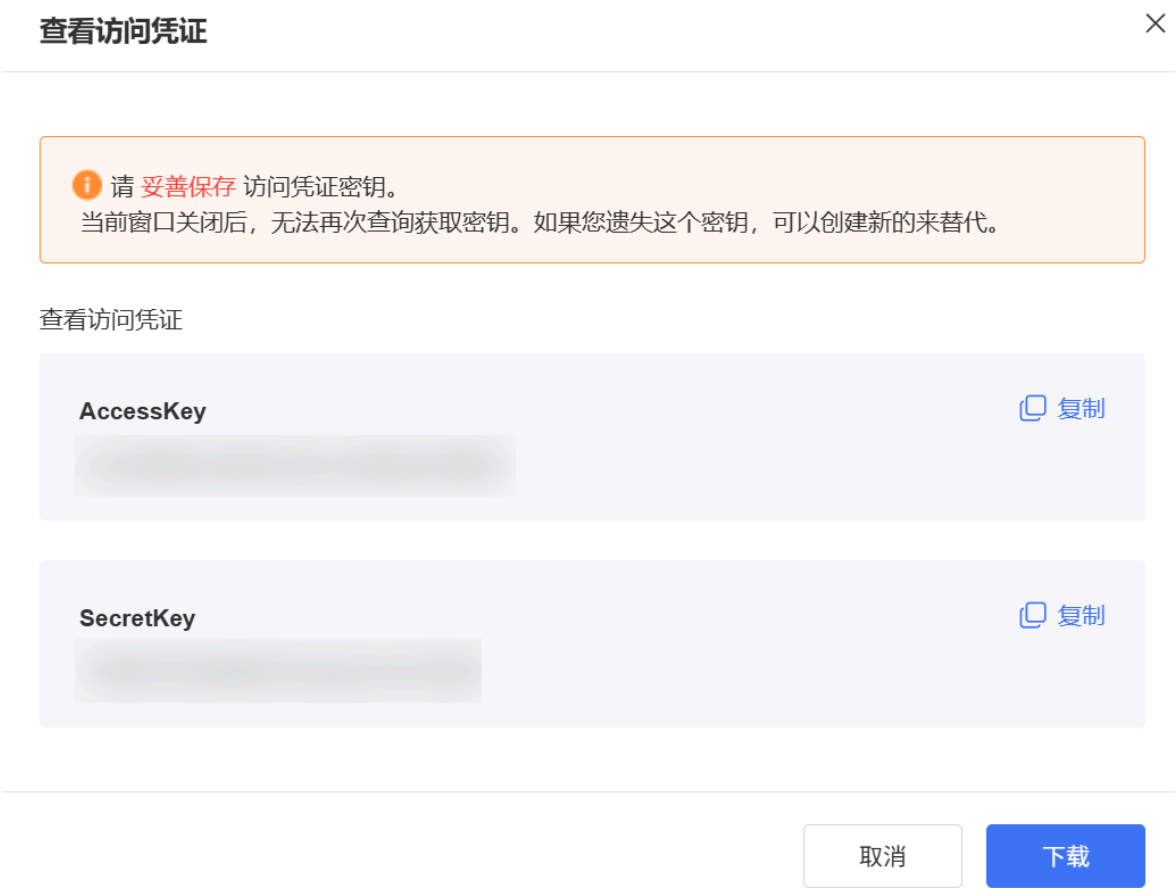
   配置项说明：

| 配置项 | 说明 |
| --- | --- |
| 应用接入点名称 | 自定义名称。 |
| 企业项目 | 选择所属的企业项目。 |
| 虚拟私有云 | 选择当前区域下的虚拟私有云（Virtual Private Cloud，VPC）。<br>说明<br>此处对应的是您应用所在的VPC，即需要连通KMS服务的VPC。 |
| 子网 | 选择当前VPC内子网。 |
| 认证方式 | 默认为“AKSK认证”，不支持修改。 |

5. 创建成功后，您可以在应用接入点列表获取“接入点地址”，后续集成SDK时需要。


6. 选择需要创建AKSK的应用接入点，单击“详情”，进入应用接入点详情页，选择“身份凭证”页签。

7. 单击“创建AccessKey”即可创建访问凭证，请在弹窗中复制或下载该访问凭证。



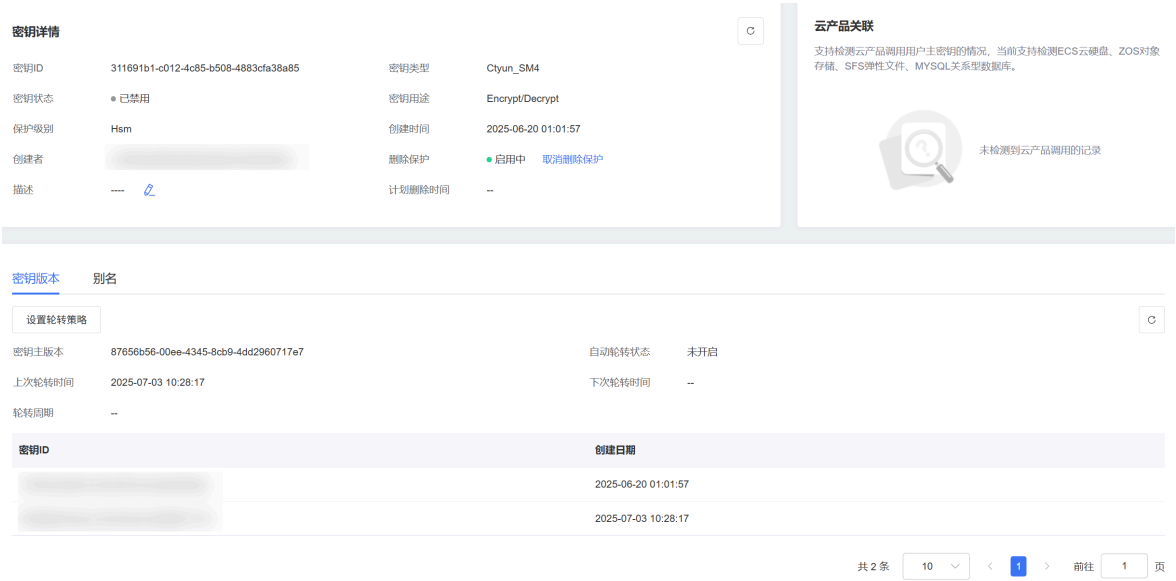
**步骤二：创建密钥**

1. 在密钥列表的“用户主密钥”中，单击 **创建密钥** ，在弹出的**创建密钥**对话框，根据页面提示进行配置。

**配置项说明：**

| 配置项 | 说明 |
| --- | --- |
| 密钥类型 | • 对称密钥类型：<br>AES_256<br>Ctyun_SM4（企业版支持）<br>• 非对称密钥类型：<br>RSA_2048<br>Ctyun_SM2（企业版支持） |
| 密钥用途 | • Encrypt/Decrypt：数据加密和解密。<br>• Sign/Verify：产生和验证数字签名。<br>说明<br>仅非对称密钥（RSA_2048、Ctyun_SM2）支持Sign/Verify用途。 |
| 别名 | 用户主密钥的可选标识。更多操作，请参见别名管理。 |
| 保护级别 | • Software：通过软件模块对密钥进行保护。<br>• Hsm：将密钥托管在密码机中，使密钥获得高安全等级的专用硬件的保护。 |
| 轮转周期 | 自动轮转的时间周期。取值：<br>• 不开启：不开启轮转<br>• 30天<br>• 90天<br>• 180天<br>• 自定义：7~730天<br>说明<br>仅对称密钥（AES_256、Ctyun_SM4）支持设置自动轮转周期。 |
| 描述 | 密钥的说明信息。 |
| 密钥材料来源 | • 天翼云KMS：密钥材料将由KMS生成。<br>• 外部：KMS将不会生成密钥材料，您需要将自己的密钥材料导入KMS。更多信息，请参见导入密钥材料。 |
| 企业项目 | 选择密钥归属的企业项目，默认为default。 |

2. 点击确定，完成密钥创建。您可以在密钥列表查看密钥ID、密钥状态、密钥类型、密钥用途、密钥保护级别等信息。




### 步骤三：使用密钥

您可以将创建的密钥集成到自建应用中，实现应用层的密码技术改造。同时可用于已集成KMS服务的云产品中，满足云产品服务端加密。

- 自建应用集成KMS实现密码技术改造
  - KMS服务提供极简的OpenAPI，您可以轻松实现调用，用于数据加解密、签名验签等场景。

    具体调用方式，请参见API参考。
  - KMS提供SDK，方便用户集成，并通过私网服务地址访问KMS服务。

    具体调用方式，请参见SDK参考。
- 云产品集成KMS密钥实现服务端加密

  当前KMS服务已为云硬盘、对象存储、弹性文件、关系数据库MySQL版产品提供服务端加密能力，您在创建云资源时，可一键开启加密，加密过程透明无感知。更多信息，请参见云产品服务端加密。

# 概览

总览页面帮助您快速了解KMS服务的实际使用情况，包含KMS服务规格、到期时间、资源占用情况等指标。您可以根据使用数据，选择是否需要进行服务续订、资源扩容等。

## 服务版本

- 服务规格：当前账号已开通的服务规格，包括基础版、企业版，规格描述详见产品规格。
- 到期时间：当前包周期服务的到期时间。若您根据业务需求判断是否需要持续使用KMS服务，若需要继续使用，请在到期前及时续订，否则KMS服务将在到期后进入冻结状态，服务将不可用。

### 资源用量

- 用户主密钥数量：用户开通包周期服务后，通过控制台/API接口自主创建的用户主密钥个数，以及当前已创建数量占用服务版本对应配额的数量/总数量。
- 证书数量：用户开通包周期服务后，通过控制台/API接口自主创建的证书个数，以及当前已创建数量占用服务版本对应配额的数量/总数量。
- 默认密钥数量：用户在使用云产品加密功能时，由云产品触发创建的默认密钥数量。

#### 计算性能

- 处理对称算法：对称算法所对应接口的请求配额（上限），超过API请求配额后，KMS会限制请求（即拒绝访问）。
- 处理非对称算法：非对称算法所对应接口的请求配额（上限），超过API请求配额后，KMS会限制请求（即拒绝访问）。

# 服务管理

## 查看KMS服务信息

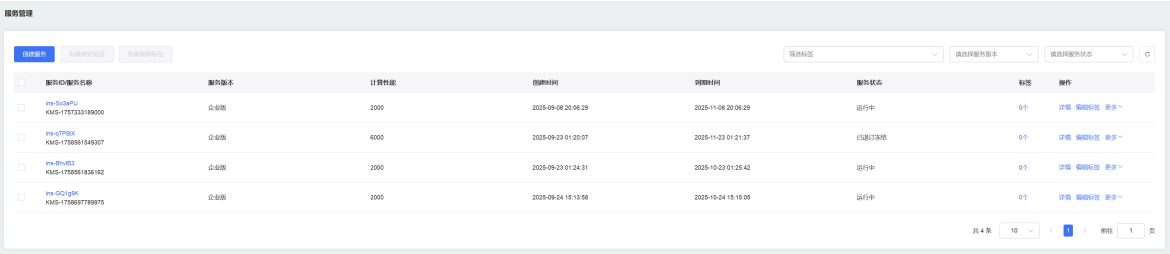
### 前提条件

已购买开通KMS服务。

#### 查看KMS服务信息

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏的资源池下拉列表，选择服务所在的区域。
3. 在左侧导航栏，选择“服务管理”。

4. 在服务管理列表页查看服务基本信息，同时支持对服务进行标签管理。




5. 如需查看服务详情，可以点击服务ID进入详情页，支持查看服务基础信息、性能与额度信息。


6. 在服务详情页，您可以更新服务名称及描述信息。

## 管理KMS服务

### 前提条件

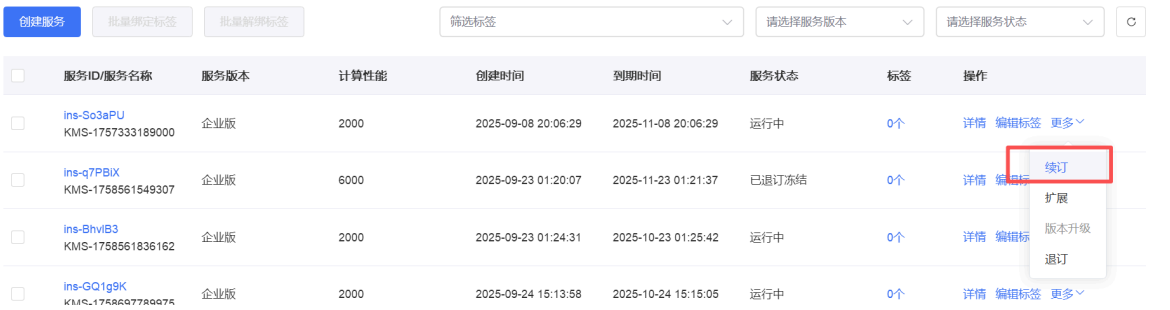
已购买开通KMS服务。

#### 续订KMS服务

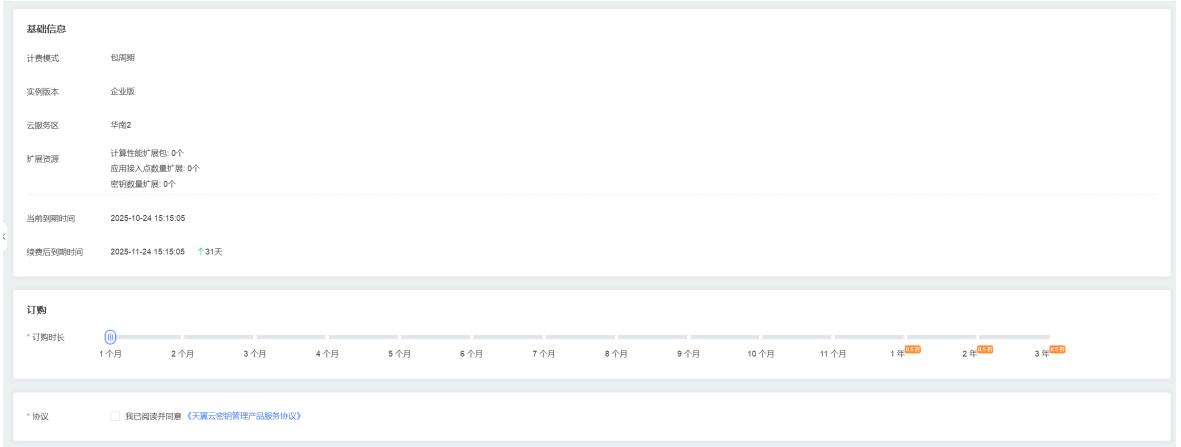
购买KMS服务后，在服务到期销毁前，您可以随时为服务续订。

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏的资源池下拉列表，选择服务所在的区域。
3. 在左侧导航栏，选择“服务管理”。

4. 在服务列表找到目标服务，点击操作列的“续订”。




5. 进入续订页面，选择订购时长，确认无误后，勾选“我已阅读并同意《天翼云密钥管理产品服务协议》”后，点击“确认”后进入支付页面。



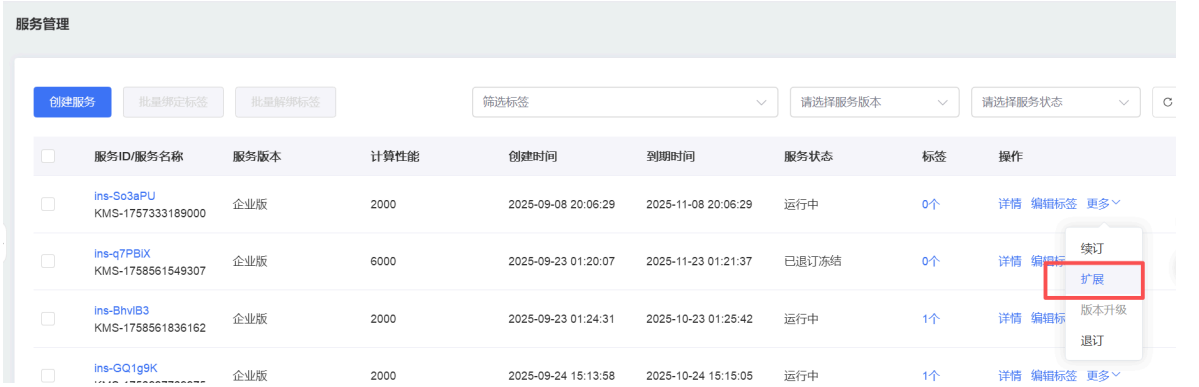

6. 完成订单支付，可在订单详情页查看订单状态，状态更新为“已完成”后代表续订成功。

**扩展KMS服务**

购买KMS服务后，您可以根据业务需求扩展KMS服务资源，获得更高的资源额度和性能指标。

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏的资源池下拉列表，选择服务所在的区域。
3. 在左侧导航栏，选择“服务管理”。

4. 在服务列表找到目标服务，点击操作列的“扩展”。




5. 进入该服务的信息概览页面，在资源扩展模块选择需要扩展的资源。

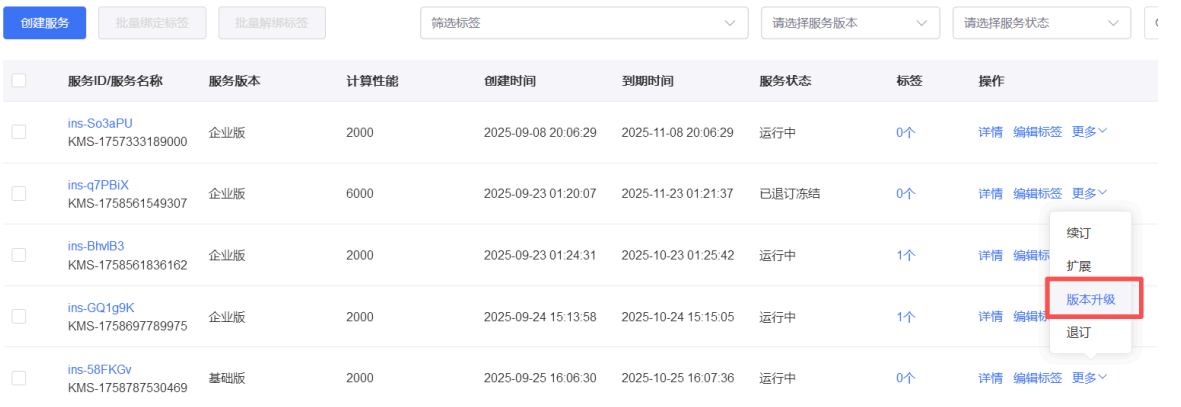
6. 点击对应资源的“扩展购买”按钮，输入扩展数量。确认无误后，勾选“我已阅读并同意《天翼云密钥管理产品服务协议》”后，点击“确认”后进入支付页面。


7. 完成订单支付，可在订单详情页查看订单状态，状态更新为“已完成”后代表资源扩展成功。

升级KMS服务版本

如果您购买了基础版服务，您可以根据业务需求升级至企业版，企业版支持国密算法，同时支持硬件保护。

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏的资源池下拉列表，选择服务所在的区域。
3. 在左侧导航栏，选择“服务管理”。
4. 在服务列表找到目标服务，点击操作列的“版本升级”。



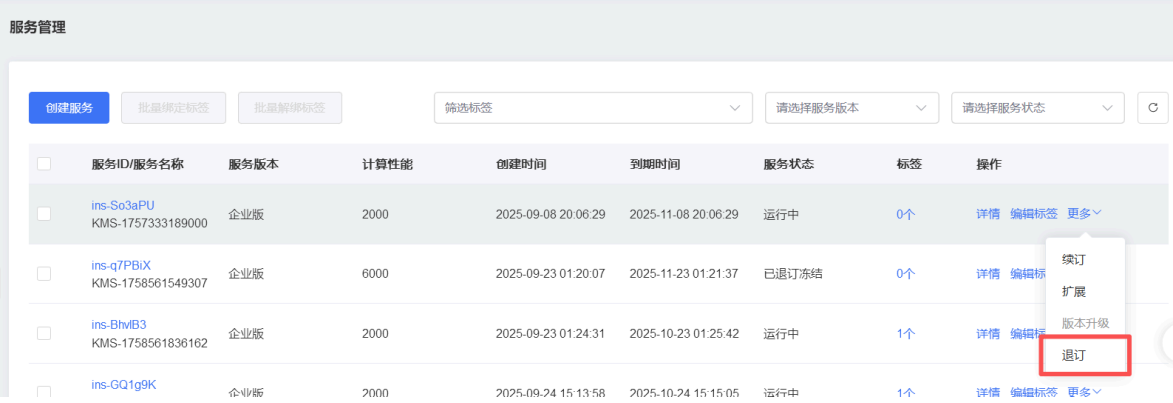
5. 进入该服务的升级页面，确认服务信息无误后，勾选“我已阅读并同意《天翼云密钥管理产品服务协议》”后，点击“确认”后进入支付页面。


6. 完成订单支付，可在订单详情页查看订单状态，状态更新为“已完成”后代表版本升级成功。

退订KMS服务

如果您购买了KMS服务，在服务到期销毁前，您可以随时退订。

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏的资源池下拉列表，选择服务所在的区域。
3. 在左侧导航栏，选择“服务管理”。
4. 在服务列表找到目标服务，点击操作列的“退订”。




5. 二次确认需要退订服务后，进入该服务的退订申请页面，确认退订服务信息，信息确认无误后选择退订原因，勾选“我已确认本次退订金额和相关费用”后，点击“退订”后即可进行退订。
6. 系统提示退订申请提交成功，可前往订单详情查看退订进度。

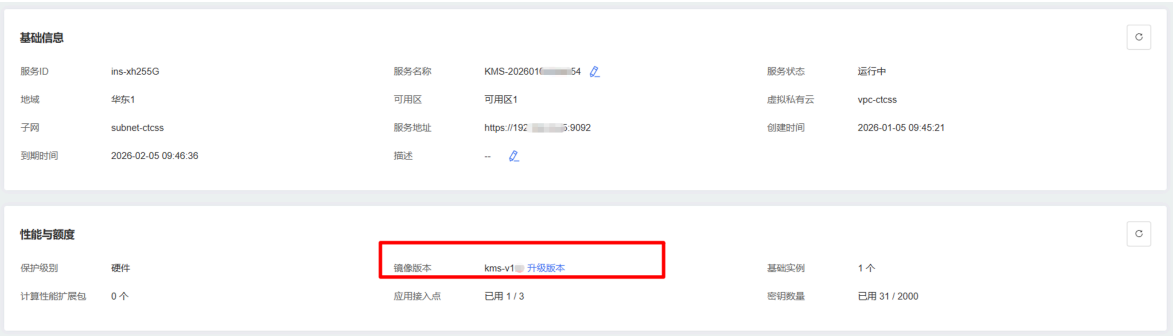
# 升级KMS服务实例镜像版本

## 升级影响

升级时长约为30分钟，过程中可能会存在业务闪断，升级结束后自动恢复正常。因此建议您在业务低峰期进行升级。

### 操作步骤

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏的资源池下拉列表，选择服务所在的区域。
3. 在左侧导航栏，选择“服务管理”。
4. 在服务列表找到目标服务，点击进入服务详情页。
5. 查看镜像版本，如提示“升级版本”则表示KMS服务实例镜像可以升级，如提示“当前已是最新版 本”则表示无需升级。



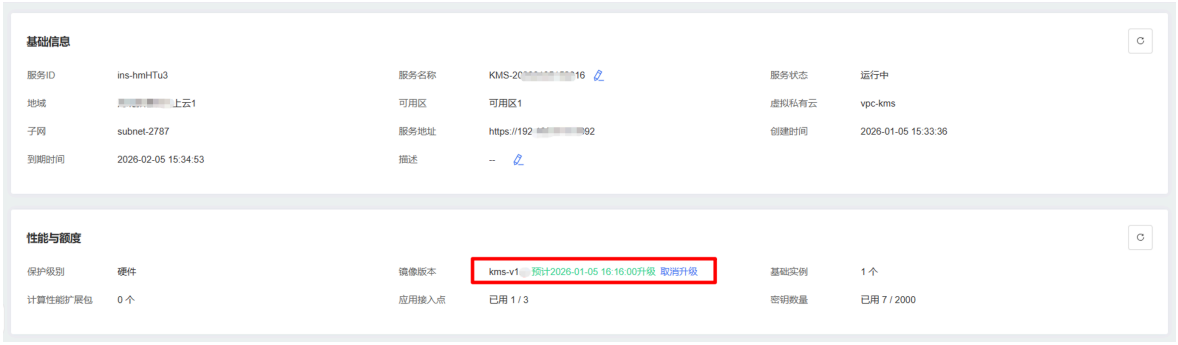
6. 点击升级版本，查看新版本镜像的新功能说明，并配置升级。

> 说明
>
> 当前仅支持升级到镜像的最新版本，不支持指定升级到中间版本。

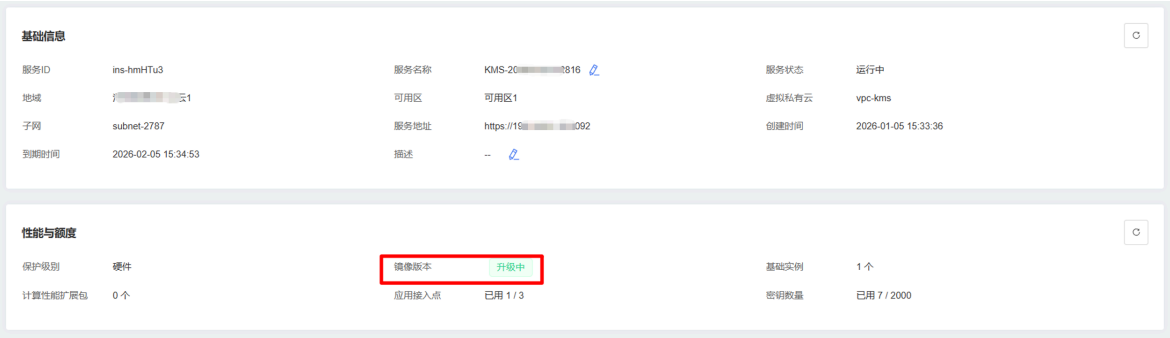
KMS支持如下两种升级方式：

- 自动升级：计划升级，设置升级时间点，到达既定时间系统自动执行升级。支持设置未来7天内的任意时间，您也可以在升级前取消当前升级计划，重新设置升级时间。
- 手动升级：立即升级，点击确定后立即执行升级。


7. 若您设置了自动升级，镜像版本进入等待升级状态，您可以在控制台查看具体的升级时间。若需要改变升级计划，可以点击“取消升级”，并重新配置升级计划。



8. 系统执行升级时，镜像版本状态变为“升级中”，此过程大概约30分钟。




9. 等待约30分钟后，查看镜像版本升级结果。镜像版本状态为“当前已是最新版本”，则表示升级成 功。提示“升级失败”时，请联系天翼云技术支持。

# 密钥管理

## 密钥管理概述

密钥管理服务提供密钥的全托管的生命周期管理能力，支持基于API接口的数据加解密和数字签名验签。

### KMS支持的密钥类型说明

KMS对加密算法、保护级别以及应用场景的支持情况请参见如下表格。

| 密码算法大类 | 密码算法子类 | 保护级别 | 是否支持加解密 | 是否支持签名验签 |
| --- | --- | --- | --- | --- |
| 对称密钥 | AES_256 | Software<br>HSM | 支持 | 不支持 |
| | SM4 | HSM | 支持 | 不支持 |
| 非对称密钥 | RSA_2048 | Software<br>HSM | 支持 | 支持 |
| | SM2 | HSM | 支持 | 支持 |

- 对称密钥主要用于数据的加密保护场景，可通过接口调用进行在线加密或者信封加密。更多信息，请参见对称密钥概述。
- 非对称密钥可用于数据加密和数字签名。在KMS创建的非对称用户主密钥（CMK），由一对关联的公钥和私钥构成。公钥可以被分发给任何人，而私钥由KMS确保安全性，不提供任何接口导出非对称密钥的私钥。使用者仅能通过接口调用私钥进行签名运算或者数据解密。更多信息，请参见非对称密钥概述。

### KMS密钥管理功能

KMS提供集中托管的密钥全生命周期管理，您可以轻松创建并使用密钥。

| 功能 | 说明 | 参考文档 |
| --- | --- | --- |
| 密钥生命周期管理 | 通过KMS可创建用户主密钥CMK（Customer Master Key），支持对CMK进行启用、禁用、删除等生命周期管理。<br>密钥支持软件或硬件的密钥保护级别，硬件密钥通过硬件安全模块（HSM）的保护，满足更高的安全性。<br>支持导入自带密钥材料到KMS中（BYOK），满足一些特定的安全需求。 | 创建密钥<br>导入密钥材料<br>启用禁用密钥<br>计划删除密钥 |
| 密钥版本管理 | 支持通过密钥版本化或定期轮转来加强密钥使用的安全性，实现数据保护的安全策略。 | 密钥版本管理 |
| 密钥别名管理 | 支持设置密钥别名，更方便的使用密钥。 | 别名管理 |

**KMS外部导入的密钥材料与KMS创建的密钥材料的区别**

导入的密钥材料与通过KMS创建密钥时自动生成的密钥材料的区别，如下表所示。

| 密钥材料来源 | 区别 |
| --- | --- |
| 外部 | • 支持手动删除密钥材料，但该主密钥及其元数据仍然保留。<br>• 导入密钥材料时，可以设置密钥材料过期时间，密钥材料过期后，KMS将自动删除密钥材料，但该主密钥及其元数据仍然保留。<br>• 导入的密钥材料被删除后，可以再次导入相同的密钥材料使得CMK再次可用。用户需自行备份密钥材料，以便密钥材料失效或误删除时重新导入该密钥材料。 |
| 天翼云KMS | • 不能手动删除密钥材料。<br>• 不能设置密钥材料过期时间。<br>• 密钥材料只能通过设置CMK计划删除时间后，到期后随CMK一并删除。 |

**密码运算**

KMS提供了云原生的密码运算API，快速满足数据加密解密、数字签名验签等多样性需求。

| 功能 | 说明 | 参考文档 |
| --- | --- | --- |
| 对称密钥运算 | 在线加密：适用于少量信息（6KB）的加密，直接通过用户主密钥CMK对数据进行加解密的操作。 | 在线加密 |
| | 信封加密：适用于海量数据的高性能加密，通过生成数据密钥DEK，在本地实现数据的高效对称加解密处理。 | 信封加密 |
| 非对称密钥运算 | 签名验签：适用于敏感信息的传递，信息发送者通过发送签名和数据提供身份证明，信息接收者进行签名验证，校验数据的安全性。 | 签名验签 |
| | 非对称密钥加解密：适用对敏感信息加密后进行传递，通过使用非对称密钥公钥对数据进行加密、私钥进行解密处理。 | 非对称密钥加解密 |

## 创建密钥

开通密钥管理服务后，您可以在控制台轻松地创建密钥，以便后续使用密钥加解密自己的数据。

### 操作步骤

1. 登录密钥管理服务控制台。

2. 在页面最上方的导航栏的资源池下拉列表，选择服务所在的区域。
3. 在左侧导航栏，选择“密钥管理”，在页面上方选择目标服务。

4. 点击“创建密钥”，在弹出的创建密钥对话框，根据页面提示进行配置。


配置项说明：

| 配置项 | 说明 |
| --- | --- |
| 密钥类型 | • 对称密钥类型：<br>AES_256<br>Ctyun_SM4（企业版支持）<br>• 非对称密钥类型：<br>RSA_2048<br>Ctyun_SM2（企业版支持） |
| 密钥用途 | • Encrypt/Decrypt：数据加密和解密。<br>• Sign/Verify：产生和验证数字签名。<br>说明<br>仅非对称密钥（RSA_2048、Ctyun_SM2）支持Sign/Verify用途。 |
| 别名 | 用户主密钥的可选标识。更多操作，请参见别名管理。 |
| 保护级别 | • Software：通过软件模块对密钥进行保护。<br>• Hsm：将密钥托管在密码机中，使密钥获得高安全等级的专用硬件的保护。 |
| 描述 | 密钥的说明信息。 |
| 轮转周期 | 自动轮转的时间周期。<br>• 不开启：不开启轮转<br>• 30天<br>• 90天<br>• 180天<br>• 自定义：7~730天<br>说明<br>仅对称密钥（AES_256、Ctyun_SM4）支持设置自动轮转周期。 |
| 密钥材料来源 | • 天翼云KMS：密钥材料将由KMS生成。<br>• 外部：KMS将不会生成密钥材料，您需要将自己的密钥材料导入KMS。更多信息，请参见导入密钥材料。 |
| 企业项目 | 选择密钥归属的企业项目。默认为default。 |

5. 单击**确定**，完成密钥创建。您可以在密钥列表查看密钥ID、密钥状态、密钥类型、密钥用途、密钥保护级别等信息。

## 导入对称密钥材料

用户主密钥包含密钥元数据（密钥ID、密钥别名、描述、密钥状态与创建日期）和用于加解密数据的密钥材料。

- 当用户使用KMS管理控制台创建用户主密钥时，KMS系统会自动为该用户主密钥生成密钥材料。
- 当用户希望使用自己的密钥材料时，可通过KMS管理控制台的导入密钥功能创建密钥材料为空的用户主密钥，并将自己的密钥材料导入该用户主密钥中。

### 注意事项

当您选择密钥材料来源为外部，使用您自己导入的密钥材料时，需要注意以下几点：

- 请确保您使用了符合安全要求的随机源生成密钥材料。
- 在使用导入密钥时，需要对自己密钥材料的可靠性负责。
- 请保存密钥材料的原始备份，以便在意外删除密钥材料时，能及时将备份的密钥材料重新导入KMS。

#### 功能特性

- **可用性与持久性**

  在将密钥材料导入KMS之前，用户需要确保密钥材料的可用性和持久性。

  导入的密钥材料与通过KMS创建密钥时自动生成的密钥材料的区别，如下表所示。

| 密钥材料来源 | 说明 |
| --- | --- |
| 外部导入 | 支持手动删除密钥材料，但该主密钥及其元数据仍然保留。<br>导入密钥材料时，可以设置密钥材料过期时间，密钥材料过期后，KMS将自动删除密钥材料，但该主密钥及其元数据仍然保留。导入的密钥材料被删除后，可以再次导入相同的密钥材料使得CMK再次可用。用户需自行备份密钥材料，以便密钥材料失效或误删除时重新导入该密钥材料。 |
| KMS创建 | 不能手动删除密钥材料，不能设置密钥材料过期时间。密钥材料只能通过设置CMK计划删除时间后，到期后随CMK一并删除。 |

- **关联性**

  当您将密钥材料导入CMK时，该CMK与该密钥材料永久关联，不能将其他密钥材料导入该CMK中，即便密钥材料已经过期或者被删除。

- **独立性**

  CMK具有唯一性，即您使用CMK加密的数据，无法使用其他CMK进行解密，即便这些CMK都使用相同的密钥材料。

#### 限制条件

- AES_256类型的CMK需导入256位对称密钥作为密钥材料。
- 从KMS获取到的导入令牌与加密密钥材料的公钥具有绑定关系，一个令牌只能为其生成时指定的主密钥导入密钥材料。导入令牌的有效期为24小时，在有效期内可以重复使用，失效以后需要获取新的导入令牌和加密公钥。

操作步骤-导入密钥材料

1. 创建用户主密钥，其中**密钥材料来源**选择“外部”并勾选“**我了解使用外部密钥材料的方法和意义**”。


创建密钥
* 密钥类型
RSA_2048
* 密钥用途
请选择密钥用途
* 别名
alias/
0 / 64
* 保护级别
请选择保护级别
* 轮转周期
不开启
描述
0 / 255
* 密钥材料来源
天翼云KMS
外部
您可以将256位(AES)的对称密钥作为密钥材料导入KMS
我了解试用外部密钥材料的方法和意义。
参考文档
* 企业项目
请选择企业项目
取消
确认

2. 获取导入密钥材料参数。

a. 在密钥列表，单击“密钥ID”，进入“密钥详情”，在密钥材料区域，单击**获取导入密钥材料参数**。


b. 在**获取导入密钥材料参数**对话框，选择“公钥类型”、“加密算法”，单击“确定”。


**配置项说明：**

| 配置项 | 说明 |
| --- | --- |
| 公钥类型 | 取值：RSA_2048（默认） |
| 加密算法 | 取值：<br>• RSAES_PKCS1_V1_5<br>• RSAES_OAEP_SHA_1<br>• RSAES_OAEP_SHA_256 |

c. 在**获取导入密钥材料参数**对话框，下载“加密公钥”和“导入令牌”，然后单击“确定”。


注意

导入令牌存在过期时间，请关注过期时间，及时进行导入。

3. 使用OPENSSL加密密钥材料。

   加密公钥是一个2048比特的RSA公钥，使用的加密算法需要与获取导入密钥材料参数时指定的一致。由于加密公钥经过Base64编码，因此在使用时需要先进行Base64解码。

   您可以通过OPENSSL加密公钥，您可通过以下步骤获取加密的密钥材料。

   a. 创建一个密钥材料，使用OPENSSL产生一个32字节的随机数。

   b. 将加密公钥进行Base64解码。

   c. 根据指定的加密算法（以RSAES_OAEP_SHA_1为例）加密密钥材料。

   d. 将加密后的密钥材料进行Base64编码，保存为文本文件。

   **代码示例：**

```
openssl rand -out KeyMaterial.bin 32
openssl enc -d -base64 -A -in PublicKey_base64.txt -out PublicKey.bin
openssl rsautl -encrypt -in KeyMaterial.bin -oaep -inkey PublicKey.bin  -keyform DER  -pubin -out EncryptedKeyMaterial.bin
openssl enc -e -base64 -A -in EncryptedKeyMaterial.bin -out EncryptedKeyMaterial_base64.txt
```

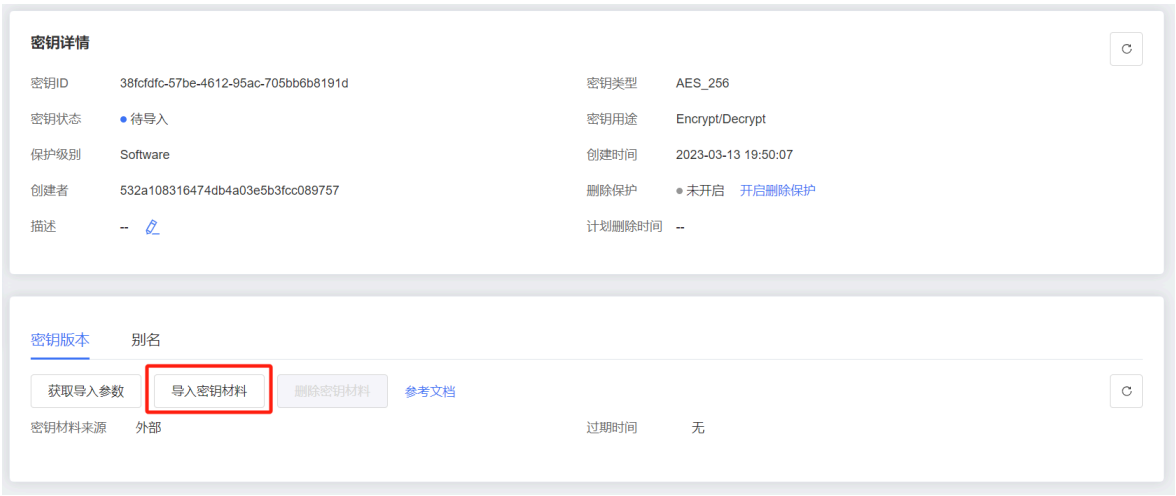
   采用OpenSSL加密密钥材料，支持RSAES_OAEP_SHA_256、RSAES_PKCS1_V1_5 和RSAES_OAEP_SHA_1 三种密钥算法。

   命令代码示例如下表所示：

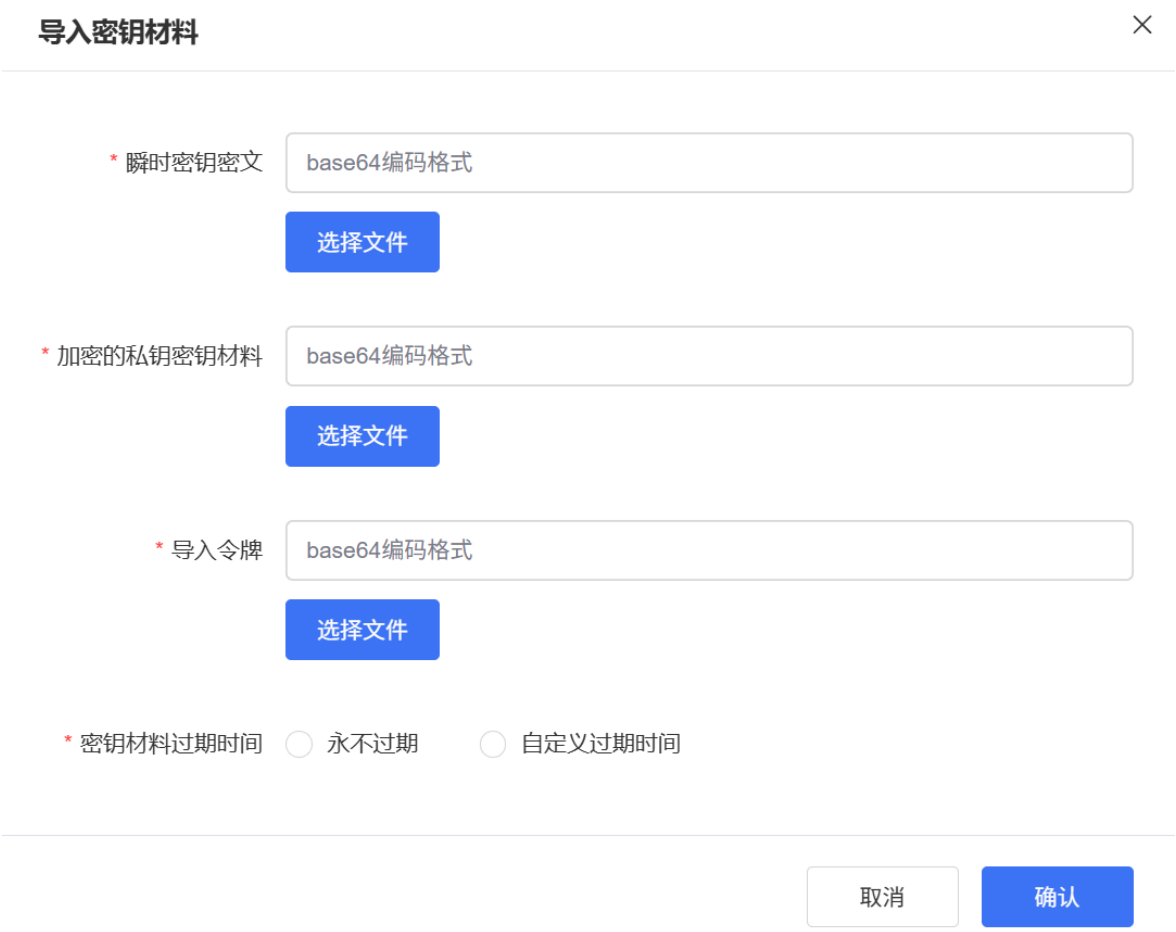
| 密钥算法 | OpenSSL加密生成密钥材料命令代码示例 |
| --- | --- |
| RSAES_OAEP_SHA_256 | openssl pkeyutl -in PlaintextKeyMaterial.bin -inkey PublicKey.bin -out EncryptedKeyMaterial.bin -keyform der -pubin - encrypt -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256 |
| RSAES_PKCS1_V1_5 | openssl rsautl - encrypt -in PlaintextKeyMaterial.bin - pkcs -inkey PublicKey.bin -keyform der - pubin -out EncryptedKeyMaterial.bin |
| RSAES_OAEP_SHA_1 | openssl rsautl -encrypt -in KeyMaterial.bin -oaep -inkey PublicKey.bin -keyform DER -pubin -out EncryptedKeyMaterial.bin |

4. 导入密钥材料。

a. 在密钥列表，在密钥列表，单击“密钥ID”，进入“密钥详情”，在“密钥管理材料区域”，单击导入密钥材料。




b. 在导入密钥材料对话框，上传**加密密钥材料**和**导入令牌**，单击**确定**。

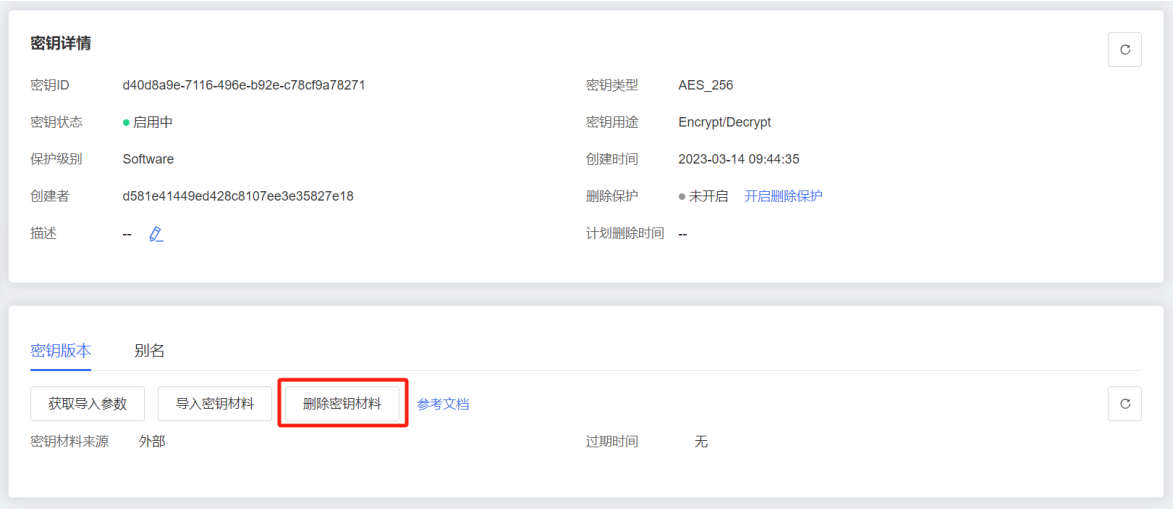



c. 设置密钥材料过期时间，单击“确定”。导入密钥材料成功后，密钥状态从待导入更新为“启用中”。

**操作步骤-删除密钥材料**

1. 登录密钥管理服务控制台。
2. 在页面左上角的地域下拉列表，选择密钥所在的地域。

3. 在密钥列表，点击**密钥ID**，进入**密钥详情**，在密钥材料区域，单击**删除密钥材料**。




4. 在删除密钥材料对话框，单击“确定”。密钥材料删除成功后，密钥状态从启用中更新为“待导入”。

## 别名管理

别名是用户主密钥的可选标识，同一个用户在一个地域中的别名具有唯一性。每个别名只能指向同地域的一个用户主密钥，但是每个用户主密钥可以绑定多个别名。

别名必须依附于用户主密钥存在。其特点如下：

- 一个用户主密钥下可以绑定多个别名，删除别名不会删除其关联的用户主密钥。
- 别名不可修改。您可以通过为一个用户主密钥创建新的别名，并且删除旧的别名来达到修改主密钥别名的目的。
- 可以调用UpdateAlias接口更改别名绑定的用户主密钥，而不会影响用户主密钥。
- 默认主密钥的别名不能删除和添加。

### 创建别名

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏的资源池下拉列表，选择密钥所在的区域。
3. 在左侧导航栏，单击 **密钥管理服务**，进入密钥列表。
4. 在密钥列表点击 **密钥ID**，进入密钥详情页。

5. 在别名区域，点击 **创建别名** ，填写别名，单击 **确定**。


### 删除别名

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏的资源池下拉列表，选择密钥所在的区域。
3. 在左侧导航栏，单击 **密钥管理服务** ，进入密钥列表。
4. 在密钥列表点击 **密钥ID** ，进入密钥详情页。
5. 在别名区域的别名列表，选择对应别名，点击删除别名。
6. 在弹出的确认框中，单击**确定**。

### 别名相关API接口

您可以通过调用别名的相关接口，实现别名的创建、删除、更新、查询等操作。

| 功能 | API | 描述 |
| --- | --- | --- |
| 密钥别名管理 | createAlias | 创建密钥别名。 |
| | updateAlias | 更新密钥别名。 |
| | deleteAlias | 删除密钥别名。 |
| | listAlias | 列出云账号在本地域的所有别名。 |
| | listAliasByUuid | 列出与指定用户主密钥绑定的别名。 |

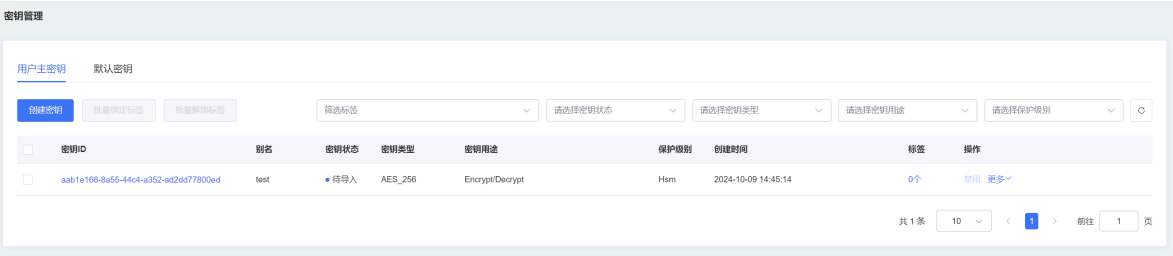
## 查看密钥

成功创建了用户主密钥之后，您可以通过控制台查看密钥列表以及密钥详情信息。

### 操作步骤

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏的资源池下拉列表，选择密钥所在的区域。

3. 在左侧导航栏，单击 **密钥管理服务** ，进入 **密钥列表** 。




4. 在密钥列表中，查看密钥信息。密钥列表参数说明如下表所示。

| 参数 | 说明 |
| --- | --- |
| 密钥ID | 创建密钥时自动生成的密钥ID。可点击进入密钥详情。 |
| 别名 | 密钥的别名。 |
| 密钥状态 | 密钥的状态，包含：<br>• 启用中<br>• 已禁用<br>• 待删除<br>• 待导入 |
| 密钥类型 | 创建密钥时选择的算法类型，包含：<br>• 对称密钥：AES_256、Ctyun_SM4（企业版支持）<br>• 非对称密钥：RSA_2048、Ctyun_SM2（企业版支持） |
| 密钥用途 | 创建密钥时选择的用途，包含：<br>• Encrypt/Decrypt<br>• Sign/Verify，仅非对称密钥支持 |
| 保护级别 | 创建密钥时选择的保护级别，包含：<br>• Software<br>• Hsm |
| 创建时间 | 创建该密钥的时间。 |
| 操作 | 用户可以对密钥进行启用/禁用、计划删除密钥/取消计划删除密钥、编辑标签操作。 |

5. 在密钥列表点击 **密钥ID** ，进入 **密钥详情页** 。
   - 在密钥详情区域可查看当前密钥的详细信息。

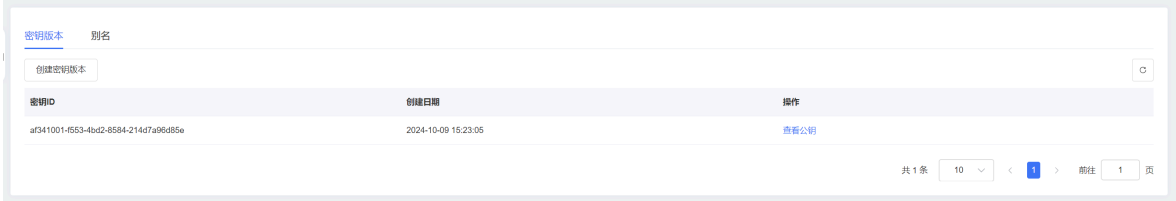

密钥详情参数说明如下表所示：

| 参数 | 说明 |
| --- | --- |
| 密钥类型 | 创建密钥时选择的算法类型，包含：<br>• 对称密钥：AES_256、Ctyun_SM4（企业版支持）<br>• 非对称密钥：RSA_2048、Ctyun_SM2（企业版支持） |
| 密钥用途 | 创建密钥时选择的用途，包含：<br>• Encrypt/Decrypt<br>• Sign/Verify，仅非对称密钥支持 |
| 创建者 | 即User_id。 |
| 密钥状态 | 密钥的状态，包含：<br>• 启用中<br>• 已禁用<br>• 待删除<br>• 待导入 |
| 保护级别 | 创建密钥时选择的保护级别，包含：<br>• Software<br>• Hsm |
| 创建时间 | 创建该密钥的时间。 |
| 删除保护 | 状态：<br>• 未开启<br>• 启用中<br>说明<br>开启删除保护状态的密钥，将无法直接删除该密钥，从而避免误删除密钥。若确认要将密钥删除，需要将删除保护关闭。 |
| 描述 | 描述信息，可修改。 |

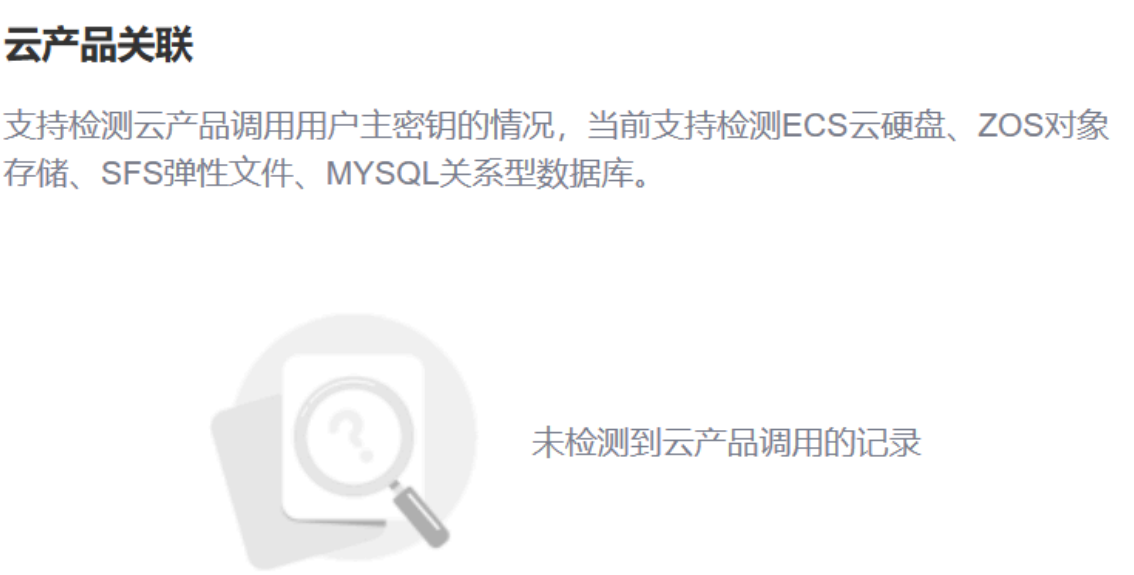
- 在**密钥详情页**的**别名管理**区域，可为密钥创建别名，同时可删除不需要的别名。详情请参见别名管理。


- 在**密钥详情页**的**密钥版本**区域，可为对称密钥设置 **轮转策略** ，为非对称密钥手动 **更新密钥版本** ，同时可查看当前密钥的版本列表。详情请参见密钥版本管理。
  - 对称密钥，设置轮转策略：


  - 非对称密钥，创建密钥版本：



- 在**密钥详情页**的**云产品关联**区域，可查看当前密钥绑定的天翼云云上产品。

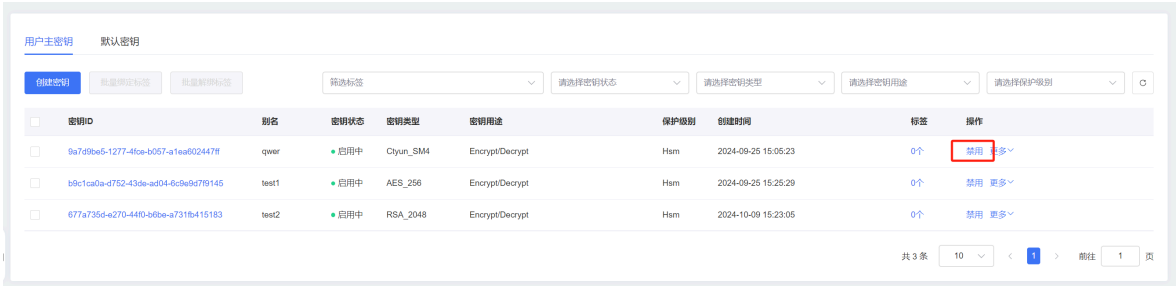



## 启用禁用密钥

密钥创建完成后，默认为启用状态。您可以禁用密钥，被禁用的密钥无法用于加密和解密。

### 禁用

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏的资源池下拉列表，选择密钥所在的区域。
3. 在左侧导航栏，单击 **密钥管理服务** ，进入 **密钥列表** 。
4. 定位待禁用的密钥，单击右侧操作列的 **禁用** 。




5. 在弹出的禁用密钥对话框，单击 **确定** 。

### 启用

1. 找到待启用的密钥，单击右侧操作列的**启用**。


2. 在弹出的启用密钥对话框，单击**确定**。

## 密钥版本管理

密钥常用于保护特定的数据，因此，数据的安全依赖于密钥的安全。您可以通过密钥版本化和定期轮转来加强密钥使用的安全性，实现数据保护的安全策略和最佳实践。

### 密钥版本概述

KMS中的用户CMK支持多个密钥版本。每一个密钥版本是一个独立生成的密钥，同一个CMK下的多个密钥版本在密码学上互不相关。

- 对于对称密钥，密钥版本可通过自动轮转策略，由系统自动生成。
- 对于非对称密钥，可人工创建新的密钥版本。

### 设置自动轮转

对称密钥支持设置自动轮转，生成新的密钥版本。对称密钥版本分为主版本和非主版本：

- **主版本（Primary Key Version）**
  - 系统根据自动轮转策略，定期生成新的密钥版本，并自动设为主版本。
  - 主版本是CMK的活跃加密密钥（Active Encryption Key）。每个CMK在任何时间点上有且仅有一个主版本。
  - 调用GenerateDataKey、Encrypt等加密API接口时，KMS使用指定CMK的主版本对明文进行加密。
- **非主版本（Non-primary Key Version）**
  - 非主版本是CMK的非活跃加密密钥（Inactive Encryption Key）。每个CMK可以有零到多个非主版本。非主版本历史上曾经是主版本，在当时被用作活跃加密密钥。
  - 密钥轮转产生新的主版本后，KMS不会删除或禁用非主版本，它们需要被用作解密数据。

### 创建密钥版本

由于公私钥使用场景的特殊性，KMS不支持对非对称的用户主密钥进行自动轮转。可在指定用户主密钥中人工创建新的密钥版本，生成全新的一对公钥和私钥。

除此之外，和对称类型的用户主密钥不同，非对称的用于主密钥没有主版本（PrimaryKeyVersion）的概念，因此使用非对称密码运算的接口除需指定用户主密钥标志符（或别名）之外，还需指定密钥版本。

### 不适用范围

KMS管理的以下类型的密钥不支持多个版本：

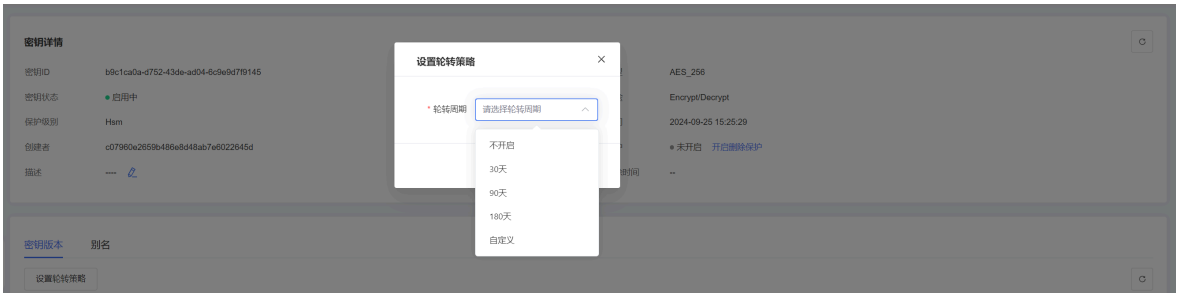
- 云产品的默认密钥：特定云产品托管在KMS上的、用于加密保护您的数据的默认密钥。这类密钥由特定云产品为用户代为管理，为您的数据提供最基本的加密保护。
- 用户自带密钥（BYOK）：您导入到KMS中的密钥。这类CMK的Origin属性为External，KMS不负责为用户生成密钥材料，无法自动发起轮转行为。更多信息，请参见导入密钥材料。

**操作步骤**

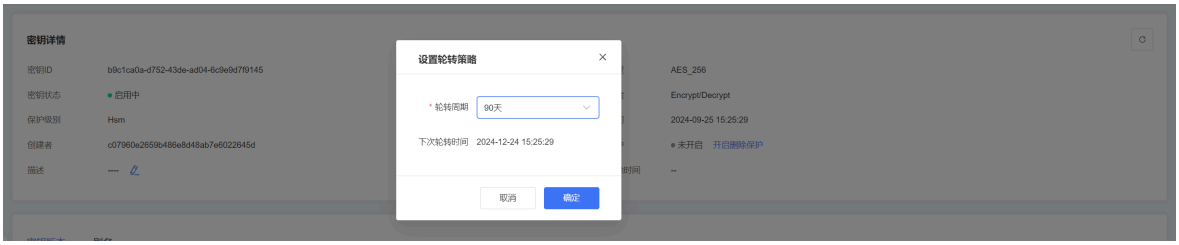
### 设置自动轮转（对称密钥）

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏的资源池下拉列表，选择密钥所在的区域。
3. 在左侧导航栏，单击 **密钥管理服务** ，进入 **密钥列表** 。
4. 定位到待设置的对称密钥，点击 **密钥ID** ，进入 **密钥详情页** 。
5. 在密钥版本区域，点击 **设置轮转策略** 。


6. 在设置轮转策略对话框，选择轮转周期， **30天** 、 **90天** 、 **180天** ，或 **自定义天数** 。




7. 设置了自动轮转策略后，将显示密钥下次轮转时间，点击**确定**完成设置。

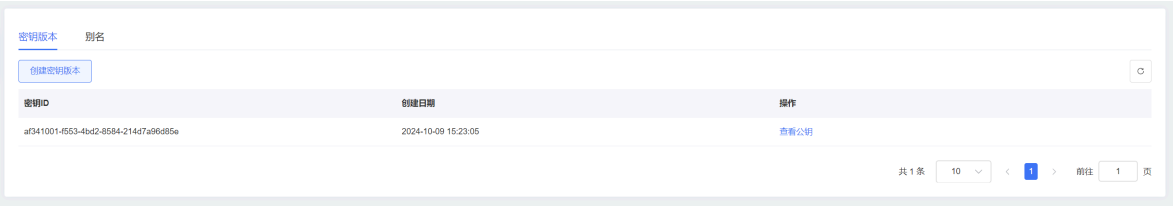



8. 可通过相同的步骤更改轮转周期，也可取消轮转策略。

### 创建密钥版本（非对称密钥）

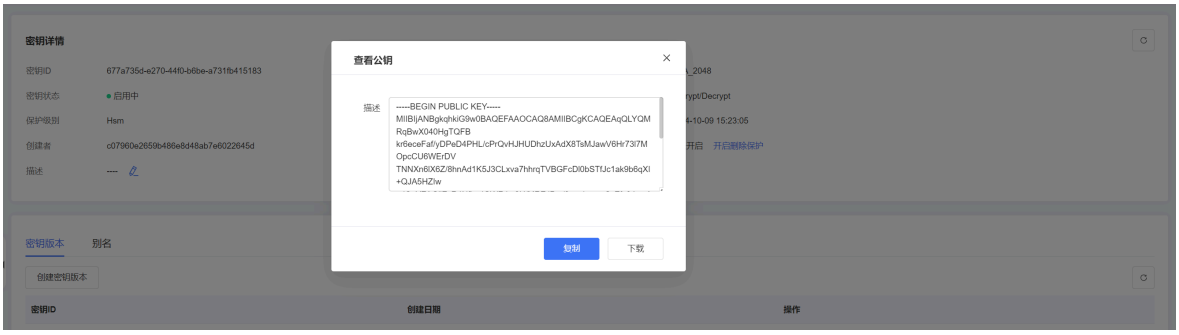
1. 登录密钥管理服务控制台。

2. 在页面最上方的导航栏的资源池下拉列表，选择密钥所在的区域。
3. 在左侧导航栏，单击 **密钥管理服务** ，进入密钥列表。
4. 定位待设置的非对称密钥，点击 **密钥ID** ，进入密钥详情页。
5. 在密钥版本区域，点击 **创建密钥版本** 。




6. 在弹出的对话框内，点击 **确定** 。


7. 在密钥版本列表，可查看密钥版本ID、创建日期。点击 **查看公钥** ，在弹出的对话框，可复制或下载公钥。




## 删除密钥

用户主密钥（CMK）一旦删除，将无法恢复，使用该CMK加密的内容及产生的数据密钥也将无法解密。因此，对于CMK的删除，KMS只提供计划删除的方式，而不提供直接删除的方式。如果不再使用CMK，推荐您使用禁用密钥功能。

### 前提条件

开启删除保护状态的密钥，将无法直接删除该密钥，从而避免误删除密钥。若确认要将密钥删除，需要将删除保护关闭。

#### 计划删除密钥

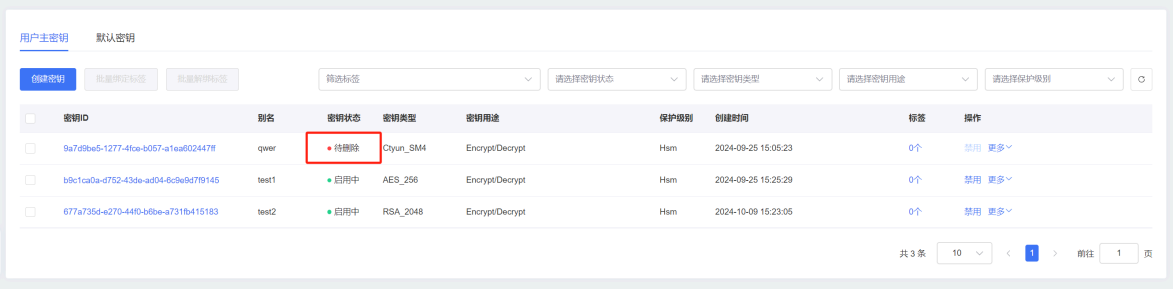
1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏的资源池下拉列表，选择密钥所在的区域。

3. 在左侧导航栏选择“密钥管理（包周期）> 密钥管理”，进入 **密钥列表** 页面。
4. 选中需计划删除的密钥，在右侧操作列选择 **更多 > 计划删除密钥** 。

5. 在计划删除密钥对话框，填写预删除周期，并且逐一确认各个确认项，确认无误后点击 **确定** 。

预删除周期取值为：7~30天，默认值：30天。

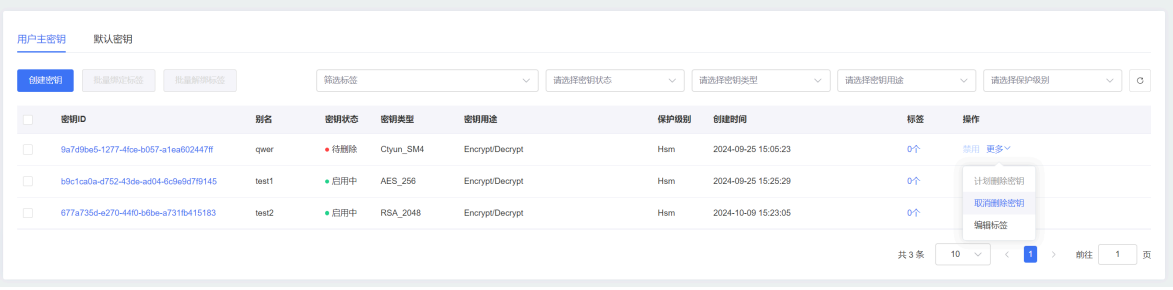
6. 此时密钥状态由启用中变为 **待删除** 。处于待删除状态的密钥无法用于加密、解密和产生数据密钥。




**相关操作**

### 取消计划删除密钥

1. 处于待删除状态的密钥，您可以通过在右侧操作列选择 **更多 > 取消删除密钥** ，撤销删除密钥的申请。




2. 在弹出的对话框，点击 **确定** ，即可取消计划删除，密钥恢复可用状态。

# 对称密钥运算

## 对称加密概述

对称加密是最常用的数据加密保护方式。KMS提供了简单易用的接口，方便您在云上轻松实现数据加解密功能。密钥管理服务支持主流的对称密钥算法并且提供足够的安全强度，保证数据加密的安全性。

### KMS支持的对称密钥类型

KMS支持的对称密钥算法类型如下：

| 算法 | 密钥长度 | 密钥规格 | 保护级别 |
| --- | --- | --- | --- |
| AES | 256比特 | AES_256 | SoftwareHSM |
| SM4 | 128比特 | Ctyun_SM4 | HSM |

### 对称密钥功能特性

KMS生成的对称主密钥支持多个密钥版本，同时支持用户主密钥基于密钥版本进行自动轮转，您可以自定义密钥轮转的策略。为了满足特殊的安全合规要求，KMS支持您使用自带密钥（BYOK）进行数据的加密保护。

| 功能 | 功能描述 |
| --- | --- |
| 自动轮转 | 支持设置自动轮转策略，生成新的密钥版本，并自动设为主版本（primaryKeyVersion），KMS会使用主版本密钥实现加解密。 密钥轮转产生新的主版本后，KMS不会删除或禁用非主版本，他们需要被用作解密操作。 |
| 导入密钥材料（BYOK） | 默认情况下，当创建CMK时，会由KMS生成密钥材料。也可以选择创建密钥材料来源为外部的密钥，将自带密钥材料导入到CMK中。导入的密钥材料可以进行删除，也可以设置过期时间，在密钥材料过期后进行删除（CMK不会被删除）。导入的密钥材料被删除后，可以再次导入相同的密钥材料使得CMK再次可用，因此您需要自行保存密钥材料的副本。每个CMK只能拥有一个导入密钥材料。当您将一个密钥材料导入CMK时，CMK将与密钥材料绑定，即便密钥材料已经过期或者被删除，也不能导入其他密钥材料。如果您需要轮换使用外部密钥材料的CMK，只能创建一个新的CMK然后导入新的密钥材料。 |

**对称密钥应用场景**

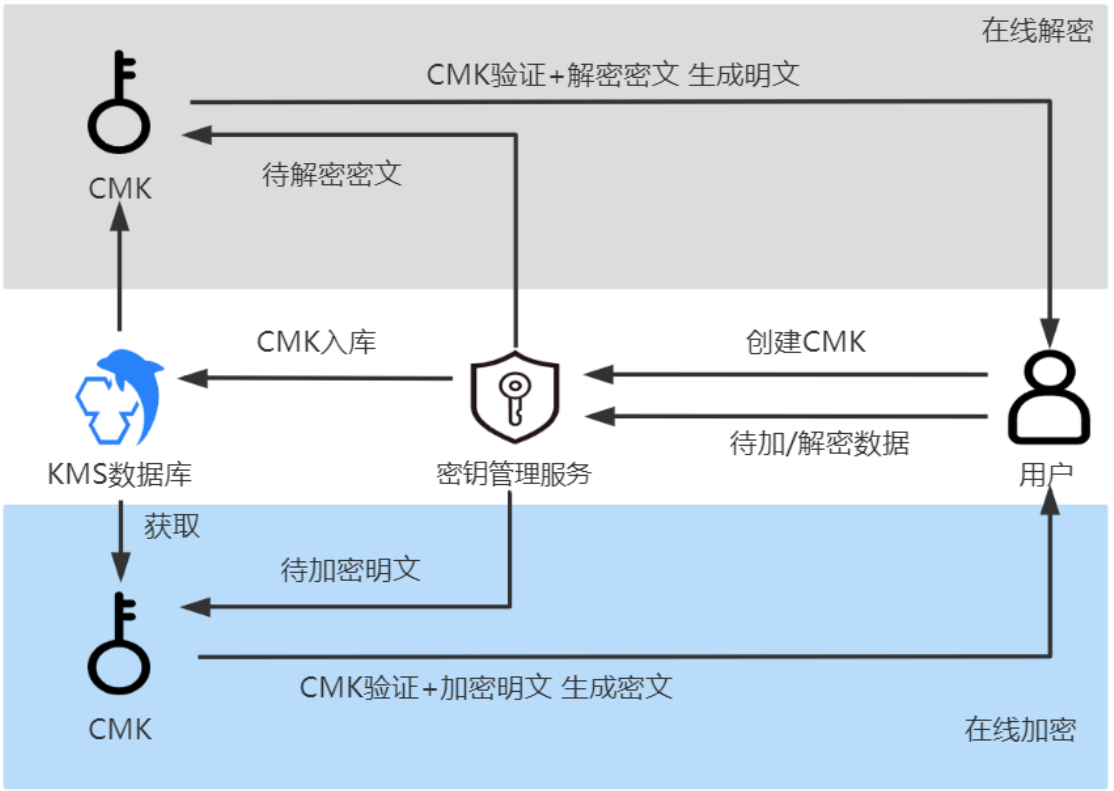
KMS生成的对称密钥支持如下数据加密方式，满足多样化的数据保护场景。

| 场景 | 场景描述 |
| --- | --- |
| 在线加密 | 适用于保护小型敏感数据（小于6KB）的加解密，如密钥、证书、配置文件等。 用户的数据会通过安全信道传递到KMS服务端，服务端通过指定CMK完成加密和解密后，操作结果通过安全信道返回给用户。 |
| 信封加密 | 适用于海量数据的高性能加解密，如规模较大的对性能敏感的本地文件。通过KMS生成数据密钥DEK，并返回DEK明文及经指定CMK加密的DEK密文。用户使用数据密钥DEK明文在本地进行高效的加解密处理，然后将内存中的DEK明文销毁，将DEK密文及密文文件落盘存储。 |

## 在线加密

敏感信息加密是密钥管理系统 KMS 核心的能力，适用于保护小型敏感数据（小于6KB），如口令、证书、配置文件等。通过密钥管理服务KMS的在线加密API，使用 用户主密钥（CMK）直接加密敏感数据信息，而非直接将明文存储，确保敏感数据安全。

### 场景示意图




### 操作流程（以证书加密为例）

1. 通过KMS控制台或者调用CreateKey接口，创建一个用户主密钥（CMK）。
2. 调用KMS服务的Encrypt接口，将明文证书加密为密文证书。
3. 将密文证书部署在服务器上。
4. 当服务器启动需要使用证书时，调用KMS服务的Decrypt接口将密文证书解密为明文证书。

### 相关API

您可以调用以下KMS API，轻松完成对数据的加密或解密操作。

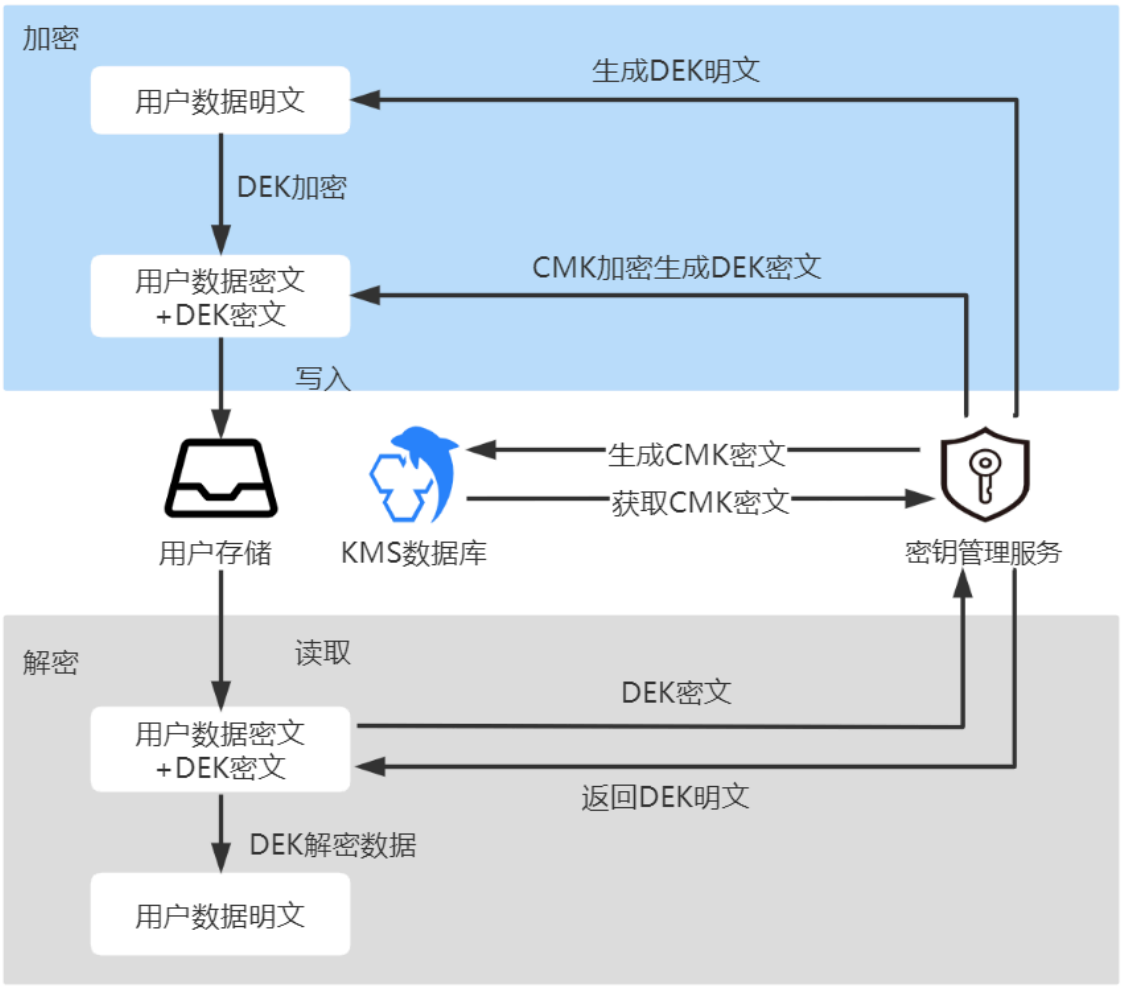
| API名称 | 说明 |
| --- | --- |
| createkey | 创建用户主密钥（CMK）。 |
| encrypt | 指定CMK，直接输入明文数据，由KMS在线加密数据。 |
| decrypt | 解密由encrypt接口加密的数据，不需要指定CMK即可完成在线解密。 |

## 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。这种技术不再使用用户主密钥（CMK）直接加密和解密数据，而是通过生成加密数据的数据密钥（DEK），将其封入信封中（即通过CMK加密）存储、传递和使用，由KMS确保数据密钥的随机性和安全性。

实际使用时，用户无需将大量业务数据上传至KMS服务端，直接通过离线的数据密钥在本地实现加解密，有效避免安全隐患，保证了业务加密性能的要求。

### 场景示意图




### 操作流程

### 信封加密

1. 通过KMS控制台或者调用CreateKey接口，创建一个用户主密钥（CMK）。
2. 调用GenerateDataKey接口创建一个数据密钥。KMS会返回一个明文的数据密钥和一个经用户主密钥（CMK）加密的密文数据密钥。

3. 使用明文的数据密钥加密本地文件，产生密文文件，然后销毁内存中的明文数据密钥。
4. 用户将密文数据密钥和密文文件一同存储到持久化存储设备或服务中。

### 信封解密

1. 从本地文件中读取密文数据密钥。
2. 调用KMS服务的Decrypt接口，将密文数据解密为明文数据密钥。
3. 用明文数据密钥为本地密文文件解密，再销毁内存中的明文密钥。

### 相关API

您可以调用以下KMS API，实现对本地数据的加密或解密操作。

| API名称 | 说明 |
| --- | --- |
| createKey | 创建用户主密钥（CMK） |
| generateDataKey | 生成信封加密的数据密钥，返回数据密钥的明文和经过指定用户主密钥加密的密文 |
| decrypt | 解密由generateDataKey接口生成的数据密钥密文，不需要指定CMK |

# 非对称密钥运算

## 非对称密钥概述

相比对称加密，非对称密钥通常用于在信任程度不对等的系统之间，实现数字签名验签或者加密传递敏感信息。

非对称密钥由一对密钥组成，分别是公开密钥（public key，简称公钥）和私有密钥（private key，简称私钥）。公钥可以任意对外发布，私钥必须由用户自行严格秘密保管。非对称密钥具有双向性，即公钥和私钥中的任一个均可用作加密，此时另一个则用作解密。

密钥管理服务（KMS）支持主流的非对称密钥算法并且提供足够的安全强度，保证数据加密和数字签名的安全性。

### KMS支持的非对称密钥类型

非对称密钥支持的算法类型如下：

| 算法 | 密钥规格 | 保护级别 |
| --- | --- | --- |
| RSA | RSA_2048 | SoftwareHSM |
| SM2 | Ctyun_SM2 | HSM |

### 非对称密钥功能特性

由于非对称密钥公、私钥使用场景的特殊性，KMS不支持对非对称的用户主密钥进行自动轮转。您可以自主在指定用户主密钥中创建新的密钥版本，生成全新的一对公钥和私钥。

非对称密钥区分公钥运算和私钥运算，公钥主要用于数据加密和验签，私钥主要用于数字签名和数据解密。

| 功能 | 功能描述 |
| --- | --- |
| 创建密钥版本 | 支持自主创建新密钥版本，不支持设置自动轮转策略。区别于对称密钥，非对称密钥无密钥主版本概念，则在调用非对称密码运算API接口时，在指定使用的用户主密钥（CMK）的同时，还需指定使用的密钥版本（keyVersion）。 |
| 公钥运算 | 大多数情况下，您可以调用GetPublicKey接口获取公钥，之后分发给公钥使用者。使用者在业务端通过OpenSSL、Java JCE等常用的密码运算库在本地进行加密、验签处理。密钥管理服务（KMS）也提供公钥运算的非对称密钥加密接口（asymmetricEncrypt）和数字签名验签接口（asymmetricVerify），满足特定的业务需求。 |
| 私钥运算 | 由于私钥的不公开性，用户仅能通过调用KMS提供的私钥运算的产生数字签名接口（asymmetricSign）和非对称密钥解密接口（asymmetricDecrypt），实现签名、解密处理。 |

**非对称密钥应用场景**

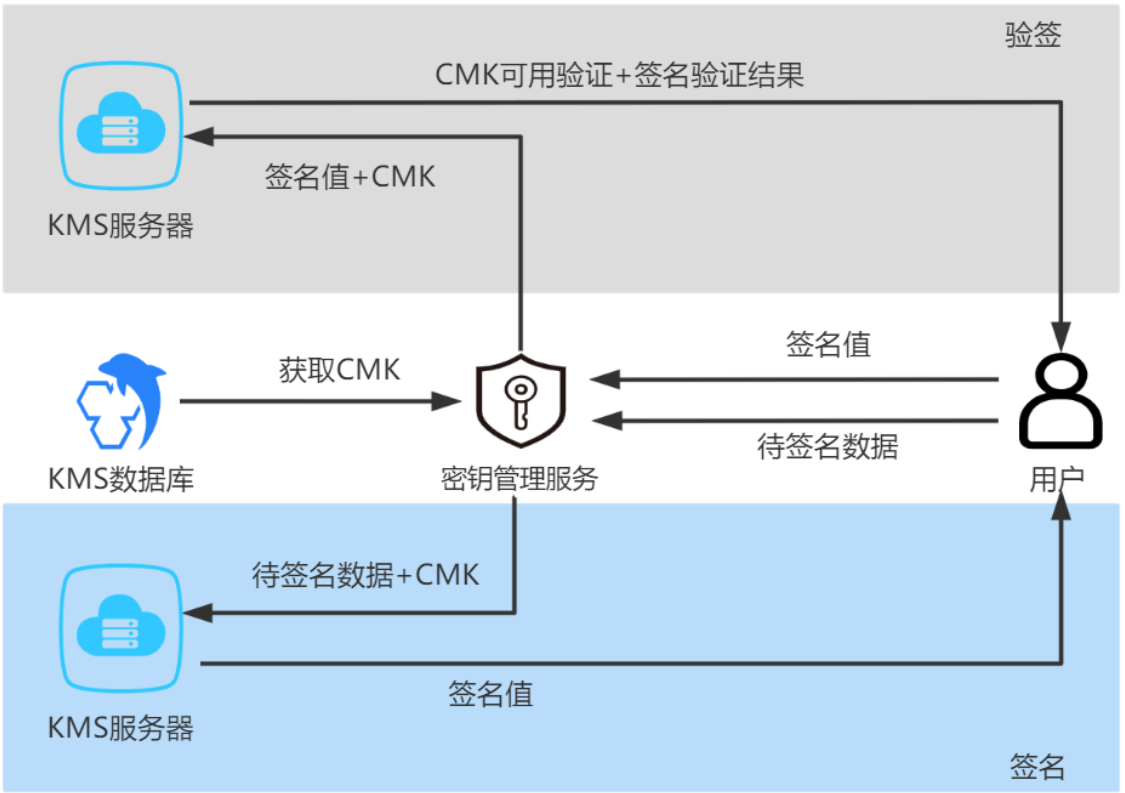
| 场景 | 场景描述 |
| --- | --- |
| 签名验签 | 数字签名技术是非对称加密算法的另一种典型应用。数字签名分为签名和验证两个过程，消息发送者使用私钥对数据签名，消息接收者使用公钥进行签名验证。由于签名是使用私钥加密产生，而私钥不公开，这使得签名具有唯一的特征，广泛用于数据防篡改、身份认证等相关技术领域。 |
| 数据加解密 | 非对称密钥加密通信的过程类似于对称加密，区别在于需要使用公钥进行数据加密，使用私钥进行数据解密。 由于密文只有通过私钥才可以解密，而私钥是不公开的，所以即使由于传输介质的安全性比较低而导致信息泄露，拿到密文的人也无法将其破译，从而保证了敏感信息的安全。这种敏感信息传递的方式，被广泛用于各类密钥交换场景。 |

## 签名验签

数字签名技术是非对称加密算法的另一种典型应用。数字签名分为签名和验证两个过程，消息发送者使用私钥对数据签名，消息接收者使用公钥进行签名验证。

由于签名是使用私钥加密产生，而私钥不公开，这使得签名具有唯一的特征，广泛用于数据防篡改、身份认证等相关技术领域。

### 场景拓扑图




### 操作流程

1. 信息发送者通过KMS控制台或者调用CreateKey接口，创建一个非对称的用户主密钥（CMK）。
2. 信息发送者通过调用KMS的getPublicKey接口获取到公钥，并将公钥分发给消息接收者。
3. 信息发送者通过调用KMS的asymmetricSign接口，使用创建的CMK私钥对需要传输的数据生成签名。
4. 信息发送者将签名和数据传递给信息接收者。
5. 信息接收者拿到签名和数据之后，在本地通过gmssl、openssl、密码库、KMS 的国密 Encryption SDK 等验签方法，使用信息发送者分发的公钥进行验证。特殊需求场景下，也可调用KMS的asymmetricVerify接口，使用CMK进行签名校验。

### 相关API

您可以调用以下KMS API，完成对数据的签名验签处理。

| API名称 | 说明 |
| --- | --- |
| createKey | 创建用户主密钥（CMK）。 |
| getPublicKey | 获取非对称密钥的公钥，可用于离线验证数字签名，或者加密数据。 |
| asymmetricSign | 非对称密钥的私钥运算：产生数字签名。 |

| API名称 | 说明 |
| --- | --- |
| asymmetricVerify | 非对称密钥的公钥运算：验证私钥产生的数字签名。 |

## 非对称密钥加解密

非对称密钥加密通信的过程类似于对称加密，区别在于需要使用公钥进行数据加密，使用私钥进行数据解密。

由于密文只有通过私钥才可以解密，而私钥是不公开的，所以即使由于传输介质的安全性比较低而导致信息泄露，拿到密文的人也无法将其破译，从而保证了敏感信息的安全。这种敏感信息传递的方式，被广泛用于各类密钥交换场景。

### 操作流程

1. 信息接收者通过KMS控制台或者调用KMS的CreateKey接口，创建一个非对称的用户主密钥（CMK）。
2. 信息接收者通过调用KMS的getPublicKey接口获取到公钥，并将公钥分发给消息发送者。
3. 信息发送者使用公钥在本地通过OpenSSL等方式对数据进行加密。特殊需求场景下，也可通过调用KMS的asymmetricEncrypt接口，使用CMK进行加密。
4. 信息发送者将密文数据传递给信息接收者。
5. 信息接收者拿到密文数据之后，可调用KMS的asymmetricDecrypt接口，使用私钥进行数据解密。

### 相关API

您可以调用以下KMS API，完成对敏感数据传输中的加解密处理。

| API名称 | 说明 |
| --- | --- |
| createKey | 创建用户主密钥（CMK）。 |
| getPublicKey | 获取非对称密钥的公钥，可用于离线验证数字签名，或者加密数据。 |
| asymmetricEncrypt | 非对称密钥的公钥运算：加密数据。 |
| asymmetricDecrypt | 非对称密钥的私钥运算：解密公钥加密的数据。 |

# 应用接入点

## 应用接入点概述

应用接入点是KMS提供的一种身份认证和访问控制机制，当应用需要使用密钥进行加解密时，可通过应用接入点对应用进行身份认证和行为管控。

应用接入点包含三个关键信息：权限规则、身份凭证和应用接入地址。

通过应用接入点访问KMS服务为私网访问，认证方式采用AK/SK方式，对应可集成服务SDK。关于服务SDK的详细介绍，请参见服务SDK。

说明

- 建议您为每个集成KMS的应用单独创建应用接入点，以确保访问控制权限的独立性。
- 当前KMS提供3个免费的应用接入点额度。
- 成功开通KMS服务实例后，KMS会在服务实例所在VPC自动生成并启用默认应用接入点（default）。
- 默认应用接入点生成后不会生成身份凭证并默认关闭权限规则开关，如需使用请自行创建和配置。

### 身份凭证

身份凭证用于对KMS资源访问者进行身份认证和行为鉴权。

- 当前KMS通过AK/SK的身份验证方式，其中包含AK（Accesskey）和SK（Secretkey）。
- 一个应用接入点支持创建多个身份凭证。

注意

- 生成访问凭证（AK/SK）后，您需要立即在弹窗中复制或下载文件，关闭后不再支持下载。若您未能成功保存，可删除后重新创建。
- 如果访问凭证（AK/SK）泄露，会带来数据泄露风险，建议妥善保管。

#### 权限规则

应用接入点可配置对应的权限，包括可使用的密钥、证书等资源范围以及接口级操作权限。

- 允许访问的资源：应用允许访问的密钥、证书。
- 操作权限：应用允许使用的功能点。

说明

权限规则开关默认关闭，即允许访问当前账号下的所有资源及操作。若您需要为应用接入点配置特定权限，请开启开关并配置。

关于应用接入点权限的详细介绍请参考应用接入点权限。

#### 应用接入点地址

成功创建应用接入点后，KMS会生成内网endpoint地址，VPC内的应用通过该地址访问KMS服务。

## 管理应用接入点

### 创建应用接入点

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏选择服务所在的区域。

3. 进入“应用接入点”页面，点击 **创建应用接入点** 。


创建应用接入点
* 应用接入点名称
请输入应用接入点名称
* 企业项目
请选择企业项目
* 虚拟私有云
请选择虚拟私有云
+ 配置虚拟私有云
* 子网
请选择子网
+ 配置子网
* 认证方式
AKSK认证
描述信息
请输入描述信息
取消
确认

4. 在弹出的创建对话框，根据页面提示进行配置。

| 配置项 | 说明 |
| --- | --- |
| 应用接入点名称 | 自定义名称。 |
| 企业项目 | 选择所属企业项目。 |
| 虚拟私有云 | 选择当前地域下的虚拟私有云（Virtual Private Cloud，VPC）。<br>说明<br>此处对应的是您应用所在的虚拟私有云，即需要连通KMS服务的虚拟私有云。 |
| 子网 | 选择当前VPC内子网。 |

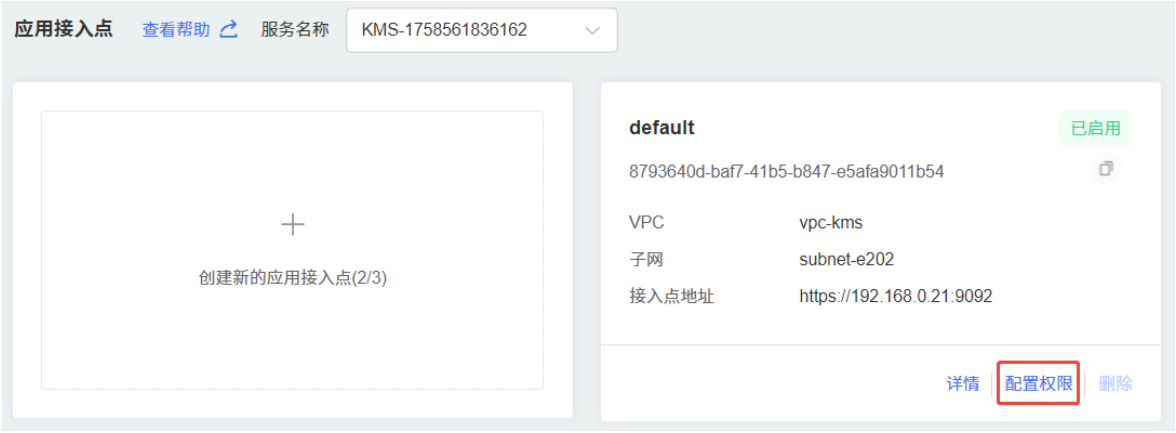
5. 创建成功后，您可以在应用接入点列表查看对应信息。


### 配置权限

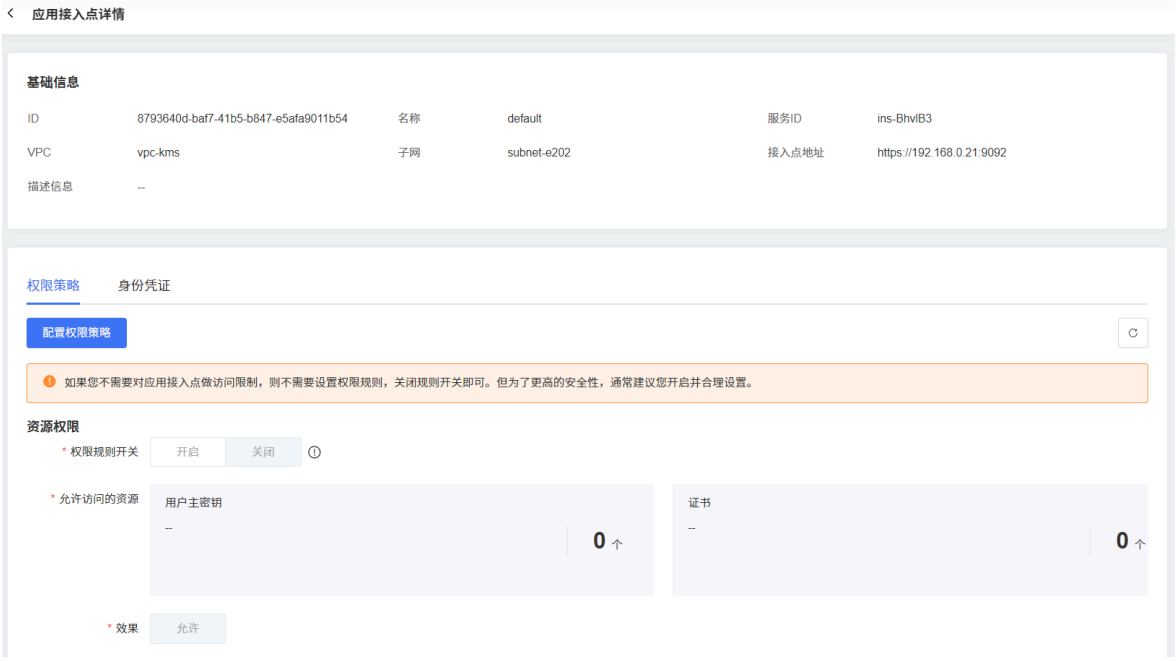
可以为应用接入点配置允许/访问的密钥和证书。

如果您不需要对应用接入点做访问限制，则不需要设置权限规则，关闭规则开关即可。但为了更高的安全性，通常建议您开启并合理设置。

1. 在应用接入点页面，单击“配置权限”，进入配置权限页面。




或单击“详情”，进入应用接入点详情页，在“权限策略”页签，单击“配置权限策略”，进入配置权限页面。



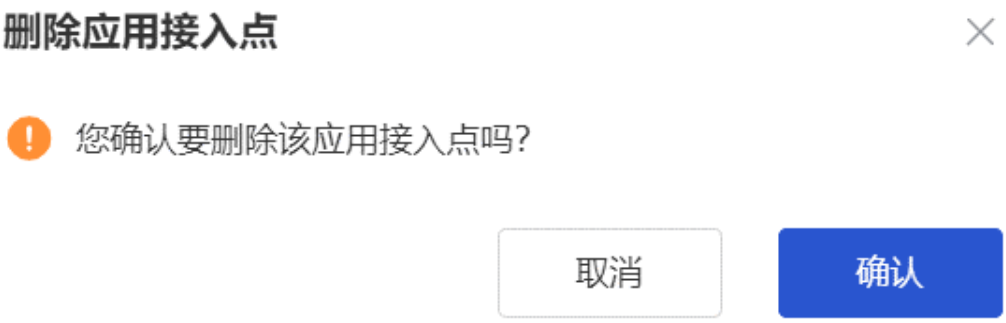
2. 根据界面提示配置资源权限。

- **权限规则开关**：默认关闭，即允许访问当前账号下的所有资源及操作。若您需要为应用接入点配置特定权限，请开启开关并配置。
- **允许访问的资源**：选择允许应用接入点操作的资源。
- **效果**：仅支持“允许”。
- **操作**：选择允许应用接入点执行的操作。包括写操作和读操作两类。

3. 配置完成后，单击“确认”。

### 删除应用接入点

若您不再需要使用应用接入点资源，您可以单击“删除”，对该应用接入点进行删除。




### 创建访问凭证（AK/SK）

成功创建应用接入点后，您需要在该应用接入点下创建访问凭证（AK/SK），在调用KMS服务时，需要导入访问凭证（AK/SK），进行身份验证。

1. 在应用接入点页面，单击应用接入点的“详情”，进入应用接入点详情页，选择“身份凭证”页签。

2. 单击“创建AccessKey”即可创建访问凭证，请在弹窗中复制或下载该访问凭证。


# 证书管理

## 证书管理概述

证书管理组件为您提供高可用、高安全的密钥和证书托管能力，您可以通过KMS提供的云原生接口实现签名验签运算。

### 证书生命周期管理

证书管理模块提供高可用、高安全的密钥和证书托管能力，您可以通过控制台或API集中管理证书。

| 功能 | 说明 |
| --- | --- |
| 证书托管 | 支持管理密钥和证书，可以生成证书请求、导入证书和证书链、启用/禁用证书、吊销或删除证书等。 |
| 密钥安全存储 | 证书管家使用托管密码机保障证书密钥的产生、存储安全。 |
| API便于集成 | 支持多个API接口，帮助在开发环境高效集成证书服务，快速进行产品部署，为您提供快速开发上线证书相关功能的能力。 |

### 支持的证书类型

| 证书类型 | 说明 |
| --- | --- |
| 数字证书（含私钥） | 支持通过证书管理服务生成证书请求，导入或导出数字证书及其证书链，证书私钥由KMS硬件安全模块保护。 |
| Ukey证书（不含私钥） | 支持将Ukey中的证书（不含私钥）导出并存入KMS，由KMS统一托管，并支持调用KMS提供的接口实现身份认证中的验签运算。 |

### 证书运算API

KMS提供云原生的证书运算类API，帮助在开发环境高效集成证书服务，快速实现证书调用。

| 功能 | 说明 | 参考文档 |
| --- | --- | --- |
| 加密解密 | 证书公钥运算：使用指定证书加密数据。<br>证书私钥运算：使用指定证书解密数据。 | 证书公钥加密<br>证书私钥解密 |
| 签名验签 | 证书私钥运算：使用指定证书生成数字签名。<br>证书公钥运算：使用指定证书验证数字签名。 | 证书私钥签名<br>证书公钥验签 |

### 功能优势

- **密钥安全存储**

  证书管家使用托管密码机保障证书密钥的产生、存储安全。

- **生命周期管理**

  支持管理密钥和证书，可以生成证书请求、导入证书和证书链、检查证书链签名有效性，并检查证书有效性。

- **API便于集成**

  支持多个API接口，帮助您在开发环境高效集成证书服务，快速进行产品部署，为您提供快速开发上线证书相关功能的能力。

## 创建证书

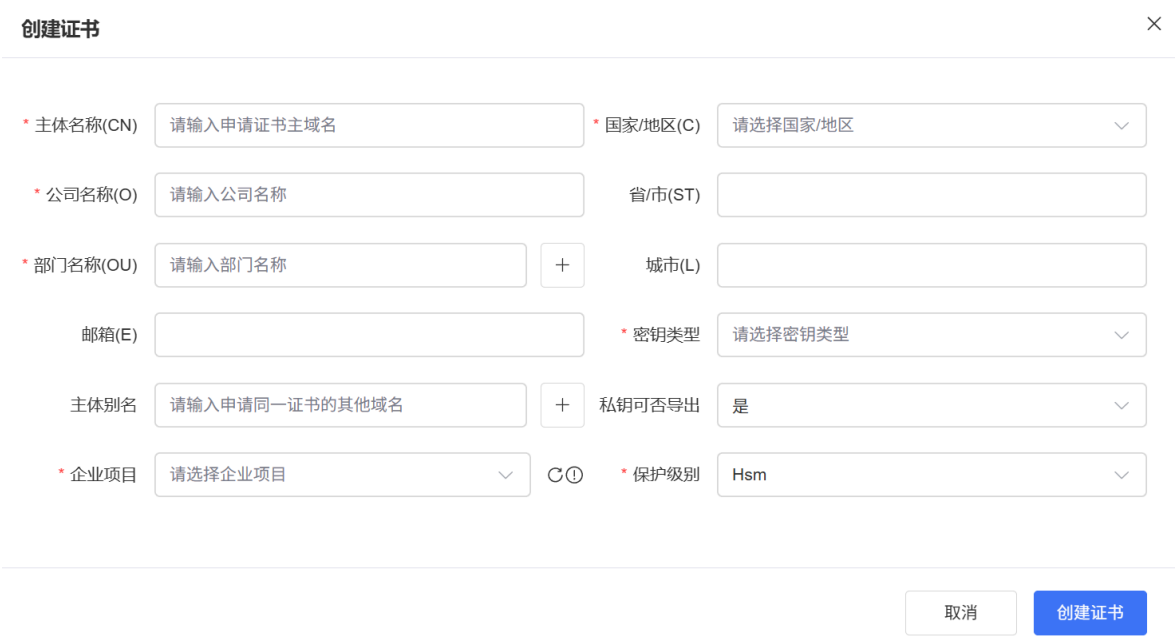
支持数字证书和Ukey证书，关于两种证书的区别，请参见证书管理概述。

### 创建数字证书

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏的资源池下拉列表，选择服务所在的区域。

3. 在左侧导航栏，点击**证书管理**，进入数字证书管理页，点击创建证书。


4. 在弹出的创建证书对话框，根据页面提示进行配置信息填写。

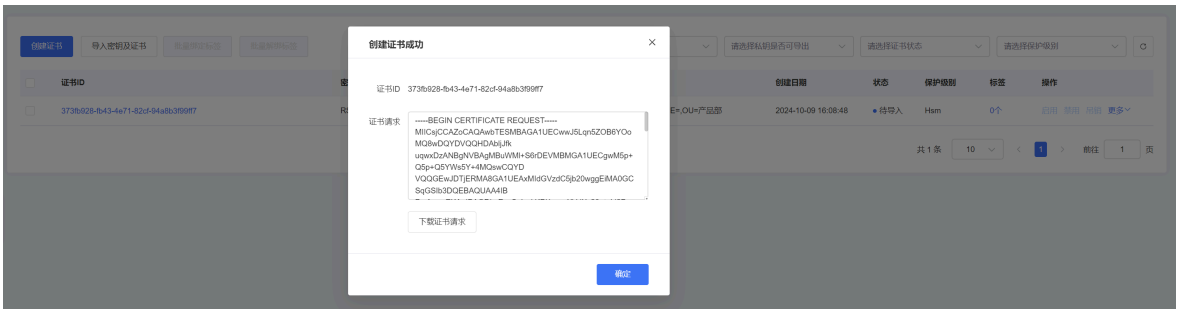



**配置项说明：**

| 配置项 | 说明 |
| --- | --- |
| 主体名称（CN） | 证书使用的主体名称。 |
| 国家/地区（C） | 使用ISO 3166-1的二位国家代码，例如：CN代表中国。 |
| 省/市（ST） | 省、直辖市、自治区或特别行政区名称。 |
| 城市（L） | 城市名称。 |
| 公司名称（O） | 企业、单位、组织或机构的法定名称。 |
| 部门名称（OU） | 部门名称。 单击右侧加号，可以添加多个部门名称，最多可添加5个。 |
| 邮箱（E） | 证书持有者或管理者邮箱。 |

| 配置项 | 说明 |
| --- | --- |
| 主体别名 | 当证书为DV证书时，可使用主体别名生成多域名证书请求。最多可添加10个。 |
| 密钥类型 | 取值：RSA_2048、SM2（企业版支持） |
| 私钥可否导出 | 证书私钥是否需要导出使用。取值：<br>• 是：证书私钥需要导出使用。<br>• 否：证书私钥不需要导出使用。<br>建议选择否，以便使用更高安全级别的密钥保护。 |
| 企业项目 | 选择证书归属的企业项目，默认为default。 |

5. 证书信息填写完成后，点击 **创建证书** ，系统会返回证书ID及证书请求，点击 **下载证书请求** ，下载完成点击 **确定** 。




6. 下载csr格式的证书请求文件后，将其提交给CA机构，获取正式的证书和证书链。
7. 将证书和证书链导入证书管理服务，在证书列表页面，找到目标证书，点击 **更多-导入证书**。

8. 在导入证书对话框，输入或上传CA机构颁发的证书和证书链，点击 **确定** 。


9. 导入证书成功后，证书状态为 **启用中** ，您可以使用证书进行签名验签等操作。

**创建UKey证书**

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏的资源池下拉列表，选择服务所在的区域。
3. 在左侧导航栏，点击 **证书管理，** 进入数字证书管理页。

4. 在左上角选择**Ukey证书（不含私钥）**，进入Ukey证书管理页，点击导入Ukey证书。


5. 在弹出的导入Ukey证书对话框，根据页面提示进行配置信息填写。

| 配置项 | 说明 |
| --- | --- |
| 证书名称 | 证书使用的主体名称。 |
| 证书算法 | 可选：RSA_2048、SM2 |
| 证书 | 填写Base64格式的证书内容 |

6. 单击“上传证书”，上传证书文件，上传完成后单击“确定”即可完成Ukey证书导入。

## 导入密钥和证书

当您需要将其他证书系统的证书迁移并托管至天翼云证书管理服务中，需要先从其他证书系统导出PFX/PKCS12格式的密钥文件，并将其导入到密钥管理服务-证书管理控制台。

### 操作步骤

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏的资源池下拉列表，选择服务所在的区域。
3. 在左侧导航栏，点击**证书管理**，在证书列表右上方，点击**导入密钥及证书**。

4. 在导入密钥及证书对话框，输入PKCS12文件保护口令，并输入或上传PKCS12格式文件。


5. 完成填写后，点击确定。

## 禁用、吊销或删除证书

证书成功导入证书管理控制台后，您可以调用实现签名验签。当您不再使用该证书时，可以通过控制台禁用、吊销或删除证书。

### 禁用证书

当您暂时无需使用证书时，可以禁用证书。禁用后的证书信息将保留，后续您可以根据需求再次启用证书。

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏的资源池下拉列表，选择服务所在的区。

3. 在左侧导航栏，点击 **证书管理** ，在证书列表找到目标证书，点击操作列的 **禁用** 。


4. 在禁用证书对话框，点击 **确定** 。

### 吊销证书

当CA机构作废了证书时，您可以将证书管理控制台中证书的状态设置为已吊销。吊销后的证书信息将保留，后续您仅可以查看证书信息，但不可以启用或禁用证书。

1. 单击目标证书右侧操作列的 **吊销**。
2. 在吊销证书对话框，单击确定。

### 删除证书

当您无需使用证书管家管理证书时，可以删除证书。删除证书前，请确保证书没有用于签名验签。

1. 在目标证书右侧操作列的 **删除证书**。
2. 在删除证书对话框，单击 **确定** 。

## 客户端加密模块License管理

### 解绑License

当您暂时无需在当前环境的机器上使用客户端加密模块时，可以解绑License。解绑后的License信息将保留，您可以根据需求再次启用绑定到其他机器。

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏选择密钥所在的区域。
3. 在左侧导航栏，选择“**客户端加密模块 > 授权管理**”，在License列表找到目标License，点击操作列的“解绑”。


4. 在解绑License对话框，点击“确认”。

### 退订License

License支持7天内无理由退订，超过7天将无法退订。退订后的License信息将保留，后续您仅可以 查看License信息。

1. 单击目标License右侧操作列的“退订”。


2. 在退订申请对话框，选择退订原因，单击“确认”。

### 查看License

当您需要查看或绑定License时，可以查看或复制License信息。

1. 在目标License右侧操作列的“查看License”。
2. 在查看License对话框，单击“复制”，可将未绑定的License绑定到其他机器。

# 云产品服务端加密

## 云产品集成KMS加密概述

密钥管理服务（KMS）与云硬盘、对象存储、弹性文件、关系型数据库MYSQL版等产品实现了服务端集成，在使用这些云服务时，可通过密钥管理服务实现对数据的加解密，并集中使用密钥管理服务（KMS）对密钥进行管理。

### 支持服务端加密的密钥类型

服务端加密支持选择默认密钥及用户自行创建的用户主密钥，具体可选择的密钥类型如下。

| 密钥创建者 | 密钥类型 | 密钥算法 |
| --- | --- | --- |
| 云产品 | 默认密钥 | AES_256（默认） |
| 用户自行创建 | 用户主密钥-软件 | AES_256 |
| | 用户主密钥-硬件 | AES_256<br>SM4 |

- **默认密钥**
  - 系统为云产品自动创建的用于服务端加密的默认密钥，默认密钥与云产品对应，每个天翼云账号下的每个云产品在每个资源池支持创建1个默认密钥。
  - 默认密钥的别名定义为alias_<云产品代码>，例如alias_ecs。
  - 默认密钥的密钥材料由KMS生成，不支持导入外部密钥材料，同时不支持自动轮转、启用/禁用、计划删除、自定义别名等操作。

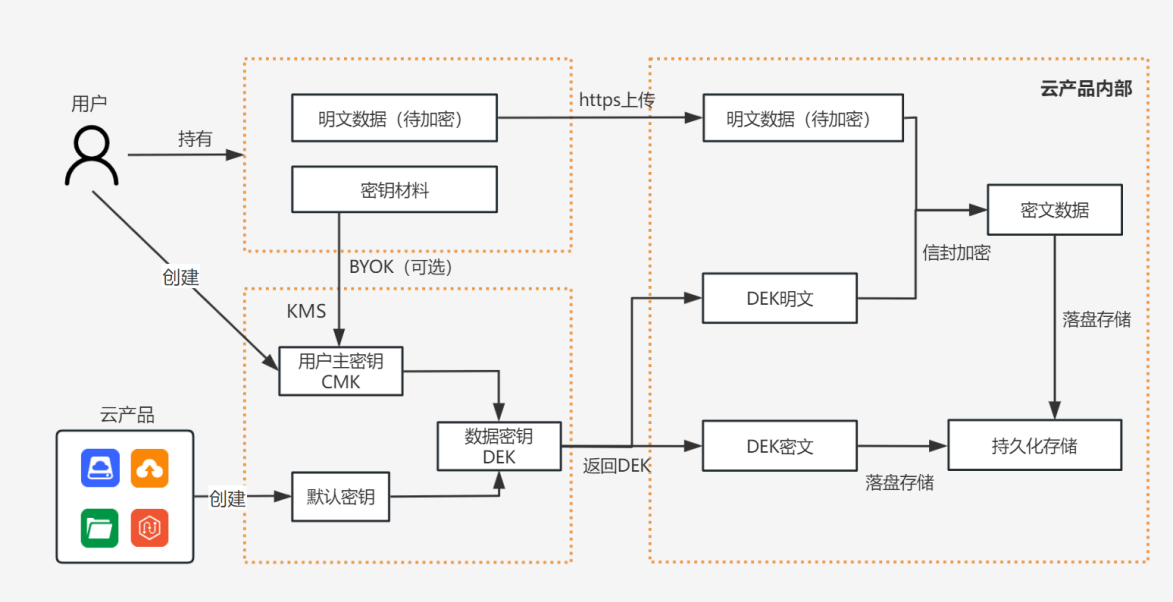
- **用户主密钥**
  - 云产品加密时，可选用户在KMS服务中自建的用户主密钥，密钥类型为对称密钥，算法支持AES_256、SM4，保护级别可选软件保护、硬件保护。
  - 用户主密钥按照KMS服务标准资费进行计费，请您确保账户余额充足，避免因KMS服务冻结导致云产品无法正常调用KMS服务进行加解密操作，云产品可能会出现异常。
  - 用户主密钥支持计划删除，操作计划删除前请确保该密钥非未被用于云产品加密，避免删除后导致云产品无法正常加解密而出现异常。为避免误删，您可以为密钥开启删除保护功能。

注意

当前云产品加密仅支持选择按需版本中的自建用户主密钥，当前包周期版本中的用户主密钥暂不支持做云产品加密使用。若您为2024年9月10日之后购买了KMS包周期服务，您可选择使用默认密钥进行云产品加密。

**云产品服务端加密的流程**

通常情况下，云产品采用信封加密的机制实现对云产品数据的加密，即通过KMS生成数据密钥，并应用数据密钥在云产品服务端完成加解密操作，并将数据密钥密文及数据密文落盘存储，实现流程如下示意图。




1. 用户在KMS中创建一个用户主密钥，或由云产品触发创建默认密钥。
2. 云产品调用KMS的GenerateDataKey接口请求数据密钥。
3. KMS返回数据密钥，包含数据密钥明文和数据密钥密文。其中数据密钥密文，是由指定的密钥加密数据密钥明文生成的。
4. 云产品使用数据密钥明文加密数据明文，并将数据密钥密文（由KMS使用密钥加密）与数据密文（由云产品使用数据密钥加密）一同写入持久化存储介质中。

## 支持KMS服务端加密的云产品

当前天翼云KMS已与部分云产品集成，为云产品提供服务端加密功能，您可以在云产品控制台一键开启加密功能，加解密过程透明无感知。

### 存储

| 产品名称 | 描述 | 相关文档 |
| --- | --- | --- |
| 云硬盘 | 云硬盘支持加密功能，加密云硬盘使用的密钥由KSM提供，并保护密钥的安全。<br>在创建加密云硬盘并将其挂载到实例后，以下数据都将关联此密钥并进行加密：<br>• 云硬盘中的静态数据<br>• 云硬盘和实例间传输的数据（实例操作系统内的数据不加密）<br>• 通过加密云硬盘创建的快照 | 管理加密云硬盘 |
| 对象存储 | 对象存储（简称ZOS）在数据写入数据中心内的磁盘之前，支持在对象级别上应用数据加密的保护策略，并在访问数据时自动解密。<br>加密和解密这一操作过程都是在服务端完成，这种服务端加密功能可以有效保护静态数据。 | 服务端加密 |
| 弹性文件 | 在创建文件系统时可以根据实际需要选择是否开启加密服务，无须授权，选择开启即可对新创建的文件系统进行加密。 | 加密 |

### 数据库

| 产品名称 | 描述 | 相关文档 |
| --- | --- | --- |
| 关系数据库MySQL版 | 关系数据库MySQL版服务支持设置透明数据加密TDE，在数据落盘时对数据进行加密，从而保证数据的安全性，用户业务对此加密过程无感知。 | 设置透明数据加密TDE |
| 关系型数据库PostgreSQL版 | 关系型数据库PostgreSQL版支持透明数据加密，通过用户在KMS服务中创建的对称主密钥来生成DEK（Data Encryption Key）数据密钥，并使用数据密钥对数据进行加密。 | 透明数据加密概述 |
| 文档数据库服务 | 文档数据库服务支持磁盘加密，磁盘加密通过KMS提供的密钥实现。 | 磁盘加密 |

# 权限管理

## IAM权限

您通过IAM服务定义企业项目、创建子用户，轻松实现IAM子用户对KMS资源的访问控制、权限分配等。

说明

IAM 权限作用于KMS产品控制台的功能访问以及KMS服务的OpenAPI接口调用。

## 权限管理

默认情况下，主账号创建的IAM用户没有任何权限，需要将其加入特定的用户组，并给用户组授予KMS产品的权限策略（包括系统策略和自定义策略），授权后IAM用户就能获得策略中定义的KMS产品的使用权限。

KMS产品支持企业项目管理，若您需要对KMS服务中的资源进行分组和管理，形成逻辑隔离，您可以创建企业项目，并将资源划分至不同的企业项目中，不同的企业项目可以绑定不同的用户组，并给用户组授予KMS产品的权限策略（包括系统策略和自定义策略），从而实现对特定资源的授权。

### 权限配置

IAM权限管理：进入天翼云IAM权限配置界面，可以进行IAM用户及用户组的创建，并在用户组列表中点击“授权”，为用户组添加KMS产品对应的权限策略。KMS权限策略分为系统策略和自定义策略，系统策略默认提供，您也可以在“策略管理”界面创建自定义策略。用户组授权记录均可在“授权管理”界面查看并管理。

企业项目管理：进入天翼云IAM权限 配置界面，在“企业项目”界面可以创建并管理企业项目，创建企业项目后可进行资源的迁入迁出，绑定用户组，并给用户组授予KMS产品的权限策略（包括系统策略和自定义策略）。

### KMS权限策略

KMS权限策略包含系统策略和自定义策略，如果系统策略不满足授权要求，您可以创建自定义策略，并 为IAM用户授予自定义策略来进行精细的访问控制。目前IAM支持以下两种方式创建自定义策略：

- 可视化视图：通过可视化视图创建自定义策略，无需了解JSON语法，按可视化视图导航栏选择云 服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图：通过JSON视图创建自定义策略，可以直接在编辑框内编写JSON格式的策略内容。

详细介绍请参考IAM关于策略管理的介绍。

KMS支持的授权项

- 密钥管理

| 权限 | 对应API接口 | 授权项 | 读写类型 |
| --- | --- | --- | --- |
| 创建密钥 | /v1/cmkManage/createKey | kms:cmk:create | 写 |
| 启用密钥 | /v1/cmkManage/enableKey | kms:cmk:enable | 写 |
| 禁用密钥 | /v1/cmkManage/disableKey | kms:cmk:disable | 写 |
| 计划删除密钥 | /v1/cmkManage/scheduleKeyDeletion | kms:cmk:delete | 写 |
| 取消计划删除密钥 | /v1/cmkManage/cancelKeyDeletion | kms:cmk:undelete | 写 |
| 更新密钥描述 | /v1/keyManage/updateKeyDescription | kms:cmk:update | 写 |
| 查看密钥列表 | /v1/keyManage/listAliasKeys | kms:cmk:list | 读 |
| 查看密钥详情 | /v1/keyManage/describeKey | kms:cmk:describe | 读 |
| 开启删除保护 | /v1/cmkManage/scheduleKeyDeletion | kms:cmk:deleteProtect | 写 |
| 取消删除保护 | /v1/cmkManage/cancelKeyDeletion | kms:cmk:cancelDeleteProtect | 写 |
| 获取导入密钥材料参数 | /v1/importKey/getParametersForImport | kms:cmk:getParameters | 写 |
| 导入密钥材料 | /v1/importKey/importKeyMaterial | kms:cmk:importMaterial | 写 |
| 删除密钥材料 | /v1/importKey/deleteKeyMaterial | kms:cmk:deleteMaterial | 写 |

| 权限 | 对应API接口 | 授权项 | 读写类型 |
| --- | --- | --- | --- |
| 设置/更新轮转策略 | /v1/versionControl/updateRotationPolicy | kms:cmk:updateRotation | 写 |
| 创建密钥版本 | /v1/versionControl/createKeyVersion | kms:cmk:createVersion | 写 |
| 列出主密钥所有密钥版本 | /v1/versionControl/listKeyVersions | kms:cmk:listVersions | 读 |
| 查看指定密钥版本信息 | /v1/versionControl/describeKeyVersion | kms:cmk:describeVersion | 读 |
| 创建别名 | /v1/keyName/createAlias | kms:cmk:createAlias | 写 |
| 删除别名 | /v1/keyName/deleteAlias | kms:cmk:deleteAlias | 写 |
| 更新别名（非控制台功能） | /v1/keyName/updateAlias | kms:cmk:updateAlias | 写 |
| 列出与指定密钥绑定的别名 | /v1/keyName/listAliasByUuid | kms:cmk:listAliasByUuid | 读 |
| 列出所有别名（非控制台功能） | /v1/keyName/listAlias | kms:cmk:listAlias | 读 |
| 在线加密 | /v1/keyCompute/encrypt | kms:cmk:encrypt | 写 |
| 产品数据密钥（信封加密） | /v1/keyCompute/generateDataKey | kms:cmk:generateDataKey | 写 |
| 产生无明文返回值的数据密钥（信封加密） | /v1/keyCompute/generateDataKeyWithoutPlaintext | kms:cmk:generateDataKeyWithoutPlaintext | 写 |
| 导出数据密钥 | /v1/keyCompute/exportDataKey | kms:cmk:exportDataKey | 写 |
| 产生并导出数据密钥 | /v1/keyCompute/generateAndExportDataKey | kms:cmk:generateAndExportDataKey | 写 |
| 解密 | /v1/keyCompute/decrypt | kms:cmk:decrypt | 写 |
| 转加密 | /v1/cmkManage/reEncrypt | kms:cmk:reEncrypt | 写 |
| 产生数字签名 | /v1/asymmetric/asymmetricSign | kms:cmk:asymmetricSign | 写 |
| 验证签名 | /v1/asymmetric/asymmetricVerify | kms:cmk:asymmetricVerify | 写 |
| 非对称密钥加密 | /v1/asymmetric/asymmetricEncrypt | kms:cmk:asymmetricEncrypt | 写 |
| 非对称密钥解密 | /v1/asymmetric/asymmetricDecrypt | kms:cmk:asymmetricDecrypt | 写 |
| 获取非对称密钥公钥 | /v1/asymmetric/getPublicKey | kms:cmk:getPublicKey | 写 |

- 证书管理

| 权限 | 对应API接口 | 授权项 | 读写类型 |
| --- | --- | --- | --- |
| 创建证书csr | /v1/manageCertificate/createCertificate | kms:cert:create | 写 |
| 导入证书 | /v1/manageCertificate/importCertificate | kms:cert:import | 写 |
| 查看证书列表 | /manageCertificate/listCertificate | kms:cert:list | 读 |

| 权限 | 对应API接口 | 授权项 | 读写类型 |
| --- | --- | --- | --- |
| 查询证书信息 | /v1/manageCertificate/describeCertificate | kms:cert:describe | 读 |
| 更新证书状态 | /v1/manageCertificate/updateCertificateStatus | kms:cert:update | 写 |
| 获取证书 | /v1/manageCertificate/getCertificate | kms:cert:get | 读 |
| 导出证书私钥 | /v1/manageCertificate/exportCertifiicatePrivatkey | kms:cert:exportPrivatkey | 写 |
| 删除证书 | /v1/manageCertificate/deleteCertificate | kms:cert:delete | 写 |
| 证书私钥签名 | /v1/certificateCompute/certificatePrivateKeySign | kms:cert:privateKeySign | 写 |
| 证书公钥验签 | /v1/certificateCompute/certificatePublicKeyVerify | kms:cert:publicKeyVerity | 写 |
| 证书公钥加密 | /v1/certificateCompute/certificatePublicKeyEncrypt | kms:cert:publicKeyEncrypt | 写 |
| 证书私钥解密 | /v1/certificateCompute/certificatePrivateKeyDecrypt | kms:cert:privateKeyDecrypt | 写 |
| 生成随机数 | /v1/certificatecompute/getRandom | kms:cert:getRandom | 写 |

- 服务管理

| 权限 | 对应OpenAPI接口 | 授权项 | 读写类型 |
| --- | --- | --- | --- |
| 实例服务列表 | - | kms:instance:list | 读 |
| 密钥管理服务订购 | - | kms:instance:purchase | 写 |
| 密钥管理服务续订 | - | kms:instance:renew | 写 |
| 密钥管理服务退订 | - | kms:instance:refund | 写 |
| 密钥管理服务扩容 | - | kms:instance:expand | 写 |
| 密钥管理服务升级 | - | kms:instance:upgrade | 写 |

## 应用接入点权限

说明

应用接入点权限作用于KMS服务SDK中的接口调用，即当您的应用通过集成KMSSDK访问KMS服 务接口，服务将依旧应用接入点的权限策略进行身份认证和行为鉴权。

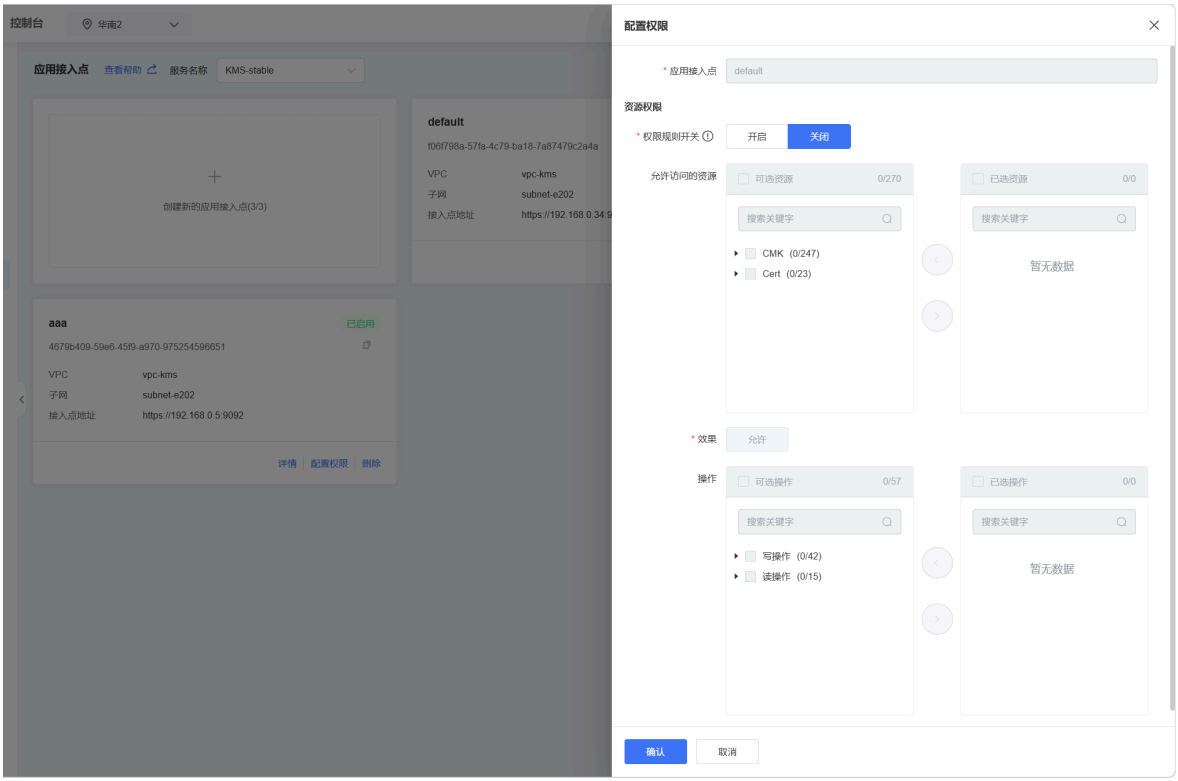
### 权限管理

应用接入点可配置对应的权限，包括可使用的密钥、证书等资源范围以及接口级操作权限。

- 允许访问的资源：应用允许访问的密钥、证书。
- 操作权限：应用允许使用的功能点。

**权限配置**

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏选择服务所在的区域。
3. 进入“应用接入点”页面，在页面上方切换至目标KMS服务实例。
4. 找到目标应用接入点，点击配置权限。
5. 在权限策略配置页签，配置对应的权限。




| 配置 | 说明 |
| --- | --- |
| 权限规则开关 | 应用接入点创建成功后，权限规则开关默认关闭，即允许访问当前账 权限规则开关 号下的所有资源及操作。若您需要为应用接入点配置特定权限，请开启开关并配置。 |
| 允许访问的资源 | 可选：<br>• 密钥<br>• 证书<br>请勾选应用通过应用接入点需要访问的密钥或证书资源。 |

| 配置 | 说明 |
| --- | --- |
| 效果 | 默认为允许，即您当前的规则为允许当前应用访问的资源及接口。 |
| 操作 | 选择允许应用访问的功能点。 |

6. 配置完成后，点击确认，页面提示“权限配置成功”表示权限控制已经生效。

# 云审计服务支持的关键操作

## 操作场景

本服务现已对接天翼云云审计服务，云审计服务提供对各种云资源操作的记录和查询功能，用于支撑合规审计、安全分析、操作追踪和问题定位等场景，同时提供事件跟踪功能，将操作日志转储至对象存储实现永久保存。

云审计可提供的功能服务具体如下：

- 记录审计日志：支持用户通过管理控制台或API接口发起的操作，以及各服务内部自触发的操作。
- 审计日志查询：支持在管理控制台对7天内操作记录按照事件类型、事件来源、资源类型、筛选类型、操作用户和事件级别等多个维度进行组合查询。
- 审计日志转储：支持将审计日志周期性的转储至对象存储服务（ZOS）下的ZOS桶。

### 使用限制

- 云审计服务本身免费，包括时间记录以及7天内时间的存储和检索。若您使用云审计提供的转储功能，需要开通对象存储服务并支付产生的费用，该费用以对象存储产品的计费为准，参考计费说明-对象存储。
- 用户通过云审计能查询到多久前的操作事件：7天。
- 用户操作后多久可以通过云审计查询到数据：5分钟。
- 其它限制请参考使用限制-云审计。

**关键操作列表**

| 操作事件 | 字段 |
| --- | --- |
| 创建数据密钥 | generateDataKey |
| 创建数据密钥（无明文） | generateDataKeyWithoutPlaintext |
| 导出数据密钥 | exportDataKey |
| 创建并导出数据密钥 | generateAndExportDataKey |
| 数据加密 | encrypt |
| 数据解密 | decrypt |
| 禁用主密钥 | disableKey |
| 启用主密钥 | enableKey |
| 创建主密钥 | createKey |
| 计划删除密钥 | scheduleKeyDeletion |
| 取消计划删除密钥 | cancelKeyDeletion |

| 操作事件 | 字段 |
| --- | --- |
| 密钥删除保护 | deleteProtect |
| 取消密钥删除保护 | cancelDeleteProtect |
| 转加密 | reEncrypt |
| 创建默认密钥 | createDefaultKey |
| 非对称签名 | asymmetricSign |
| 非对称验签 | asymmetricVerify |
| 非对称加密 | asymmetricEncrypt |
| 非对称解密 | asymmetricDecrypt |
| 获取公钥 | getPublicKey |
| 获取密钥列表 | listAliasKeys |
| 获取密钥详情 | describeKey |
| 更新密钥描述 | updateKeyDescription |
| 获取对称密钥详情 | listSymmetricKeys |
| 查询数据密钥详情 | getDataKey |
| 创建非对称密钥版本 | createKeyVersion |
| 查询密钥版本列表 | listKeyVersions |
| 获取密钥版本详情 | describeKeyVersion |
| 更新密钥轮转策略 | updateRotationPolicy |
| 创建密钥别名 | createAlias |
| 更新密钥别名 | updateAlias |
| 删除密钥别名 | deleteAlias |
| 获取别名列表 | listAlias |
| 获取密钥别名 | listAliasByUuid |
| 计算hmac | hmaccompute |
| 计算SM3摘要 | messageDigest |
| 获得导入密钥材料 | getParametersForImport |
| 导入密钥 | importKeyMaterial |
| 删除导入密钥材料 | deleteKeyMaterial |
| 证书公钥加密 | certificatePublicKeyEncrypt |
| 证书私钥解密 | certificatePrivateKeyDecrypt |
| 证书私钥签名 | certificatePrivateKeySign |
| 证书公钥验签 | certificatePublicKeyVerify |
| 获取随机数 | getRandom |

| 操作事件 | 字段 |
| --- | --- |
| Ukey证书公钥验签 | certificatePublicKeyVerifyForUsbKey |
| 创建证书csr | createCertificate |
| 更新证书状态 | updateCertificateStatus |
| 删除证书 | deleteCertificate |
| 获取证书详情 | describeCertificate |
| 获取证书链详情 | describeCertificateChain |
| 查询证书 | getCertificate |
| 导入证书 | importCertificate |
| 导入PKCS12证书 | importCertificateByPKCS12 |
| 导出证书私钥 | exportCertificatePrivatkey |
| 查询证书列表 | listCertificate |
| 导入Ukey证书 | importCertificateForUK |
| 查询Ukey证书列表 | listCertificateForUk |
| 获取Ukey证书详情 | describeCertificateForUk |
| 查询Ukey证书信息 | getCertificateForUk |
| 更新Ukey证书状态 | updateCertificateStatusForUk |
| 删除Ukey证书 | deleteCertificateForUk |
| 获取vpc列表 | listVpc |
| 获取子网列表 | listSubnet |
| 创建应用接入点 | createApplicationAccessPoint |
| 查询接入点的接口权限列表 | listAllUri |
| 获取接入点的接口权限详情 | listPointUriPolicy |
| 接入点的接口权限变更 | changePointUriPolicy |
| 删除应用接入点 | deleteApplicationAccessPoint |
| 查询应用接入点列表 | listApplicationAccessPoint |
| 接入点的资源权限变更 | changePointResourcePolicy |
| 查询接入点的资源权限列表 | listPointResourcePolicy |
| 获取接入点的资源权限详情 | describeResourcePolicy |
| 关闭接入点权限控制 | closePolicyCheck |
| 检查接入点是否开启权限控制 | policyCheckIsOpen |
| 添加终端节点白名单 | addEndpointWhitelist |
| 查询终端节点白名单列表 | showEndpointWhitelist |
| 云产品关联检测 | detectAssociation |

| 操作事件 | 字段 |
| --- | --- |
| 创建租户ak | createUserAk |
| 启用租户ak | enableUserAk |
| 禁用租户ak | disableUserAk |
| 删除租户ak | deleteUserAk |
| 查询租户ak列表 | listUserAk |
| 查询资源信息 | resourceInfo |

**操作步骤**

1. 开通云审计服务。

   参见开通云审计服务-云审计。

2. 查看云审计事件。

   参见查看审计事件-云审计。

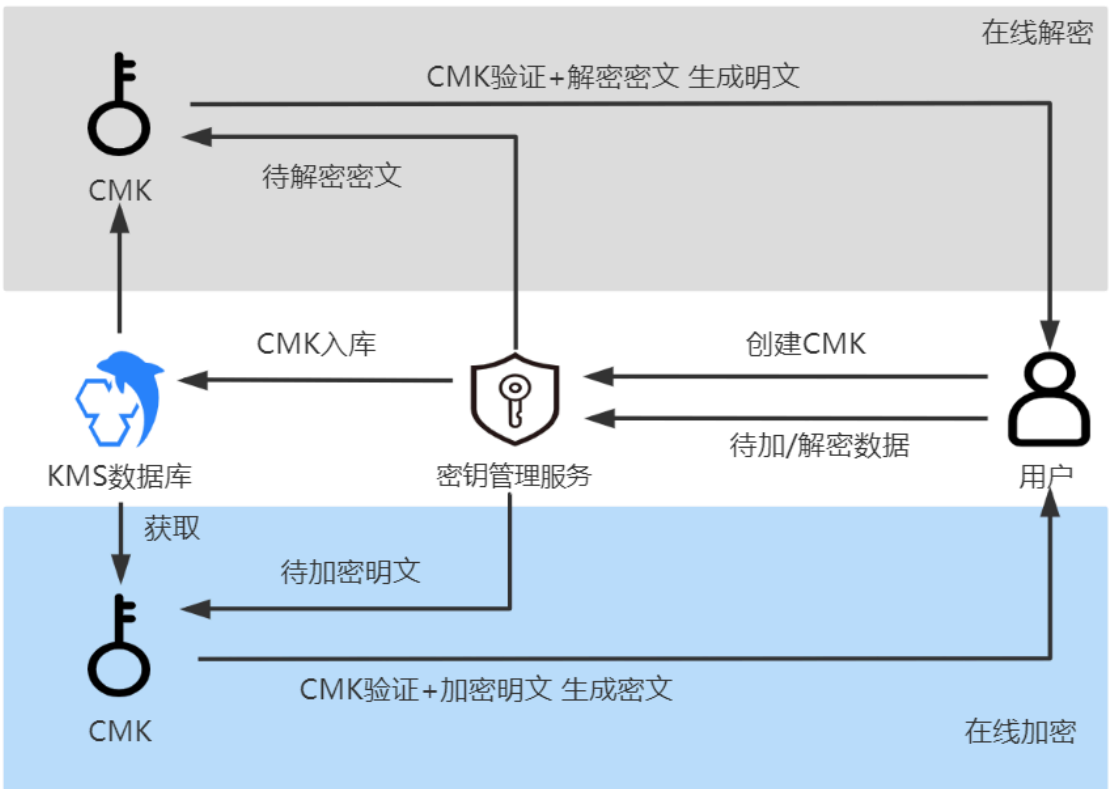
更多云审计相关使用说明和常见问题请参考用户指南、 常见问题。

# 使用KMS用户主密钥在线加解密数据

KMS提供针对敏感信息的加密能力，适用于保护小型敏感数据（小于6KB），如口令、身份信息、证书、后台配置文件等。

通过密钥管理服务KMS的在线加密API，使用用户主密钥（CMK）直接加密敏感数据信息，而非直接将明文存储，确保敏感数据安全。

## 场景示意图




### 操作流程（以证书加密为例）

1. 通过KMS控制台或者调用CreateKey接口，创建一个用户主密钥（CMK）。
2. 调用KMS服务的Encrypt接口，将明文证书加密为密文证书。
3. 将密文证书部署在服务器上。
4. 当服务器启动需要使用证书时，调用KMS服务的Decrypt接口将密文证书解密为明文证书。

### 相关API

您可以调用以下KMS API，轻松完成对数据的加密或解密操作。

# 最佳实践

| API名称 | 说明 |
| --- | --- |
| createKey | 创建用户主密钥（CMK）。 |
| encrypt | 指定CMK，直接输入明文数据，由KMS在线加密数据。 |
| decrypt | 解密由encrypt接口加密的数据，不需要指定CMK即可完成在线解密。 |

### 操作步骤

1. 通过密钥管理服务控制台创建用户主密钥CMK。


2. 通过OpenAPI在线加密接口，对敏感数据进行加密。

**请求参数说明**

| 参数 | 是否必填 | 参数位置 | 参数类型 | 说明 |
| --- | --- | --- | --- | --- |
| cmkUuid | 是 | body | String | 主密钥（CMK）的全局唯一标识符。 |
| plaintext | 是 | body | String | 待加密明文（必须经过Base64编码）。 |

请求示例


```
{
   "plaintext":"SGVsbG8gd29ybGQ=",
   "cmkUuid":"241ede22-6261-4617-9caf-10d89990516c"
}
```


成功返回


```
{
   "code":200,
   "result":{
      "ciphertextBlob":"MDA2NE1q
UXhaV1JsTWpJdE5qSTJNUzAwTmpFM0xUbGpZV110TVRCa09EazVPVEExTVRaakpqUTVaV00zTm1RM0xXTmpOR010TkRBd1pT
      "cmkUuid":"241ede22-6261-4617-9caf-10d89990516c",
      "keyVersionId":"49ec76d7-cc4c-400e-9f19-f9001587ae0f"
   },
   "statusCode":200,
   "success":1
}
```


返回参数说明

| 参数 | 说明 |
| --- | --- |
| ciphertextBlob | 数据被指定CMK的主版本加密后的密文。 |
| cmkUuid | CMK的全局唯一标识符。如果请求中的Cmk_uuid参数使用的是CMK的别名，在响应中会返回别名对应的CMK标志符。 |
| keyVersionId | 用于加密明文的密钥版本标志符，是指定CMK的主版本。 |

3. 将加密后的数据存储。

根据业务的应用场景，将密文进行存储。

4. 通过OpenAPI解密接口，对密文数据进行解密。

**请求参数说明**

| 参数 | 是否必填 | 参数位置 | 参数类型 | 说明 |
| --- | --- | --- | --- | --- |
| ciphertextBlob | 是 | body | String | 主密钥（CMK）加密的数据密钥的密文。 |

**成功返回**


```
{
  "statusCode": 800,
  "returnObj": {
    "code": 200,
    "result": {
      "cmkUuid": "8bca8f33-d42a-448a-866b-a064f44b29b7",
      "keyVersionId": "73670b28-4eea-4260-b497-ae0334cc0c85",
      "plaintext": "sc728O+klUSln3Y9FHdfKGUT+6kPrcIMW41uZQeXxGU="
    },
    "statusCode": 200,
    "success": 1
  }
}
```


**返回参数说明**

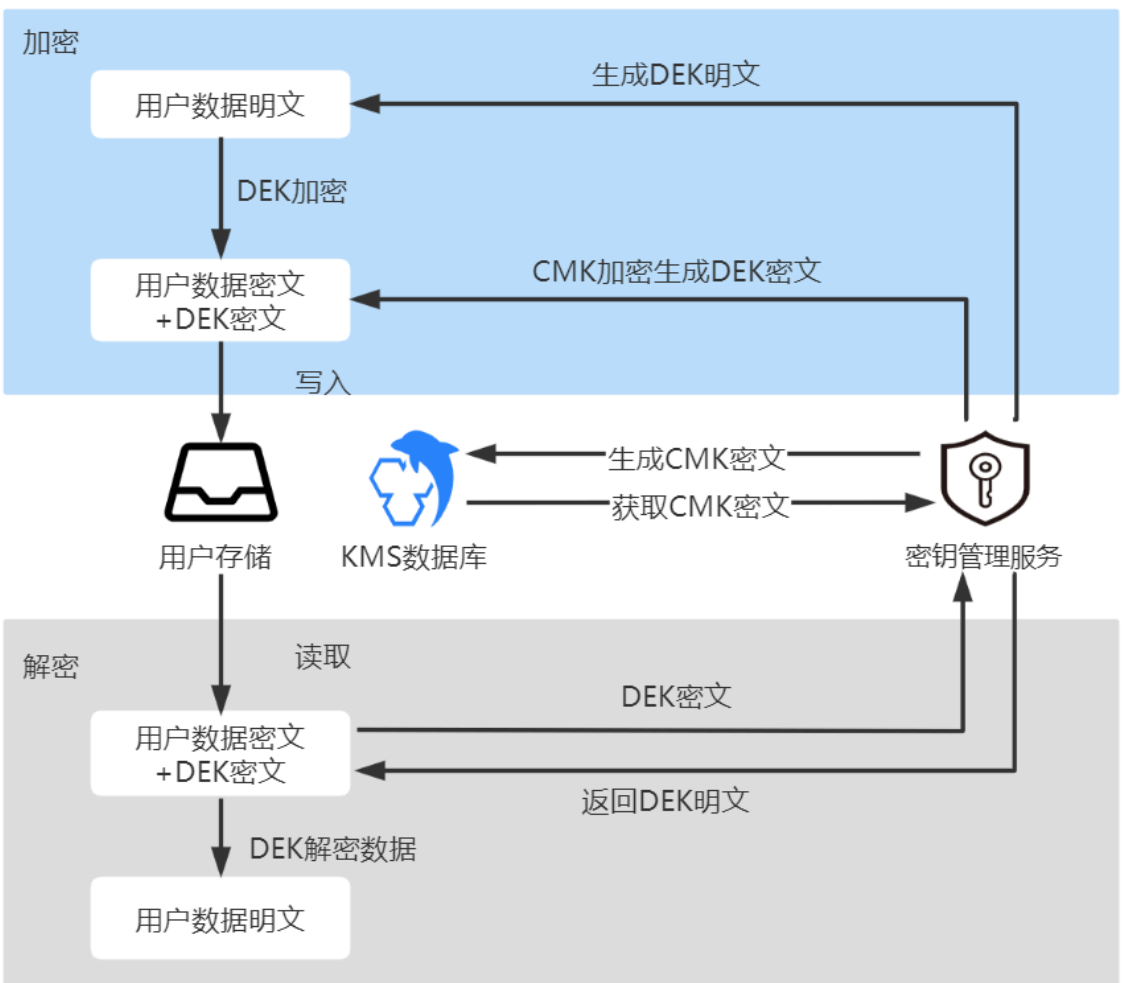
| 参数 | 说明 |
| --- | --- |
| cmkUuid | CMK的全局唯一标识符。如果请求中的Cmk_uuid参数使用的是CMK的别名，在响应中会返回别名对应的CMK标志符。 |
| keyVersionId | 密钥版本ID。主密钥版本的全局唯一标识符。 |
| plaintext | 解密后的明文经过Base64编码的后的值。 |

# 使用信封加密技术实现本地大规模数据加解密

信封加密（Envelope Encryption）是一种应对海量数据的高性能加解密方案。这种技术不再使用用户主密钥（CMK）直接加密和解密数据，而是通过生成加密数据的数据密钥（DEK），将其封入信封中（即通过CMK加密）存储、传递和使用，由KMS确保数据密钥的随机性和安全性。

实际使用时，用户无需将大量业务数据上传至KMS服务端，直接通过离线的数据密钥在本地实现加解密，有效避免安全隐患，保证了业务加密性能的要求。

## 场景示意图




加解密流程

## 信封加密过程

1. 通过KMS控制台或者调用CreateKey接口，创建一个用户主密钥（CMK）。

2. 调用GenerateDataKey接口创建一个数据密钥。KMS会返回一个明文的数据密钥和一个经用户主密钥（CMK）加密的密文数据密钥。
3. 使用明文的数据密钥加密本地文件，产生密文文件，然后销毁内存中的明文数据密钥。
4. 用户将密文数据密钥和密文文件一同存储到持久化存储设备或服务中。

### 信封解密过程

1. 从本地文件中读取密文数据密钥。
2. 调用KMS服务的Decrypt接口，将密文数据解密为明文数据密钥。
3. 用明文数据密钥为本地密文文件解密，再销毁内存中的明文密钥。

#### 相关API

您可以调用以下KMS API，实现对本地数据的加密或解密操作。

| API名称 | 说明 |
| --- | --- |
| createKey | 创建用户主密钥（CMK）。 |
| generateDataKey | 生成信封加密的数据密钥，返回数据密钥的明文和经过指定用户主密钥加密的密文。 |
| decrypt | 解密由generateDataKey接口生成的数据密钥密文，不需要指定CMK。 |

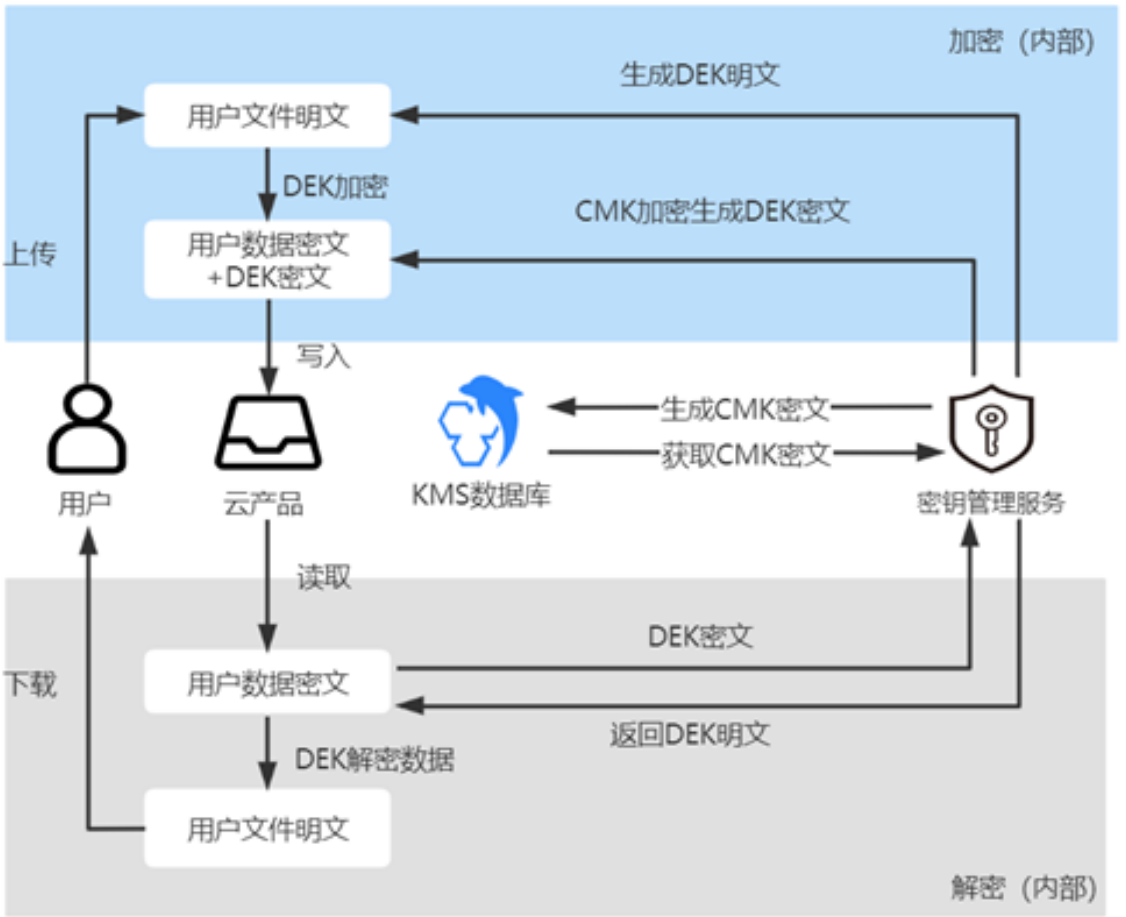
## 云服务通过KMS实现服务端加密

密钥管理系统与天翼云产品无缝集成，在云产品中，仅需要选择在KMS中托管的主密钥，即可轻松实现对云产品数据的服务端加密。

云产品通过集成KMS实现对云上数据的加密存储，密钥由KMS托管，满足监管合规要求。整个服务端加密过程对用户透明无感知，只需要开启加密功能并指定密钥即可。同时用户无须自定构建和维护密钥管理基础设施，节省开发成本。

用户可以选择KMS为云产品自动创建的默认主密钥加密，也可以选择通过KMS创建的用户主密钥。其中默认密钥不收取密钥托管费用。

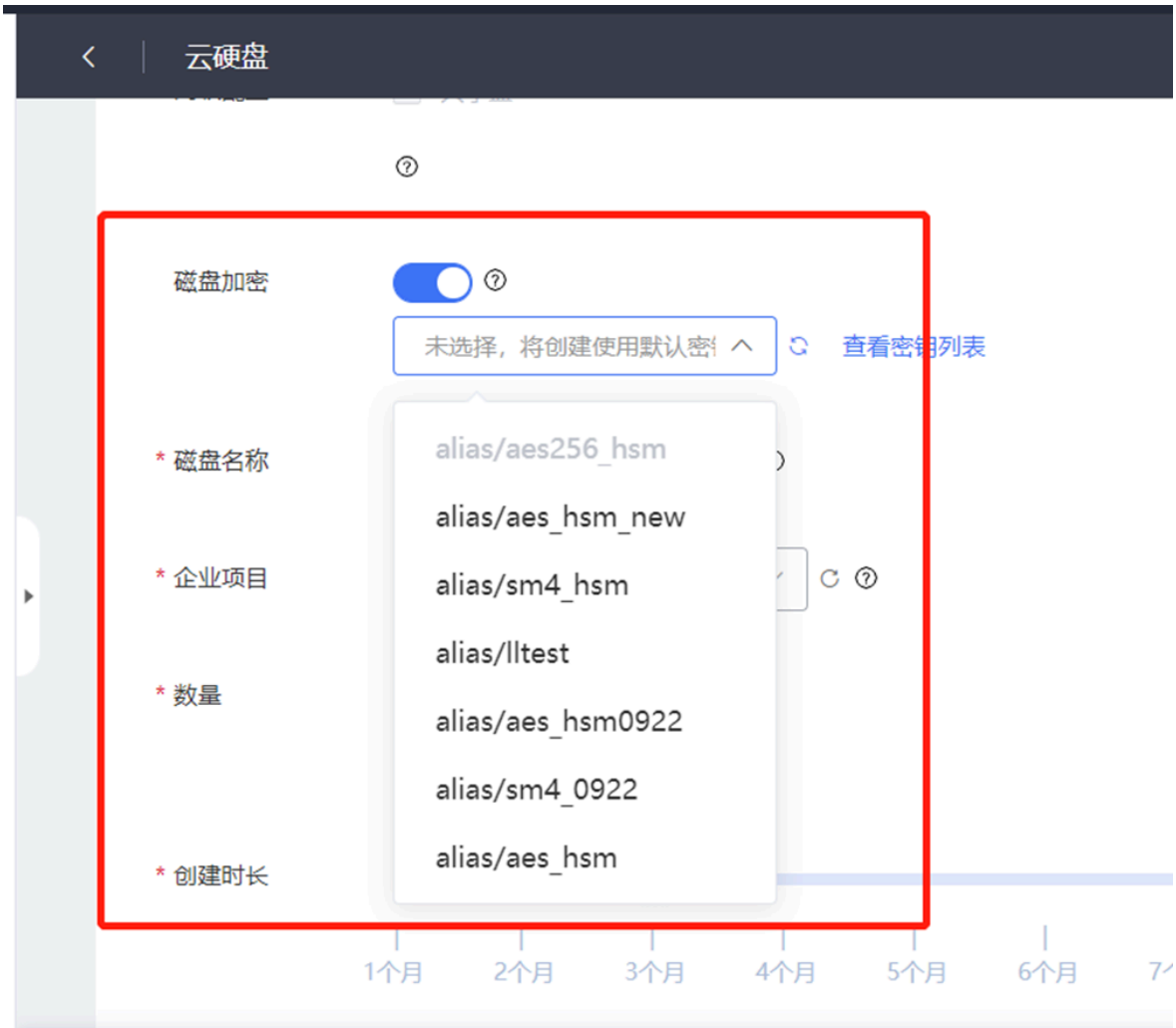
## 场景示意图




云产品开启服务端加密流程

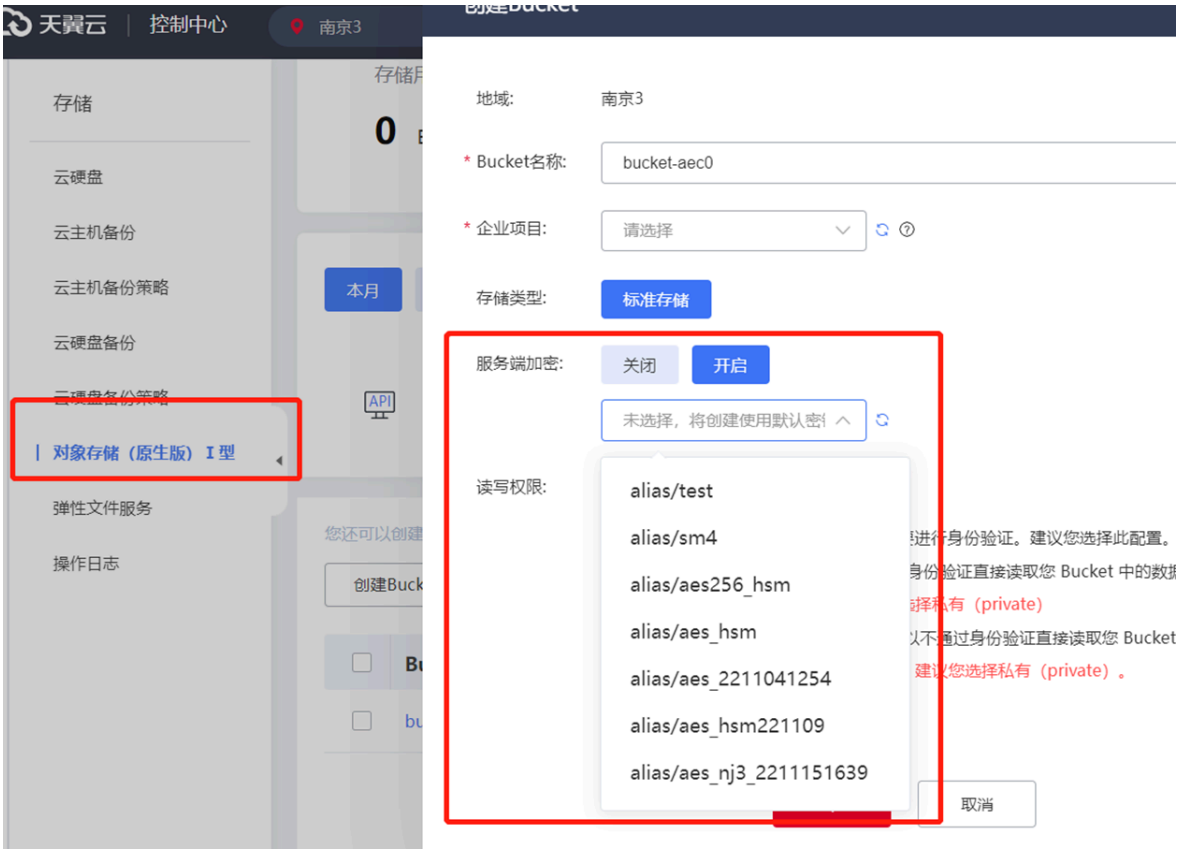
## 加密云硬盘

在创建云硬盘页面，选择开启“磁盘加密”，并在密钥列表中选择加密密钥。




## 加密对象存储

在创建对象存储Bucket页面，选择开启“服务端加密”，并在密钥列表中选择加密密钥。




## 加密弹性文件

在创建文件系统页面，选择开启KMS加密，并在密钥列表中选择加密密钥。


## 通过KMS实现签名验签

数字签名技术是非对称加密算法的另一种典型应用。数字签名分为签名和验证两个过程，消息发送者使用私钥对数据签名，消息接收者使用公钥进行签名验证。

通过密钥管理服务（KMS）创建的非对称密钥可以实现签名验签功能，签名者通过调用密码运算API使用私钥计算消息签名，同时获取公钥并分发至消息接收者，接收者使用公钥对消息进行签名验证。

- 场景特点

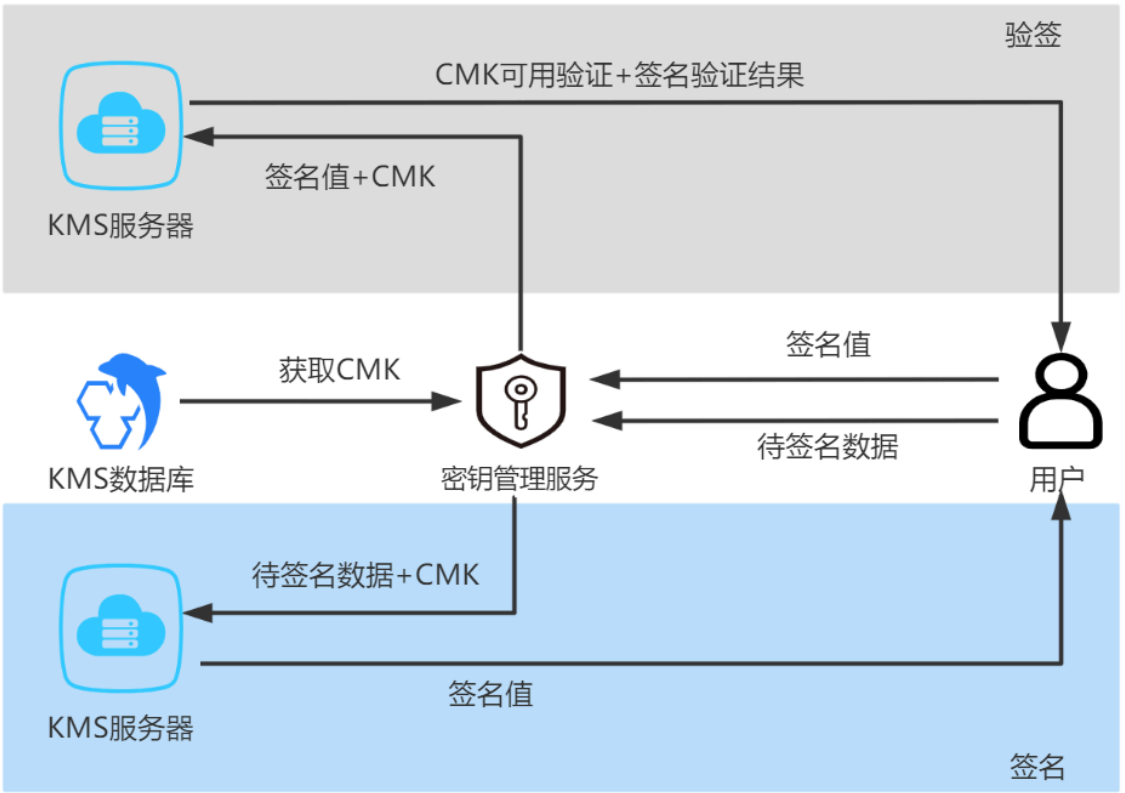
用于信任程度不对等的系统之间，实现敏感信息的安全传递。

- 优势

应用广泛：通过非对称密钥实现签名验签，广泛用于数据防篡改、身份认证等相关技术领域。

安全保障：支持主流的非对称密钥算法并且提供足够的安全强度，保证数字签名的安全性。

## 场景示意图




### 操作流程

1. 信息发送者通过KMS控制台或者调用CreateKey接口，创建一个非对称的用户主密钥（CMK）。
2. 信息发送者通过调用KMS的getPublicKey接口获取到公钥，并将公钥分发给消息接收者。
3. 信息发送者通过调用KMS的asymmetricSign接口，使用创建的CMK私钥对需要传输的数据生成签名。
4. 信息发送者将签名和数据传递给信息接收者。
5. 信息接收者拿到签名和数据之后，在本地通过gmssl、openssl、密码库、KMS 的国密 Encryption SDK 等验签方法，使用信息发送者分发的公钥进行验证。特殊需求场景下，也可调用KMS的asymmetricVerify接口，使用CMK进行签名校验。

### 相关API

您可以调用以下KMS API，完成对数据的签名验签处理。

| API名称 | 说明 |
| --- | --- |
| createKey | 创建用户主密钥（CMK）。 |
| getPublicKey | 获取非对称密钥的公钥，可用于离线验证数字签名，或者加密数据。 |
| asymmetricSign | 非对称密钥的私钥运算：产生数字签名。 |

| API名称 | 说明 |
| --- | --- |
| asymmetricVerify | 非对称密钥的公钥运算：验证私钥产生的数字签名。 |

# 通过密钥轮转加强密钥使用的安全性

KMS提供密钥轮转功能实现密钥版本化，从而加强密钥使用的安全性，有效提升业务数据加密的安全性。本文为您介绍如何配置对称密钥和非对称密钥的轮转。

## 密钥轮转的必要性

- 密码合规要求

相关行业标准中明确规范，要求密钥进行周期性轮转。

- 减少每个密钥版本加密的数据量，降低密码分析攻击风险

一个密钥的安全性与被它加密的数据量呈反相关。数据量通常是指同一个密钥加密的数据总字节数。通过定期轮转密钥，可使每个密钥具有更小的密码分析攻击面，使加密方案整体具有更高的安全性。

- 减少密钥破解的时间窗口

如果在定期轮转密钥的基础上，将旧密钥加密的密文数据用新密钥重新加密，则轮转周期即为一个密钥的破解时间窗口。这意味着恶意者只有在两次轮转事件之间完成破解，才能拿到数据。

### 密钥版本概述

KMS中的用户CMK支持多个密钥版本。每一个密钥版本是一个独立生成的密钥，同一个CMK下的多个密钥版本在密码学上互不相关。

## 对称密钥版本

密钥版本可通过自动轮转策略，由系统自动生成，对称密钥的版本分为主版本和非主版本。

- 一个对称密钥版本包含一个主版本和多个非主版本。密钥创建后KMS会生成初始密钥版本并将其设置为主版本，轮转后会生成一个新的密钥版本，并将新的密钥版本设置为主版本，原版本设置为非主版本；
- 在调用对称密钥进行加解密操作时，KMS默认使用主版本实现；
- 密钥轮转产生新的主版本后，KMS不会删除或禁用非主版本，它们需要被用作解密数据。

## 非对称密钥版本

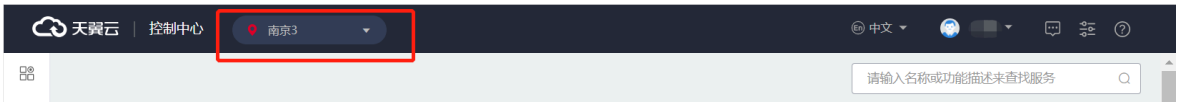
非对称密钥不支持自动轮转，需人工创建新的密钥版本，版本创建后立即生效。

- 非对称的用于主密钥没有主版本（PrimaryKeyVersion）的概念，因此使用非对称密码运算的接口除需指定用户主密钥标志符（或别名）之外，还需指定密钥版本。

### 操作步骤

## 设置自动轮转（对称密钥）

1. 登录密钥管理服务控制台。
2. 在页面最上方的导航栏的资源池下拉列表，选择密钥所在的区域；



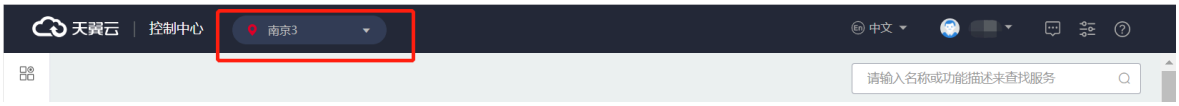

3. 在左侧导航栏，单击密钥管理服务，进入密钥列表；
4. 定位待设置的对称密钥，点击密钥ID，进入密钥详情页；
5. 在密钥版本区域，点击设置轮转策略；


6. 在设置轮转策略对话框，选择轮转周期，30天、90天、180天，或自定义天数；


7. 设置了自动轮转策略后，将显示密钥下次轮转时间。点击确定完成设置；


## 创建密钥版本（非对称密钥）

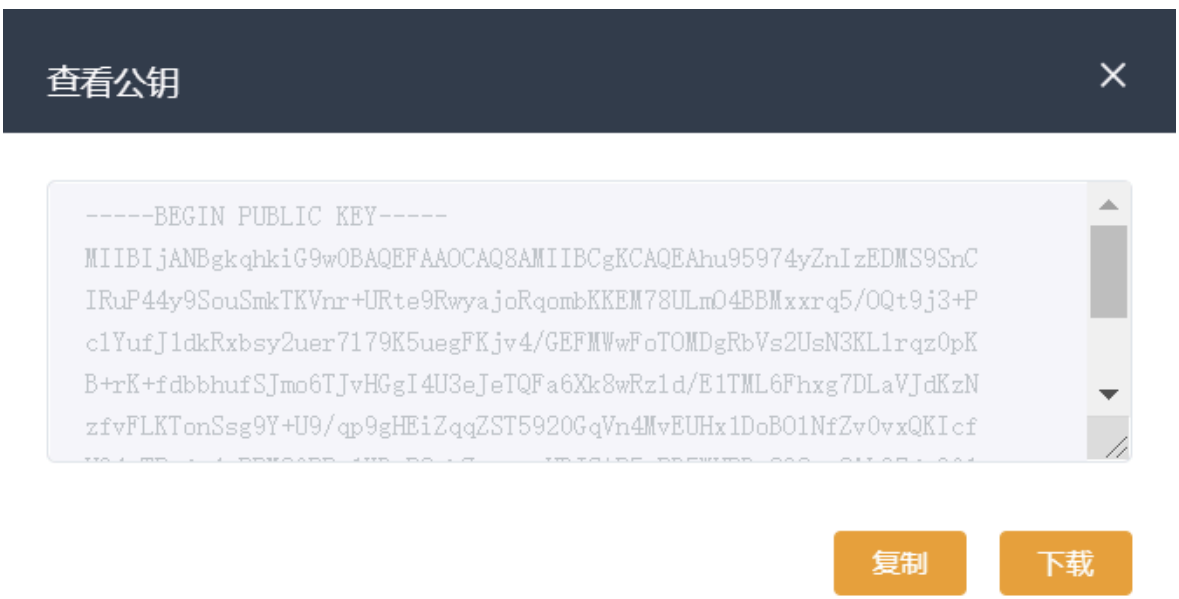
1. 登录密钥管理服务控制台；
2. 在页面最上方的导航栏的资源池下拉列表，选择密钥所在的区域；




3. 在左侧导航栏，单击密钥管理服务，进入密钥列表；
4. 定位待设置的非对称密钥，点击密钥ID，进入密钥详情页；
5. 在密钥版本区域，点击创建密钥版本；


6. 在弹出的对话框内，点击确定；


7. 在密钥版本列表，可查看密钥版本ID、创建日期。点击查看公钥，在弹出的对话框，可复制或下载公钥。



# 常见问题

## 计费类

### 密钥管理服务的计费方式是什么？

KMS产品当前支持包周期版本及按需版本，对应两种计费模式：

- 包年/包月计费：一种预付费模式，即先付费再使用。您可根据业务需要，选择合适的包周期服务版本（基础版、企业版），一次性支付一个月/多个月/一年/多年的费用，支付成功后，KMS服务资源将被系统分配给用户使用，直到超过保留期后被系统回收。
- 按使用量计费：一种后付费模式，即先使用再付费。在结算时会按照您在按需版本中，实际资源使用量收取费用，如密钥数量、API调用量等。

#### 密钥管理服务的计费项是什么？

KMS包周期版服务的计费项包括基础版、企业版。

- 基础版提供软件保护等级服务，支持客户构建专属的密钥库，具备高度可扩展性；同时提供极简的密码运算接口能力，满足应用的安全快速集成。
- 企业版提供硬件保护等级服务，底层对接使用经国家密码管理局认证的密码机硬件，提供更高安全与合规等级保证的资源管理及密码运算服务，满足监管机构的检测认证要求。

KMS按需版服务的计费项包括密钥托管费、API调用费。

- 密钥托管费：密钥创建后托管在KMS服务产生的费用，按照密钥类型、密钥个数以天为周期进行计费。
- API调用费：密钥创建后通过接口调用产生的请求费用，按照API请求次数计费，每个账户每月有20000次的免费请求次数，超过20000次后开始计费。

具体的计费项详情请参考计费项。

#### 密钥管理服务有关密钥管理的接口调用，是否算在API调用费中进行计费？

当您正在使用密钥管理按需版服务，对于API接口调用所产生的费用，计算规则如下：

密钥管理相关接口调用产生的调用次数不计费。

密钥管理服务中API调用计费项，只统计密码运算类接口的调用次数并计费。

#### 服务因欠费或到期后，密钥是否还能进行解密？

不可以。用户欠费或服务到期后，KMS会冻结服务，所有对于KMS的访问均被限制，对密钥解密接口同样无法实现调用。

因此，为避免您的业务因无法解密造成影响，请及时进行充值及续费，确保KMS服务可用。

## 操作类

### 如何使用密钥实现数据加解密？

KMS提供了REST（Representational State Transfer）风格API，支持通过HTTPS请求调用。用户可使用提供的API实现加解密运算等操作。下面以使用用户主密钥进行数据加解密为例介绍实现过程：

加密流程（以加密证书为例）：

1.通过KMS控制台或者调用CreateKey接口，创建一个用户主密钥（CMK）；

2.调用KMS服务的Encrypt接口，将明文证书加密为密文证书；

3.将密文证书部署在服务器上；

4.当服务器启动需要使用证书时，调用KMS服务的Decrypt接口将密文证书解密为明文证书。

### 如何导入外部自带密钥？

创建密钥后，首先进入密钥详情页获取导入主密钥材料的参数，参数包括加密公钥及导入令牌，用户使用获取到的公钥加密自带密钥材料，然后在控制台密钥详情页，根据页面提示上传自带密钥材料即可。

从KMS获取到的导入令牌与加密密钥材料的公钥具有绑定关系，一个令牌只能为其生成时指定的主密钥导入密钥材料。导入令牌的有效期为24小时，在有效期内可以重复使用，失效以后需要获取新的导入令牌和加密公钥。

### 如何删除密钥？

KMS不支持立即删除，仅支持计划删除，即用户需设置预删除周期（自定义7~30天），系统会在到期时自动删除密钥，预删除期间密钥仍托管至系统中，但无法被调用实现加解密等相关功能。

设置密钥计划删除后，密钥将不再产生费用。若您在预删除期间发现密钥仍需继续使用，则可以选择取消计划删除，使密钥重新变为可用。

### 为什么KMS不支持立即删除密钥？

由于密钥删除后不可恢复，一旦删除密钥，所有使用该密钥加密的数据均无法解密，因此删除密钥的操作需要非常谨慎，KMS通过计划删除的机制，即执行计划删除操作后，密钥状态变为待删除，密钥不会立即删除，系统会根据用户设置的预删除周期推迟删除密钥。到达执行时间点，系统才会真正删除密钥，在此之前用户均可以取消删除计划。KMS通过这种方式来减少用户误操作所带来的损失。

处于待删除状态的密钥不可用，无法用于加解密、产生数据密钥等。

如果您不再使用密钥，推荐您先禁用密钥，确保不影响您的业务后再通过计划删除密钥来进行删除。为避免误删，您可以开启删除保护功能。

### KMS是否支持国密算法？

支持。KMS支持创建SM2、SM4类型的密钥，适用于数据加解密、签名验签等场景。

| 密码算法大类 | 密码算法子类 | 保护级别 | 是否支持加解密 | 是否支持签名验签 |
| --- | --- | --- | --- | --- |
| 对称密钥 | AES_256 | Software<br>HSM | 支持 | 不支持 |
| | SM4 | HSM | 支持 | 不支持 |
| 非对称密钥 | RSA_2048 | Software<br>HSM | 支持 | 支持 |
| | SM2 | HSM | 支持 | 支持 |

### 软件保护级别和硬件保护级别的区别是什么？

软件保护级别的密钥通过软件模块进行保护，其根密钥通过公钥加密形成密文存储在软件文件系统中；而用于解密根密钥密文的私钥，通过对称加密形成密文存储在文件系统中的不同位置；同时对称密钥也存储在不同位置，进而增加系统根密钥的安全性；

硬件保护级别的密钥通过专用硬件保护密钥，硬件根密钥需要存储密码机的内部密钥索引，通过索引确认根密钥；所有涉及根密钥使用的过程均在密码机内部完成，包括加密解密等。

**密钥自动轮转周期的可设置范围是什么？**

对称密钥支持设置自动轮转周期，周期最短为7天，最长为730天（2年）。

对称密钥支持设置自动轮转，系统根据自动轮转周期自动生成新的密钥版本，并将最新的版本设置为主版本，原密钥版本作为非主版本保存在KMS中，KMS不会删除或禁用非主版本，它们需要被用作解密数据。

**非对称密钥是否支持自动轮转？**

非对称密钥不支持设置自动轮转，可以手动创建新的版本。

由于公私钥使用场景的特殊性，KMS不支持对非对称的用户主密钥进行自动轮转。可在指定用户主密钥中人工创建新的密钥版本，生成全新的一对公钥和私钥。

除此之外，和对称类型的用户主密钥不同，非对称的用于主密钥没有主版本（PrimaryKeyVersion）的概念，因此使用非对称密码运算的接口除需指定用户主密钥标志符（或别名）之外，还需指定密钥版本。

**什么情况下需要导入外部密钥？**

当用户拥有自己的密钥材料，需要继续使用该密钥材料实现数据加解密，比如用户需要将本地加密数据迁移到云上时，云上云下共用同一个密钥材料，此时可以将密钥材料导入至KMS中进行托管，便于后续使用。

当您选择密钥材料来源为外部，使用您自己导入的密钥材料时，需要注意以下几点：

- 请确保您使用了符合安全要求的随机源生成密钥材料；
- 在使用导入密钥时，需要对自己密钥材料的可靠性负责；
- 请保存密钥材料的原始备份，以便在意外删除密钥材料时，能及时将备份的密钥材料重新导入KMS。

**什么类型的密钥支持导入外部密钥材料？**

当前AES_256类型的对称密钥，支持导入外部密钥材料。

您可通过控制台创建密钥，选择AES_256类型的对称密钥后，密钥材料来源选项选择 **外部** ，并勾选“我了解使用外部密钥材料的方法和意义”，点击确定即可完成密钥创建；

密钥创建成功后，您需要进入密钥详情页，进行密钥材料导入操作。导入密钥材料前需要先获取导入材料参数，包括加密公钥、导入令牌，具体操作步骤可参考用户指南中的相关章节。

**外部导入的密钥材料是否支持自动轮转？**

不支持。外部导入的密钥材料不支持自动轮转，无密钥版本概念。

导入密钥材料时，可以设置可以设置密钥材料过期时间，密钥材料过期后，KMS将自动删除密钥材料，但该主密钥及其元数据仍然保留。

外部导入的密钥材料支持手动删除，但该主密钥及其元数据仍然保留。

**当密钥材料被误删或已经过期导致密钥不可用，如何处理使密钥恢复可用？**

密钥材料被删除或过期时，可以再次导入相同的密钥材料，成功后密钥将恢复可用。您需要自行备份密钥材料，以便密钥材料失效或误删除时进行重新导入。

用户主密钥CMK与密钥材料具有关联性，当您将密钥材料导入某个CMK时，该CMK与该密钥材料永久关联，不能将其他密钥材料导入该CMK中，即便密钥材料已经过期或者被删除。

**当用户主密钥的密钥材料删除或过期后，是否可以导入其他的密钥材料到该主密钥中？**

不可以。用户主密钥包含密钥元数据（密钥ID、密钥别名、描述、密钥状态与创建日期）和用于加解密数据的密钥材料。

将密钥材料成功导入主密钥后，该主密钥与密钥材料永久关联，不能再将其他密钥材料导入该主密钥中。

**具备相同密钥材料的不同用户主密钥，是否可以相互加解密数据？**

不可以。用户主密钥包含密钥元数据（密钥ID、密钥别名、描述、密钥状态与创建日期）和用于加解密数据的密钥材料。

用户主密钥具有唯一性，使用主密钥加密的数据，只能用相同的主密钥解密。即使其他主密钥具有相同的密钥材料，也无法解密该主密钥加密的数据。

**用户主密钥别名的作用是什么？**

为密钥创建别名方便用户管理密钥，一个别名对应唯一的用户主密钥。在通过openAPI调用KMS服务接口时，参数中的密钥ID可以用别名代替。

别名必须依附于用户主密钥存在，其特点如下：

- 一个用户主密钥下可以绑定多个别名，删除别名不会删除其关联的用户主密钥。
- 别名不可修改。您可以通过为一个用户主密钥创建新的别名，并且删除旧的别名来达到修改主密钥别名的目的。
- 可以调用UpdateAlias接口更改别名绑定的用户主密钥，而不会影响用户主密钥。
- 默认主密钥的别名不能删除和添加。

**用户主密钥与别名的对应关系是什么？**

别名作为用户主密钥的可选标识，必须与密钥关联。同一个账户在一个地域中的别名具有唯一性。

一个用户主密钥可以绑定多个别名，同一个别名只能指向唯一的用户主密钥。

默认主密钥的别名不支持删除、更改。

**别名支持修改吗？**

别名不支持直接修改，您可以通过创建新的别名，并删除旧的别名来达到修改别名的目的。

为密钥创建新的别名时，不会影响已有的其他别名。删除旧的别名前，请确保该别名已不再使用，否则可能会导致数据加密失败。

默认主密钥的别名不支持删除和添加。

**删除别名是否会影响用户主密钥的使用？**

别名是用户主密钥的可选标识，支持删除别名，删除别名不会删除其关联的用户主密钥。

创建别名的作用是可以在调用API接口时，使用别名来代替密钥ID。因此删除如果仍在使用别名作为api调用参数时，删除别名会导致服务调用失败，请确保预删除的别名已不再使用。

**同一资源池内的用户主密钥，是否可以设置相同的别名？**

不可以。同一个账户在同一个地域中的别名具有唯一性，每个别名只能指向同地域的一个用户主密钥，但是每个用户主密钥可以绑定多个别名。

相同的别名可以绑定不同资源池内的用户主密钥。

### 为用户主密钥设置自动轮转的目的是什么？

KMS提供密钥轮转功能，支持通过密钥版本化和定期轮转来加强密钥使用的安全性，有效提升业务数据的安全性。

通过密钥轮转，可以减少每个密钥版本加密的数据量，降低没密码分析攻击风险；

密钥轮转可以减小破解密钥的时间窗口。应对密码分析攻击风险的有效实践是在定期轮转密钥的基础上，将旧密钥加密的密文数据使用新版本的密钥重新加密，这意味着如果想要破解密码拿到明文数据，需要在密钥轮转周期内完成密码破解。密钥轮转周期即为密钥破解时间窗口，该窗口越小，破解难度越大。

### 密钥经过轮转产生新的密钥版本后，是否会影响旧数据的解密？

不影响。密钥轮转产生新的版本后，加密数据时将使用新的版本；同时旧版本不会删除或禁用，在解密旧数据时，需要使用旧版本密钥完成。

对称密钥版本分为主版本和非主版本。主版本是CMK的活跃加密密钥（Active Encryption Key）。每个CMK在任何时间点上有且仅有一个主版本。调用GenerateDataKey、Encrypt等加密API接口时，KMS使用指定CMK的主版本对明文进行加密。非主版本是CMK的非活跃加密密钥（Inactive Encryption Key）。每个CMK可以有零到多个非主版本。非主版本历史上曾经是主版本，在当时被用作活跃加密密钥。密钥轮转产生新的主版本后，KMS不会删除或禁用非主版本，它们需要被用作解密数据。

### 使用密钥进行加密数据时，是否需要指定密钥版本？

使用密钥加密是否需要指定密钥版本与密钥类型有关。

调用对称密钥加密数据时，不需要指定密钥版本，系统会默认使用最新的主版本进行数据加密。

调用非对称密钥加密数据时，除了要指定主密钥外，还需要指定密钥版本。

# 管理类

## 是否可以导出用户主密钥？

不可以。为确保用户主密钥的安全，用户只能在KMS中创建，并通过API接口调用实现加密等操作，无法导出用户主密钥。

创建密钥时，若您选择密钥材料来源于天翼云，则KMS系统会自动为用户主密钥生成密钥材料，且密钥材料无法单独删除、不可导出，仅支持随用户主密钥一并删除；

创建密钥时，若您选择密钥材料来源于外部，则支持手动删除密钥材料。

### 哪些云服务支持密钥管理系统加密数据？

KMS服务无缝对接云硬盘、对象存储和弹性文件、数据库产品，提供服务端加密能力。您只需要在创建云硬盘时，勾选“加密”功能，则可一键开启硬盘加密功能，加密过程透明无感知。

产品底层通过信封加密的方式，实现云产品中数据的加密。

### 用户自建主密钥与默认主密钥有何区别？

用户主密钥：是用户通过控制台或 API 来创建的用户主密钥。您可以对用户密钥进行创建/设置别名/上传自带密钥材料/启用/禁用/轮转/版本管理/删除等操作。用户主密钥按照标准资费进行计费。

默认主密钥：是用户首次通过云服务调用KMS实现加密时，由系统自动生成的主密钥，别名以云产品命名，如“alias/ecs”。不支持禁用/删除/轮转/上传自带密钥材料等操作。默认主密钥免费提供密钥管理服务，API调用费与用户主密钥一同统计收费。

**如果用户主密钥被禁用/删除，用户数据是否还可以解密？**

不可以。被禁用的密钥无法用于加密和解密。若想继续使用密钥解密，则需将密钥变为启用中。

若用户主密钥被彻底删除，KMS将不再保留任何该密钥的数据，使用该密钥加密的数据将无法解密；

因此密钥管理不支持立即删除操作，仅支持计划删除，在用户设置的计划删除的期限到达时删除密钥，用户可以通过KMS界面取消计划删除用户主密钥。

若用户主密钥是通过KMS导入的密钥，且仅删除了密钥材料，则可以将本地备份的密钥材料再次导入原来的空密钥，回收用户数据。若密钥材料没有在本地备份，则无法回收用户数据。

**用户最多可以创建多少个主密钥？**

对于对称密钥，暂不限制创建个数。对于非对称密钥，目前限制密钥的版本数量，即同一用户在同一资源池最多创建50个版本。