天翼云·数据加密

用户使用指南

天翼云科技有限公司

目 录

1 产品简介

1.1 什么是数据加密服务

数据加密服务（Data Encryption Workshop）是一个综合的云上数据加密服务。它可以提供专属加密、密钥管理等服务，安全可靠的为用户解决了数据安全、密钥安全、密钥管理复杂等问题。其密钥由硬件安全模块（Hardware Security Module，HSM） 保护，并与多个云服务集成。

- 密钥管理

  密钥管理，即密钥管理服务（Key Management Service，KMS），是一种安全、可靠、简单易用的密钥托管服务，帮助您轻松创建和管理密钥，保护密钥的安全。

  KMS 通过使用硬件安全模块（Hardware Security Module，HSM）保护密钥安全，帮助用户轻松创建和管理密钥，所有的用户密钥都由 HSM 中的根密钥保护，避免密钥泄露。

- 专属加密

  专属加密（Dedicated Hardware Security Module，Dedicated HSM）为您提供的云上数据加密的服务，可处理加解密、签名、验签、产生密钥和密钥安全存储等操作。

  Dedicated HSM 为您提供经国家密码管理局检测认证的专属加密实例，帮助您保护弹性云服务器上数据的安全性和隐私性要求，满足监管合规要求。同时，用户能够对专属加密实例生成的密钥进行安全可靠的管理，也能使用多种加密算法来对数据进行可靠的加解密运算。

1.2 密钥管理

密钥管理，即密钥管理服务（Key Management Service，KMS），是一种安全、可靠、简单易用的密钥托管服务，帮助您轻松创建和管理密钥，保护密钥的安全。

KMS 通过使用硬件安全模块 HSM（Hardware Security Module）保护密钥的安全，所有的用户密钥都由 HSM 中的根密钥保护，避免密钥泄露。

KMS 对密钥的所有操作都会进行访问控制及日志跟踪，提供所有密钥的使用记录，满足审计和合规性要求。

功能介绍

用户可通过密钥管理界面，对用户主密钥进行以下操作：

- 创建、查看、启用、禁用、计划删除、取消删除用户主密钥
- 修改用户主密钥的别名和描述
- 导入密钥、删除密钥材料
- 在线工具加解密小数据
- 添加、搜索、编辑、删除标签

KMS 支持的密码算法

- 通过管理控制台创建的密钥仅支持 AES-256 加解密算法。
- 通过外部导入的密钥支持的加解密算法为，用户仅能导入 256 位对称密钥。

表1-1 算法说明

算法	说明	设置
RSAES_OAEP_SHA_256	具有“SHA-256”哈希函数的 OAEP 的 RSA 加密算法。	请您根据自己的 HSM 功能选择加密算法。 1. 如果您的 HSM 支持“RSAES_OAEP_SHA_256”加密算法，推荐使用“RSAES_OAEP_SHA_256”加密密钥材料。 2. 如果您的 HSM 不支持“OAEP”选项，用户可以使用“RSAES_PKCS1_V1_5”加密密钥材料。 **注意** “RSAES_OAEP_SHA_1”加密算法已经不再安全，请谨慎选择。
RSAES_PKCS1_V1_5	PKCS#1 v1.5 版本的 RSA 加密算法。	
RSAES_OAEP_SHA_1	具有“SHA-1”哈希函数的 OAEP 的 RSA 加密算法。	

1.3 专属加密

专属加密（Dedicated Hardware Security Module，Dedicated HSM）为您提供的云上数据加密的服务，可处理加解密、签名、验签、产生密钥和密钥安全存储等操作。

Dedicated HSM 旨在满足用户将线下加密设备能力转移到云上的要求，提供可独占、高性能、安全合规的加密域计算资源。用户作为设备使用者完全控制密钥的产生、存储和访问授权。华为云只负责监控和管理设备及其相关网络设施。

同时，Dedicated HSM 可提供认证合规的金融数据加密机、服务器加密机以及签名验签服务器等，灵活支撑用户业务场景。能够帮助用户满足数据安全方面的监管要求，以及云上业务数据的隐私性要求。

功能介绍

Dedicated HSM 提供以下功能：

- 生成、存储、导入、导出和管理加密密钥，包括对称密钥和非对称密钥。
- 使用对称和非对称算法加密和解密数据。
- 使用加密哈希函数计算消息摘要和基于哈希的消息身份验证代码。
- 对数据进行加密签名（包括代码签名）并验证签名。
- 以加密方式生成安全随机数据。

支持的密码算法

对称密码算法	SM1、SM4、DES、3DES、AES、SM7
非对称密码算法	SM2、 RSA（1024-4096）
摘要算法	SM3、 SHA1、SHA256、SHA384

权限认证

- 专属加密实例设备管理与内容（敏感信息）管理权限分离，即使华为云的运维人员也无法获取到用户的密钥。
- 可对敏感指令支持分类授权控制，有效防止越权行为。
- 支持用户名口令认证，数字证书认证等多种权限认证方式。

可靠性

专属加密实例之间独享加密芯片，即使部分硬件芯片损坏也不影响使用。

1.4 使用场景

1.5 访问与使用

1.5.1 如何访问

公有云提供了 Web 化的服务管理平台，即管理控制台管理方式。

如果用户已注册公有云，可直接登录管理控制台，单击页面上方的“服务列表”，选择“安全 > 数据加密服务 > 专属加密服务”。

1.5.2 如何使用

与云服务配合使用

表1-2 使用 KMS 加密的云服务列表

服务名称	如何使用
对象存储服务	对象存储服务支持普通方式和服务端加密方式上传和下载对象。当用户使用服务端加密方式上传对象时，数据会在服务端加密成密文后安全地存储在对象存储服务中；用户下载加密对象时，存储的密文会先在服务端解密为明文，再提供给用户。对象存储服务支持 KMS 托管密钥的服务端加密方式（即 SSE-KMS 加密方式），该加密方式是通过 KMS 提供密钥的方式进行服务端加密。 用户如何使用对象存储服务的 SSE-KMS 加密方式上传对象，具体操作请参见《对象存储服务控制台指南》。
云硬盘	在购买云硬盘时，用户启用云硬盘的加密功能，选择 KMS 提供的用户主密钥对云硬盘进行加密，则在使用该云硬盘时，存储到云硬盘的数据将会自动加密。 用户如何使用云硬盘加密功能，具体操作请参见《云硬盘用户指南》。
镜像服务	用户通过外部镜像文件创建私有镜像时，可启用私有镜像加密功能，选择 KMS 提供的用户主密钥对镜像进行加密。 用户如何使用镜像服务的私有镜像加密功能，具体操作请参见《镜像服务用户指南》。

与弹性云服务器配合使用

用户可通过创建专属加密实例的方式，使用专属加密实例生成的密钥加解密部署在弹性云服务器内业务系统的敏感数据。

1.5.3 与其他云服务的关系

与对象存储服务的关系

KMS 为对象存储服务提供用户主密钥管理控制能力，应用于对象存储服务的服务端加密功能（SSE-KMS 加密方式）。

与云硬盘的关系

KMS 为云硬盘提供用户主密钥管理控制能力，应用于云硬盘的加密功能。

与镜像服务的关系

KMS 为镜像服务提供用户主密钥管理控制能力，应用于镜像服务的私有镜像加密功能。

与弹性云服务器的关系

Dedicated HSM 提供的专属加密实例可以为部署在弹性云服务器内的业务系统加密敏感数据，用户可完全控制密钥的生成、存储和访问授权，保证数据在传输、存储过程中的完整性、保密性。

2 密钥管理

2.1 创建密钥

该任务指导用户通过密钥管理界面创建用户主密钥。用户最多可创建 20 个用户主密钥，不包含默认主密钥。

用户主密钥可用于如下场景：

- 对象存储服务中对象的服务端加密
- 云硬盘中数据的加密
- 私有镜像的加密
- 用户主密钥直接加解密小数据
- 用户应用程序的 DEK 加解密

说明
因为默认主密钥的别名后缀为“/default”，所以用户创建的密钥别名后缀不能为“/default”。

前提条件

已获取管理控制台的登录帐号与密码。

创建密钥

步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤 3 在界面右上角，单击“创建密钥”。

步骤 4 在弹出的“创建密钥”对话框中，填写密钥的“别名”与“描述”。

图2-1 创建密钥

步骤 5 （可选）用户可根据自己的需要为用户主密钥添加标签，输入“标签键”和“标签值”。

说明

- 当用户在创建密钥时，没有为该用户主密钥添加标签。若用户需要为该用户主密钥添加标签，可单击该用户主密钥的别名，进入密钥详情页面，为该用户主密钥添加标签。
- 同一个用户主密钥下，一个标签键只能对应一个标签值；不同的用户主密钥下可以使用相同的标签键。
- 用户最多可以给单个用户主密钥添加 10 个标签。
- 当同时添加多个标签，需要删除其中一个待添加的标签时，可单击该标签所在行的“删除”，删除标签。

步骤 6 单击“确定”，在页面右上角弹出“创建密钥成功”，则说明密钥创建完成。

用户可在密钥列表上查看已完成创建的密钥，密钥默认状态为“启用”。

----结束

相关操作

- 对象存储服务中对象的服务端加密方法，具体请参见《对象存储服务控制台指南》的“使用服务端加密方式上传文件”章节。
- 云硬盘中数据加密方法，具体请参见《云硬盘用户指南》的“购买云硬盘”章节。
- 私有镜像的加密方法，具体请参见《镜像服务用户指南》的“加密镜像”章节。

2.2 导入密钥

2.2.1 概述

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

- 安全性

  用户需要确保符合自己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安全性负责。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。
- 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，如表 2-1 所示。

表2-1 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

密钥材料来源	区别
导入的密钥	• 可以手动删除密钥材料，但不能删除该用户主密钥及其元数据。 • 在导入密钥材料时，可以设置密钥材料失效时间，密钥材料失效后，KMS 将在 24 小时以内自动删除密钥材料，但不会删除该用户主密钥及其元数据。 建议用户在本地密钥管理基础设施中安全地备份一份密钥材料，以便密钥材料失效或误删除时重新导入该密钥材料。
KMS 创建的密钥	• 不能手动删除密钥材料。 • 不能设置密钥材料的失效时间。

- 关联性

  当用户将密钥材料导入用户主密钥时，该用户主密钥与该密钥材料永久关联，不能将其他密钥材料导入该用户主密钥中。
- 唯一性

  当用户使用导入的密钥加密数据时，加密后的数据必须使用加密时采用的用户主密钥（即用户主密钥的元数据及密钥材料与导入的密钥匹配）才能解密数据，否则解密会失败。

2.2.2 导入密钥材料

操作场景

当用户希望使用自己的密钥材料，而不是 KMS 生成的密钥材料时，可通过密钥管理界面将自己的密钥材料导入到 KMS，由 KMS 统一管理。

该任务指导用户通过密钥管理界面导入密钥材料。

说明

- 导入的密钥与创建的用户主密钥一样支持启用、禁用、计划删除和取消删除等操作。
- 用户仅能导入 256 位对称密钥。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 已准备好待导入的密钥材料。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤 3 在界面右上角，单击“导入密钥”，弹出“导入密钥”对话框。

步骤 4 在弹出的对话框中填写密钥的“别名”和“描述”信息。

图2-2 创建空密钥

步骤 5 （可选）用户可根据自己的需要为用户主密钥添加标签，输入“标签键”和“标签值”。

说明

- 当用户在创建密钥时，没有为该用户主密钥添加标签。若用户需要为该用户主密钥添加标签，可单击该用户主密钥的别名，进入密钥详情页面，为该用户主密钥添加标签。
- 同一个用户主密钥下，一个标签键只能对应一个标签值；不同的用户主密钥下可以使用相同的标签键。
- 用户最多可以给单个用户主密钥添加 10 个标签。
- 当同时添加多个标签，需要删除其中一个待添加的标签时，可单击该标签所在行的“删除”，删除标签。

步骤 6 单击“安全性与持久性”阅读并了解导入密钥的安全性和持久性。

步骤 7 勾选“我已经了解导入密钥的安全性和持久性”，创建密钥材料为空的用户主密钥。

步骤 8 单击“下一步”，进入“获取包装密钥和导入令牌”页面。根据表 2-2 选择密钥包装算法。

图2-3 获取包装密钥和导入令牌

表2-2 密钥包装算法说明

密钥包装算法	说明	设置
RSAES_OAEP_SHA_256	具有“SHA-256”哈希函数的 OAEP 的 RSA 加密算法。	请用户根据自己的 HSM 功能选择加密算法。 1. 如果您的 HSM 支持“RSAES_OAEP_SHA_256”加密算法，推荐使用“RSAES_OAEP_SHA_256”加密密钥材料。 2. 如果您的 HSM 不支持“OAEP”选项，用户可以使用“RSAES_PKCS1_V1_5”加密密钥材料。 **注意** “RSAES_OAEP_SHA_1”加密算法已经不再安全，请谨慎选择。
RSAES_PKCS1_V1_5	PKCS#1 v1.5 版本的 RSA 加密算法。	
RSAES_OAEP_SHA_1	具有“SHA-1”哈希函数的 OAEP 的 RSA 加密算法。	

步骤 9 单击“下载”，下载的文件包含包装密钥、导入令牌和说明文件，如图 2-4 所示。

图2-4 下载文件

- wrappingKey_*密钥 ID*_*下载时间*：即包装密钥，用于加密密钥材料的包装密钥。
- importToken_*密钥 ID*_*下载时间*：即导入令牌，KMS 导入密钥材料时需要使用。

- README_*密钥ID*_*下载时间*：即说明文件，记录包装密钥序列号、密钥包装算法、包装密钥文件名称、令牌文件名称以及包装密钥和令牌的过期时间。

注意

包装密钥和导入令牌将在 24 小时后失效，失效后将不能使用。如果包装密钥和导入令牌失效，请重新下载包装密钥和导入令牌。

同时，用户也可以通过调用 API 接口的方式获取包装密钥和导入令牌。

1. 调用“get-parameters-for-import”接口，获取包装密钥和导入令牌。

   如下以获取密钥 ID 为“43f1ffd7-18fb-4568-9575-602e009b7ee8”，加密算法为“RSAES_PKCS1_V1_5”的包装密钥和导入令牌为例。

   “public_key”：调用 API 接口返回的 base64 编码的包装密钥内容。

   “import_token”：调用 API 接口返回的 base64 编码的导入令牌内容。

   - 请求样例

     ```
     {
        "key_id": "43f1ffd7-18fb-4568-9575-602e009b7ee8",
        "wrapping_algorithm":"RSAES_PKCS1_V1_5"
     }
     ```

   - 响应样例

     ```
     {
        "key_id": "43f1ffd7-18fb-4568-9575-602e009b7ee8",
        "public_key":"public key base64 encoded data",
        "import_token":"import token base64 encoded data",
        "expiration_time":1501578672
     }
     ```

2. 保存包装密钥，包装密钥需要按照以下步骤转换格式。使用转换格式后的包装密钥进行加密的密钥材料才能成功导入管理控制台。

   a. 复制包装密钥“public_key”的内容，粘贴到“.txt”文件中，并保存为“PublicKey.b64”。

   b. 使用 OpenSSL，执行以下命令，对“PublicKey.b64”文件内容进行 base64 转码，生成二进制数据，并将转码后的文件保存为“PublicKey.bin”。

      openssl enc -d -base64 -A -in PublicKey.b64 -out PublicKey.bin

3. 保存导入令牌，复制导入令牌“import_token”的内容，粘贴到“.txt”文件中，并保存为“ImportToken.b64”。

步骤 10 使用下载的“包装密钥”对待导入的密钥材料进行加密。

- 方法一：使用下载的包装密钥在自己的 HSM 中加密密钥材料，详细信息请参考您的 HSM 操作指南。
- 方法二：采用 OpenSSL 加密密钥材料。

说明

若用户需要使用 **openssl pkeyutl** 命令，OpenSSL 需要是 1.0.2 及以上版本。

如下以使用下载的包装密钥，加密生成的密钥材料（256 位对称密钥）为例说明，操作步骤如下所示：

a. 执行以下命令，生成密钥材料（256 位对称密钥），并将生成的密钥材料以“PlaintextKeyMaterial.bin”命名保存。

openssl rand -out *PlaintextKeyMaterial.bin* 32

b. 使用下载的包装密钥加密密钥材料，并将加密后的密钥材料按“EncryptedKeyMaterial.bin”命名保存。

以下命令中的 ***PublicKey.bin*** 参数请以步骤 9 下载的包装密钥名称 *wrappingKey_密钥 ID_下载时间*进行替换。

表2-3 使用下载的包装密钥加密生成的密钥材料

包装密钥算法	加密生成的密钥材料
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 pkeyutl** **-in *PlaintextKeyMaterial.bin*** **-inkey *PublicKey.bin*** **-out *EncryptedKeyMaterial.bin*** **-keyform der** **-pubin -encrypt** **-pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha1**

步骤 11 单击“下一步”，进入“导入密钥材料”页面。根据表 2-4 配置参数。

图2-5 导入密钥材料

表2-4 导入密钥材料参数说明

参数	操作说明
密钥 ID	创建密钥时，随机生成的密钥 ID。
密钥材料	1. 选择使用步骤 9 下载的“包装密钥”加密的密钥材料。 2. 单击“导入”，导入密钥材料。

步骤 12 单击“下一步”，进入“导入密钥令牌”页面。根据表 2-5 设置参数。

图2-6 导入密钥令牌

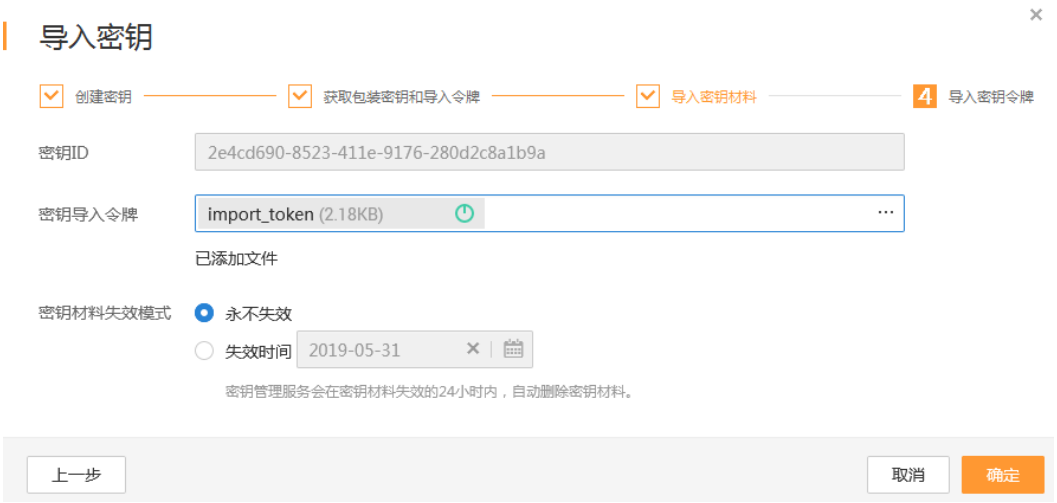


表2-5 导入密钥令牌参数说明

参数	操作说明
密钥 ID	创建密钥时，随机生成的密钥 ID。

参数	操作说明
密钥导入令牌	选择步骤 9 中“下载”的导入令牌。
密钥材料失效模式	• 永不失效：导入的密钥材料永久不失效。 • 失效时间：用户可指定导入的密钥材料的失效时间，默认失效时间为 24 小时。 密钥材料失效后，KMS 会在 24 小时内自动删除密钥材料，删除后密钥将无法使用，且密钥状态变更为“等待导入”。

步骤 13 单击“确定”，页面右上角弹出“密钥导入成功”，则说明导入密钥成功。

注意

密钥 ID、导入的密钥材料和导入的令牌需要全部匹配，密钥材料才能导入成功，否则会导入失败。

用户可在密钥列表中查看到导入的密钥信息，导入密钥的默认状态为“启用”。

----结束

2.2.3 删除密钥材料

操作场景

当用户导入密钥材料时，可以指定密钥材料的失效时间。当密钥材料失效后，KMS 将删除密钥材料，用户主密钥的状态变为“等待导入”。用户也可以根据需要手动删除密钥材料。等待密钥材料到期失效与手动删除密钥材料所达到的效果是一样的。

该任务指导用户通过密钥管理界面对外部导入的密钥材料进行删除操作。

说明

- 删除密钥材料后，若需要重新导入密钥材料，导入的密钥材料必须与删除的密钥材料完全相同，才能导入成功。
- 用户重新导入相同的密钥材料后，该用户主密钥可以解密删除密钥材料前加密的所有数据。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 用户已导入密钥材料。
- “密钥材料来源”为“外部”。
- 密钥“状态”为“启用”或“禁用”。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤 3 在需要删除的密钥材料所在行，单击“删除密钥材料”。

步骤 4 在弹出的对话框中单击“确定”，页面右上角弹出“密钥材料删除成功”，则说明删除密钥材料的成功。

密钥材料删除后，密钥将无法使用，且当前密钥的状态切换为“等待导入”。

----结束

2.3 在线工具加解密小数据

该任务指导用户通过密钥管理界面使用在线工具加解密不大于 4KB 的数据。

说明
在线工具不支持通过默认主密钥加解密小数据。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 用户主密钥处于“启用”状态。

加密数据

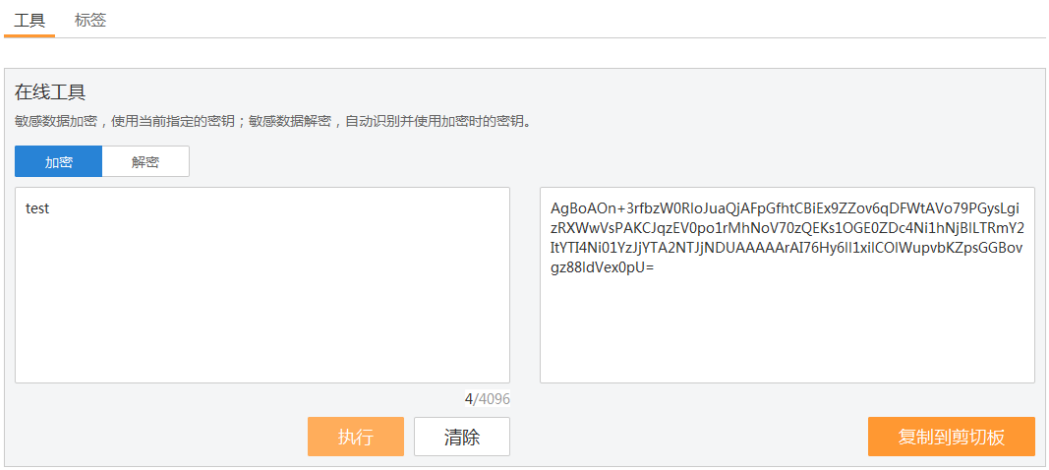
步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤 3 单击目标用户主密钥的别名，进入密钥详细信息在线工具加密数据页面。

步骤 4 在“加密”文本框中输入待加密的数据，如图 2-7 所示。

图2-7 加密数据



步骤 5 单击“执行”，右侧文本框显示加密后的密文数据。

说明

- 加密数据时，使用当前指定的密钥加密数据。
- 用户可单击“清除”，清除已输入的数据。
- 用户可单击“复制到剪切板”拷贝加密后的密文数据，并保存到本地文件中。

----结束

解密数据

步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤 3 解密数据时，可单击任意“启用”状态的非默认主密钥别名，进入该密钥的在线工具页面。

步骤 4 单击“解密”，在左侧文本框中数据待解密的密文数据，如图 2-8 所示。

说明

- 在线工具自动识别并使用数据被加密时使用的密钥解密数据。
- 若该密钥已被删除，会导致解密失败。

图2-8 解密数据

步骤 5 单击“执行”，右侧文本框中显示解密后的明文数据。

说明

用户可直接单击“复制到剪切板”拷贝解密后的明文数据，并保存到本地文件中。

----结束

2.4 管理标签

2.4.1 添加标签

标签用于标识用户主密钥。为用户主密钥添加标签，可以方便用户对用户主密钥进行分类和跟踪，并按标签汇总用户主密钥的使用情况。

注意

KMS 不支持为默认主密钥添加标签。

前提条件

已获取管理控制台的登录帐号与密码。

添加标签

步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤 3 单击目标用户主密钥的别名，进入密钥详细信息页面。

步骤 4 单击“标签”，进入标签管理页面，如图 2-9 所示。

图2-9 标签页面

步骤 5 单击“添加标签”，弹出添加标签对话框，如图 2-10 所示。

图2-10 添加标签

说明
当同时添加多个标签，需要删除其中一个待添加的标签时，可单击该标签所在行的“删除”，删除标签。

步骤 6 在弹出的“添加标签”对话框中输入“标签键”和“标签值”，参数说明如表 2-6 所示。

表2-6 标签参数说明

参数	参数说明	取值要求	样例
标签键	标签的名称。 同一个用户主密钥下，一个标签键只能对应一个标签值；不同的用户主密钥下可以使用相同的标签键。 用户最多可以给单个用户主密钥添加 10 个标签。	• 必填。 • 对于同一个用户主密钥，标签键唯一。 • 长度不超过 36 个字符。 • 只能包含以下 4 种字符： – 大写字母 – 小写字母 – 数字 – 特殊字符，包括“-”和“_”	cost

参数	参数说明	取值要求	样例
标签值	标签的值。	• 可以为空。 • 长度不超过 43 个字符。 • 只能包含以下 4 种字符： – 大写字母 – 小写字母 – 数字 – 特殊字符，包括“-”和“_”	100

步骤 7 单击“确定”，完成标签的添加。

----结束

2.4.2 搜索标签

该任务指导用户通过密钥管理界面搜索标签，可搜索当前项目下满足标签搜索条件的所有的用户主密钥。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 已添加标签。

搜索标签

步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

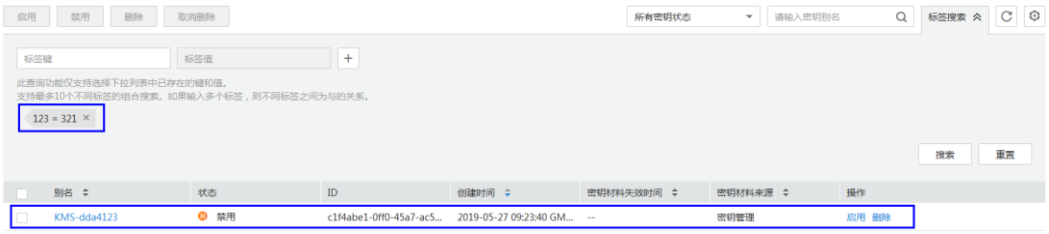
步骤 3 单击“标签搜索”，展开搜索框，如图 2-11 所示。

图2-11 标签搜索框

步骤 4 在搜索框中输入“标签键”和“标签值”。

步骤 5 单击  ，添加到搜索条件中，并单击“搜索”，显示满足搜索条件的用户主密钥列表，如图 2-12 所示。

图2-12 搜索结果



说明

- 可添加多个标签进行组合搜索，最多支持 10 个不同标签的组合搜索，若进行多个标签组合搜索，则搜索结果的每个用户主密钥均满足标签组合搜索条件。
- 若需要在搜索条件中删除添加的标签，可在搜索条件中单击指定标签后的  ，删除添加的标签。
- 若需要重新添加搜索条件，可单击“重置”，重新添加搜索条件。

----结束

2.4.3 修改标签值

该任务指导用户通过密钥管理界面修改标签值。

前提条件

已获取管理控制台的登录帐号与密码。

修改标签值

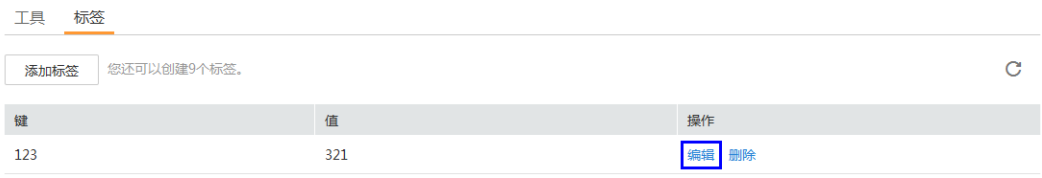
步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤 3 单击目标用户主密钥的别名，进入密钥详细信息页面。

步骤 4 单击“标签”，进入标签管理页面，如图 2-13 所示。

图2-13 标签页面



步骤 5 单击目标标签所在行的“编辑”，弹出编辑标签对话框，如图 2-14 所示。

图2-14 编辑标签

步骤 6 在弹出的编辑标签对话框中修改标签值，单击“确定”，完成标签值的修改。

----结束

2.4.4 删除标签

该任务指导用户通过密钥管理界面删除标签。

前提条件

已获取管理控制台的登录帐号与密码。

删除标签

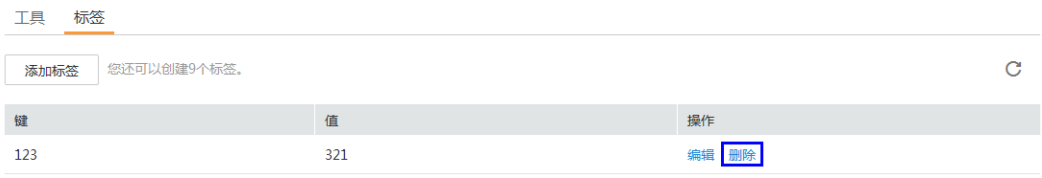
步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤 3 单击目标用户主密钥的别名，进入密钥详细信息页面。

步骤 4 单击“标签”，进入标签管理页面，如图 2-15 所示。

图2-15 标签页面



步骤 5 单击目标标签所在行的“删除”，弹出删除标签对话框。

步骤 6 在弹出的删除标签对话框中单击“确定”，完成标签的删除。

----结束

2.5 管理密钥

2.5.1 查看密钥

该任务指导用户通过 KMS 界面查看用户主密钥的信息，包括密钥别名、状态、ID 和创建时间。密钥状态包括“启用”、“禁用”、“计划删除”、和“等待导入”。

前提条件

已获取管理控制台的登录帐号与密码。

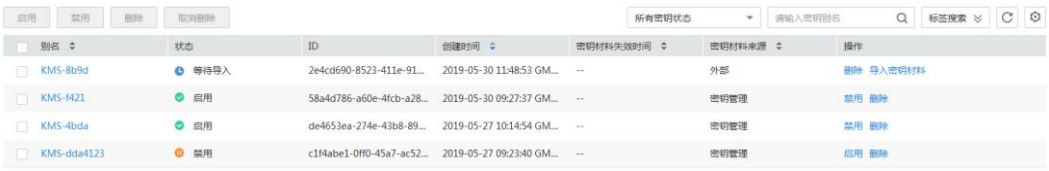
查看密钥

步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤 3 在密钥列表中，查看密钥信息，如图 2-16 所示。

图2-16 密钥列表



说明

- 在密钥列表右上角的搜索框中输入密钥的别名，单击 或按“Enter”，可以搜索指定的密钥。
- 可单击“标签搜索”，搜索符合标签搜索条件的用户主密钥。
- 可单击密钥列表右上角的，设置密钥列表展示的列。

密钥列表参数说明，如表 2-7 所示。

表2-7 密钥列表参数说明

参数	操作说明
别名	密钥的别名。
状态	密钥的状态，包含： • 启用 密钥处于启用状态 • 禁用 密钥处于禁用状态 • 计划删除 密钥处于计划删除状态 • 等待导入 如果密钥没有密钥材料，那么密钥的状态为“等待导入”。
ID	创建密钥时自动生成的密钥 ID。
创建时间	创建该密钥的时间。
密钥材料失效时间	密钥材料失效的时间，密钥材料失效后，当前密钥为空密钥。
密钥材料来源	密钥材料的来源，包含： • 外部 用户从外部导入到 KMS。 • 密钥管理 用户通过 KMS 创建。

步骤 4 用户可单击密钥别名，查看密钥详细信息。

说明

用户可单击该密钥的“别名”或“描述”所在行的，修改密钥的别名或描述信息。

- 默认主密钥（密钥别名后缀为“/default”），别名和描述不可以修改。
- 密钥状态处于“计划删除”时，别名和描述不可修改。

----结束

2.5.2 启用密钥

该任务指导用户通过密钥管理界面对单个或多个用户主密钥进行启用操作，使被禁用的密钥恢复到数据加解密能力。新建的用户主密钥默认为“启用”状态。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 待启用的密钥需处于“禁用”状态。

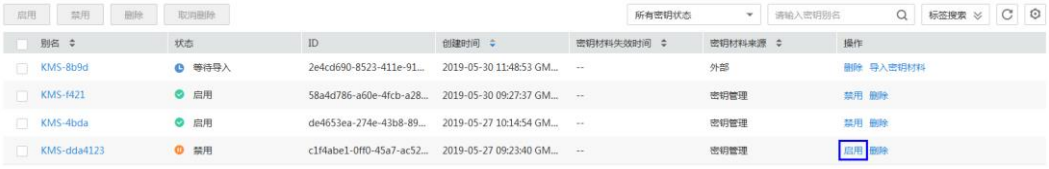
启用单个密钥

步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤 3 在需要启用的密钥所在行，单击“启用”。

图2-17 启用单个密钥



步骤 4 在弹出窗口中，单击“确定”，完成启用单个密钥操作。

----结束

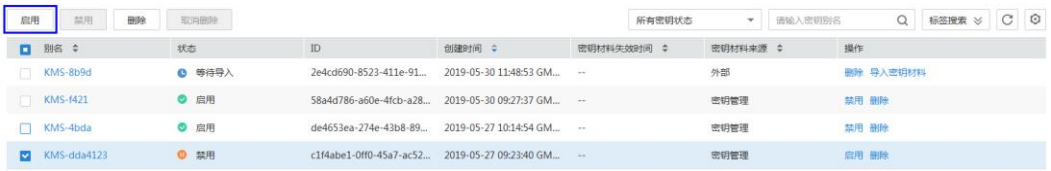
批量启用密钥

步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤 3 在密钥列表中，勾选所有需要启用的密钥，单击“启用”。

图2-18 批量启用密钥



步骤 4 在弹出窗口中，单击“确定”，完成批量启用密钥操作。

----结束

2.5.3 禁用密钥

该任务指导用户通过密钥管理界面对指定的用户主密钥进行禁用，以紧急保护数据。

用户主密钥被禁用后，用户将不能使用该密钥进行加解密任何数据。如果要使用该密钥进行加解密数据，用户需将该密钥重新启用，具体操作请参见 2.5.2 启用密钥。

说明
默认主密钥为密钥管理自动创建，不支持禁用操作。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 待禁用的密钥需处于“启用”状态。

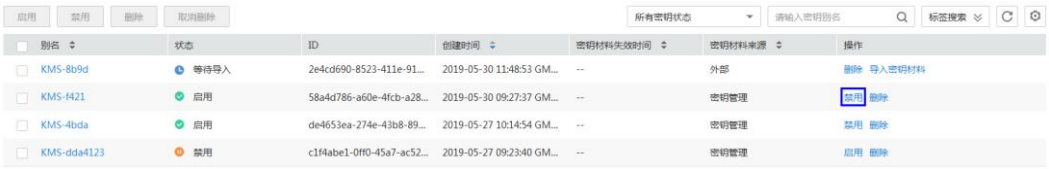
禁用单个密钥

步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤 3 在需要禁用的密钥所在行，单击“禁用”。

图2-19 禁用单个密钥



步骤 4 在弹出窗口中，单击“确定”，完成禁用单个密钥操作。

----结束

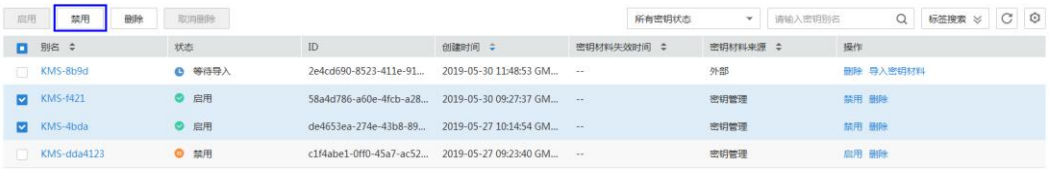
批量禁用密钥

步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤 3 在密钥列表中，勾选所有需要禁用的密钥，单击“禁用”。

图2-20 批量禁用密钥



步骤 4 在弹出窗口中，单击“确定”，完成批量禁用密钥操作。

----结束

2.5.4 计划删除密钥

该任务指导用户通过密钥管理界面对不再使用的用户主密钥进行有计划删除。

用户执行删除密钥操作后，密钥不会立即删除，密钥管理会将该操作按用户指定时间推迟执行，推迟时间范围为 7 天～1096 天。在推迟删除时间未到时，若需要重新使用该密钥，可以执行取消删除密钥操作。若超过推迟时间，密钥将被 KMS 彻底删除，使用该密钥加密的数据将无法解密，请谨慎操作。

在删除密钥前，用户需要确保该密钥没有被使用或将来也不会被使用。

说明

- 默认主密钥为服务自动创建，不支持删除操作。
- 密钥处于“冻结”状态时，不支持删除操作。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 待删除的密钥需处于“启用”、“禁用”或者“等待导入”状态。

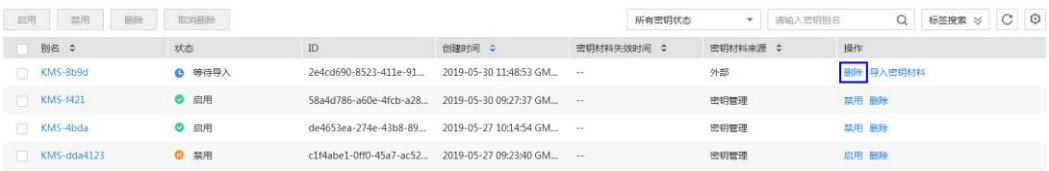
删除单个密钥

步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤 3 在需要删除的密钥所在行，单击“删除”。

图2-21 删除单个密钥



步骤 4 在弹出的窗口中，填写“推迟删除”的时间。

步骤 5 单击“确定”，完成删除单个密钥操作。

----结束

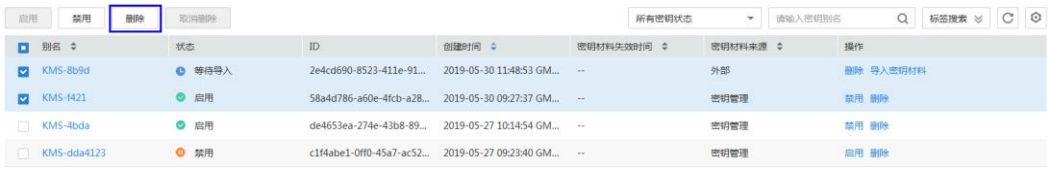
批量删除密钥

步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤 3 在密钥列表中，勾选所有需要删除的密钥，单击“删除”。

图2-22 批量删除密钥



步骤 4 在弹出的窗口中，填写“推迟删除”的时间。

步骤 5 单击“确定”，完成批量删除密钥操作。

----结束

2.5.5 取消删除密钥

该任务指导用户在未超出删除密钥的推迟时间，通过密钥管理界面对用户主密钥进行取消删除操作，取消删除后密钥处于“禁用”状态。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 待取消删除的密钥需处于“计划删除”状态。

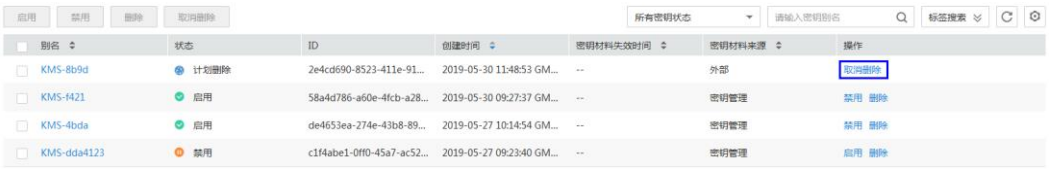
取消删除单个密钥

步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤 3 在需要取消删除的密钥所在行，单击“取消删除”。

图2-23 取消删除单个密钥



步骤 4 在弹出的窗口中，单击“确定”，完成取消删除单个密钥操作。

- 如果是通过 KMS 创建的密钥，取消删除后密钥状态为“禁用”，如需启用密钥，请参见 2.5.2 启用密钥操作。
- 如果是外部导入的密钥，且有密钥材料，取消删除后密钥状态为“禁用”，如需启用密钥，请参见 2.5.2 启用密钥操作。
- 如果是外部导入的密钥，且没有密钥材料，取消删除后密钥状态为“等待导入”，如需使用该密钥，请参见 2.2 导入密钥操作。

----结束

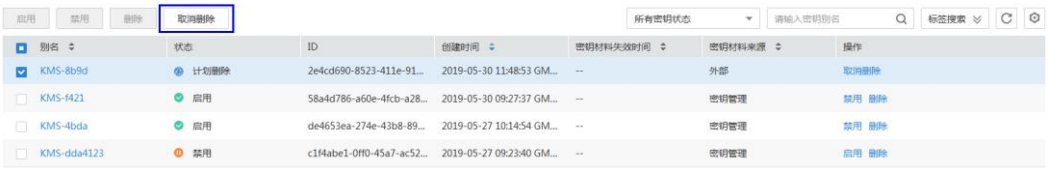
批量取消删除密钥

步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤 3 在密钥列表中，勾选所有需要取消删除的密钥，单击“取消删除”。

图2-24 批量取消删除密钥



步骤 4 在弹出的窗口中，单击“确定”，完成批量取消删除密钥操作。

- 如果是通过 KMS 创建的密钥，取消删除后密钥状态为“禁用”，如需启用密钥，请参见 2.5.2 启用密钥操作。
- 如果是外部导入的密钥，且有密钥材料，取消删除后密钥状态为“禁用”，如需启用密钥，请参见 2.5.2 启用密钥操作。
- 如果是外部导入的密钥，且没有密钥材料，取消删除后密钥状态为“等待导入”，如需使用该密钥，请参见 2.2 导入密钥操作。

----结束

3 专属加密

3.1 操作指引

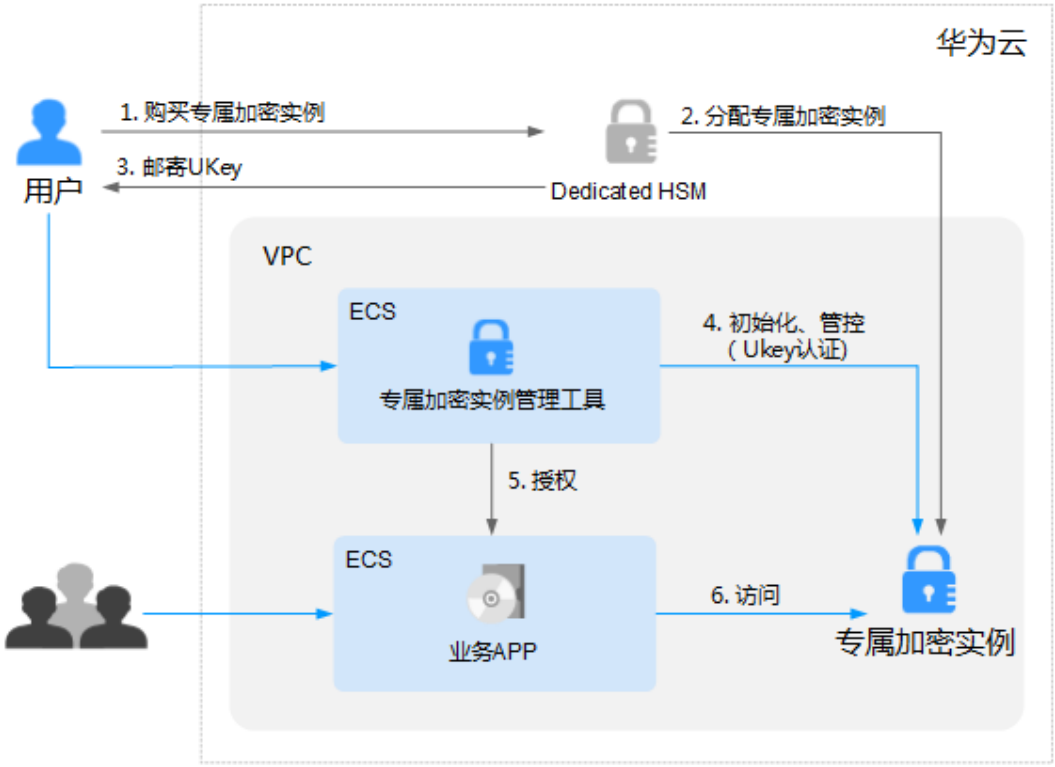
限制说明

- 专属加密实例需要配合虚拟私有云（VPC）一起使用。购买专属加密实例后，需要在管理控制台中实例化专属加密实例（配置 VPC 网络、安全组、网卡），才能正常使用。
- 专属加密实例出于安全性的考虑，不对公网提供服务，您需要将专属加密实例管理工具部署到与专属加密实例同一 VPC 网络中，才能对专属加密实例进行管理。

操作指引

当用户需要在云上使用专属加密服务时，可通过 Dedicated HSM 界面购买专属加密实例。购买专属加密实例后，当用户收到 Dedicated HSM 邮寄的 Ukey 后，通过 Ukey 初始化，并管控专属加密实例。用户通过专属加密实例管理工具授权业务 APP，允许业务用户通过业务 APP 访问专属加密实例。操作指引如图 3-1 所示。

图3-1 操作指引



操作指引说明如表 3-1 所示。

表3-1 操作指引说明

编号	操作步骤	说明	操作角色
1	购买专属加密实例	通过 Dedicated HSM 界面购买专属加密实例。	用户
2	分配专属加密实例	Dedicated HSM 分配专属加密实例给用户。	专属加密服务安全专家
3	邮寄 UKey 并提供配套初始化文档及软件	• 安全专家将通过您提供的 Ukey 收件地址将 Ukey 邮寄给您。 Ukey 是 Dedicated HSM 提供给您的身份识别卡，此卡仅购买专属加密实例的用户持有，请妥善保管。 • 安全专家将会为您提供初始化专属加密实例的软件及相关指导文档。 若您对软件或指导文档的使用有疑问，请联系安全专家进行指导。	专属加密服务安全专家

编号	操作步骤	说明	操作角色
4	初始化、管控（UKey认证）	1. 在专属加密实例管理节点上安装我们为您提供的管理工具。 2. 使用 Ukey 和管理工具初始化专属加密实例，并注册相应的管理员，管控专属加密实例，对密钥进行管理。 详细操作请参见初始化专属加密实例。	用户
5	安装安全代理软件并授权	在业务 APP 节点上安装我们为您提供的安全代理软件并执行相关初始化操作。 详细操作请参见安装安全代理软件并授权。	用户
6	访问	业务 APP 通过 API 或者 SDK 的方式访问专属加密实例。	用户

3.2 购买专属加密实例

该任务指导用户通过专属加密界面购买专属加密实例。

前提条件

已获取管理控制台的登录帐号与密码。

购买专属加密实例

步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务 > 专属加密”，默认进入专属加密服务界面。

步骤 3 在界面右上角，单击“购买专属加密实例”。

步骤 4 在“购买专属加密实例”页面中，选择“计费模式”。

图3-2 计费

步骤 5 选择“当前区域”和“可用区”。

图3-3 当前区域和可用区

步骤 6 填写网络信息，如图 3-4 所示，相关参数说明如表 3-2 所示。

图3-4 网络信息

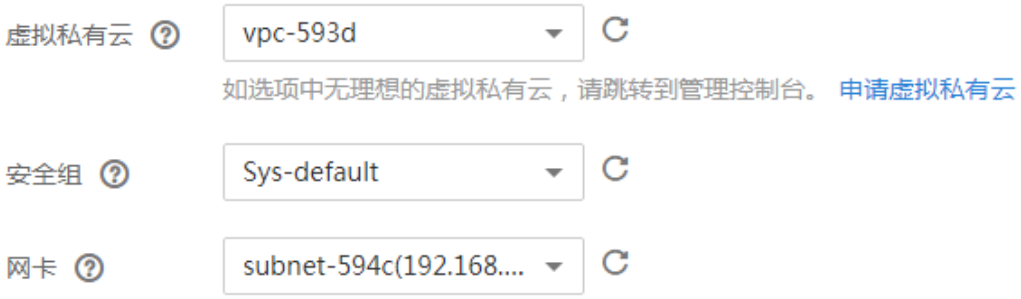


表3-2 网络参数说明

参数名称	说明	取值样例
虚拟私有云	可以选择使用已有的虚拟私有云（Virtual Private Cloud，VPC）网络，或者单击“申请虚拟私有云”创建新的虚拟私有云。 更多关于虚拟私有云的信息，请参见《虚拟私有云用户指南》。	vpc-sec
安全组	界面显示专属加密实例已配置的安全组。选择专属加密实例的安全组后，该专属加密实例将受到该安全组访问规则的保护。 更多关于安全组的信息，请参见《虚拟私有云用户指南》。	sg-533c
网卡	界面显示所有可选择的子网，系统自动分配一个未使用的 IP 地址。 更多关于子网的信息，请参见《虚拟私有云用户指南》。	subnet1（10.1..0.0/16）

步骤 7 选择专属加密实例的规格信息，如图 3-5 所示，相关参数说明如图 3-5 所示。

图3-5 规格信息

表3-3 规格参数说明

参数名称	说明	取值样例
服务版本	基础版专属加密实例在密码运算上独占加密卡资源、共享非密钥计算相关资源，满足用户基本加密需求。	基础版
功能类型	可选择的功能类型，包含“金融密码机”、“服务器密码机”和“签名服务器”。	金融密码机
加密算法	基础版专属加密实例支持的加密算法。 • 对称算法：SM1、SM4、DES、3DES、AES、SM7 * • 非对称算法：SM2、RSA（1024-4096）* • 摘要算法：SM3、SHA1、SHA256、SHA384 **说明** 带*条目不同型号设备略有不同，请联系客服进行确认。	-
性能规格	基础版专属加密实例支持的性能规格。 • 数据通讯协议：TCP/IP（最大并发链接：64） • SM1 加密运算性能：600tps • SM2 签名运算性能：3000tps • SM2 验签运算性能：2000tps	-

参数名称	说明	取值样例
	• RSA2048 验签运算性能：3500tps • RSA2048 签名运算性能：400tps • SM7 加密算法性能：1000tps * 说明 带*条目不同型号设备略有不同，请联系客服进行确认。	
费用构成	基础版专属加密实例 • 初装费用：无 • 包周期费用：无	-

步骤 8 设置专属加密实例购买的数量。

1. 选择“购买时长”。

   可以选择 1 个月～3 年的购买时长。

2. 设置“购买数量”。

   您可以根据您的需要设置购买数量。

   为了保证业务的高可靠性，建议至少购买 2 个及以上专属加密实例，构建专属加密实例高可用组，提高业务可靠性，单台专属加密实例不承诺 SLA。您最多可购买 20 个专属加密实例。

步骤 9 设置专属加密实例的名称。

步骤 10 填写“联系方式”信息，如图 3-6 所示。相关参数说明如表 3-4 所示。

图3-6 联系方式

表3-4 联系方式参数说明

参数名称	说明
业务联系人姓名	业务联系人的姓名。
业务联系人手机	业务联系人手机号码。
邮箱	输入邮箱地址。
Ukey 收件地址	输入收取 Ukey 的收件地址。

步骤 11 确认当前配置无误后，单击“立即购买”。

如果您对价格有疑问，可以单击“了解计费详情”，了解产品价格。

步骤 12 在“订单详情”页面，确认订单详情，阅读并勾选“我已阅读并同意《数据加密产品服务协议》”。

步骤 13 单击“去支付”。

步骤 14 在订单详情页面，单击“立即支付”。

步骤 15 在“订单列表”页面，选择付款方式进行付款。

成功付款后，在专属加密实例列表界面，可以查看购买的专属加密实例信息。

当专属加密实例的“状态”为“创建中”时，如图 3-7 所示，表示专属加密实例购买成功。

图3-7 购买专属加密实例成功

专属加密实例包含以下三种状态：

- 创建中：系统正在分配专属加密实例给用户，等待 5-10 分钟，可分配完成。
- 创建失败：资源不够或网络故障等原因可能导致创建专属加密实例失败。
- 运行中：系统给用户分配专属加密实例已完成，专属加密实例处于“运行中”。

----结束

3.3 查看专属加密实例

该任务指导用户通过专属加密界面查看专属加密实例信息，包括专属加密实例的名称、状态、服务版本、设备厂商、设备型号、IP 地址和到期时间。

前提条件

已获取管理控制台的登录帐号与密码。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务 > 专属加密”，默认进入专属加密服务界面。

步骤 3 在专属加密实例列表中，查看专属加密实例信息，如图 3-8 所示。

图3-8 专属加密实例列表

说明

- 可在“名称”下拉列表中，选择“名称”或者“设备型号”，输入专属加密实例的名称或者设备型号，单击 ，搜索对应的专属加密实例。
- 在专属加密实例处于“创建失败”或者“冻结”时，可单击该专属加密实例所在行的“删除”，删除专属加密实例。

专属加密实例列表参数说明，如表 3-5 所示。

表3-5 专属加密实例参数说明

参数	参数说明
名称/ID	专属加密实例的名称和 ID。
服务版本	基础版：用户享有共享机框和电源，在密码运算上独占加密卡的虚拟化专属加密实例。
状态	专属加密实例的状态： • 创建中 用户购买的专属加密实例后，系统正在分配专属加密实例给用户，专属加密实例处于“创建中”状态。 • 创建失败 资源不够或网络故障等原因可能导致创建专属加密实例失败，专属加密实例处于“创建失败”状态。 • 运行中 系统已将专属加密实例分配给用户，专属加密实例处于“运行中”状态。 • 冻结 用户购买的专属加密实例到期，且没有续费，专属加密实例处于

参数	参数说明
	“冻结”状态。
设备厂商	设备厂商的名称。
设备型号	设备型号。
IP 地址	IP 地址。
购买时间	购买专属加密实例的时间。
到期时间	购买的专属加密实例的到期时间。

步骤 4 用户可单击专属加密实例的名称，查看专属加密实例的详细信息，如图 3-9 所示。

图3-9 专属加密详细信息

专属加密实例详细信息参数说明，如表 3-6 所示。

表3-6 专属加密实例详细信息参数说明

参数	参数说明
名称	专属加密实例的名称。 可单击，修改专属加密实例的名称。
ID	专属加密实例的 ID。
状态	专属加密实例的状态： • 创建中 用户购买的专属加密实例后，系统正在分配专属加密实例给用户，专属加密实例处于“创建中”状态。

参数	参数说明
	• 创建失败 资源不够或网络故障等原因可能导致创建专属加密实例失败，专属加密实例处于“创建失败”状态。 • 运行中 系统已将专属加密实例分配给用户，专属加密实例处于“运行中”状态。 • 冻结 用户购买的专属加密实例到期，且没有续费，专属加密实例处于“冻结”状态。
服务版本	基础版：用户享有共享机框和电源，在密码运算上独占加密卡的虚拟化专属加密实例。
可用区	专属加密实例所在的可用分区。
设备厂商	设备厂商的名称。
设备型号	设备型号。
功能类型	专属加密实例的功能类型，包含“金融密码机”、“服务器密码机”和“签名服务器”。
虚拟私有云	专属加密实例所在虚拟私有云。 更多关于虚拟私有云的信息，请参见《虚拟私有云用户指南》。
子网	专属加密实例所在的子网。 更多关于子网的信息，请参见《虚拟私有云用户指南》。
IP	子网内的私有 IP 地址。
安全组	专属加密实例所在的安全组。 更多关于安全组的信息，请参见《虚拟私有云用户指南》。
创建时间	购买专属加密实例的时间。
到期时间	购买的专属加密实例到期的时间。
所属订单	购买专属加密实例的订单号，可单击订单号，查询订单详情。
计费模式	包年/包月计费。

----结束

3.4 使用专属加密实例

在您支付完成后，我们会根据您反馈的邮寄地址，将初始化专属加密实例的 Ukey 邮寄给您，请您耐心等待。同时，专属加密服务安全专家会通过您提供的联系方式，与您

取得联系，将配套的软件及相关指导文档发送给您。软件分为两类，一类用于管理云加密实例；另一类是业务调用时依赖的安全代理软件和 SDK。

前提条件

在实例化专属加密实例后，用户需要获取以下信息，初始化专属加密实例、安装安全代理软件并授权。

表3-7 信息获取

名称	说明	来源
Ukey	保存专属加密实例的权限管理信息。	订单付款后，且实例化专属加密实例成功后，由专属加密服务邮寄到您的 Ukey 收件地址。
专属加密实例管理工具	配合 Ukey，远程管理专属加密实例。	安全专家会通过您提供的联系方式联系您，将配套的软件和相关指导文档发送给您。
专属加密实例配套文档	《专属加密实例用户手册》和《专属加密实例安装手册》。	
安全代理软件	与专属加密实例建立安全通道。	
SDK	用于提供专属加密实例的 API 接口，用户通过调用 SDK 与专属加密实例建立安全连接。	
专属加密实例管理节点（例如：ECS）	运行专属加密实例管理工具，与专属加密实例处于同一 VPC，并分配弹性 IP 地址用于远程连接。	请您根据自己的需要进行购买。
业务 APP 节点（例如：ECS）	运行安全代理软件和用户的业务 APP，与专属加密实例处于同一 VPC。	

初始化专属加密实例

以使用 Windows 镜像的 ECS 作为专属加密实例管理节点为例，初始化专属加密实例操作步骤如下所示。

步骤 1 购买一台 Windows 镜像的 ECS 作为专属加密实例管理节点。

1. 登录管理控制台。
2. 单击页面上方的“服务列表”，选择“计算 > 弹性云服务器”，进入弹性云服务器列表界面。
3. 单击“购买弹性云服务器”。
   - 区域、可用区：请与购买的专属加密实例保持一致。

- 镜像：请选择 Windows 公共镜像。
- VPC：请与专属加密实例所在 VPC 保持一致。
- 弹性公网 IP：为方便在您本地实例化加密机，请绑定弹性公网 IP。

说明
待初始化专属加密实例完成后，您可以解绑弹性公网 IP。若后续有需要，可重复绑定、解绑操作。

- 其他参数请根据实际情况进行选择。

步骤 2 根据收到的管理工具及配套文档，初始化专属加密实例。

步骤 3 初始化完成后，可通过管理工具进行生成、销毁、备份、恢复秘钥等操作。

说明
初始化和管理过程中有任何问题，请咨询专属加密服务安全专家。

详细信息请参见专属加密实例配套文档《专属加密实例用户手册》和《专属加密实例安装手册》。

----结束

安装安全代理软件并授权

用户需要在业务 APP 节点上安装安全代理软件，使业务 APP 与专属加密实例建立安全通道。

步骤 1 在管理工具上下载访问专属加密实例的证书。

步骤 2 在业务 APP 节点上安装安全代理软件。

步骤 3 将证书导入到安全代理软件，授予业务 APP 访问专属加密实例的权限。

步骤 4 业务 APP 即可通过 SDK 或者 API 接口的方式访问专属加密实例。

说明
您可以在安全代理软件配置多个专属加密实例，实现负载均衡功能。

----结束

4 常见问题

4.1 密钥管理类

4.1.1 为什么不能立即删除用户主密钥？

删除密钥是一个需要非常谨慎的操作。操作前，用户需确保使用该密钥加密的相关数据都已完成迁移。因为密钥一旦被删除，所有使用该密钥加密的相关数据都无法解密。因此在删除密钥时，KMS 会将该操作推迟 7 天到 1096 天执行，推迟时间由用户指定。超过推迟时间，密钥才会被真正删除。在密钥被真正删除之前，如果用户发现该密钥仍然有用，可取消删除操作。KMS 通过这种方式来减少用户误操作所带来的损失。

4.1.2 KMS 中创建的用户主密钥长度是多少？

通过 KMS 创建的用户主密钥长度为 256bit。

4.1.3 是否可以从 KMS 中导出用户主密钥？

不可以。

为确保用户主密钥的安全，用户只能在 KMS 中创建和使用用户主密钥，无法导出用户主密钥。

4.1.4 如果用户主密钥被彻底删除，用户数据是否还可以解密？

不可以。

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；若用户主密钥没有被彻底删除，则可以通过 KMS 界面取消删除用户主密钥。

4.1.5 如何使用在线工具加解密数据？

使用在线工具加解密小数据的操作步骤如下所示：

加密数据

步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤 3 单击目标用户主密钥的别名，进入密钥详细信息在线工具加密数据页面。

步骤 4 在“加密”文本框中输入待加密的数据，如图 4-1 所示。

图4-1 加密数据

步骤 5 单击“执行”，右侧文本框显示加密后的密文数据。

说明

- 加密数据时，使用当前指定的密钥加密数据。
- 用户可单击“清除”，清除已输入的数据。
- 用户可单击“复制到剪切板”拷贝加密后的密文数据，并保存到本地文件中。

----结束

解密数据

步骤 1 登录管理控制台。

步骤 2 单击页面上方的“服务列表”，选择“安全 > 数据加密服务”，默认进入数据加密服务的“密钥管理”界面。

步骤 3 解密数据时，可单击任意“启用”状态的非默认主密钥别名，进入该密钥的在线工具页面。

步骤 4 单击“解密”，在左侧文本框中数据待解密的密文数据，如图 4-2 所示。

说明

- 在线工具自动识别并使用数据被加密时使用的密钥解密数据。
- 若该密钥已被删除，会导致解密失败。

图4-2 解密数据

步骤 5 单击“执行”，右侧文本框中显示解密后的明文数据。

说明
用户可直接单击“复制到剪切板”拷贝解密后的明文数据，并保存到本地文件中。

----结束

4.1.6 是否可以更新 KMS 管理的密钥？

不可以。

通过 KMS 创建的密钥无法更新，用户只能通过 KMS 创建新密钥，使用新的密钥加解密数据。

4.1.7 在什么场景下推荐使用导入的密钥？

- 如果用户不想使用 KMS 中创建的密钥材料，而使用自己的密钥材料，并且可以随时删除密钥材料，或者密钥材料被意外删除，用户可以重新导入相同的密钥材料的情况下，推荐用户使用导入的密钥。
- 当用户把本地的加密数据迁移到云上时，想在云上云下共用一个密钥材料时，可以把云下的密钥材料导入到 KMS。

4.1.8 可以导入哪些类型的密钥？

用户可以导入 256 位对称密钥。

4.1.9 密钥材料被意外删除时如何处理？

如果密钥材料被意外删除，用户可以在原用户主密钥下将备份的密钥材料重新导入 KMS。

注意

导入密钥材料时需要及时备份，重新导入的密钥材料必须与被意外删除的密钥材料保持一致，否则导入会失败。

4.2 专属加密类

4.2.1 什么是专属加密？

专属加密（Dedicated Hardware Security Module，Dedicated HSM）是一种云上数据加密的服务，可处理加解密、签名、验签、产生密钥和密钥安全存储等操作。

Dedicated HSM 为您提供经国家密码管理局检测认证的加密硬件，帮助您保护弹性云服务器上数据的安全性与完整性，满足监管合规要求。同时，您能够对专属加密实例生成的密钥进行安全可靠的管理，也能使用多种加密算法来对数据进行可靠的加解密运算。

4.2.2 如何获取身份识别卡（Ukey）？

购买专属加密实例后，需要使用身份识别卡（Ukey）来进行实例的管理。

请在专属加密实例购买界面，通过提交工单的方式，反馈 Ukey 邮寄地址。专属加密服务专家会尽快将身份识别卡(USB key)邮寄给您。

4.2.3 用户本地部署的加密机如何迁移到云上专属加密服务？

用户需要联系专属加密服务专家及本地加密机厂家，详细核对当前使用的接口、功能等规格参数，制定迁移方案，确保本地密钥能够批量、安全地迁移到云上进行平滑过渡。

4.2.4 专属加密如何保障密钥生成的安全性？

- 密钥是由用户自己远程创建，且创建过程需要仅用户持有的 Ukey 参与认证。
- 加密机的配置和内部密钥的准备，都必须要使用这一组 Ukey 作为鉴权凭证才能操作。

用户作为设备使用者完全控制密钥的产生、存储和访问授权，Dedicated HSM 只负责监控和管理设备及其相关网络设施。

4.2.5 机房管理员是否有超级管理权限，在机房插入特权 Ukey 窃取信息？

机房管理员没有超级管理权限，Ukey 是 Dedicated HSM 提供给您的身份识别卡，此卡仅购买专属加密实例的用户持有。

敏感数据（密钥）存储在国家规定的硬件加密卡中，即使加密机制造商也无法读取内部密钥信息。

A 修订记录

发布日期	修改说明
2018-12-30	第一次正式发布。

