密钥管理

用户使用指南

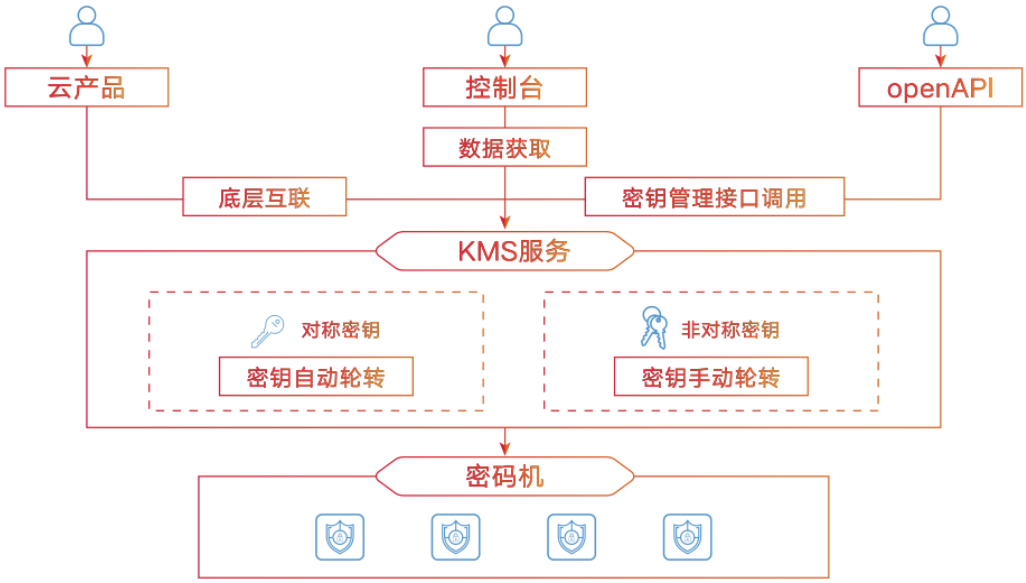
天翼云科技有限公司

目 录

1. 产品简介

1.1. 产品定义

密钥管理服务（Key Management Service，KMS）提供密钥全生命周期管理，用户可轻松创建并管理密钥，满足数据加解密及数字签名验签等需求。同时与天翼云云硬盘、对象存储、弹性文件等云产品无缝集成，实现云上资源原生数据的加密保护。



1.2. 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、集中托管、广泛集成以及稳定可靠等优势。

安全合规

- 通过国家密码管理局安全性审查，符合 GM/T 0051《密码设备管理 对称密钥管理技术规范》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

- 提供密码基础设施的完全托管，用户无需投入密码基础设施及运维资源。
- 轻松实现密钥全生命周期管理，集中控制密钥策略。

广泛集成

- 与云硬盘、对象存储、弹性文件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。
- 通过集成的密钥管理服务可实现一键加密，无需额外的复杂配置。

稳定可靠

- 采用分布式部署，构建多地域冗余的密码计算能力，保证服务可靠性。
- 对外提供极简的 API 接口实现服务调用，确保服务高可用性。

1.3. 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、弹性文件产品中的原生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。

云产品集成的加密服务支持通过默认主密钥或用户主密钥进行数据加密，用户可根据数据保护需求，选择不同的密钥类型用于云产品的加密。

1.4. 相关术语解释

- **对称密钥加密**：又称单密钥加密，即采用一个密钥进行信息的加密和解密。
- **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，而私钥必须被安全的保护起来，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 API CreateKey 创建一个用户主密钥。
- **默认主密钥（Default CMK）**：用户第一次使用云产品服务端加密功能时，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 API GenerateDataKey 或 GenerateDataKeyWithoutPlaintext 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，由用户主密钥 CMK 加密生成。
- **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。

1.5. 应用场景

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

场景一：敏感数据加密

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。

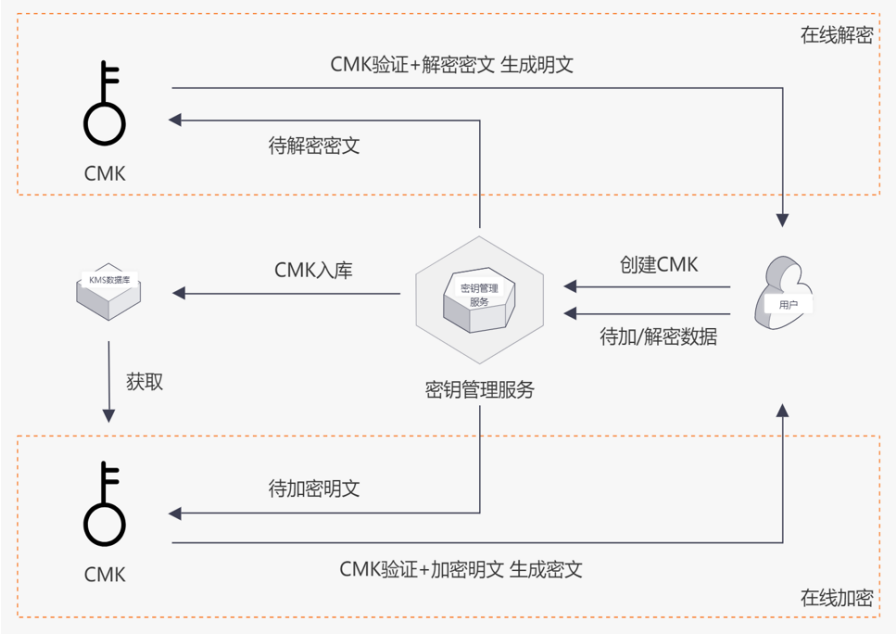
场景特点

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



场景二：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。

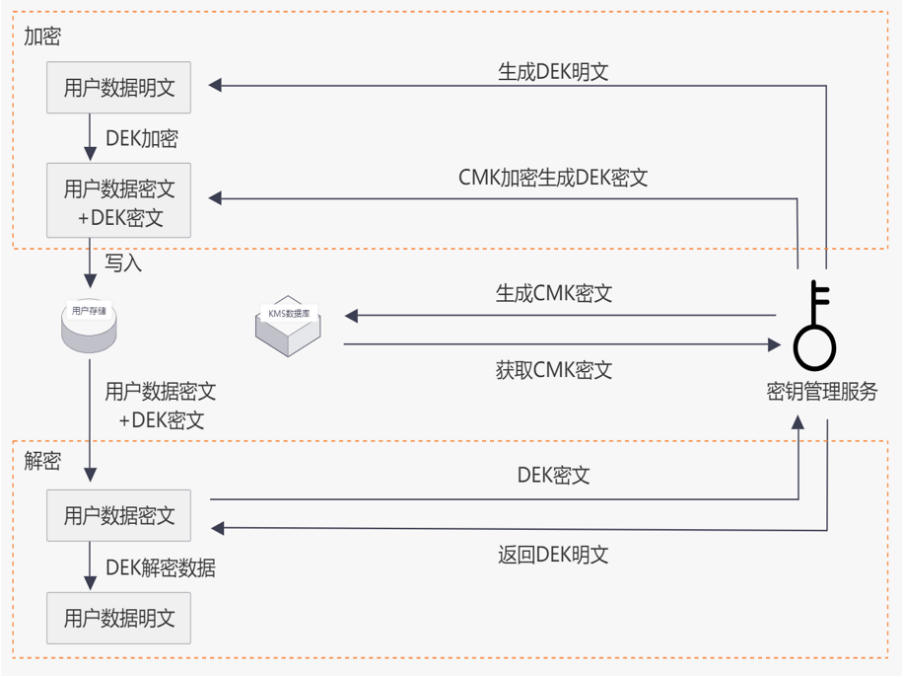
场景特点

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



场景三：签名验签

通过密钥管理服务（KMS）创建非对称密钥，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。

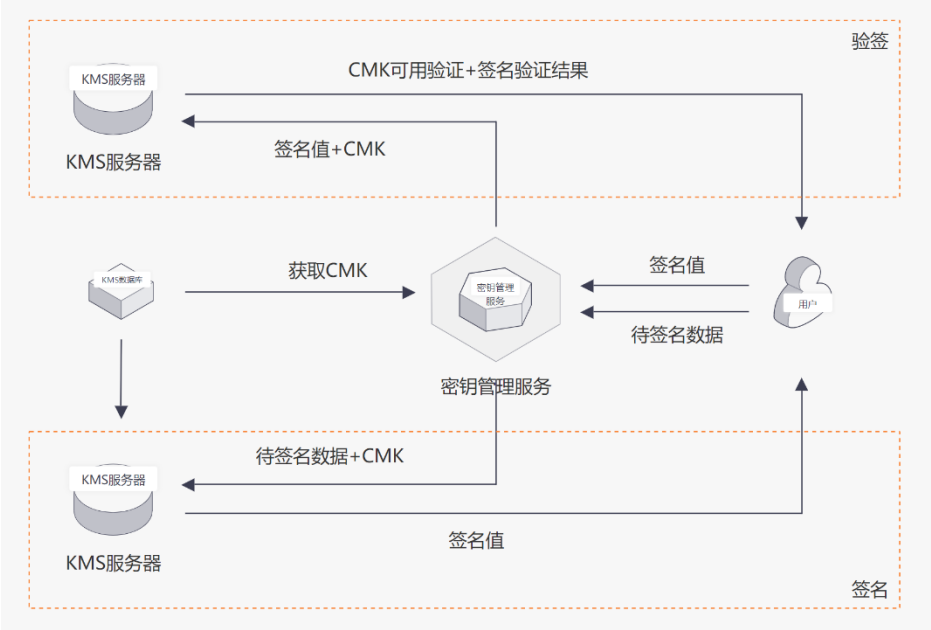
场景特点

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



1.6. 产品规格

密钥管理服务（KMS）支持创建对称、非对称类型的用户主密钥，并支持软件及硬件两种保护级别。针对不同的业务场景，可选择创建不同类型的密钥。

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/HSM	支持	不支持
	SM4	HSM	支持	不支持
非对称密钥	RSA_2048	Software/HSM	支持	支持
	SM2	HSM	支持	支持

在使用云产品集成的加密服务时，用户可选择默认主密钥实现云上数据的加密。默认主密钥由系统自动创建，并与云产品对应，密钥类型默认为 AES_256。

1.7. 使用限制

密钥管理服务（KMS）是一个区域化的服务，在不同区域资源池的使用限制相对独立。

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。

1.8. 与其他云服务关系

密钥管理服务（KMS）与云硬盘、对象存储、弹性文件服务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。

云产品集成的加密服务支持通过默认主密钥和用户主密钥进行数据加密，用户可根据数据保护需求，选择不同的密钥类型用于云产品的加密。

- **默认主密钥**

  在首次使用云产品加密时，系统为云产品自动创建的用于服务端加密的默认密钥，默认主密钥与云产品对应，默认定义别名为 alias_<云产品代码>，例如 alias_ecs。默认主密钥不产生密钥托管费用，同时默认主密钥不支持上传密钥材料、轮转、禁用、删除等操作。

- **用户主密钥**

  用户通过密钥管理服务自行创建的主密钥，您可以选择使用 KMS 生成的密钥材料，也可以导入自带密钥材料（BYOK）。使用用户主密钥，将产生密钥托管费用，可通过密钥管理服务对密钥进行轮转、禁用、删除等操作。

1.9. 资源节点

当前密钥管理服务已开放的区域节点如下表。

现已支持的资源池（44 个）		
西安 5	晋中	西安 4
内蒙 6	海口 2	武汉 4
南京 3	成都 4	昆明 2
北京 5	中卫 2	广州 6
贵州 3	西宁 2	南宁 2
华东 1	杭州 2	武汉 41
上海 36	芜湖 2	长沙 42
合肥 2	拉萨 3	长沙 3
乌鲁木齐 4	福州 3	南京 2
厦门 3	重庆 2	南京 5
福州 4	西安 3	福州 25
佛山 3	雄安 2	南宁 23

兰州 2	郴州 2	华北 2
南京 4	九江	西南 1
上海 7	武汉 3	

2. 快速入门

2.1. 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，请跳转至开通密钥管理服务。

1. 登录天翼云门户 http://www.ctyun.cn，点击**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。

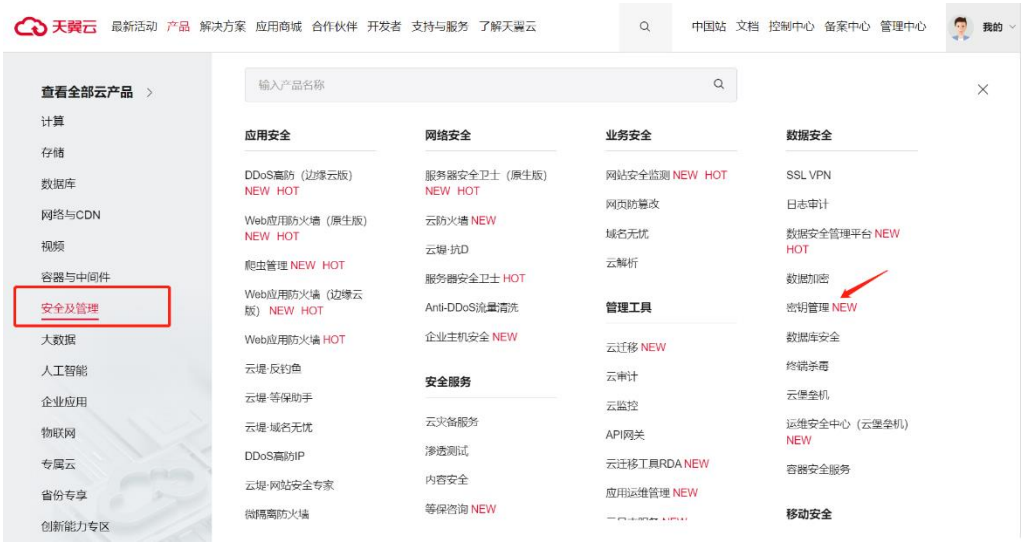
2.2. 开通密钥管理服务

以下为密钥管理服务（KMS）的购买流程。

当您具备已通过实名认证的 ctyun 账号后，可以通过以下两种方式开通密钥管理服务（KMS）。

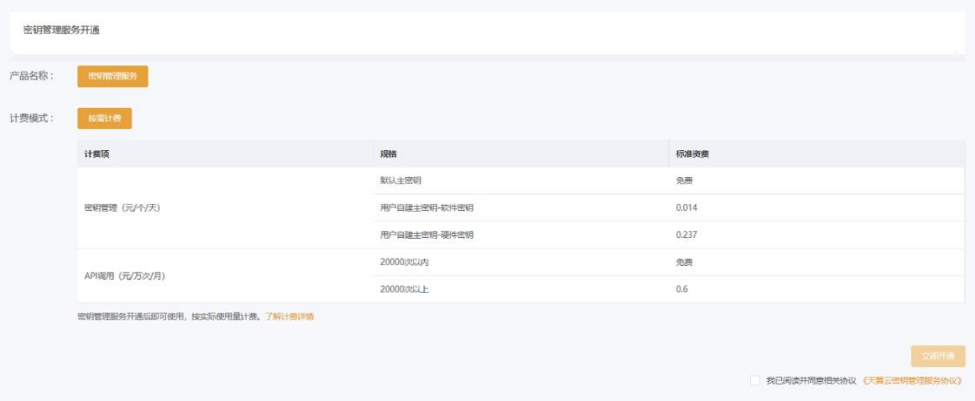
通过产品详情页进入并开通服务

1. 通过产品导航栏，定位到安全分类，找到密钥管理，点击进入；



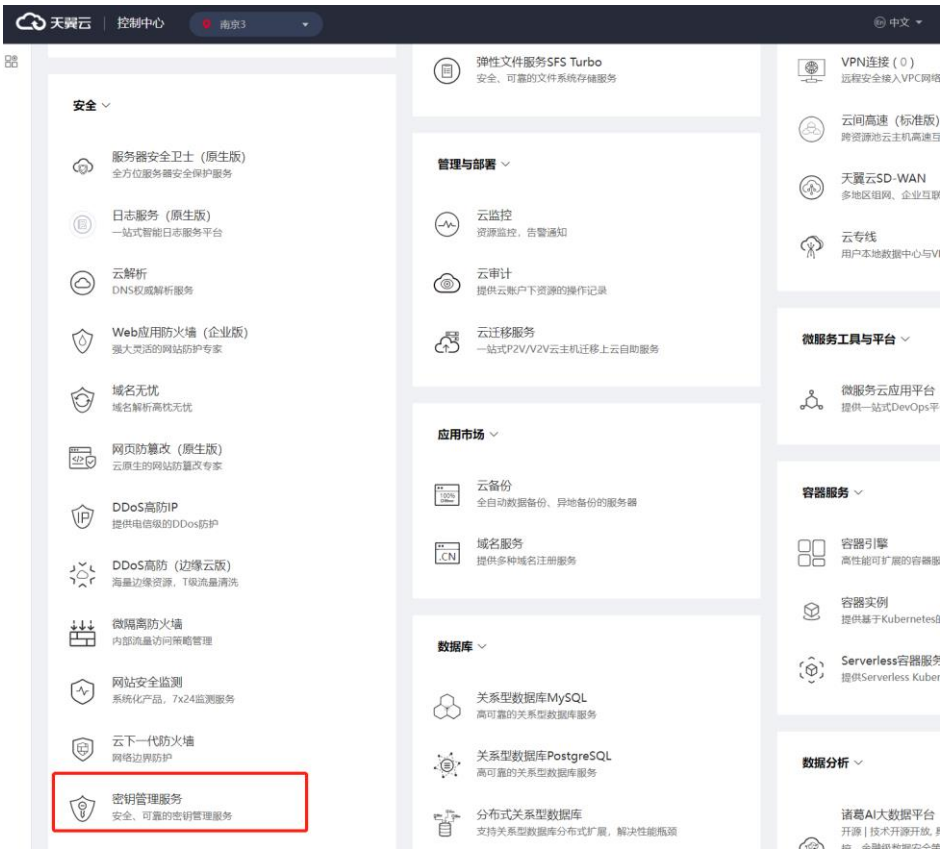
2. 进入密钥管理服务 KMS 产品详情页，单击**立即开通**；

3. 进入到密钥管理服务购买页面，勾选“我已阅读，理解并接受《天翼云密钥管理服务协议》”，点击**立即开通**按钮。即可开通服务。



通过控制台页面进入并开通服务。

1. 进入控制台页面，选择对应资源池，找到密钥管理服务，点击后进入服务开通页面，勾选“我已阅读，理解并接受《天翼云密钥管理服务协议》”，点击**立即开通**按钮。即可开通服务。

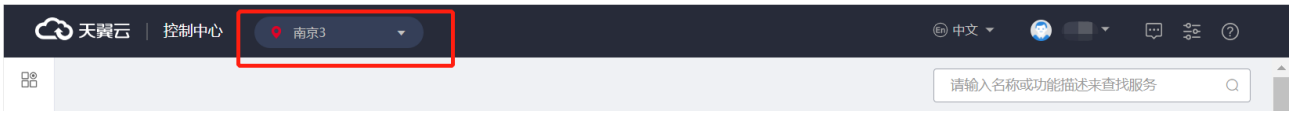


2.3. 创建用户主密钥

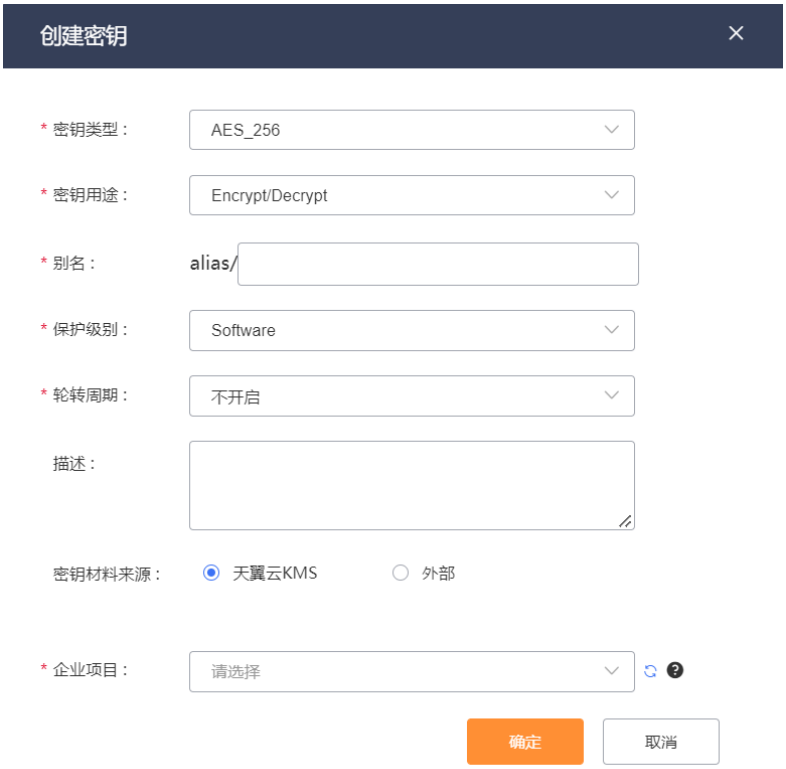
开通密钥管理服务后，您可以在控制台轻松地创建密钥，以便后续使用密钥加解密自己地数据。

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，选择密钥所在的区域；



3. 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	取值： 对称密钥类型： • AES_256 • Ctyun_SM4 非对称密钥类型： • RSA_2048 • Ctyun_SM2
密钥用途	取值： • Encrypt/Decrypt：数据加密和解密 • Sign/Verify：产生和验证数字签名 说明：对称密钥不支持 Sign/Verify 用途。

配置项	说明
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	取值： • Software：通过软件模块对密钥进行保护。 • 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	密钥的描述信息。
轮转周期	自动轮转的时间周期。取值： • 不开启：不开启轮转 • 30 天 • 90 天 • 180 天 • 自定义：7~730 天 **说明**：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	取值： • 天翼云 KMS：密钥材料将由 KMS 生成。 • 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。 **说明**：仅对称密钥的 AES_256 支持设置导入密钥材料。
企业项目	选择密钥归属的企业项目。默认为 default。

4. 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。

3. 用户指南

3.1. 密钥管理服务概述

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 • HSM	支持	不支持
	SM4	• HSM	支持	不支持
非对称密钥	RSA_2048	• Software • 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，请参见对称加密概述。
- 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，请参见非对称加密概述。

密钥管理

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
密钥托管	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。 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。 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 查看密钥详情 启用禁用密钥 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

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

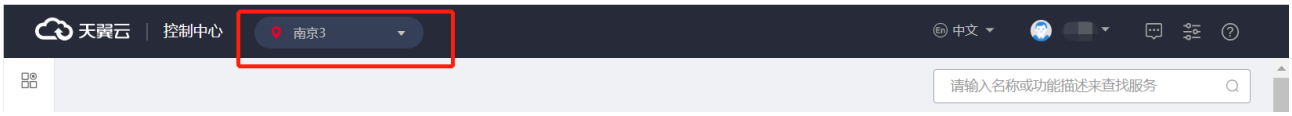
3.2. 密钥管理

3.2.1. 创建密钥

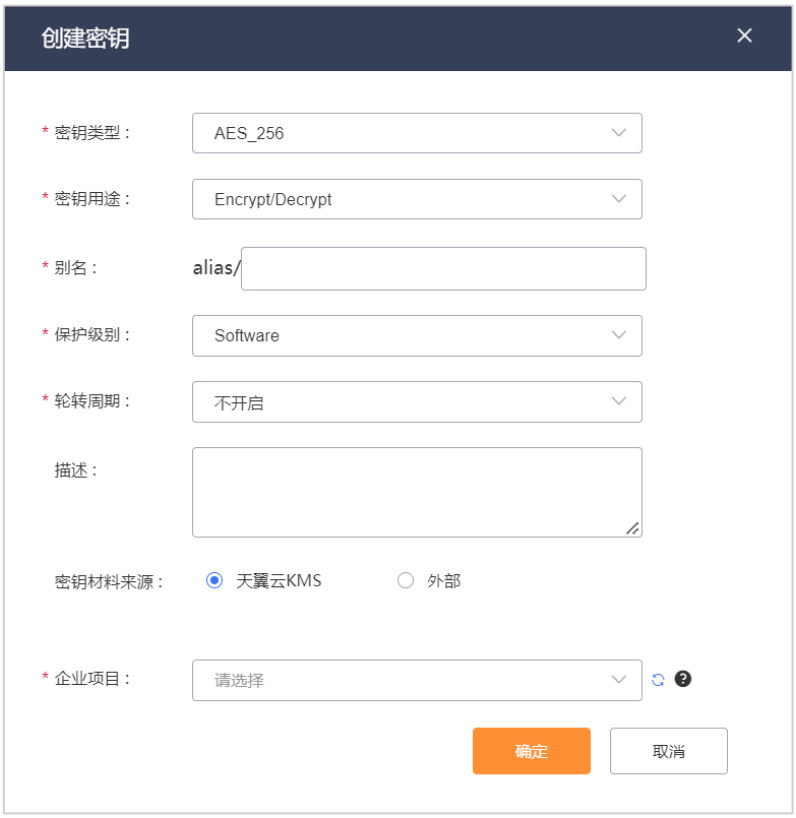
本文为您介绍在控制台创建密钥的操作步骤。

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. 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	取值： 对称密钥类型： • AES_256 • Ctyun_SM4 非对称密钥类型： • RSA_2048 • Ctyun_SM2
密钥用途	取值： • Encrypt/Decrypt：数据加密和解密 • Sign/Verify：产生和验证数字签名 说明：对称密钥不支持 Sign/Verify 用途。

配置项	说明
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	取值： • Software：通过软件模块对密钥进行保护。 • 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。取值： • 不开启：不开启轮转 • 30 天 • 90 天 • 180 天 • 自定义：7~730 天 说明：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	取值： • 天翼云 KMS：密钥材料将由 KMS 生成。 • 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。 说明：仅对称密钥的 AES_256 类型支持设置导入密钥材料。
企业项目	选择密钥归属的企业项目。默认为 default。

4. 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。

3.2.2. 导入密钥材料

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；
- 用户在使用导入密钥时，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。

导入密钥材料的功能特性

- **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。 • 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。

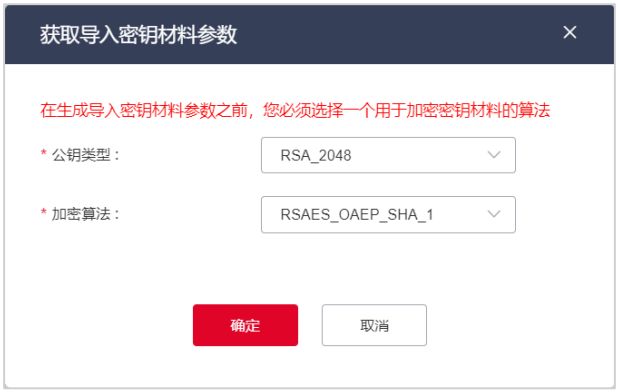
操作步骤-导入密钥材料

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”**；

2. 获取导入密钥材料参数。

1）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**获取导入密钥材料参数**。

2）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： • RSAES_PKCS1_V1_5 • RSAES_OAEP_SHA_1 • RSAES_OAEP_SHA_256

3）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。您可以使用 OPENSSL 通过以下步骤获取加密的密钥材料。

1）创建一个密钥材料，使用 OPENSSL 产生一个随机数。

2）将加密公钥进行 Base64 解码。

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

4）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_SH A_256，RSAES_PKCS1_V1 _5 和 RSAES_OAEP_SH A_1 三种密钥算法。OpenSSL 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。

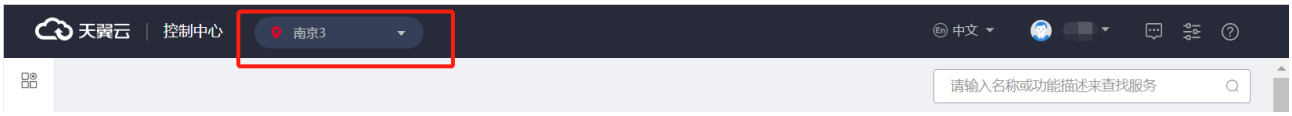
1）在密钥列表，点击**密钥 ID**，进入**密钥详情**，在**密钥材料**区域，单击**导入密钥材料**。

2）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**。

3）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**更多**，进入**密钥详情**，在**密钥材料**区域，单击**删除密钥材料**。

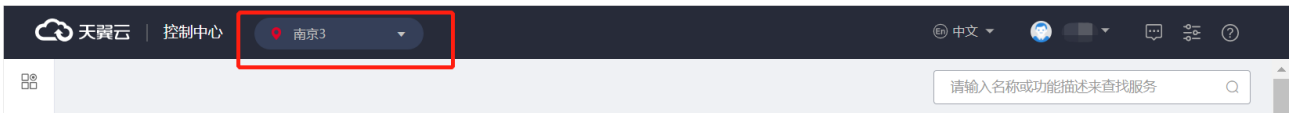
4. 在删除密钥材料对话框，单击**确定**。密钥材料删除成功后，密钥状态从**启用中**更新为**待导入**。

3. 2. 3. 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： • 启用中 • 已禁用 • 待删除 • 待导入
密钥类型	创建密钥时选择的算法类型，包含： 对称密钥： • AES_256 • Ctyun_SM4 非对称密钥： • RSA_2048 • Ctyun_SM2
密钥用途	创建密钥时选择的用途，包含： • Encrypt/Decrypt • 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： • Software • Hsm
创建日期	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/取消计划删除密钥操作。

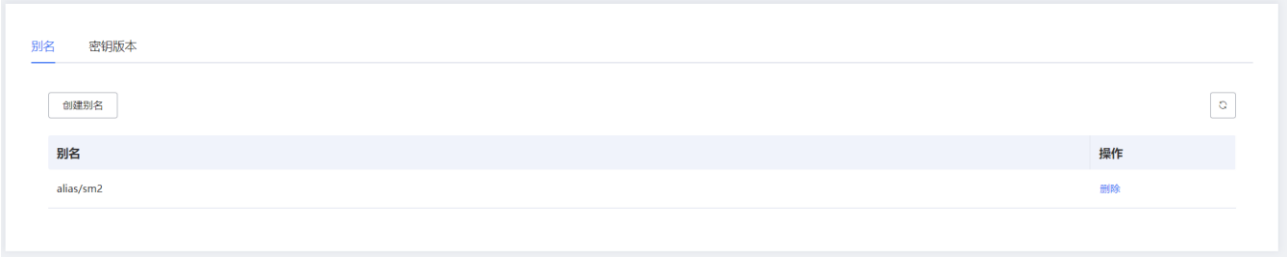
5. 在密钥列表点击密钥 ID，进入密钥详情页。

1）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

参数	说明
密钥类型	创建密钥时选择的算法类型，包含： 对称密钥： • AES_256 • Ctyun_SM4 非对称密钥： • RSA_2048 • Ctyun_SM2
密钥用途	创建密钥时选择的用途，包含： • Encrypt/Decrypt • 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： • 启用中 • 已禁用 • 待删除 • 待导入
保护级别	创建密钥时选择的保护级别，包含： • Software • Hsm
创建日期	创建该密钥的时间。
描述	描述信息，可修改。

2）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；



3）在用户主密钥详情页的**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：

3.2.4. 别名管理

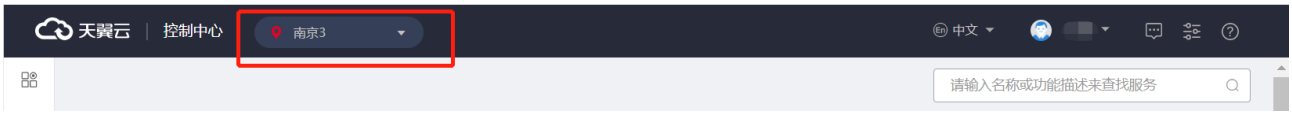
别名是用户主密钥的可选标识，同一个用户在一个地域中的别名具有唯一性。每个别名只能指向同地域的一个用户主密钥，但是每个用户主密钥可以绑定多个别名。

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。

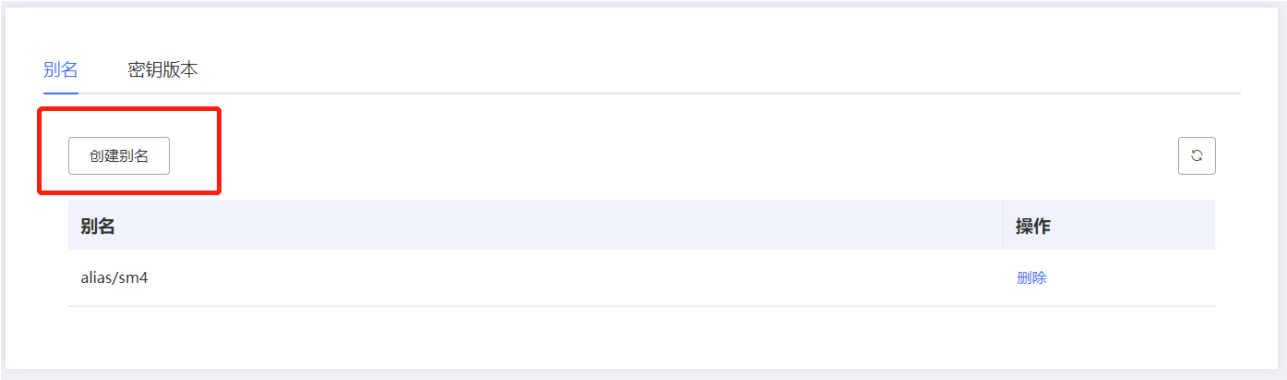
操作步骤-创建别名

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**。

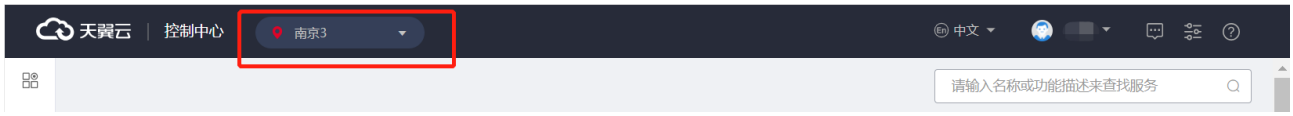
4. 在密钥列表点击**密钥 ID**，进入**密钥详情页**；



5. 在**别名**区域，点击**创建别名**，填写别名，单击**确定**。

操作步骤-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**，单击**确定**。

别名管理相关 API 接口

您可以通过调用别名管理的相关接口，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。

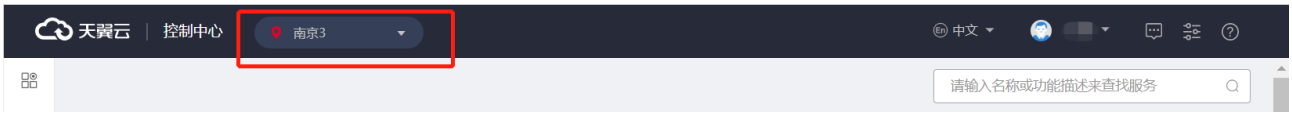
3.2.5. 启用禁用密钥

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。

操作步骤

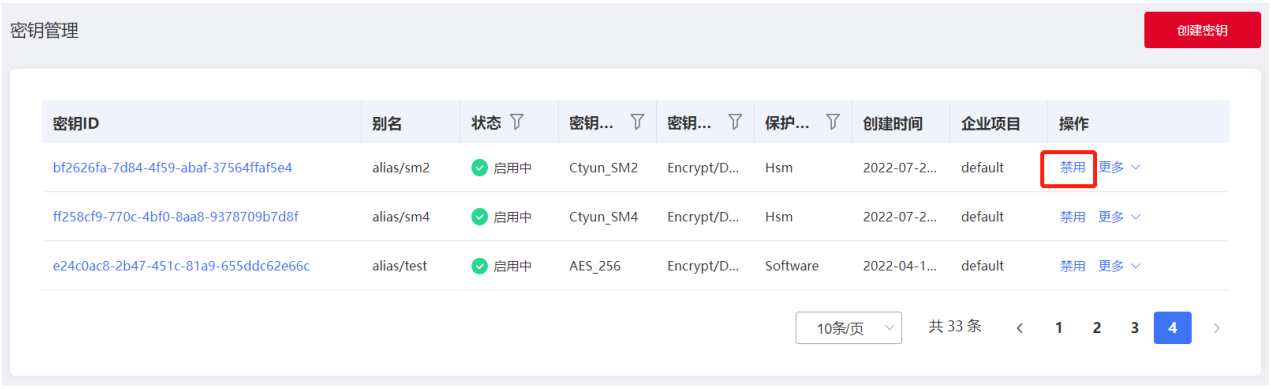
- **禁用**

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**；

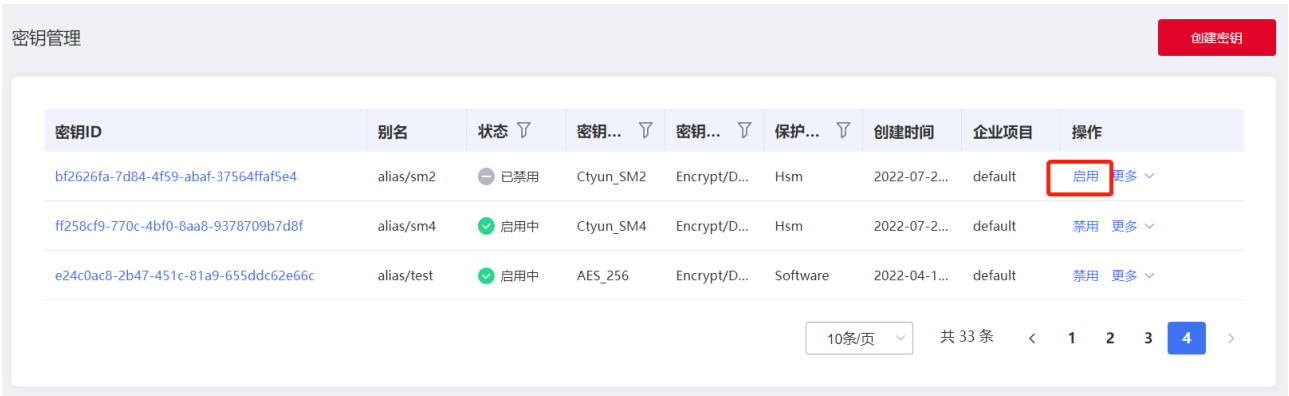
4. 定位待禁用的密钥，单击右侧操作列的**禁用**；



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**。

3.2.6. 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

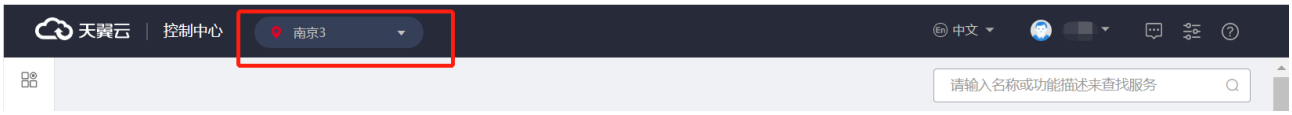
KMS 管理的以下类型的密钥不支持多个版本：

- 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**；

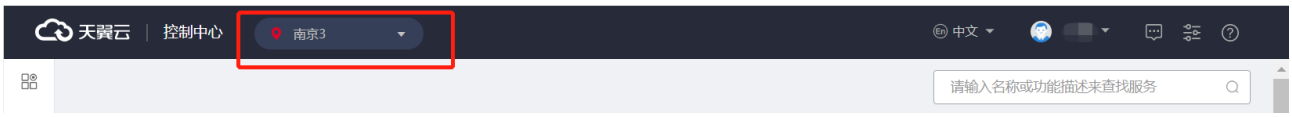
6. 在**设置轮转策略**对话框，选择轮转周期，**30 天**、**90 天**、**180 天**，或**自定义天数**；

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）

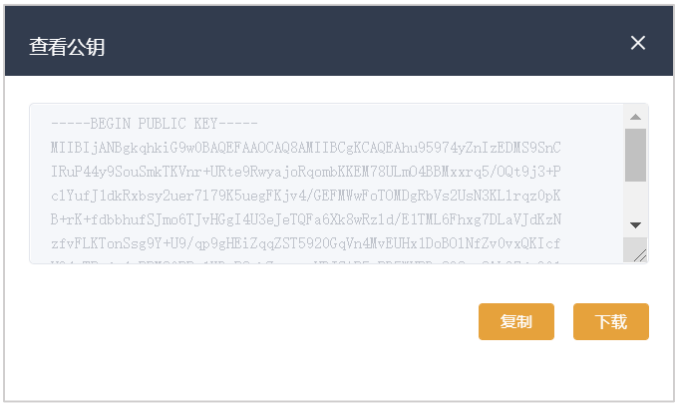
1. 登录密钥管理服务控制台；
2. 在页面最上方的导航栏的资源池下拉列表，选择密钥所在的区域；



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。

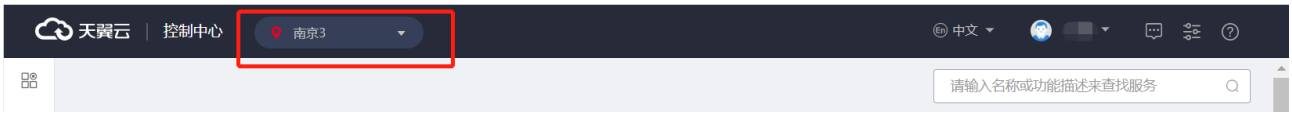


3.2.7. 删除密钥

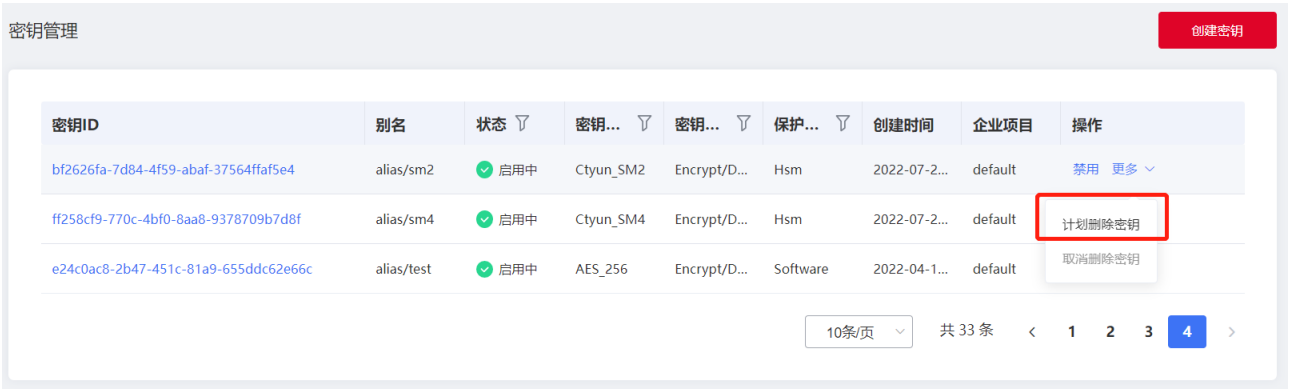
用户主密钥（CMK）一旦删除，将无法恢复，使用该 CMK 加密的内容及产生的数据密钥也将无法解密。因此，对于 CMK 的删除，KMS 只提供计划删除的方式，而不提供直接删除的方式。如果不再使用 CMK，推荐您使用禁用密钥功能。

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；

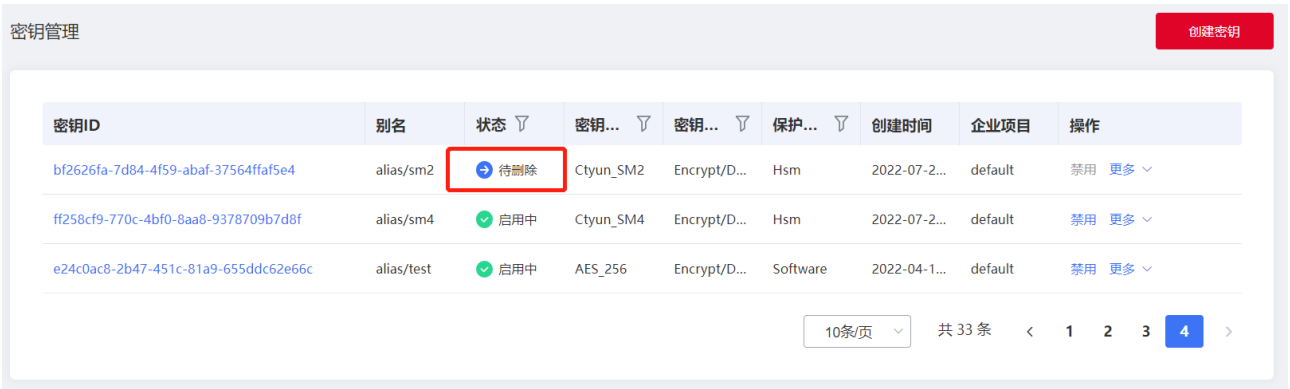


3. 在左侧导航栏，单击**密钥管理服务**，进入**密钥列表**；
4. 定位计划删除的密钥，在右侧操作列选择**更多>计划删除密钥**；

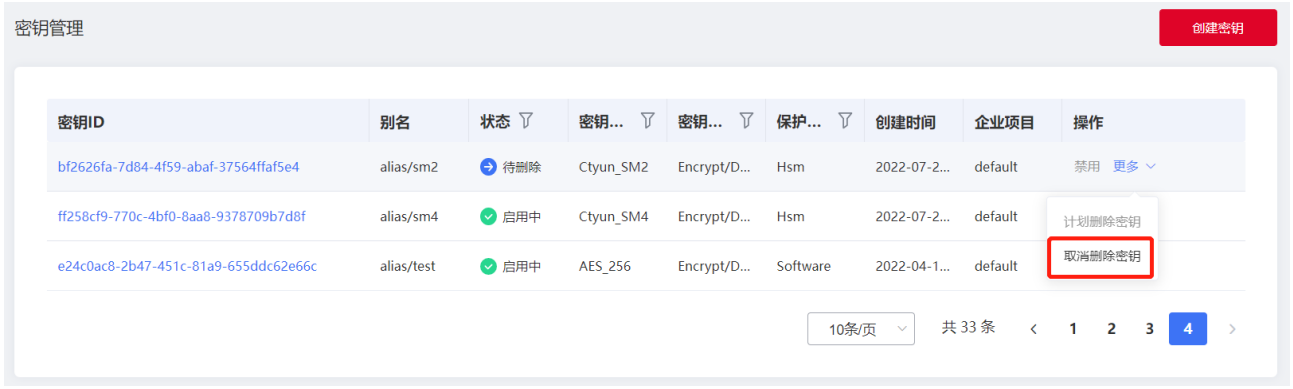


5. 在计划删除密钥对话框，填写预删除周期，点击**确定**。预删除周期可选值为：7~30 天；

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；



7. 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>取消计划删除密钥**，撤销删除密钥的申请；



8. 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。

3.3. 对称密钥运算

3.3.1. 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

算法	密钥长度	密钥规格	保护级别
AES	256 比特	AES_256	• Software • HSM
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。

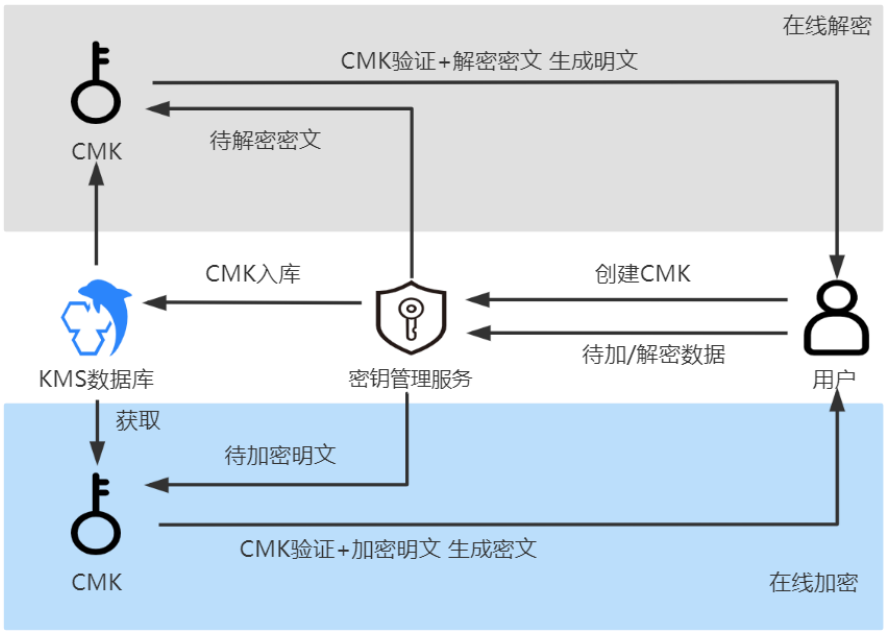
场景	场景描述
在线加密	• 适用于保护小型敏感数据（小于 6KB）的加解密，如密钥、证书、配置文件等。 • 用户的数据会通过安全信道传递到 KMS 服务端，服务端通过指定 CMK 完成加密和解密后，操作结果通过安全信道返回给用户。

场景	场景描述
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。

3.3.2. 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。

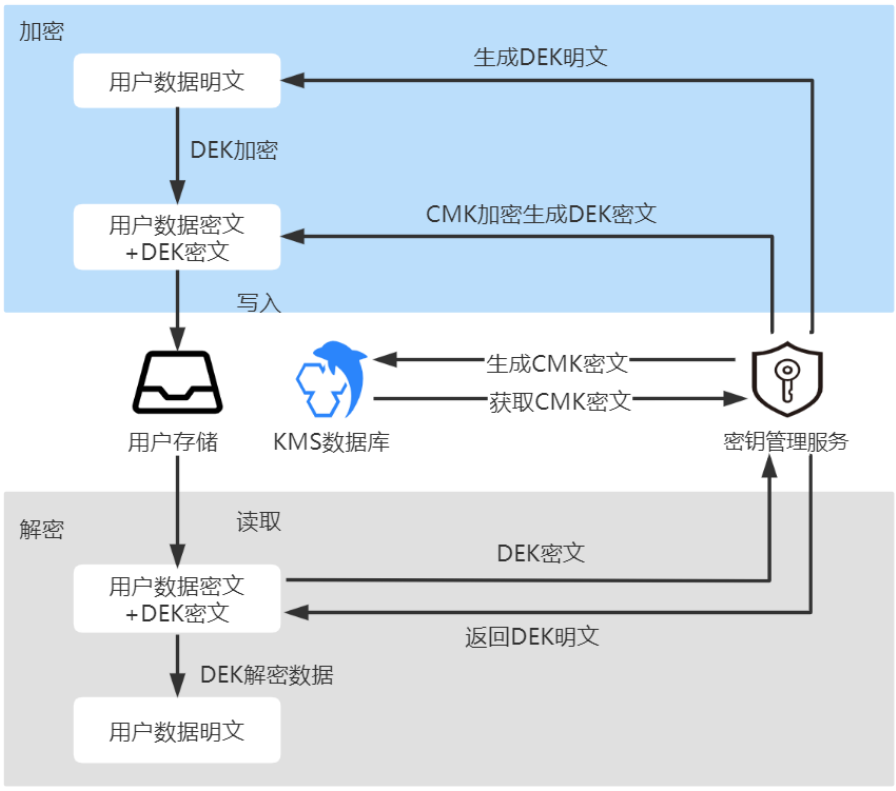
API 名称	说明
createKey	创建用户主密钥（CMK）。
encrypt	指定 CMK，直接输入明文数据，由 KMS 在线加密数据。
decrypt	解密由 encrypt 接口加密的数据，不需要指定 CMK 即可完成在线解密。

3.3.3. 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，将密文数据密钥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

3.4. 非对称密钥运算

3.4.1. 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

算法	密钥规格	保护级别
RSA	RSA_2048	• Software • HSM
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

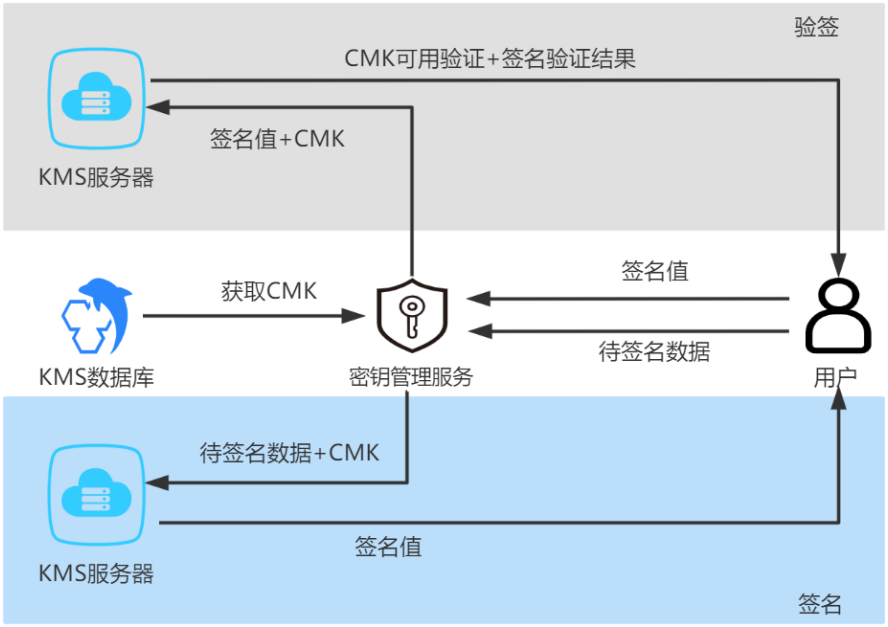
场景	场景描述
签名验签	• 数字签名技术是非对称加密算法的另一种典型应用。数字签名分为签名和验证两个过程，消息发送者使用私钥对数据签名，消息接收者使用公钥进行签名验证。 • 由于签名是使用私钥加密产生，而私钥不公开，这使得签名具有唯一的特征，广泛用于数据防篡改、身份认证等相关技术领域。
数据加解密	• 非对称密钥加密通信的过程类似于对称加密，区别在于需要使用公钥进行数据加密，使用私钥进行数据解密。 • 由于密文只有通过私钥才可以解密，而私钥是不公开的，所以即使由于传输介质的安全性比较低而导致信息泄露，拿到密文的人也无法将其破译，从而保证了敏感信息的安全。这种敏感信息传递的方式，被广泛用于各类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

3.4.2. 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。
asymmetricVerify	非对称密钥的公钥运算：验证私钥产生的数字签名。

3.4.3. 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。

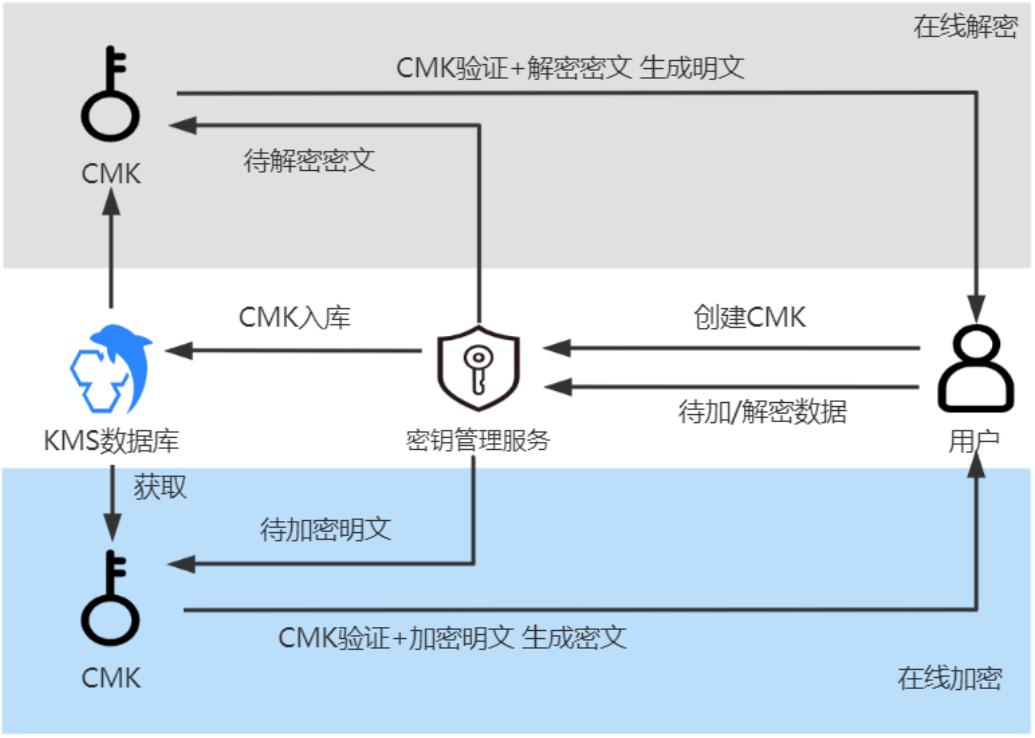
4. 最佳实践

4.1. 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。

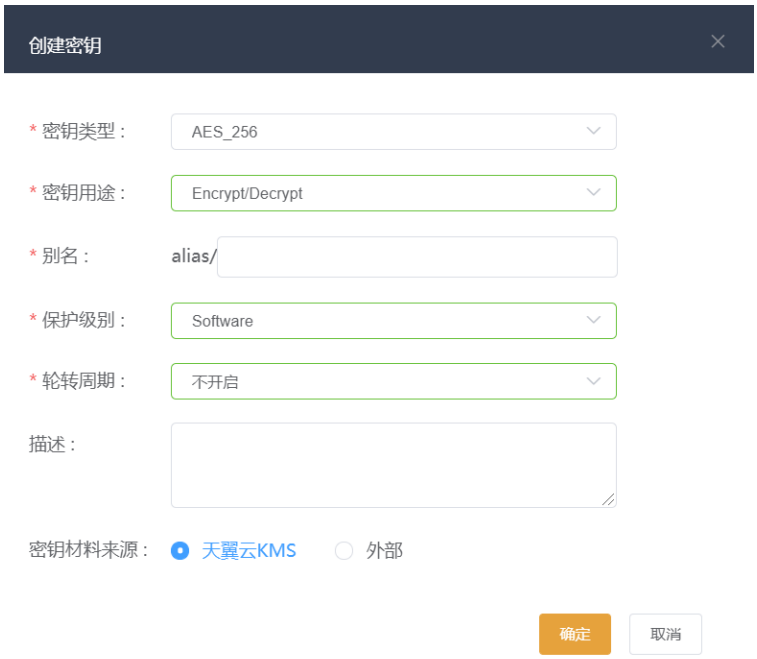
相关 API

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。

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

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":
"MDA2NE1qUXhaV1JsTWpJdE5qSTJNUzAwTmpFM0xUbGpZV1l0TVRCa09EazVPVEExTVRaakpqUTVaV00zTm1RM0xXTmpOR010TkRBd1pTMDVaakU1TFdZNU1EQXhOVGczWVdVd1pnPT3oCYiGAy7mNTLitIlJaQ92",
"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

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":
           "sc7280+klUSln3Y9FHdfKGUT+6kPrcIMW41uZQeXxGU="
      },
      "statusCode": 200,
      "success": 1
     }
}
```


返回参数说明

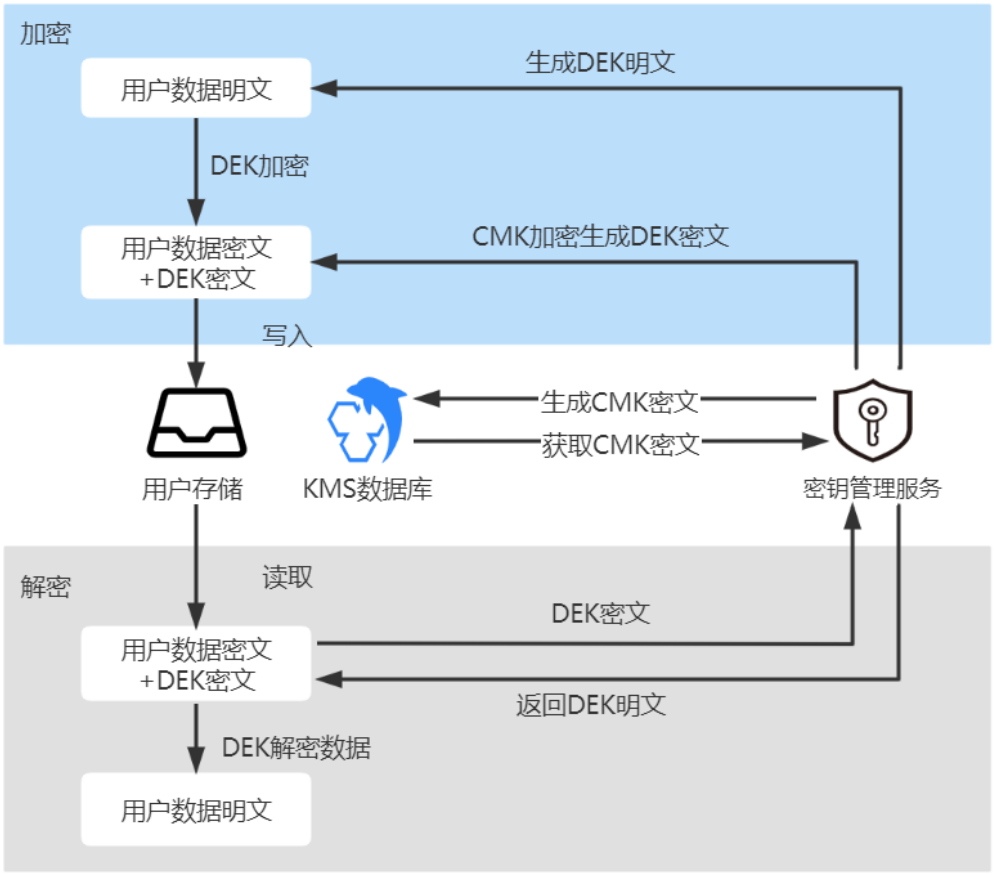
参数	说明
cmkUuid	CMK 的全局唯一标识符。如果请求中的 Cmk_uuid 参数使用的是 CMK 的别名，在响应中会返回别名对应的 CMK 标志符。
keyVersionId	密钥版本 ID。主密钥版本的全局唯一标识符。
plaintext	解密后的明文经过 Base64 编码的后的值。

4.2. 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



加密操作流程

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。

解密操作流程

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，将密文数据密钥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

API 名称	说明
createKey	创建用户主密钥（CMK）

API 名称	说明
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

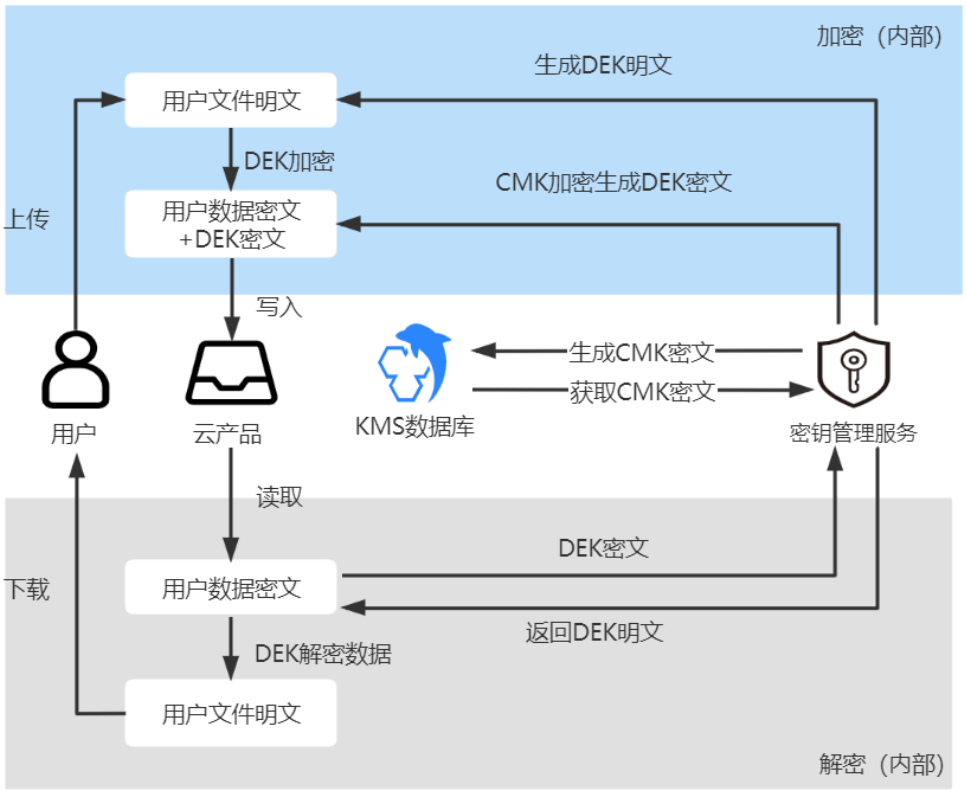
4.3. 云服务通过 KMS 实现服务端加密

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



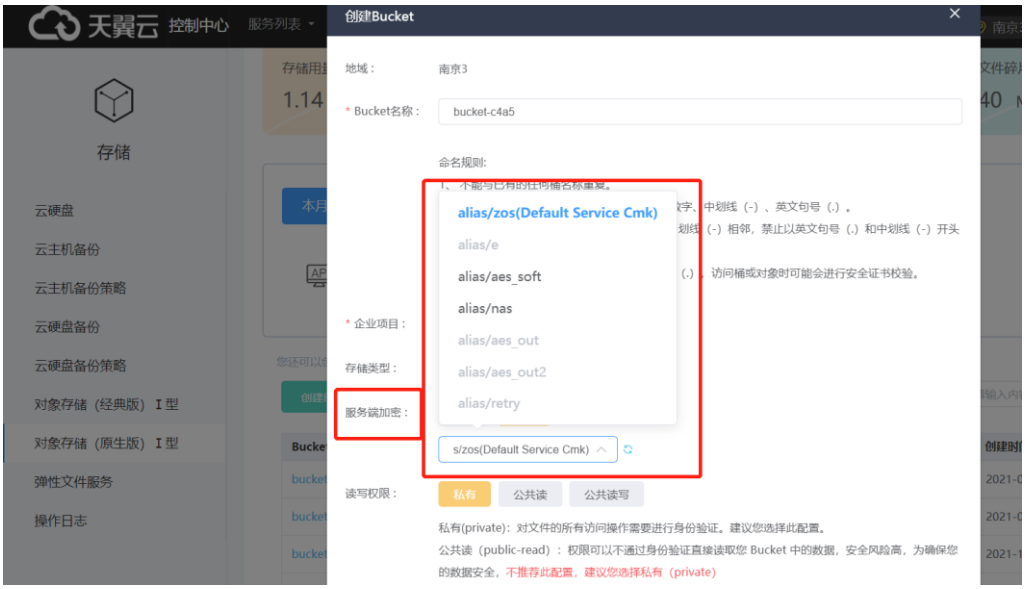
云产品开启服务端加密流程

1. 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。

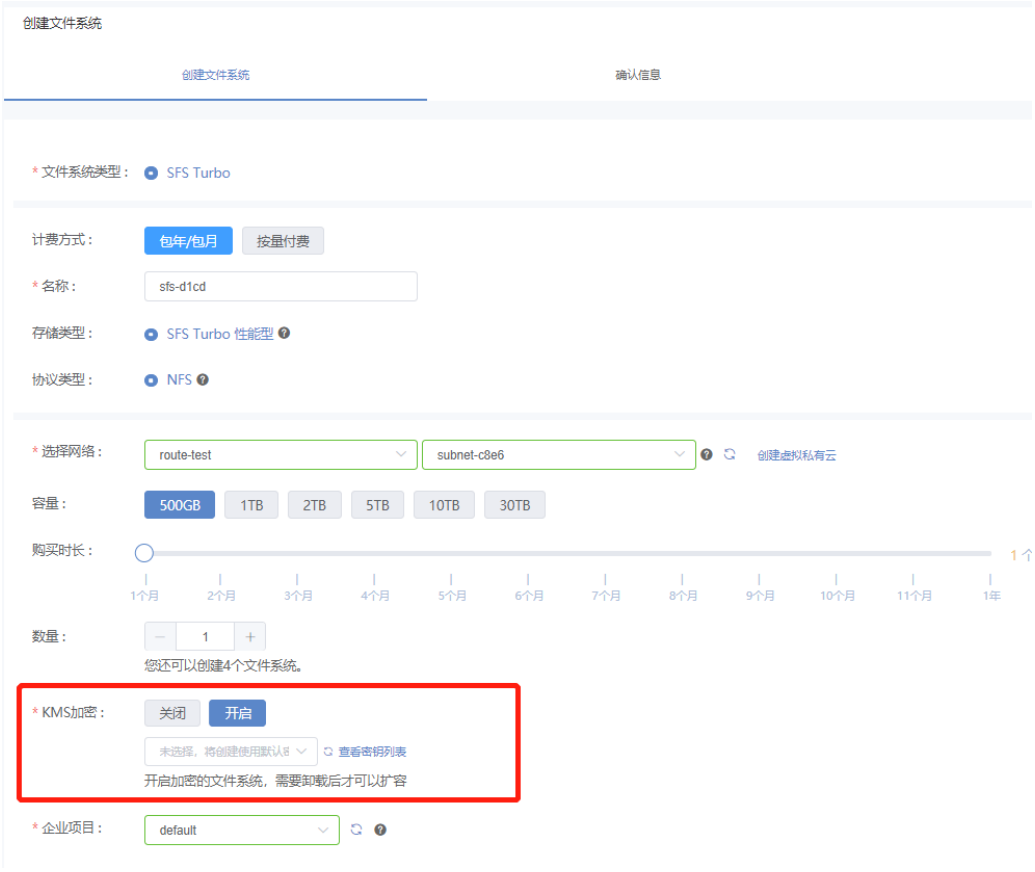
2. 加密对象存储；

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。



3. 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。



4.4. 通过 KMS 实现签名验签

通过密钥管理服务（KMS）创建非对称密钥，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

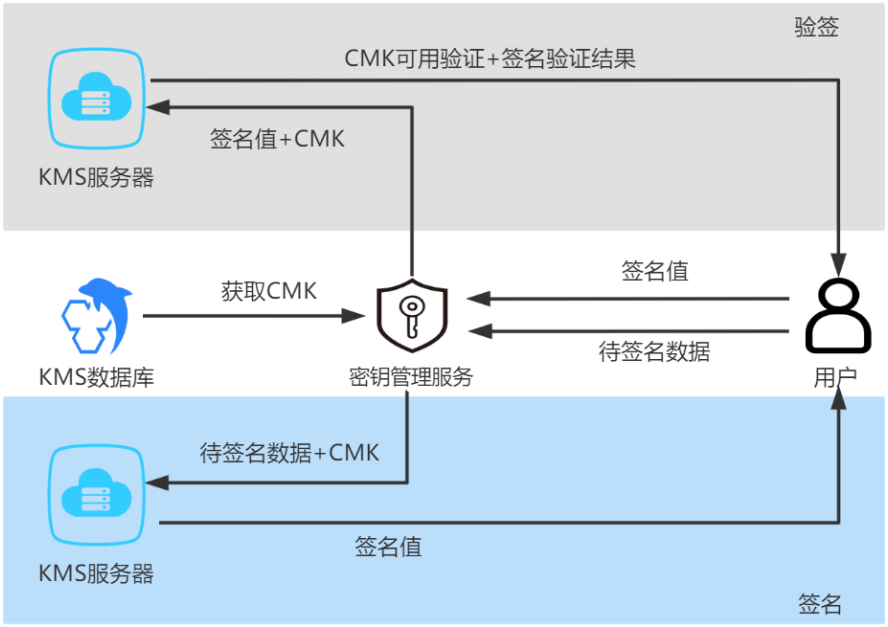
  用于信任程度不对等的系统之间，实现敏感信息的安全传递。

- 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。

4.5. 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

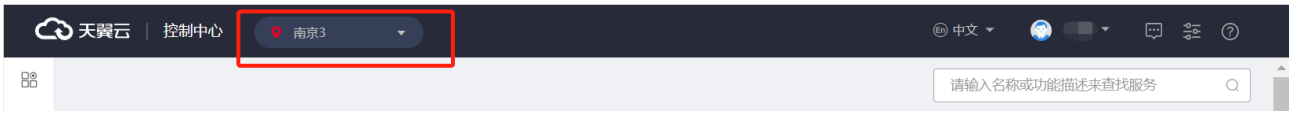
非对称密钥不支持自动轮转，需人工创建新的密钥版本，版本创建后立即生效。

- 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**；

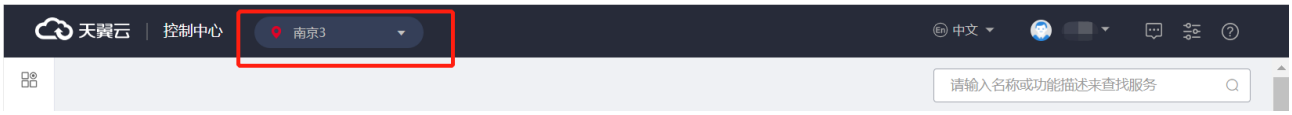
6. 在**设置轮转策略**对话框，选择轮转周期，**30 天**、**90 天**、**180 天**，或**自定义天数**；

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；

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）

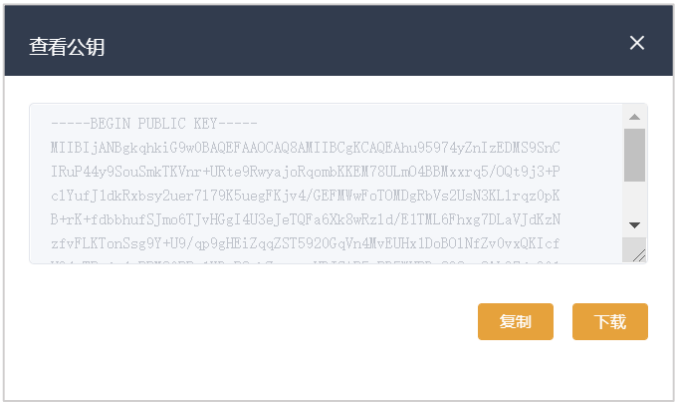
1. 登录密钥管理服务控制台；
2. 在页面最上方的导航栏的资源池下拉列表，选择密钥所在的区域；



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。



5. 常见问题

5.1. 计费类

密钥管理服务的计费方式是什么？

密钥管理服务为按需计费，以用户实际创建使用的资源量计费。开通服务不收费。

密钥管理服务的计费项是什么？

密钥管理服务共两大类计费项，分别为密钥托管费和 API 调用费。其中密钥托管费按天统计用户当前使用的密钥个数并计费，API 调用费按月统计用户调用的总次数并计费。

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？

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，密码运算类接口如下：

API	说明
encrypt	在线加密，使用指定用户主密钥加密数据，用于少量数据（不多于 6KB）的在线加密。
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。
generateDataKeyWithoutPlaintext	生成信封加密的数据密钥，返回经指定用户主密钥加密的密文。
exportDataKey	导出数据密钥，返回经指定公钥加密的数据密钥的密文。
generateAndExportDataKey	产生并导出数据密钥，生成信封加密的数据密钥，返回经指定用户主密钥加密的密文和经指定公钥加密的密文。
decrypt	解密 Encrypt 或 GenerateDataKey 接口产生的密文，不需要指定用于解密的用户主密钥。
reEncrypt	对密文进行转加密，即先解密密文，然后将解密得到的数据或者数据密钥使用新的主密钥再次进行加密，返回加密

API	说明
	结果。待转加密的密文可以为对称加密或非对称加密返回的密文数据。
asymmetricSign	非对称密钥的私钥运算：产生数字签名。
asymmetricVerify	非对称密钥的公钥运算：验证私钥产生的数字签名。
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。
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。

密钥被禁用后是否还计费？

密钥被禁用后，仍然会存储在 KMS 中，您可以根据需要随时启用该密钥。因此密钥被禁用后，仍然会计费。只有删除密钥，才会停止计费。

计划删除的密钥是否还计费？

计划删除的密钥，从计划删除日期开始，直至密钥彻底被删除，密钥不会计费。如果您在密钥被彻底删除前的等待期内取消删除密钥，该密钥将恢复计费。

欠费后，密钥是否还能进行解密？

不可以。用户欠费后，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，其中包括用户自建主密钥以及默认密钥。

5.2. 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。

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，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。

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。

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，用户设置预删除周期，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。

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。

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，其根密钥存储在软件文件系统中；硬件保护级别的密钥通过专用硬件保护密钥，其根密钥存储于密码机中且无法导出，所有涉及根密钥的使用过程均在密码机内部完成。

密钥自动轮转周期的可设置范围是什么？

7-730 天。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）。

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，并将新版本密钥的公钥分发出去。

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。

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。

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。

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。

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。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。

用户主密钥与别名的对应关系是什么？

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。

别名支持修改吗？

别名不支持修改，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。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？

删除别名不会删除其关联的用户主密钥，但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。同一个资源池中的别名具有唯一性，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。

非对称密钥是否支持自动轮转？

不支持。由于非对称密钥公钥使用场景的特殊性，KMS 不支持对非对称密钥进行自动轮转。用户可以人工手动创建新的版本，生成全新的一对公钥和私钥。

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。

5.3. 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。

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产品，通过 KMS 提供信封加密的方式对云产品数据进行加密。

用户自建用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。