阿里云
云盾加密服务

用户手册

金融加密机

20180831

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表本文档中的内容。此外，未经阿里云事先书面同意，任何人不得为了任何

营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

7. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止**： 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告**： 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	 **说明**： 导出的数据中包含敏感信息，请妥善保存。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明**： 您也可以通过按**Ctrl** + **A**选中全部文件。
>	多级菜单递进。	**设置** > **网络** > **设置网络类型**
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
courier字体	命令。	执行 cd /d C:/windows 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	bae log list --instanceid *Instance_ID*
[]或者[a|b]	表示可选项，至多选择一个。	ipconfig *[-all|-t]*
{}或者{a|b}	表示必选项，至多选择一个。	swich *{stand | slave}*

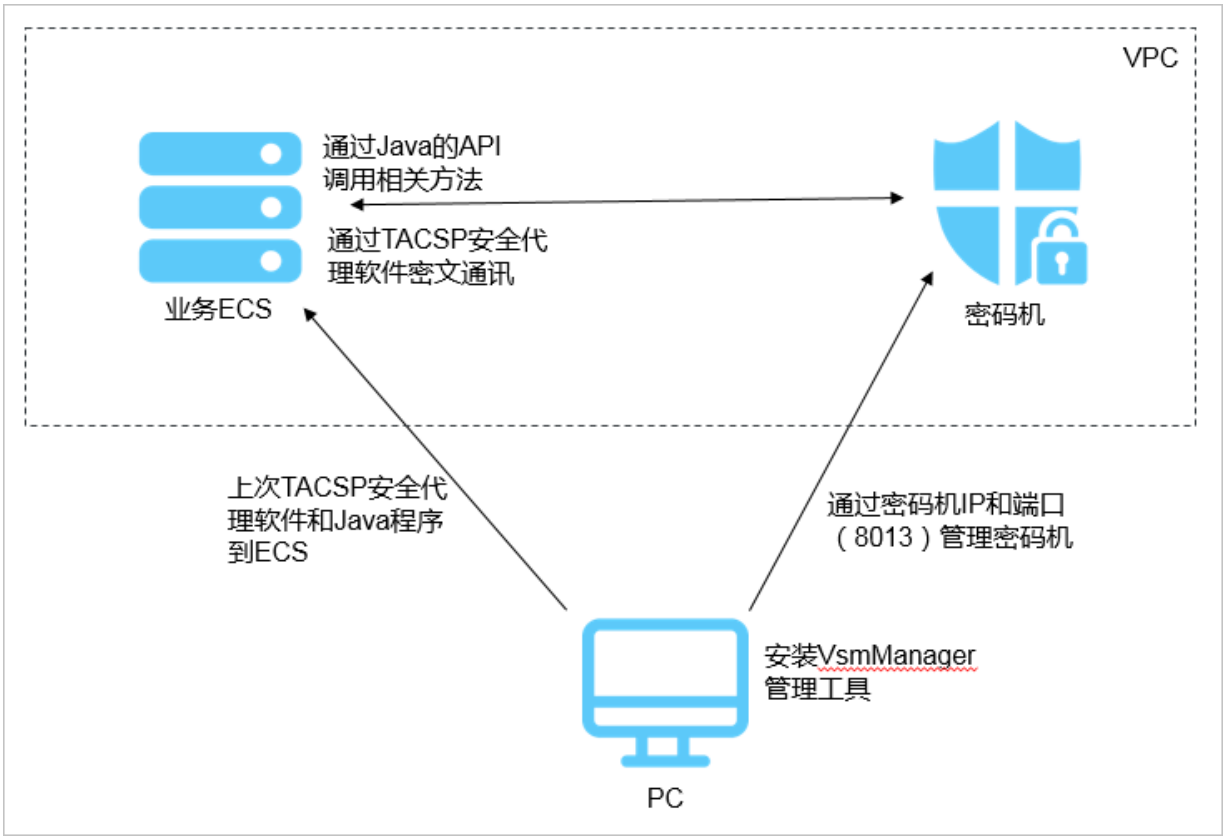
目录

1 加密服务

1.1 概述

加密服务是一款云上加密解决方案。服务底层使用经国家密码管理局检测认证的硬件密码机，通过虚拟化技术，帮助用户满足数据安全方面的监管合规要求，保护云上业务数据的隐私性要求。借助加密服务，用户能够对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。

加密服务组网如下，ECS和密码机在VPC网络中。



加密服务提供以下功能：

- 密钥管理：密钥的安全存储和使用、分散产生子密钥、安全报文形式的导入导出。
- 数据加密：全面支持国产算法以及部分国际通用密码算法，满足用户各种加密算法需求。
- 数据MAC计算：支持PBOC规范中定义的不同算法MAC运算。
- 交易认证：遵循PBOC2.0/3.0规范的ARQC验证和ARPC产生运算。

1.2 快速入门

1.2.1 使用流程

本章节介绍了如何快速开始加密服务功能。

具体步骤如下：

1. 注册管理员*UKEY*

   登录之前，需要先注册管理员UKEY。管理员UKEY主要用途包括用户开机、协商通讯和管理工具与密码机通讯运算。

2. 登录*VsmManager*管理工具

   使用管理员UKEY登录VsmManager管理工具。

3. 执行原始初始化

   完成原始初始化，制作主密钥成份UKEY和授权UKEY，并合成设备主密钥（DMK）。

4. 授权操作

   需要授权后才能进行设备管理和主机服务。

5. 生成密钥

   在加密机中生成密钥，本章节以生成对称密钥为例。

6. 配置主机端口属性

   配置加密机的通讯方式，使用密文通讯提升安全性和可靠性。

7. 签发应用许可

   生成TACSP的应用许可证。

8. 配置*TACSP*

   在ECS上安装和配置TACSP。

9. 配置密文通讯

   配置加密机和ECS之间使用密文通讯。

10. 创建*Demo*实例

    在Eclipse上创建Demo实例，调用加密API。

1.2.2 创建和配置加密实例

该章节介绍了如何创建和配置加密实例。

操作步骤

1. 登录云盾安全中心。
2. 定位到**加密服务** > **实例列表**页面，单击**创建实例**。
3. 选择加密实例的**区域**、**虚拟网络**、**设备厂商**和**设备型号**等信息。
4. 单击**创建实例**，完成加密实例的创建。
5. 在新创建加密实例的**操作**栏，单击**配置**。
6. 在**配置IP**对话框中，配置VPC网络和IP地址。

配置项	说明
所属的VPC网络ID	选择VPC网络，加密服务需要和应用服务器属于同一个VPC。
所属的VPC子网	选择VPC子网网段。
分配私网IP地址	设置私网IP，该IP需要在**所属的VPC子网**的网段中。

7. 单击**确定**，完成加密实例的配置。

1.2.3 注册管理员UKEY

该章节介绍了如何注册管理员UKEY。

前提条件

PC能够访问密码机所在的VPC网络。

背景信息

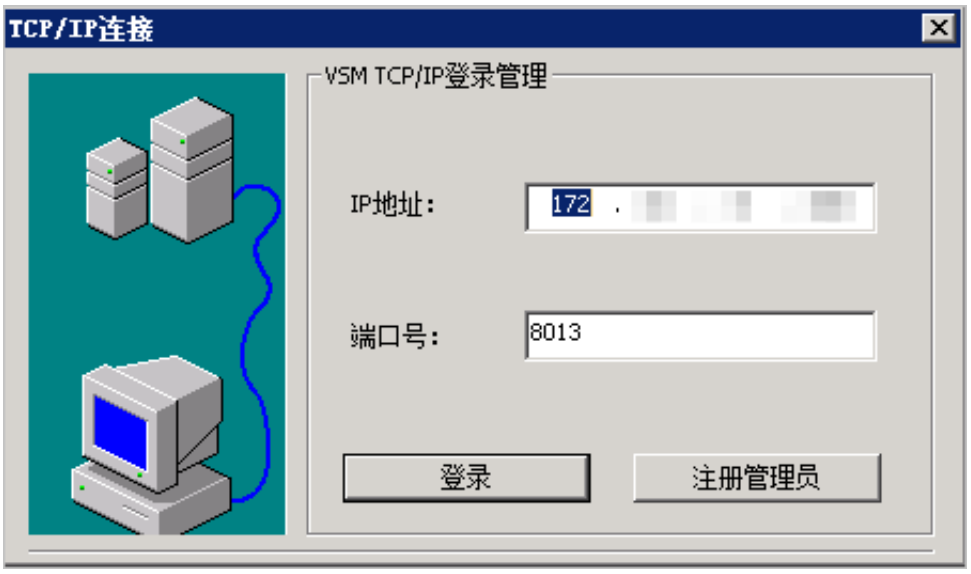
在登录VsmManager管理工具时，需要先注册管理员UKEY。

管理员UKEY用途包括：用户开机、协商通讯、管理工具与密码机通讯运算。

操作步骤

1. 在PC上双击*VsmManager.exe*管理工具。
2. 单击**系统** > **VSM登录管理**。
3. 在**TCP/IP连接**对话框中，输入密码机的IP和端口号。

> **说明**：
> 端口固定为8013。



4. 在PC上插入空UKEY，单击**注册管理员**。
5. 在**UKEY列表**窗口中选择插入的空UKEY，单击**确定**。

6. 在**VERIFY**对话框中，输入UKEY口令，单击**确定**。

> **说明**：
> 出厂初始的UEKY口令为12345678。

完成管理员UKEY的注册。

1.2.4 登录VsmManager管理工具

该章节介绍了如何登录VsmManager管理工具。

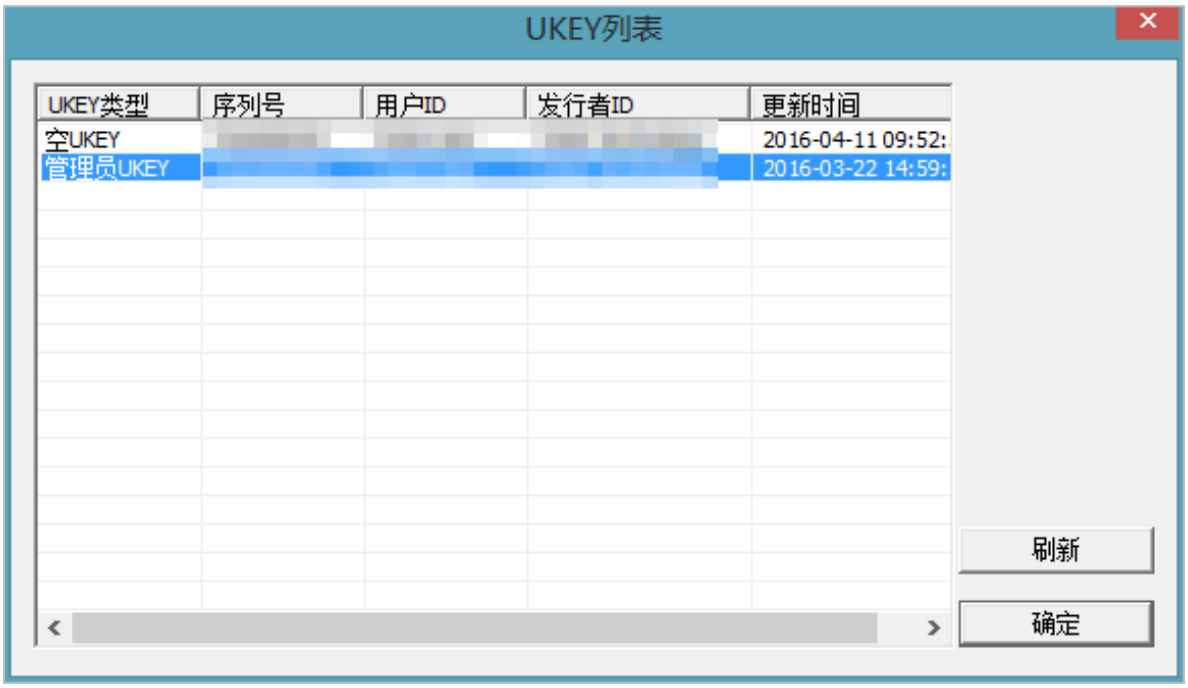
背景信息

如果在没有注册UKEY管理员的情况下直接登录系统，您将不能进行原始初始化和恢复初始化操作，仅可以在测试主密钥的环境下进行密钥管理。

操作步骤

1. 在PC上插入管理员UKEY。
2. 双击*VsmManager.exe*管理工具。
3. 单击**系统** > **VSM登录管理**。
4. 在**TCP/IP连接**对话框中，输入密码机的IP和端口号。

   说明：
   端口固定为8013。
5. 单击**登录**。
6. 在弹出的**UKEY列表**窗口中，选择**管理员UKEY**，单击**确定**。



7. 在**VERIFY**对话框中，输入UKEY口令，单击**确定**。
8. 在登录成功确认框中，单击**确定**。

   登录成功后，进入VsmManager管理工具。

1.2.5 执行原始初始化

该章节介绍如何进行原始初始化。

背景信息

密码机要投入生产环境时，必须先完成原始初始化操作，制作主密钥成份UKEY和授权UKEY，并合成设备主密钥（DMK）。

在进行原始初始化前，请规划好以下项目：

规划项目	说明	举例
设备主密钥（DMK）管理人员	需要几个DMK管理员持有主密钥成份UKEY。 取值范围：2~8	本章节以配置2个为例。
设备授权控制人员	需要几个设备授权控制人员持有授权UKEY。 取值范围：1、3、5	本章节以配置1个为例。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**密钥管理** > **原始初始化**。

   说明：
   如果进行原始初始化操作，密码机将清除内部的全部密钥。

3. 在**安全操作警示**提示框中，单击**下一步**。
4. 在**请输入成份数目**中输入*2*，单击**下一步**。

   根据规划的设备主密钥（DMK）管理人员，确定主密钥成份UKEY数目，设置范围为2~8。本章节以2个为例。

5. 依次制作2个主密钥成份UKEY，单击**下一步**。

a) 第一个主密钥管理员两次输入预定义的秘密值，或者单击**随机秘密值**。

- 手动设置秘密值为：8-32个任意字符。
- 自动的随机秘密值为：32个任意字符。

b) PC上插入空UKEY。

c) 单击**产生成份UKEY**。

d) 在弹出的**UKEY列表**中，选择刚才插入的空UKEY，单击**确定**。

e) 在**VERIFY**对话框中，输入UKEY口令，单击**确定**。

通过系统计算得到的成份数据写入UKEY中。

f) 参考步骤*5.a*~步骤*5.e*，制作第二个主密钥成份UKEY。

6. 依次导入2个主密钥成份UKEY到系统，单击**下一步**。

a) 单击**导入成份**。

b) 在**UKEY列表**中，第一个主密钥管理员选择自己的主密钥成份UKEY，单击**确定**。

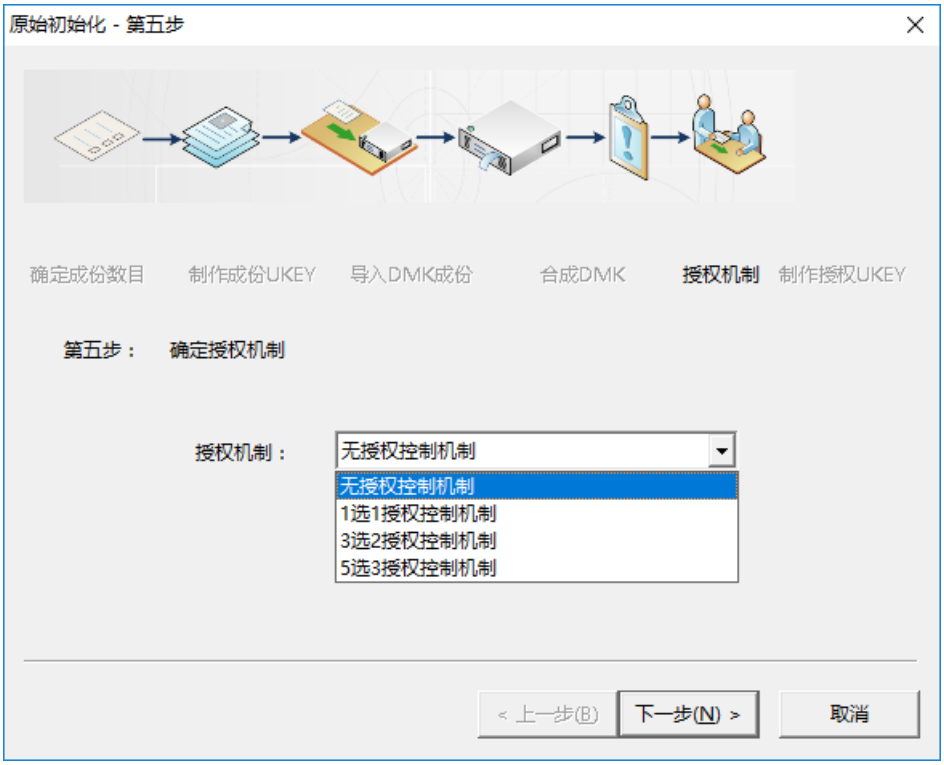
系统将读取UKEY内的成份数据。

c) 参考步骤*6.a*~步骤*6.b*，导入第二个主密钥成份UKEY。

> **说明**：
> 主密钥成份UKEY的导入次序没有要求，但不能将同一个主密钥成份UKEY多次导入。

7. 单击**合成DMK**，完成后单击**下一步**。

8. **授权机制**选择*1*选*1*授权控制机制，单击**下一个**。



本章节以选择*1*选*1*授权控制机制为例，所有可选的授权机制如下：

授权机制	说明
无授权机制	不需要授权。

授权机制	说明
1选1授权控制机制	1个授权UEKY由1个授权人员保管，当为某类操作授权时，需1个授权人员授权许可。
3选2授权控制机制	m选n授权控制机制，制作m个授权UKEY由m个授权人员保管，当为某类操作授权时，需半数以上的授权人员授权许可，即n个授权UKEY认证通过。
5选3授权控制机制	

9. 制作授权UKEY。

   a) PC上插入空UKEY。

   b) 单击**制作授权卡**。

   c) 在**UKEY列表**中，选择插入的空UKEY，单击**确定**。

   d) 在**VERIFY**对话框中，输入UKEY口令，单击**确定**。

   e) （可选）参考步骤*9.a*~步骤*9.d*，依次制作余下授权UKEY。

      如果选择多个授权UKEY，需要根据提示依次制作授权UKEY。

10. 单击**完成**。

    完成原始初始化，密码机生成新的主密钥DMK。

1.2.6 授权操作

该章节介绍如何进行授权。

背景信息

部分设备管理操作和主机指令应用需要获取授权许可，密码机支持严格灵活的授权管理控制。授权具有以下优点：

- 授权机制可配置

  支持1选1、3选2、5选3和无授权控制机制。授权控制机制需在初始化的过程中设置，完成初始化后不允许被修改。

- UKEY授权机制

  通过验证授权UKEY完成对授权人员的身份识别，安全可靠。

- 分类分时授权控制

  通过授权UKEY验证后，可选择本次授权的操作类别及给予授权的时间，当某类操作授权的时效过期后，其授权许可将自动失效。

说明：

初始化时，如果**授权机制**配置为无授权控制机制，所有的操作均不受限。则本章节不需要设置。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备管理** > **操作授权**。
3. 根据提示依次插入授权UKEY，输入口令，单击**下一步**。

   系统将根据授权机制要求半数以上的授权UKEY验证通过。授权UKEY的验证次序无关，但重复验证无效。
4. 配置授权操作信息。

   可同时为多个类别授权不同的时限。

表 1-1: 授权类别说明

主类	子类	操作范围说明
设备管理	设备配置更新	重置端口属性，包括主机服务端口。
	应用密钥管理	• 随机产生内部存储的密钥。 • 成份形式合成对称密钥。 • 删除内部对称或非对称密钥。 • 清除内部对称或非对称密钥。

主类	子类	操作范围说明
		• 内部密钥备份导出。
主机服务	账户PIN解密	使用BA/NG主机命令。
	产生公钥MAC	使用EO/TQ主机命令。
	内部密钥更新	• KR/KD/KI/SI/TW/TY，内部存储模式的对称密钥的产生或导入。 • EI/EK/EJ/TS，内部存储模式的RSA密钥对的产生或导入。 • E0/E1/TU，内部存储模式的SM2密钥对的产生或导入。

5. 单击**完成**。

1.2.7 生成密钥

该章节介绍如何生成密钥。

前提条件

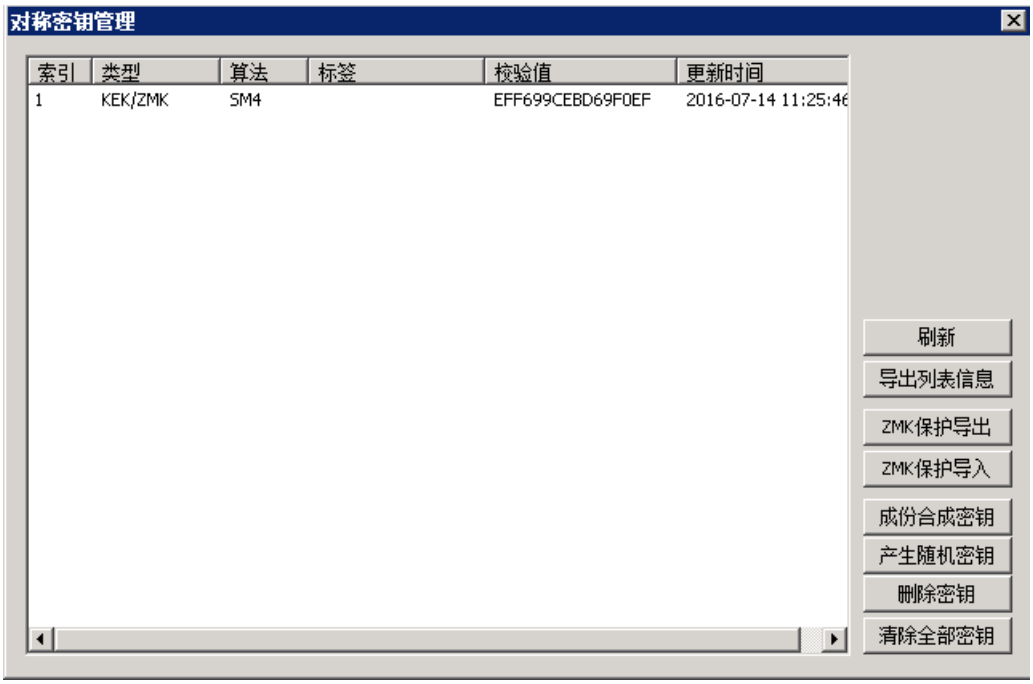
需要获取**应用密钥管理**的授权许可，具体操作参见授权操作。

背景信息

本章节以生成对称加密密钥为例，如果想生成非对称密钥，请参见产生随机密钥。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**密钥管理** > **管理对称密钥**。



3. 单击**产生随机密钥**。
4. 在对话框中配置对称密钥参数。

表 1-2: 对称密钥参数

配置项	说明
算法标识	密码机支持多种对称密码算法，使用时根据其算法标识使用相应的密码算法。标识如下： • *Z*：单倍长的DES算法密钥。 • *U*：双倍长的3DES算法密钥，LMK加密输出时使用变量方式。 • *T*：三倍长的3DES算法密钥，LMK加密输出时使用变量方式。

配置项	说明
	• *X*：双倍长的3DES算法密钥。 • *Y*：三倍长的3DES算法密钥。 • *P*：SM1算法密钥。 • *R*：SM4算法密钥。 • *L*：AES-128算法密钥。 • *M*：AES-192算法密钥。 • *N*：AES-256算法密钥。
密钥类型	不同密钥类型具有不同的用途。
存储到密码机内索引	生成的密钥是否存储到密码机索引。
密钥索引	勾选**存储到密码机内索引**后，设置索引号。 取值范围：1~2048
密钥标签	用于在密钥内部存储时标记密钥的标签说明。
LMK加密的新密钥密文	生成的密钥密文。
新密钥校验码	新密钥的校验码。

5. 单击**产生**。

   产生新的随机密钥并输出显示密文和校验值。

1.2.8 配置主机端口属性

该章节介绍如何配置主机端口属性。

背景信息

密码机和ECS之间的服务通讯方式出厂默认配置为明文通讯。

若要配置为密文通讯，则主机端口属性需要设置为密文通讯，同时还需要在TACSP安全代理软件进行相应的配置，以保证应用能够正常调用密码服务。密文通讯服务配置，参见配置密文通讯。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备管理** > **主机服务端口属性**。
3. 设置主机端口属性。

   说明：
   需要根据实际需求正确配置主机端口属性。

表 1-3: 主机端口属性

属性	说明
Socket KeepAlive时间	TCP连接保活探测时间，单位：秒。 取值范围：60~600
消息报文头长度	主机报文消息头长度，单位：字节。 取值范围：60~600
消息报文编码格式	主机报文的编码格式。 • ASCII • EBCDIC
主机服务通讯方式	• 明文通讯：与主机服务间的通讯为明文。 • 密文通讯：与主机服务间的通讯为密文。

1.2.9 签发应用许可

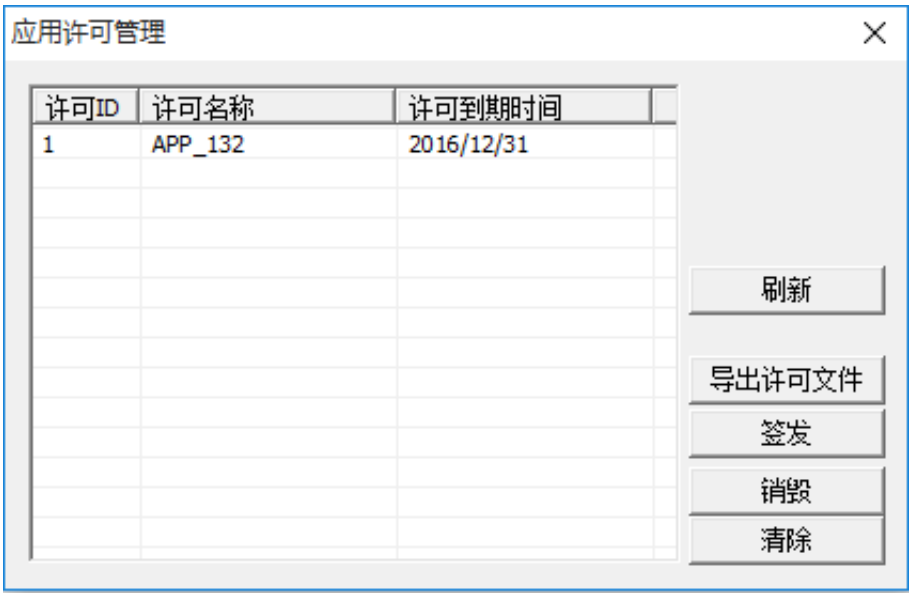
该章节介绍如何签发应用许可。

背景信息

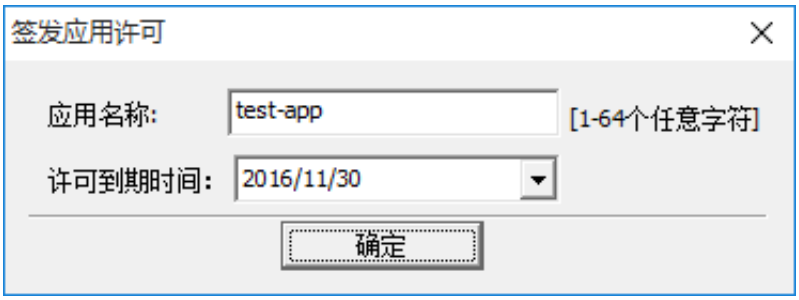
配置密文通讯时，需要为TACSP签发应用许可。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备管理** > **应用许可管理**。
3. 单击**签发**。



4. 设置应用名称和到期时间。



5. 单击**确定**。

生成应用许可文件（*.license*后缀的文件），并自动导出到VsmManager管理工具所在目录。

1.2.10 配置TACSP

该章节介绍如何配置TACSP安全代理软件。TACSP安全代理软件基于密码机的安全应用而设计开发的安全代理软件，是集多机热备、负载均衡功能为一体的密码机应用平台。

前提条件

ECS和密码机在同一个VPC网络中。

背景信息

TACSP安全代理软件支持的操作系统和加密方式如下。

- 操作系统：支持Linux、AIX、HP-UNIX等类UNIX操作系统。
- 加密方式：支持以Socket方式提供密码安全服务，应用程序通过socket方式访问安全代理软件。

操作步骤

1. 通过FTP软件上传TACSP安全代理软件到业务ECS。
2. 通过SSH登录业务ECS。
3. 进入TACSP所在路径。
4. 配置*tacsp_cfg.ini*。

   *tacsp_cfg.ini*配置文件内容如下：

```
[TACSP_IPC]
COMMAND_QUEUE_KEY           = 130
RESPONSE_QUEUE_KEY          = 131
SHARED_MEMORY_KEY           = 132
LOG_LEVEL                   = 1

[TACSP_SERVERINFO]
LISTEN_IP_FLG               = 0
LISTEN_PORT                 = 9999
HSM_LOADSIZE                = 2
HSM_LOADSELF                = 0

[TACSP_HSMINFO]
HSM_COUNT                   = 0
TOTAL_TIMEOUT               = 6
SINGLEHSM_TIMEOUT           = 2

[TACSP_HSM00]
HSM_TYPE                    = SJJ1310
HSM_IP                      = 192.168.19.51
HSM_PORT                    = 8018
HSM_WEIGHT                  = 10
HSM_ENC_COMM                = 0

[TACSP_HSM01]
HSM_TYPE                    = SJJ1310
HSM_IP                      = 192.168.119.102
HSM_PORT                    = 8018
HSM_WEIGHT                  = 10
HSM_ENC_COMM                = 1
```

表 1-4: 配置说明

节点	键名	说明
TACSP_IPC	-	TACSP使用的IPC相关ID。
	COMMAND_QUEUE_KEY	TACSP使用2个队列和1个共享内存。 此处配置的队列ID和共享内存ID，必须确保与当前系统中的相关ID不冲突。 取值范围：1~65537
	RESPONSE_QUEUE_KEY	
	SHARED_MEMORY_KEY	
	LOG_LEVEL	日志级别：

节点	键名	说明
		• *0*：不记录任务日志。 • *1*：记录错误日志。 • *2*：记录连接信息。 • *3*：记录调试信息日志。
TACSP_SERVERINFO	-	对外提供socket服务配置信息。
	LISTEN_IP_FLG	• *0*：默认值，监听127.0.0.1 • *1*：监听0.0.0.0
	LISTEN_PORT	负载热备对外提供的监听端口。 取值范围：1025~65535
	HSM_LOADSIZE	头部中表示报文长度的字节数。
	HSM_LOADSELF	头部表示报文长度中是否包含自身长度： • *0*：不包含 • *1*：包含
TACSP_HSMINFO	-	密码机相关信息
	HSM_COUNT	密码机数量。 取值范围：1~20
	TOTAL_TIMEOUT	每次socket通讯总的超时时间，单位：秒。 建议取值：加密机个数 * 单台加密机通讯超时 + 2
	SINGLEHSM_TIMEOUT	每台加密机每次socket通讯的超时时间，单位：秒。
TACSP_HSM*xx*	-	某索引密码机的信息，有n个密码机，必须有n个节配置。 *xx*取值范围：00~（n-1）
	HSM_TYPE	密码机类型
	HSM_IP	密码机的IP地址
	HSM_PORT	密码机的端口号
	HSM_WEIGHT	密码机的工作权重，即安全代理软件和此台加密机有多少个socket连接。

节点	键名	说明
		取值范围：1~65
	HSM_ENC_COMM	和密码机的通讯模式： • *0*：明文通讯 • *1*：密文通讯

5. （可选）配置环境变量TACSPCFG和CLUSTERDEBUG环境变量。

   说明：
   如不配置TACSPCFG，则配置文件必须在TACSP安全代理软件所在的路径下；如不CLUSTERDEBUG配置，则日志将默认输出在TACSP安全代理软件所在的路径下。

   a) 编辑*/etc/profile*。

   ```
   # vi /etc/profile
   ```

   b) 在*/etc/profile*中添加变量。

   ```
   export TACSPCFG=tacsp_cfg.ini所在目录
   export CLUSTERDEBUG=日志存储目录
   ```

   c) 使环境变量立即生效。

   ```
   source /etc/profile
   ```

1.2.11 配置密文通讯

该章节介绍如何配置密文通讯。

背景信息

密文通讯方式是指应用主机与密码机之间的通讯采用加密的方式，能够在专有云的环境下提供更安全更可靠的加密服务。

操作步骤

1. 配置主机端口属性。

   主机服务通讯方式修改为密文通讯。

2. 签发应用许可证。

   应用许可的内容包括VSM设备公钥、TACSP公私钥、应用名称、签发时间、到期时间及设备私钥对前述内容的签名。

说明：

如果有多个密码机，分别导出应用许可证。

3. 应用许可证通过FTP上传到TACSP安全代理软件所在路径。
4. 导入应用许可证。
   a) SSH登录ECS并进入TACSP安全代理软件所在路径。
   b) 执行**./keyMng**。

```
================== TACSP Manager-3.11 ============
|                                                  |
|    11. Start TACSP Server.                       |
|    12. Stop TACSP Server.                        |
|    13. Restart TACSP Server.                     |
|                                                  |
|    31. Import License File.                      |
|                                                  |
|    0. exit.                                      |
|                                                  |
==================================================
Please select:
```

   c) 输入*31*，按回车键（Enter）。

   开始导入应用许可证。

```
================== TACSP Manager-3.11 ============
|                                                  |
|    11. Start TACSP Server.                       |
|    12. Stop TACSP Server.                        |
|    13. Restart TACSP Server.                     |
|                                                  |
|    31. Import License File.                      |
|                                                  |
|    0. exit.                                      |
|                                                  |
==================================================
Please select:31

Enter License name: test-app
```

   d) 输入许可证名称，按回车键（Enter）。
   e) （可选）重复步骤*4.c*~步骤*4.d*，导入其他加密机的应用许可证。

   如果有多台密码机，则需要依次导入其他密码机的应用许可证。

f) 输入*11*，启动TACSP安全代理软件。

如果TACSP已经启动，则输入*13*，重启TACSP。

1.2.12 创建Demo实例

该章节介绍如何创建Java的Demo实例。

背景信息

VsmManager管理工具和密文通讯方式配置完成后，您就可以通过调用API接口，使用加密服务。

本章节创建JAVA的Demo实例后，您可以通过JAVA源文件了解如何调用加解密的API接口，实例说明参见*Demo实例说明*。

操作步骤

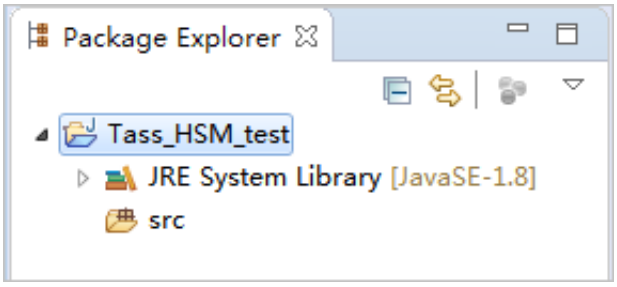
1. 在Eclipse中新建Java工程。

   a) 单击**File** > **New** > **Java Project**。

   b) 在**Project name**中输入工程名称。

   c) 单击**Finish**。

   创建Java工程实例如下所示。

2. 导入jar包。

   加密服务需要的3个jar包：

   - *TassHsmApihsmGeneralFinance_1.47.2529.jar*
   - *TassHsmDriver_SJJ1310_3.83.2529.jar*
   - *TassHsmFrame_2.57.2526.jar*

   a) 右键单击工程名称，选择**New** > **Folder**。

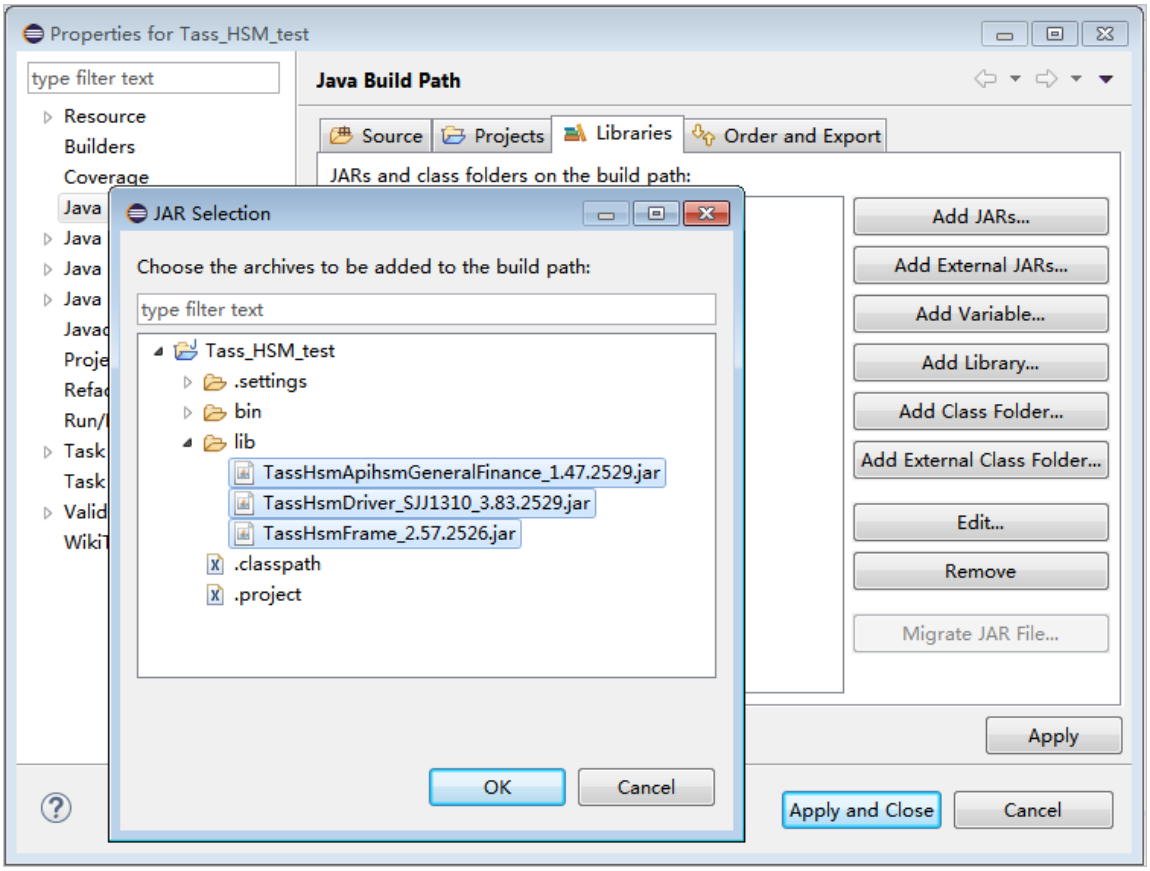
   b) 在**Folder name**中输入*lib*，单击**Finish**。

   c) 复制*TassHsmApihsmGeneralFinance_1.47.2529.jar*、*TassHsmDriver_SJJ1310_3.83.2529.jar*、*TassHsmFrame_2.57.2526.jar*包。

d) 右键单击**lib**，选择**Paste**。

e) 右键单击工程名称，选择**Build Path** > **Configure Build Path**。

f) 选择**Libraries**页签，单击**Add JARs**。



g) 选择*lib*中的3个jar包，单击**OK**。

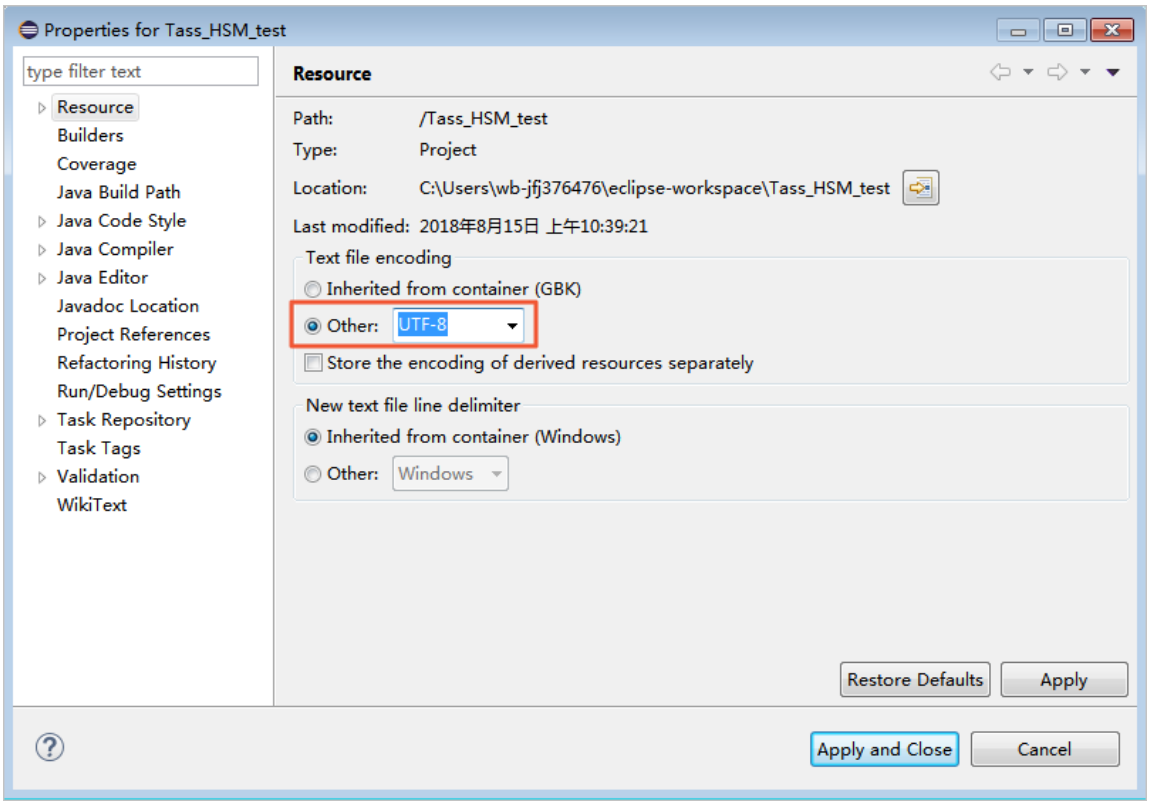
h) 单击**Apply and Close**。

3. 修改编码格式为*UTF-8*。

a) 右键单击工程名称，选择**Properties**。

b) 单击**Resource**。

c) 在**Text file encoding**中选择**Other**，并在下拉菜单中选择*UTF-8*。



d) 单击**Apply and Close**。

4. 复制Java实例文件到工程中。

   Java demo文件：*test_hsmGeneralFinance.java*。

   a) 复制*test_hsmGeneralFinance.java*。

   b) 右键单击*src*目录，选择**Paste**。

1.3 加密实例管理

1.3.1 创建加密实例

该章节介绍了如何创建加密实例。

操作步骤

1. 登录云盾安全中心。
2. 定位到**加密服务** > **实例列表**页面，单击**创建实例**。
3. 选择加密实例的**区域**、**虚拟网络**、**设备厂商**和**设备型号**等信息。
4. 单击**创建实例**，完成加密实例的创建。

1.3.2 配置加密实例

该章节介绍了如何配置加密实例。

操作步骤

1. 登录云盾安全中心。
2. 定位到**加密服务** > **实例列表**页面。
3. 在新创建加密实例的**操作**栏，单击**配置**。
4. 在**配置IP**对话框中，配置VPC网络和IP地址。

配置项	说明
所属的VPC网络ID	选择VPC网络，加密服务需要和应用服务器属于同一个VPC。
所属的VPC子网	选择VPC子网网段。
分配私网IP地址	设置私网IP，该IP需要在**所属的VPC子网**的网段中。

5. 单击**确定**，完成加密实例的配置。

1.3.3 释放加密实例

该章节介绍了如何释放加密实例。

背景信息

加密实例资源是有限的，如果您不再需要加密服务后，可以通过释放操作，释放加密实例资源。

操作步骤

1. 登录云盾安全中心。
2. 定位到**加密服务** > **实例列表**页面。
3. 在需要释放加密实例的**操作**栏，单击**释放**。
4. 在提示对话框中，单击**确定**，释放加密实例。

1.4 密码机管理

该章节介绍通过VsmManager管理工具管理密码机。

加密服务是云上的加密解决方案，为业务系统提供安全的应用层密码服务，保证业务数据产生、传输、接收到处理整个过程的安全性、有效性、完整性、不可抵赖性。

VsmManager管理工具是密码机管理工具，通过VsmManager管理工具可以实现以下管理操作：

- 系统管理：登录VsmManager管理工具。

- 密钥管理：包括设备主密钥管理和应用密钥管理。
- 设备管理：包括设备配置、授权管理和UKEY管理。
- 设备诊断维护：包括日志管理、设备运行状态、系统维护。

1.4.1 系统管理

1.4.1.1 注册管理员UKEY

该章节介绍了如何注册管理员UKEY。

前提条件

PC能够访问密码机所在的VPC网络。

背景信息

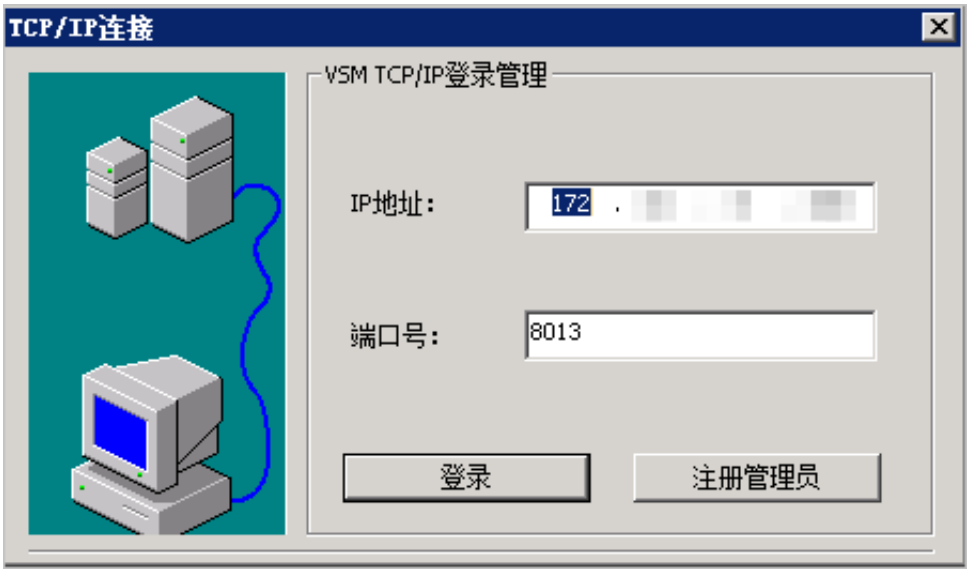
在登录VsmManager管理工具时，需要先注册管理员UKEY。

管理员UKEY用途包括：用户开机、协商通讯、管理工具与密码机通讯运算。

操作步骤

1. 在PC上双击*VsmManager.exe*管理工具。
2. 单击**系统** > **VSM登录管理**。
3. 在**TCP/IP连接**对话框中，输入密码机的IP和端口号。

> **说明**：
> 端口固定为8013。



4. 在PC上插入空UKEY，单击**注册管理员**。
5. 在**UKEY列表**窗口中选择插入的空UKEY，单击**确定**。

6. 在**VERIFY**对话框中，输入UKEY口令，单击**确定**。

> **说明**：
> 出厂初始的UEKY口令为12345678。

完成管理员UKEY的注册。

1.4.1.2 登录VsmManager管理工具

该章节介绍了如何登录VsmManager管理工具。

背景信息

如果在没有注册UKEY管理员的情况下直接登录系统，您将不能进行原始初始化和恢复初始化操作，仅可以在测试主密钥的环境下进行密钥管理。

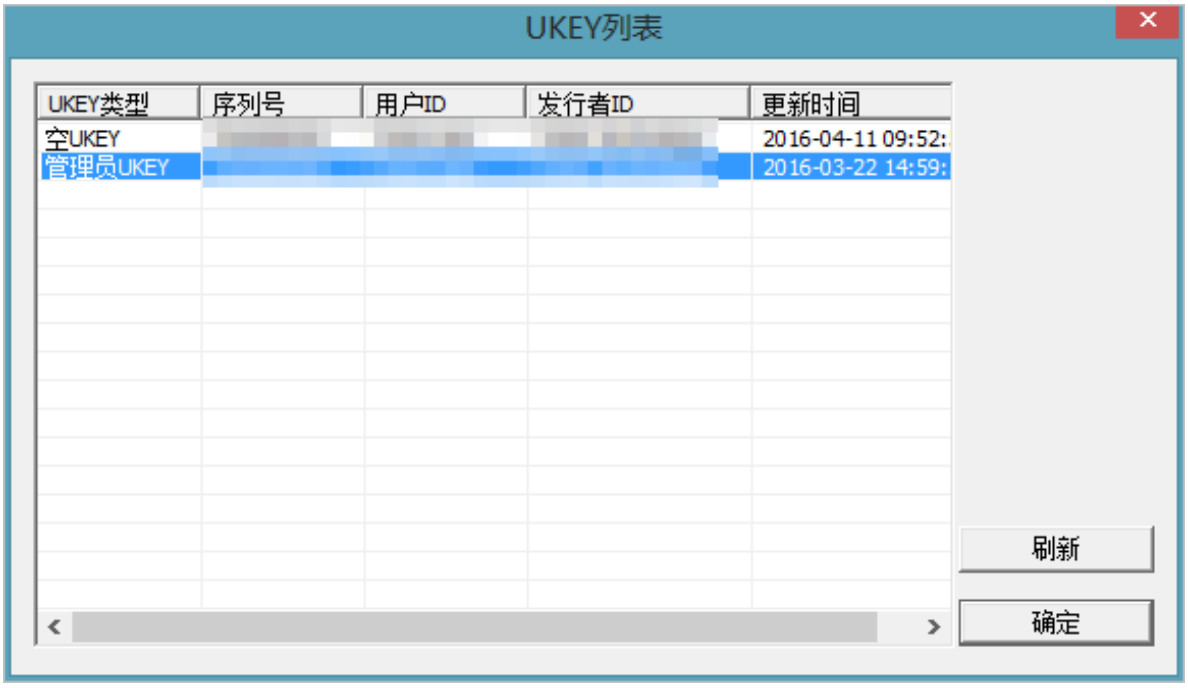
操作步骤

1. 在PC上插入管理员UKEY。
2. 双击*VsmManager.exe*管理工具。
3. 单击**系统** > **VSM登录管理**。
4. 在**TCP/IP连接**对话框中，输入密码机的IP和端口号。

说明：

端口固定为8013。

5. 单击**登录**。
6. 在弹出的**UKEY列表**窗口中，选择**管理员UKEY**，单击**确定**。



7. 在**VERIFY**对话框中，输入UKEY口令，单击**确定**。
8. 在登录成功确认框中，单击**确定**。

   登录成功后，进入VsmManager管理工具。

1.4.2 密钥管理

1.4.2.1 执行原始初始化

该章节介绍如何进行原始初始化。

背景信息

密码机要投入生产环境时，必须先完成原始初始化操作，制作主密钥成份UKEY和授权UKEY，并合成设备主密钥（DMK）。

在进行原始初始化前，请规划好以下项目：

规划项目	说明	举例
设备主密钥（DMK）管理人员	需要几个DMK管理员持有主密钥成份UKEY。 取值范围：2~8	本章节以配置2个为例。
设备授权控制人员	需要几个设备授权控制人员持有授权UKEY。 取值范围：1、3、5	本章节以配置1个为例。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**密钥管理** > **原始初始化**。

   说明：
   如果进行原始初始化操作，密码机将清除内部的全部密钥。
3. 在**安全操作警示**提示框中，单击**下一步**。
4. 在**请输入成份数目**中输入*2*，单击**下一步**。

   根据规划的设备主密钥（DMK）管理人员，确定主密钥成份UKEY数目，设置范围为2~8。本章节以2个为例。

5. 依次制作2个主密钥成份UKEY，单击**下一步**。

a) 第一个主密钥管理员两次输入预定义的秘密值，或者单击**随机秘密值**。

- 手动设置秘密值为：8-32个任意字符。
- 自动的随机秘密值为：32个任意字符。

b) PC上插入空UKEY。

c) 单击**产生成份UKEY**。

d) 在弹出的**UKEY列表**中，选择刚才插入的空UKEY，单击**确定**。

e) 在**VERIFY**对话框中，输入UKEY口令，单击**确定**。

通过系统计算得到的成份数据写入UKEY中。

f) 参考步骤*5.a*~步骤*5.e*，制作第二个主密钥成份UKEY。

6. 依次导入2个主密钥成份UKEY到系统，单击**下一步**。

a) 单击**导入成份**。

b) 在**UKEY列表**中，第一个主密钥管理员选择自己的主密钥成份UKEY，单击**确定**。

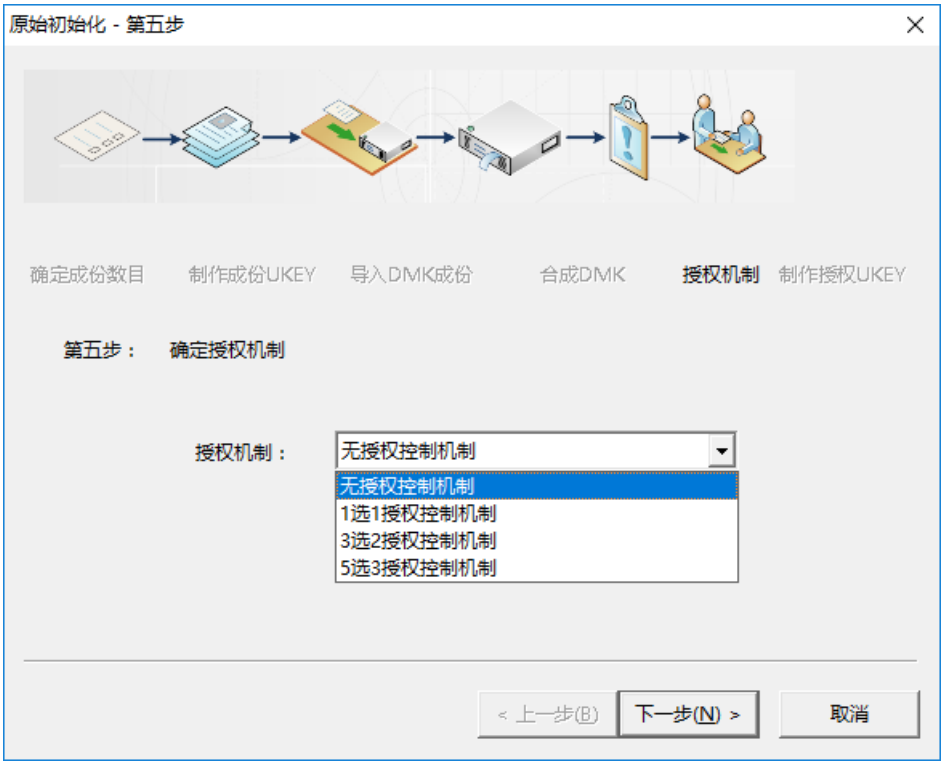
系统将读取UKEY内的成份数据。

c) 参考步骤*6.a*~步骤*6.b*，导入第二个主密钥成份UKEY。

> **说明**：
> 主密钥成份UKEY的导入次序没有要求，但不能将同一个主密钥成份UKEY多次导入。

7. 单击**合成DMK**，完成后单击**下一步**。

8. **授权机制**选择*1*选*1*授权控制机制，单击**下一个**。



本章节以选择*1*选*1*授权控制机制为例，所有可选的授权机制如下：

授权机制	说明
无授权机制	不需要授权。

授权机制	说明
1选1授权控制机制	1个授权UEKY由1个授权人员保管，当为某类操作授权时，需1个授权人员授权许可。
3选2授权控制机制	m选n授权控制机制，制作m个授权UKEY由m个授权人员保管，当为某类操作授权时，需半数以上的授权人员授权许可，即n个授权UKEY认证通过。
5选3授权控制机制	

9. 制作授权UKEY。
   a) PC上插入空UKEY。
   b) 单击**制作授权卡**。
   c) 在**UKEY列表**中，选择插入的空UKEY，单击**确定**。
   d) 在**VERIFY**对话框中，输入UKEY口令，单击**确定**。
   e) （可选）参考步骤*9.a*~步骤*9.d*，依次制作余下授权UKEY。
      如果选择多个授权UKEY，需要根据提示依次制作授权UKEY。
10. 单击**完成**。
    完成原始初始化，密码机生成新的主密钥DMK。

1.4.2.2 执行恢复初始化

该章节介绍如何进行恢复初始化。

背景信息

通过恢复初始化操作，您可以使用主密钥成份UKEY恢复原来的DMK。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**密钥管理** > **恢复初始化**。

   说明：
   如果进行恢复初始化操作，将清除密码机内所有的全部密钥。

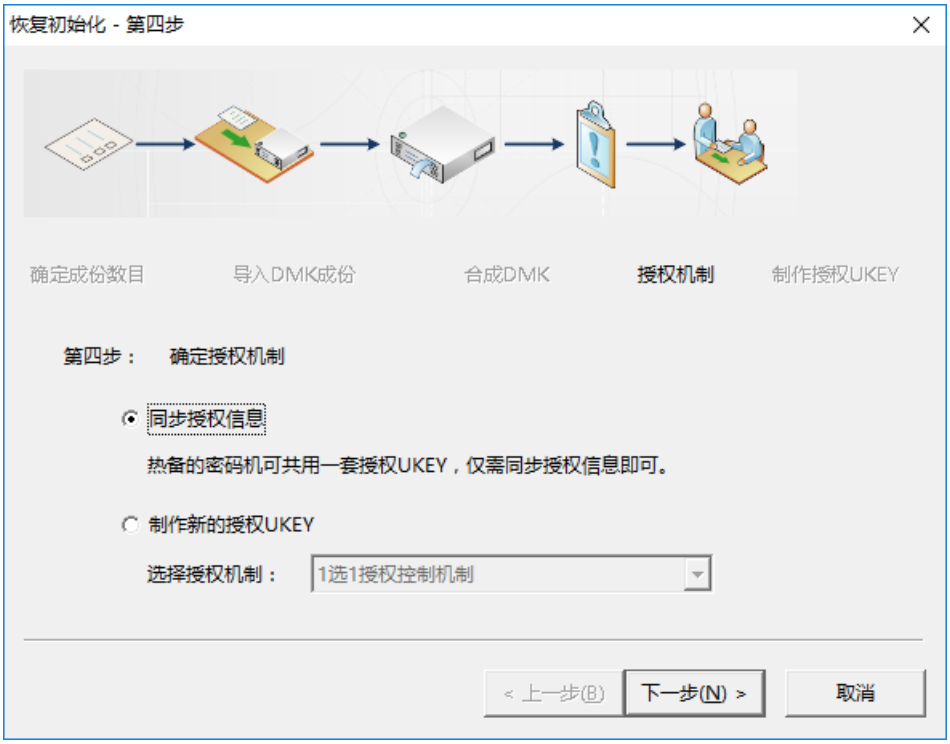
3. 在**安全操作警示**提示框中，单击**下一步**。
4. 输入主密钥成份UEKY数目，单击**下一步**。
5. 依次导入主密钥成份UKEY，单击**下一步**。
   a) 单击**导入成份UKEY**。
   b) 主密钥管理员选择自己的主密钥成份UKEY，并输入口令。

系统将读取UKEY内的成份数据。

c) 参考步骤*5.a*~步骤*5.b*，依次导入主密钥成份UKEY。

主密钥成份UKEY的导入次序没有要求，但不能将同一个主密钥成份UKEY多次导入。

6. 单击**合成DMK**，完成后单击**下一步**。
7. 确定授权机制。



- 如果多机备份的密码机共用一套授权UKEY，则选择**同步授权信息**。

  1. 选择**同步授权信息**。
  2. 单击**下一步**。
  3. 插入有效的授权UKEY，输入UKEY口令，单击**完成**。
  4. 单击**同步开始**。

- 如果每台密码机使用独立的授权UKEY，则选择**制作新的授权UEKY**。

  1. 选择**制作新的授权UEKY**。
  2. 在**选择授权机制**下拉菜单中，选择授权机制。
  3. 单击**下一步**。
  4. PC上插入第一个授权UKEY，输入UKEY口令。
  5. 单击**制作授权卡**。
  6. 参考上述两个步骤，依次制作余下授权UKEY。

1.4.2.3 执行出厂初始化

该章节介绍如何进行出厂初始化。

背景信息

用户在进行系统开发或调试时，可以为密码机进行出厂初始化，内部自动装载测试主密钥，密码机内使用公开通用的本地主密钥（LMKs）。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**密钥管理** > **出厂初始化**。

   说明：
   如果进行原始初始化操作，将清除密码机内所有的全部密钥。
3. 在**安全操作警示**提示框中，单击**下一步**。
4. 在导入测试DMK步骤中，单击**下一步**。
5. 选择**授权机制**，单击**下一个**。

授权机制	说明
无授权机制	不需要授权。
1选1授权控制机制	1个授权UEKY由1个授权人员保管，当为某类操作授权时，需1个授权人员授权许可。
3选2授权控制机制	m选n授权控制机制，制作m个授权UKEY由m个授权人员保管，当为某类操作授权时，需半数以上的授权人员授权许可，即n个授权UKEY认证通过。
5选3授权控制机制	

6. 依次制作授权UKEY。
   a) PC上插入第一个授权UKEY，输入UKEY口令。
   b) 单击**制作授权卡**。
   c) 参考步骤*6.a*~步骤*6.b*，依次制作余下授权UKEY。

1.4.2.4 获取DMK校验值

该章节介绍如何获取设备主密钥（DMK）校验值。

操作步骤

1. 登录*VsmManager*管理工具。

2. 单击**密钥管理** > **获取DMK校验值**。

   界面显示当前DMK校验值。

1.4.2.5 备份DMK

该章节介绍如何备份DMK。

背景信息

DMK导出到多个成份UKEY中，当原有的主密钥成份UKEY丢失或损坏时，保证能够重新合成出原来的DMK。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**密钥管理** > **导出DMK成份**。
3. 输入需要导出的成份UKEY数目，单击**下一步**。

   成份UKEY数目可设置范围为2~8。
4. 依次导出写入到成份UKEY。

1.4.2.6 对称密钥管理

1.4.2.6.1 产生随机密钥

该章节介绍了如何产生随机密钥。

前提条件

需要获取**应用密钥管理**的授权许可，具体操作参见授权操作。

背景信息

对称密钥状态信息如下表所示。

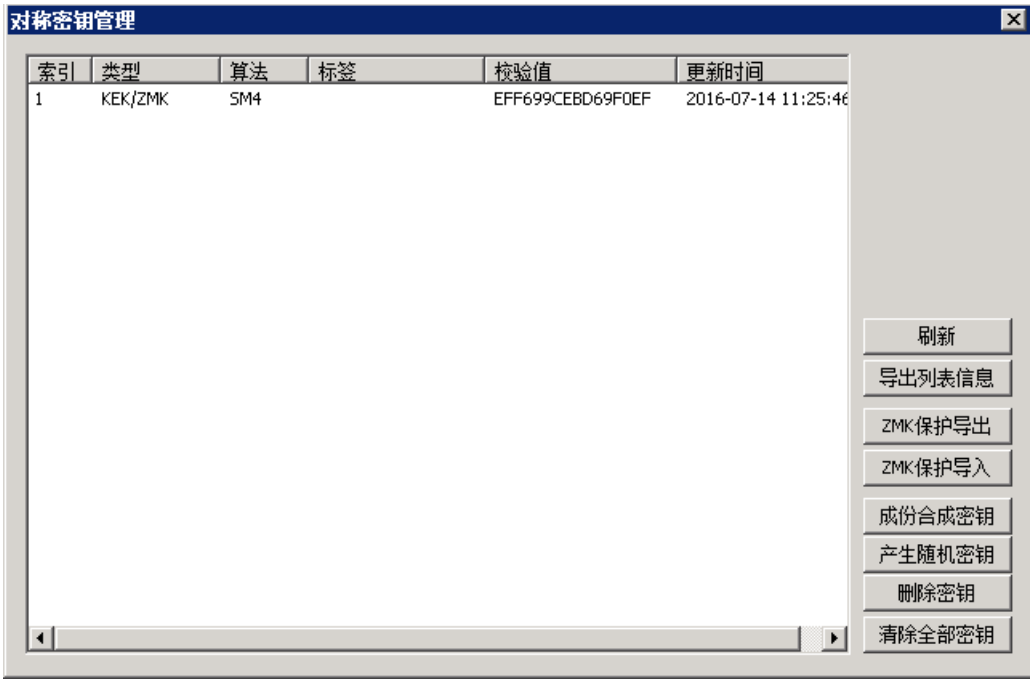
表 1-5: 对称密钥状态信息

信息	说明
密钥索引号	对称密钥索引号范围：1~2048
密钥类型	密钥的类型
密钥算法	SM1、SM4、DES/DES2/DES3、AES
密钥标签	用户自定义的密钥标识，0~16个字符

信息	说明
校验值	密钥加密一个分组全0数据的密文，取前8字节
更新时间	密钥产生或导入的时间

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**密钥管理 > 管理对称密钥**。



3. 单击**产生随机密钥**。
4. 在对话框中配置对称密钥参数。

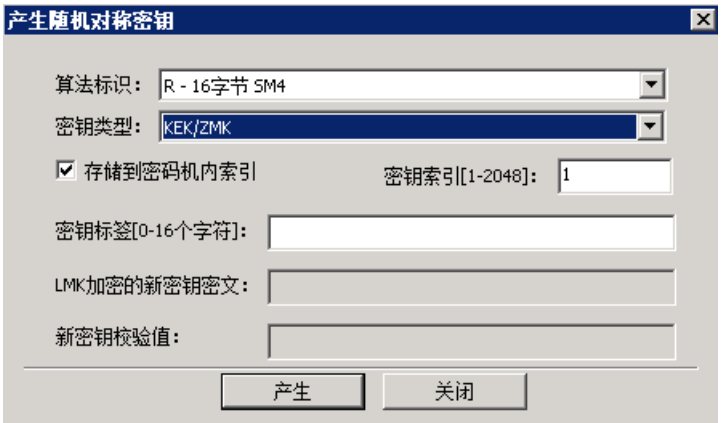


表 1-6: 对称密钥参数

配置项	说明
算法标识	密码机支持多种对称密码算法，使用时根据其算法标识使用相应的密码算法。标识如下： • *Z*：单倍长的DES算法密钥。 • *U*：双倍长的3DES算法密钥，LMK加密输出时使用变量方式。 • *T*：三倍长的3DES算法密钥，LMK加密输出时使用变量方式。 • *X*：双倍长的3DES算法密钥。 • *Y*：三倍长的3DES算法密钥。 • *P*：SM1算法密钥。 • *R*：SM4算法密钥。 • *L*：AES-128算法密钥。 • *M*：AES-192算法密钥。 • *N*：AES-256算法密钥。
密钥类型	不同密钥类型具有不同的用途。
存储到密码机内索引	生成的密钥是否存储到密码机索引。
密钥索引	勾选**存储到密码机内索引**后，设置索引号。 取值范围：1~2048
密钥标签	用于在密钥内部存储时标记密钥的标签说明。
LMK加密的新密钥密文	生成的密钥密文。
新密钥校验码	新密钥的校验码。

5. 单击**产生**。

   产生新的随机密钥并输出显示密文和校验值。

1.4.2.6.2 成份合成密钥

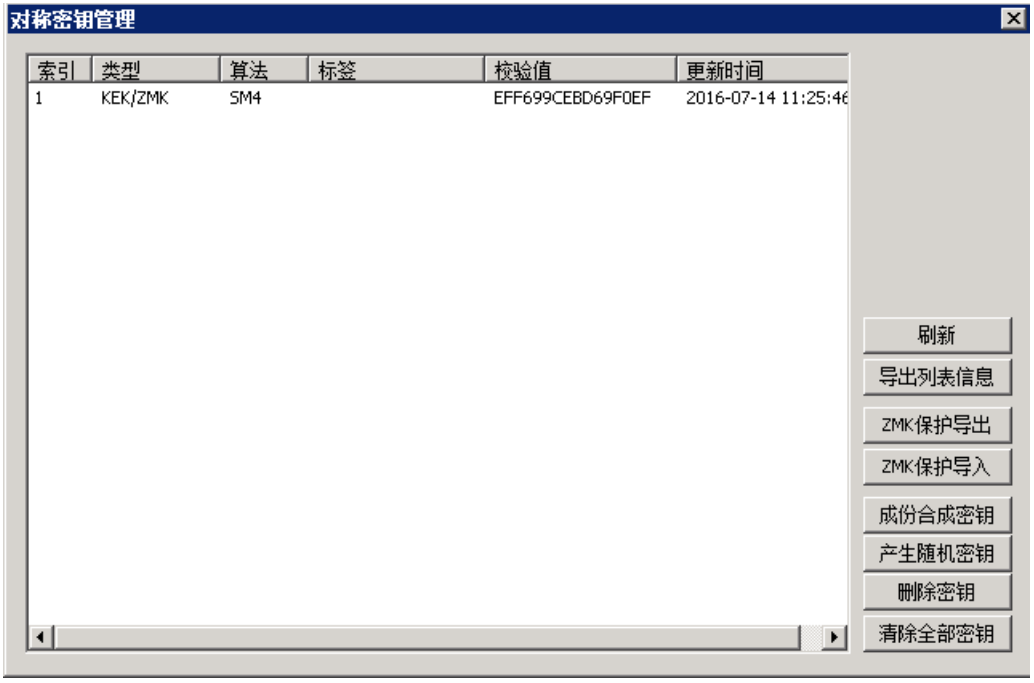
该章节介绍了如何成份合成密钥。

前提条件

需要获取**应用密钥管理**的授权许可，具体操作参见授权操作。

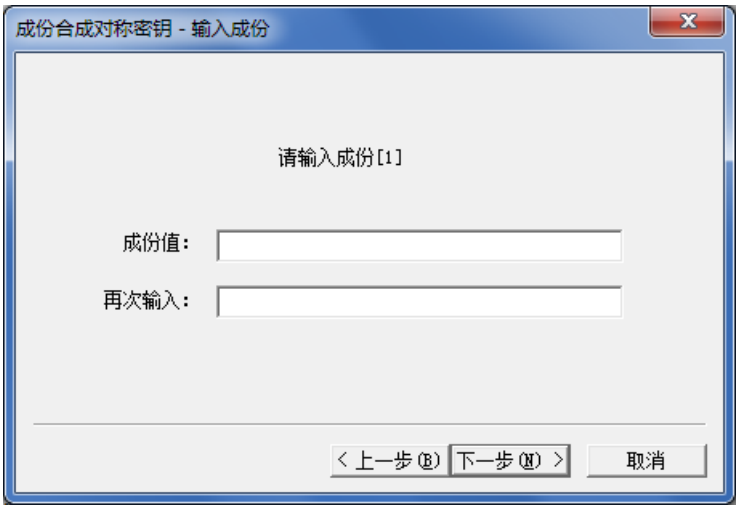
操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**密钥管理 > 管理对称密钥**。

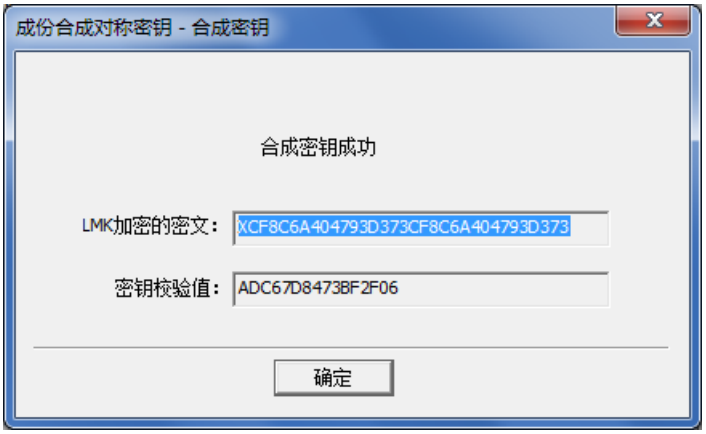


3. 单击**成份合成密钥**。
4. 在对话框中配置参数，单击**下一步**。

5. 依次输入密钥成份，单击**下一步**。



所有成份全部输入后，合成新的密钥并显示密文和校验值。



6. 单击**确定**。

1.4.2.6.3 删除密钥

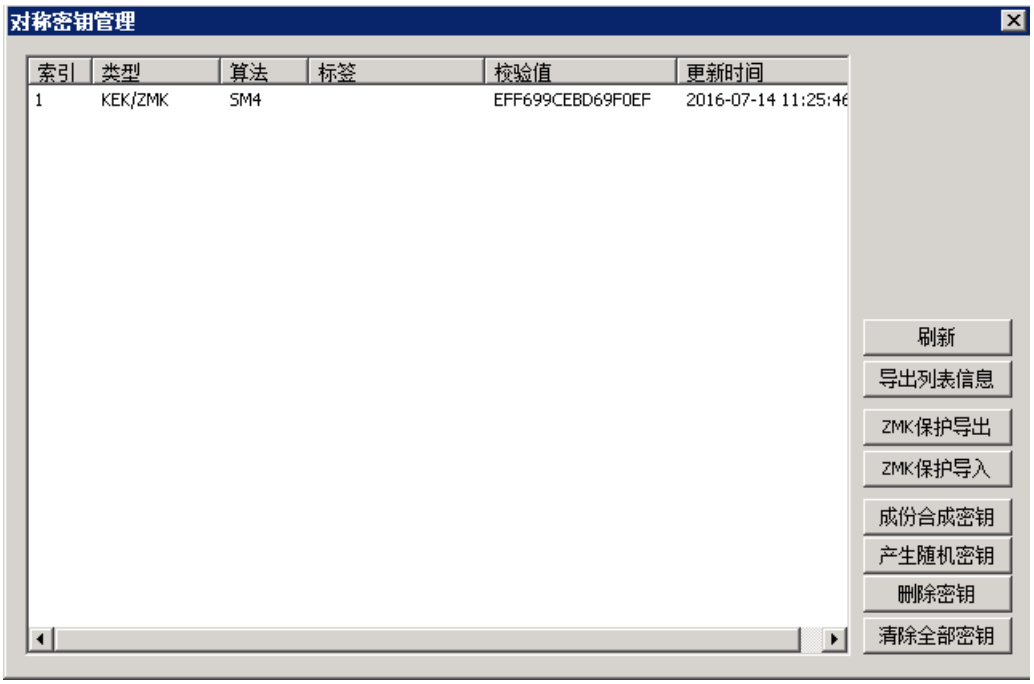
该章节介绍了如何删除密钥。

前提条件

需要获取**应用密钥管理**的授权许可，具体操作参见授权操作。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**密钥管理** > **管理对称密钥**。



3. 在左侧列表中选择密钥。
4. 单击**删除密钥**。
5. 在确认提示框中，单击**是**。

1.4.2.6.4 清除全部密钥

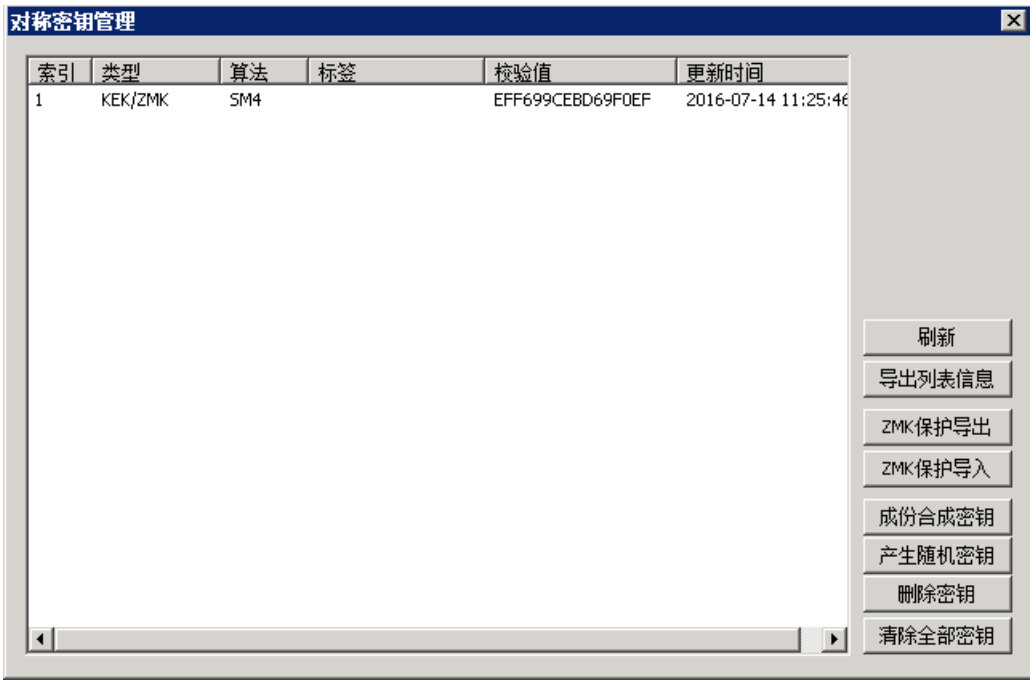
该章节介绍了如何清除全部密钥。

前提条件

需要获取**应用密钥管理**的授权许可，具体操作参见授权操作。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**密钥管理** > **管理对称密钥**。



3. 单击**清除全部密钥**。
4. 在确认提示框中，单击**是**。

1.4.2.6.5 导出列表信息

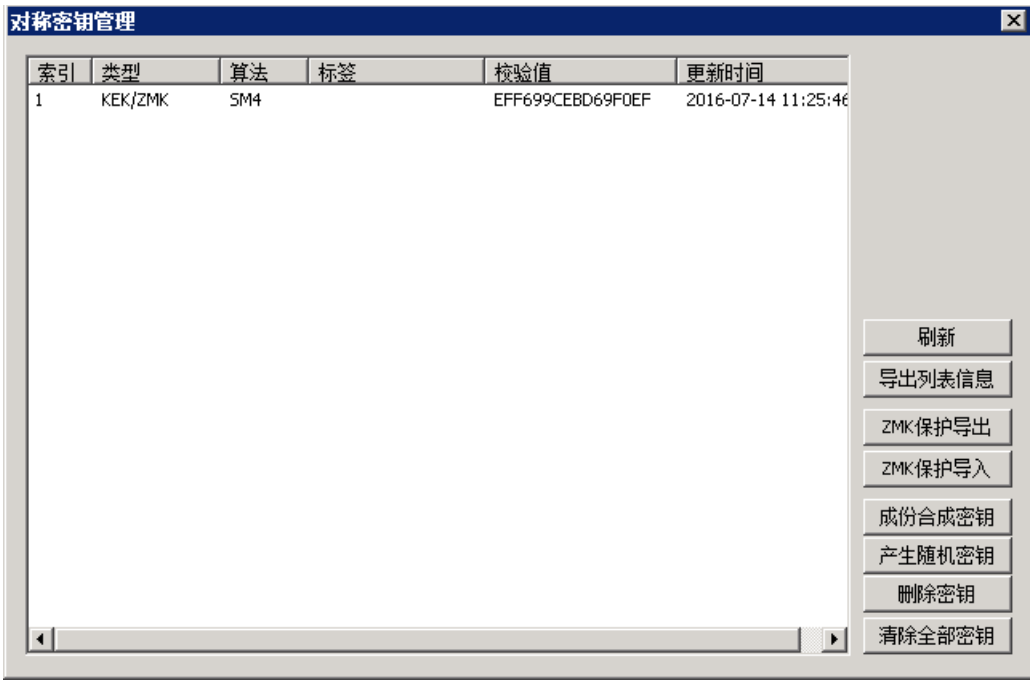
该章节介绍了如何导出对称密钥的列表信息。

前提条件

需要获取**应用密钥管理**的授权许可，具体操作参见授权操作。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**密钥管理** > **管理对称密钥**。



3. 单击**导出列表信息**。

   对称密钥列表中所有信息将采用追加模式导出到*keylist.txt*，文件位于*VsmManager.exe*所在目录。

1.4.2.6.6 ZMK保护导出

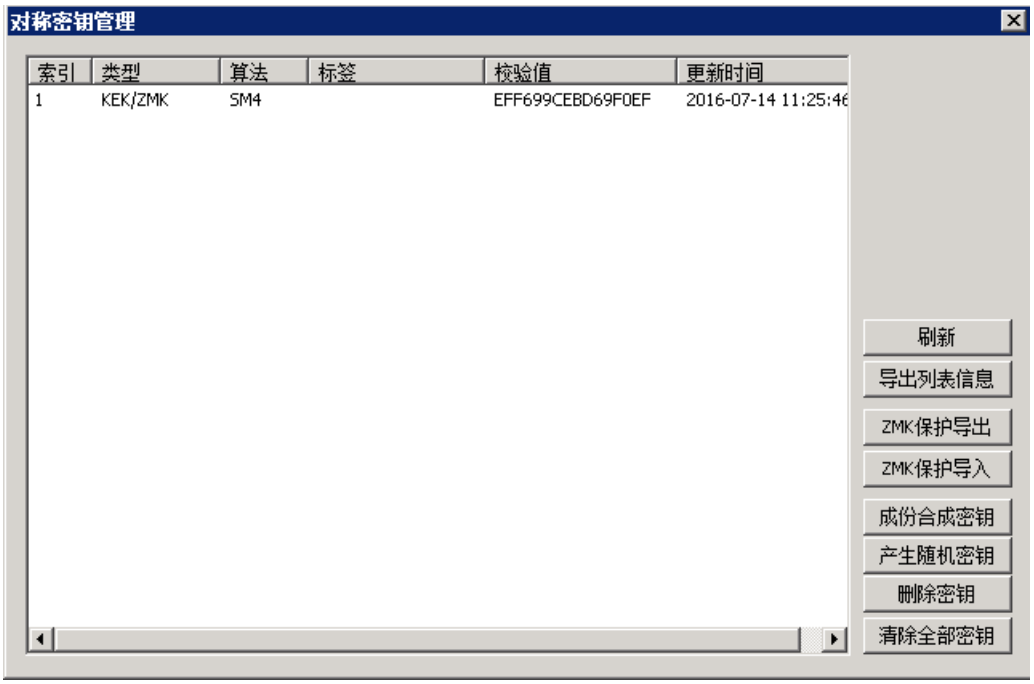
该章节介绍了如何ZMK保护导出。

背景信息

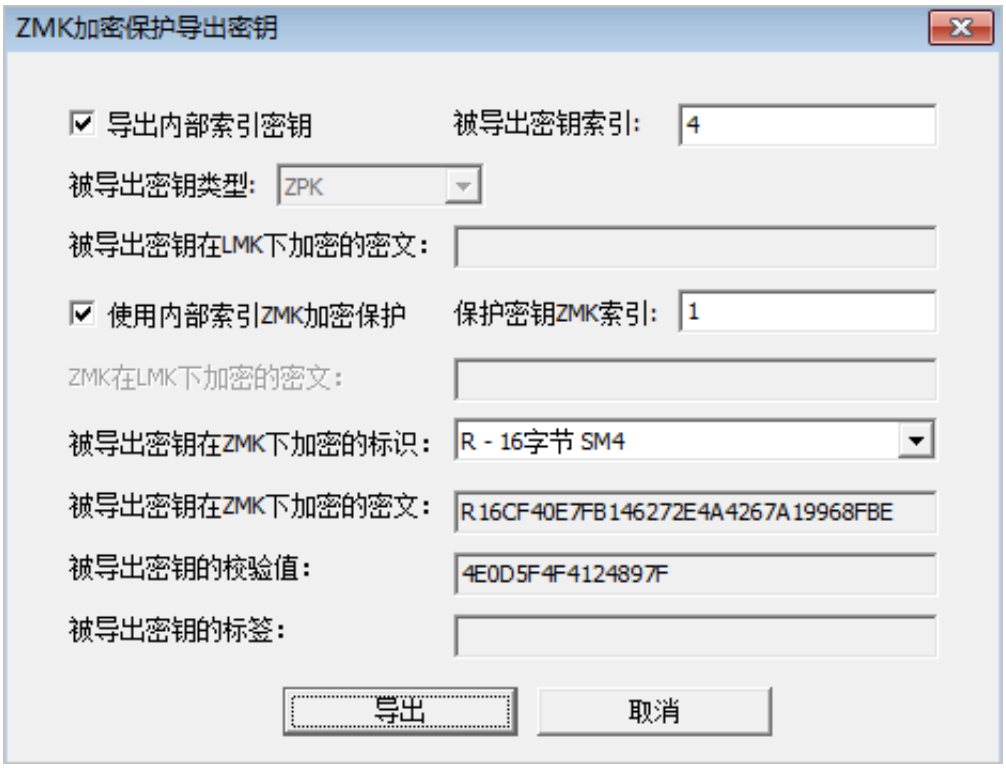
支持通过ZMK保护导出加密机内密钥或者外部输入的在LMK下加密的密文。

操作步骤

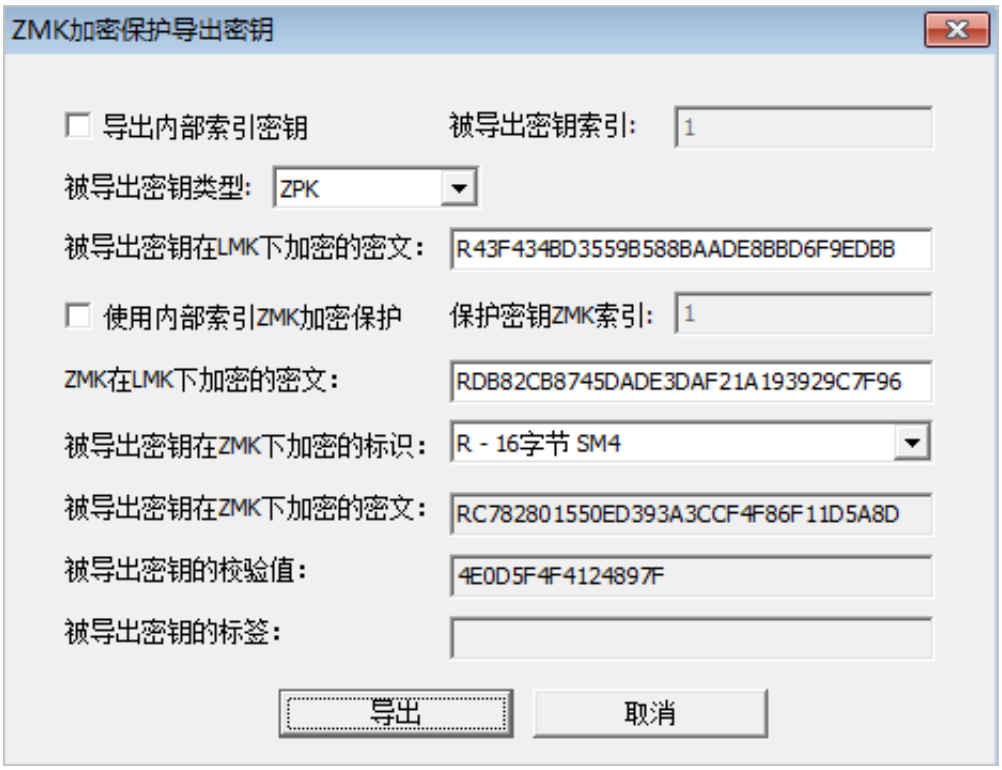
1. 登录*VsmManager*管理工具。
2. 单击**密钥管理** > **管理对称密钥**。



3. 在左侧列表中选择密钥。
4. 单击**ZMK保护导出**。
5. 配置ZMK保护导出方式。
   - 使用密码机内存储的ZMK。



   - 使用外部输入的ZMK。



说明：

被导出密钥在ZMK下加密的标识需要选择正确，否则导出失败。

例如需要导出的密钥加密时使用的加密标识为*R - 16*字节 *SM4*，则**被导出密钥在ZMK下加密的标识**也需要选择*R - 16*字节 *SM4*。

6. 单击**导出**。

1.4.2.6.7 ZMK保护导入

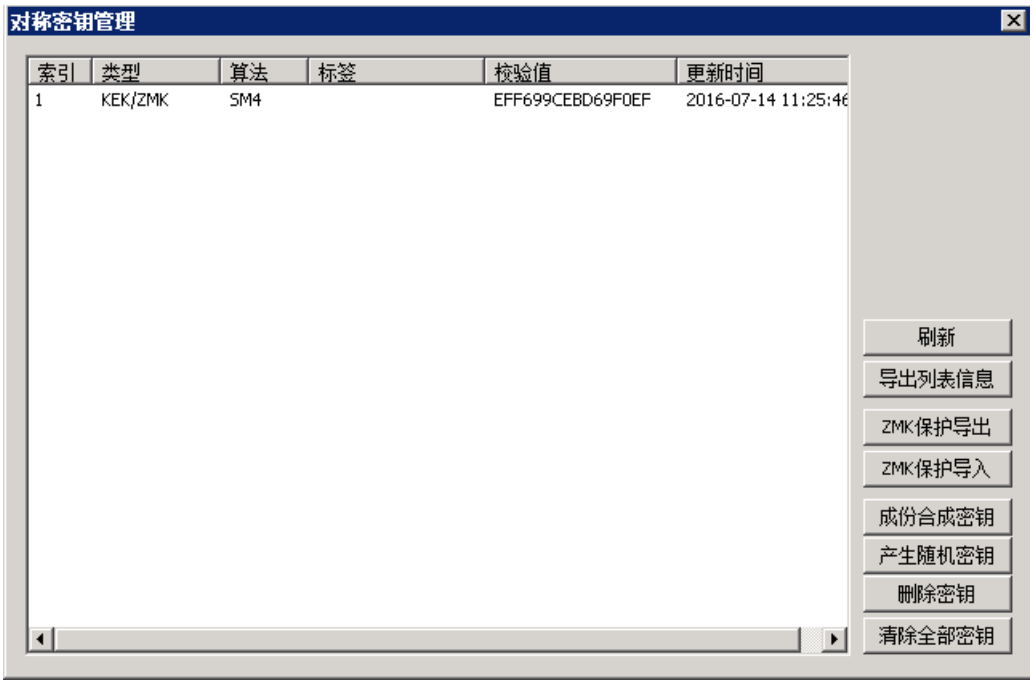
该章节介绍了如何ZMK保护导入。

背景信息

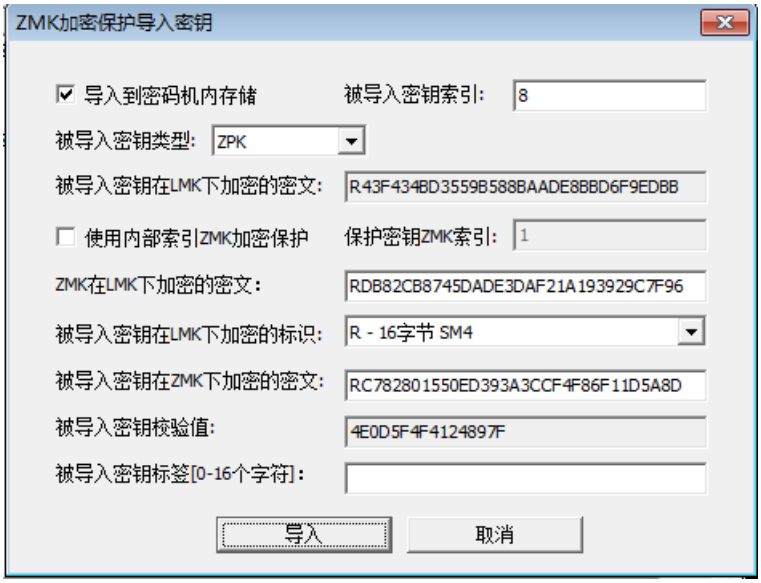
支持通过ZMK保护导入外部输入的在ZMK下加密的密钥密文并可选的存储到密码机。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**密钥管理** > **管理对称密钥**。



3. 单击**ZMK保护导入**。
4. 配置导入信息。



5. 单击**导入**。

1.4.2.7 非对称密钥管理

1.4.2.7.1 产生随机密钥

该章节介绍了如何产生随机密钥。

前提条件

需要获取**应用密钥管理**的授权许可，具体操作参见授权操作。

背景信息

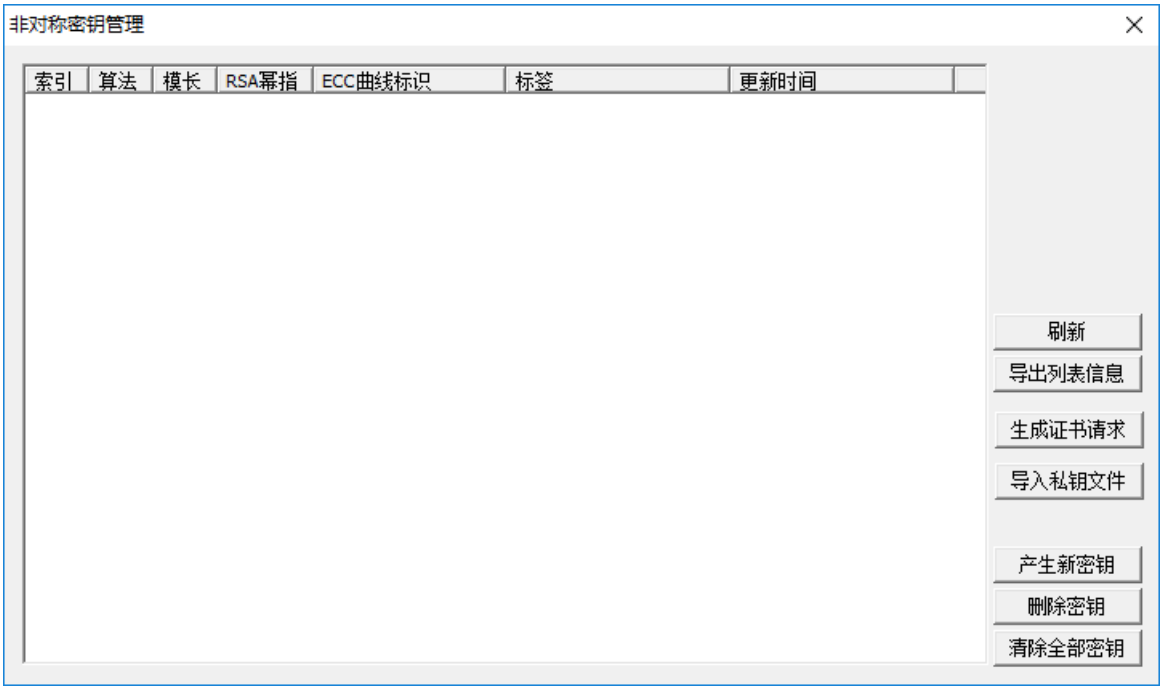
非对称密钥状态信息如下表所示。

表 1-7: 非对称密钥状态信息

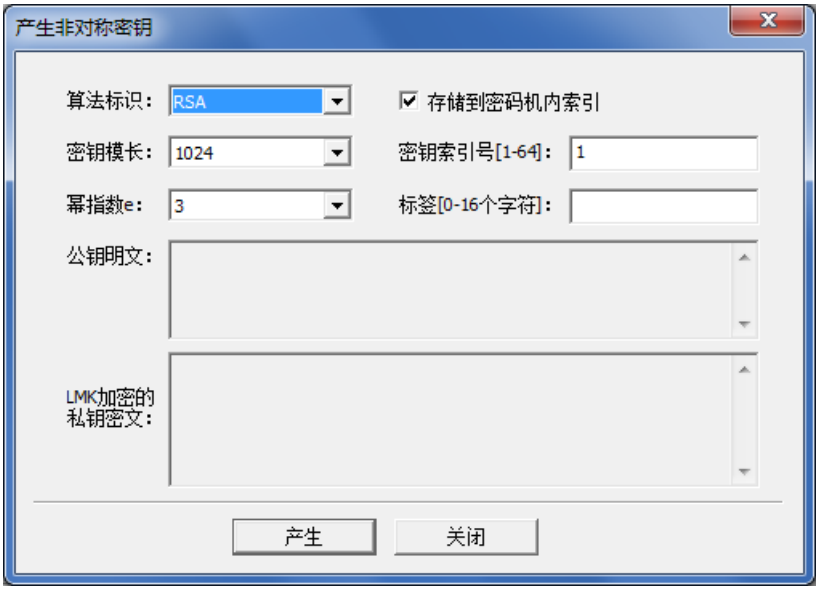
信息	说明
密钥索引号	非对称密钥索引号范围1~64，RSA和SM2密钥各自独立编号
密钥算法	RSA、ECC
模长	• RSA算法：模长支持1024、1152、1408、1912、2048位 • ECC算法：模长支持256位
RSA幂指	仅对RSA算法有效，支持3、65537
ECC曲线标识	仅对ECC算法有效，支持SM2_OSCCA_NEWFP_256曲线
密钥标签	用户自定义的密钥标识，0~16个字符
更新时间	密钥产生或导入的时间

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**密钥管理** > **管理非对称密钥**。



3. 单击**产生随机密钥**。
4. 在对话框中配置参数。



5. 单击**产生**。

   产生新的非对称密钥并输出显示公钥明文和私钥密文。

1.4.2.7.2 删除密钥

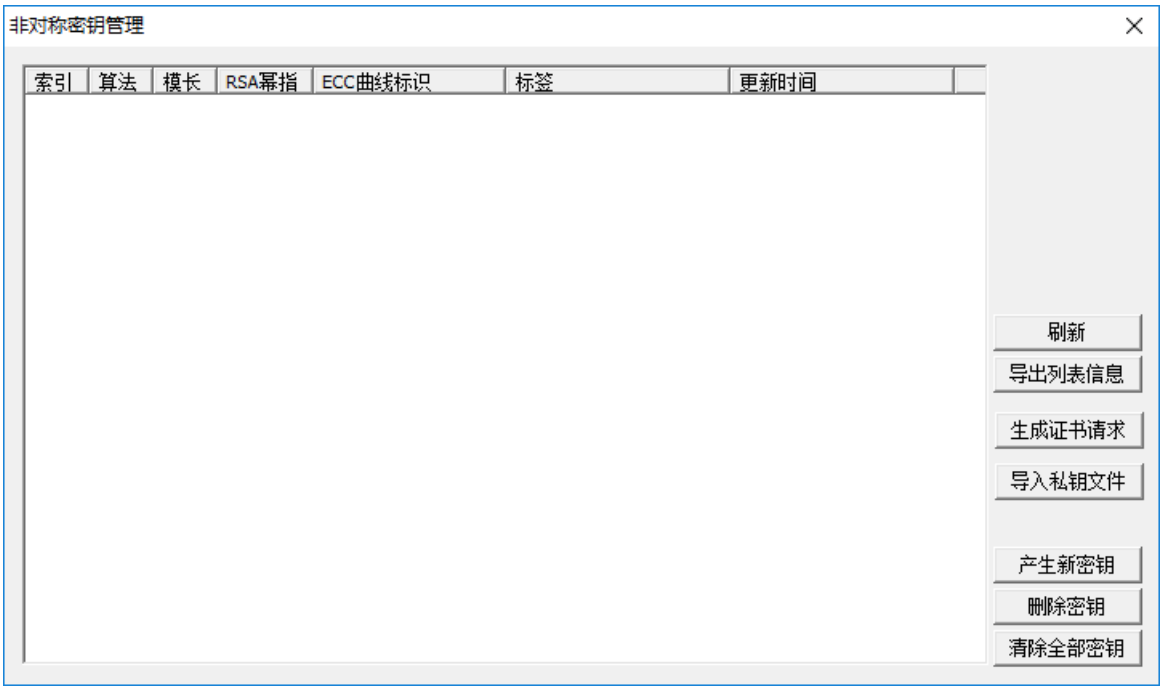
该章节介绍了如何删除密钥。

前提条件

需要获取**应用密钥管理**的授权许可，具体操作参见授权操作。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**密钥管理** > **管理非对称密钥**。



3. 在左侧列表中选择密钥。
4. 单击**删除密钥**。
5. 在确认提示框中，单击**是**。

1.4.2.7.3 清除全部密钥

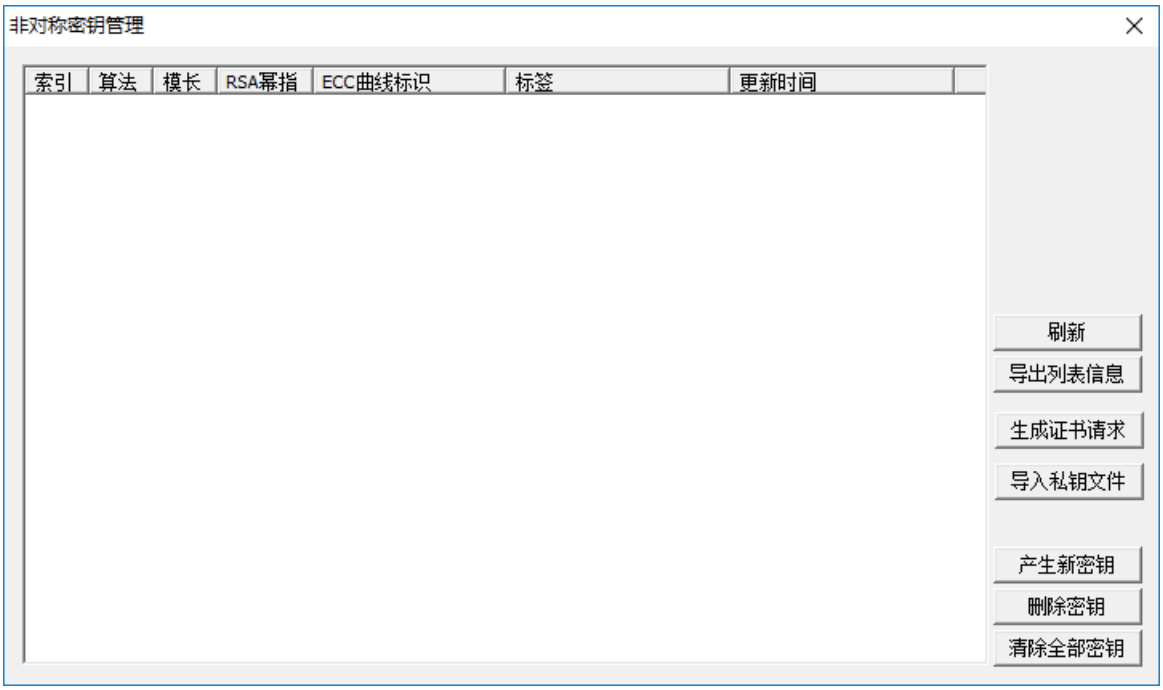
该章节介绍了如何清除全部密钥。

前提条件

需要获取**应用密钥管理**的授权许可，具体操作参见授权操作。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**密钥管理** > **管理非对称密钥**。



3. 单击**清除全部密钥**。
4. 在确认提示框中，单击**是**。

1.4.2.7.4 导出列表信息

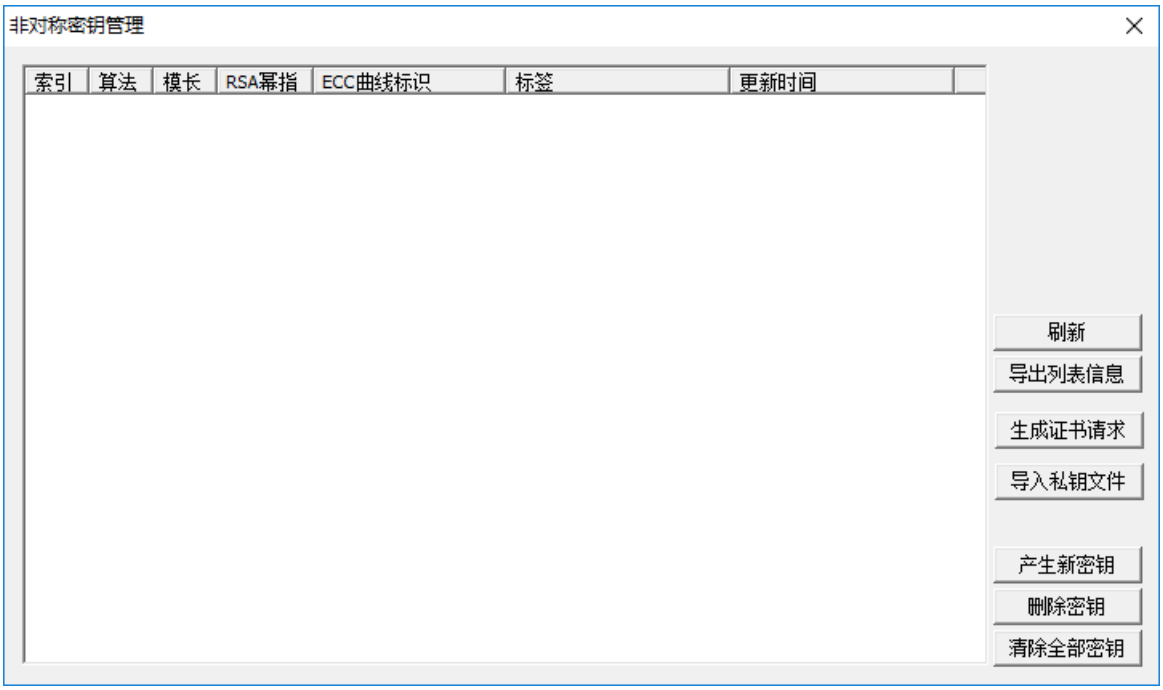
该章节介绍了如何导出对称密钥的列表信息。

前提条件

需要获取**应用密钥管理**的授权许可，具体操作参见授权操作。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**密钥管理** > **管理非对称密钥**。



3. 单击**导出列表信息**。

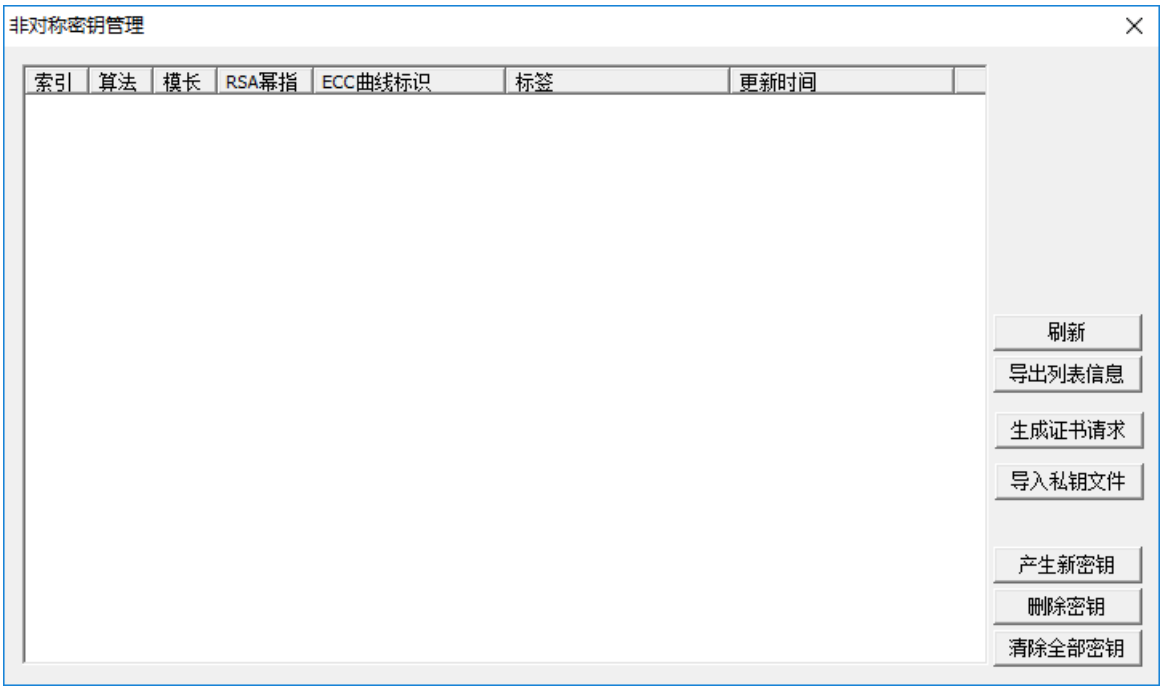
   非对称密钥列表中所有信息将采用追加模式导出到*keylist.txt*，文件位于*VsmManager.exe*所在目录。

1.4.2.7.5 生成证书请求

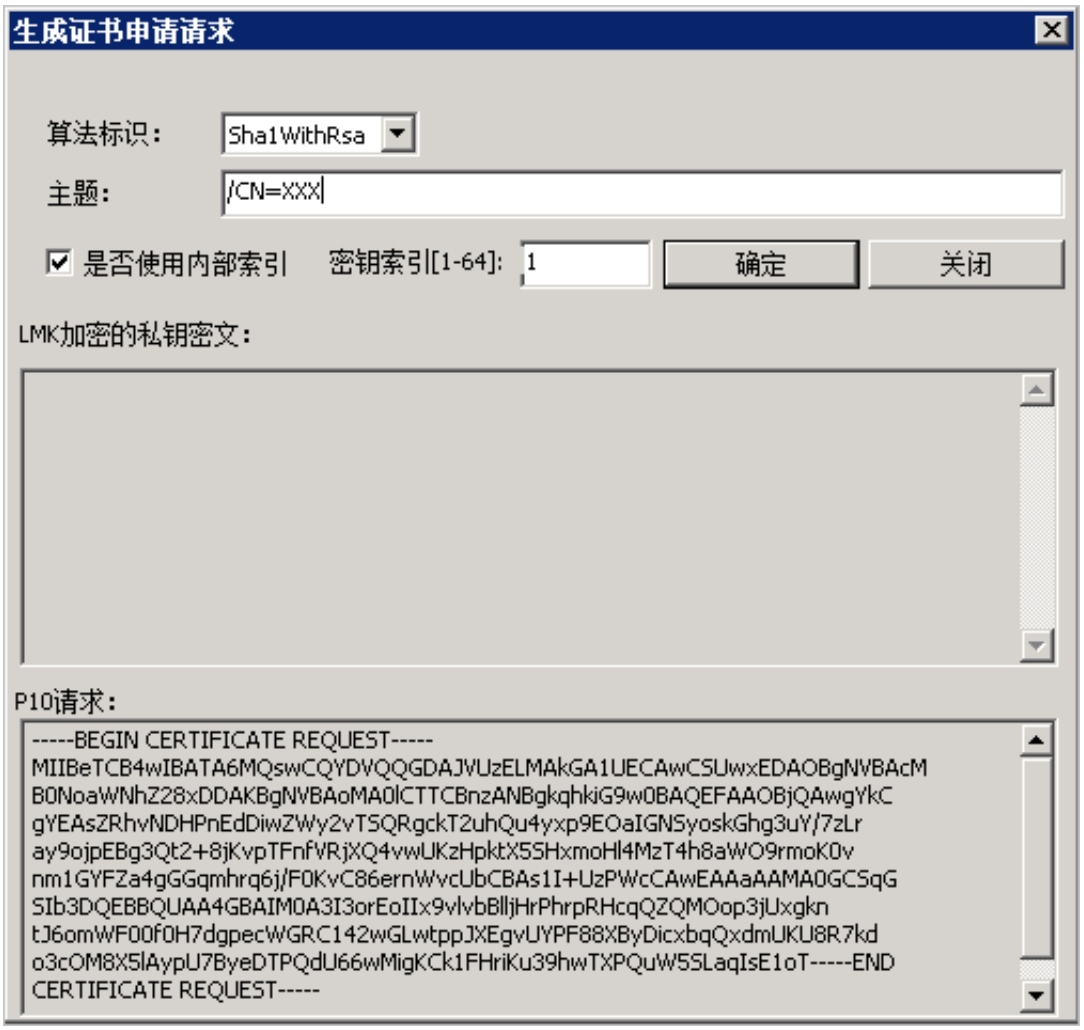
该章节介绍了如何生成证书请求。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**密钥管理** > **管理非对称密钥**。



3. 单击**生成证书请求**。
4. 配置证书申请请求。



a) 输入合法的主题，例如：/CN=XXX。

b) 选择私钥。

支持密码机内部私钥索引，或者外部输入LMK加密的私钥密文。

- 使用密码机内部私钥索引：

  勾选**是否使用内部索引**，并在**密钥索引**中输入索引号。

- 使用外部输入LMK加密的私钥密文：

  取消勾选**是否使用内部索引**，并在**LMK加密的私钥密文**中输入私钥密文。

5. 单击**确定**。

在**P10请求**中生成证书信息。

1.4.2.7.6 导入私钥文件

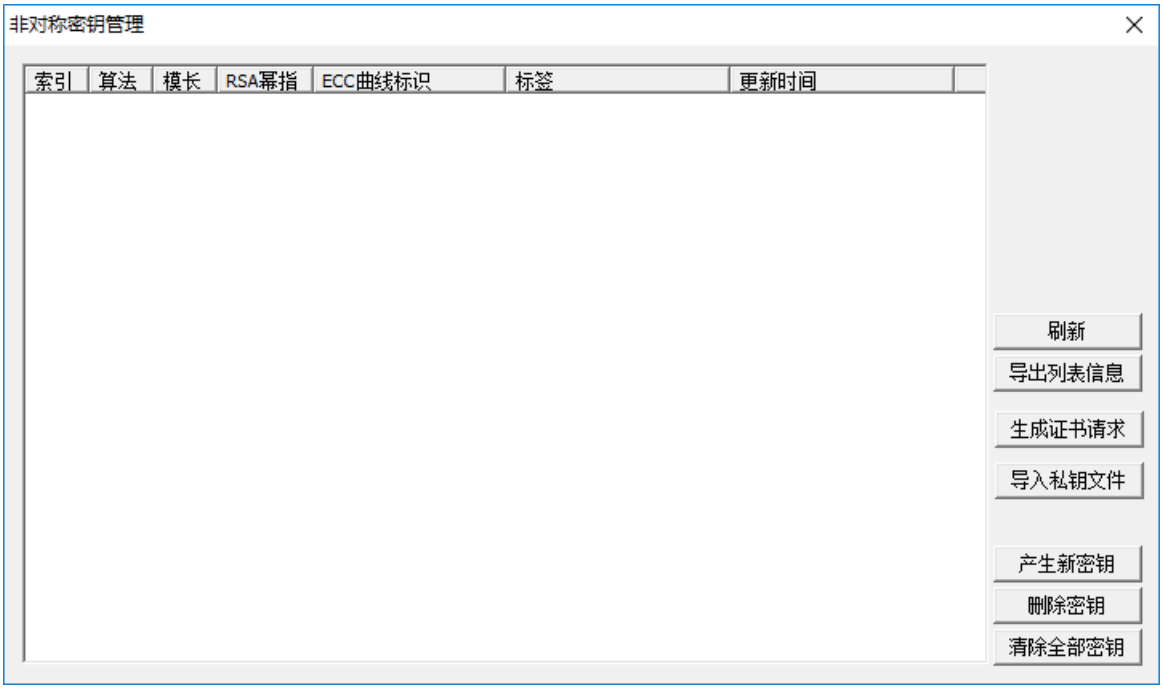
该章节介绍了如何导入私钥文件。

背景信息

支持导入RSA密钥的pfx和pem文件到密码机中保存。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**密钥管理** > **管理非对称密钥**。



3. 单击**导入私钥文件**。
4. 选择私钥文件，输入证书口令。

5. 单击**确定**。

1.4.2.8 备份与恢复

1.4.2.8.1 备份密钥

该章节介绍了如何备份密钥。密钥备份，是将密码机内部存储的全部应用密钥（包括对称和非对称密钥）以安全的方式备份导出，然后通过密钥恢复导入到其他密码机中。可用于做多机密钥同步或设备误操作后恢复应用密钥。

背景信息

备份密钥功能需要获取**应用密钥管理**的授权许可，具体操作参见授权操作。

备份密钥可以保存到密钥备份文件或者密钥存储UKEY中。

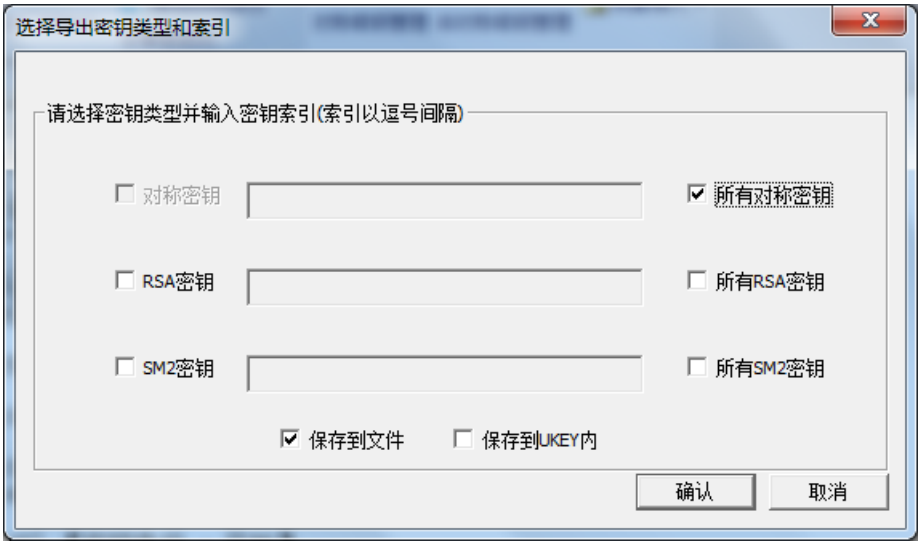
- 保存到密钥备份文件：备份导出密钥密文存储到用户选定的密钥备份文件中。
- 保存到UKEY中：备份密钥保存在密钥存储UKEY中。

说明：

3份密钥备份密钥UKEY（KBKUKEY）、备份文件（或备份密钥UKEY）需妥善保管，待密钥恢复时使用。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**密钥管理** > **备份导出**。



3. 设置备份密钥信息，单击**确认**。

表 1-8: 配置信息说明

配置项	说明
导出备份密钥类型	• 备份指定密钥：选择密钥类型，并输入密钥索引。 密钥索引格式为：num,num-num，例如1,2,4-7，等同于1,2,4,5,6,7。 • 备份全部密钥：选择**所有对称密钥**、**所有RSA密钥**、**所有SM2密钥**。
选择保存类型	• **保存到文件**：备份导出密钥密文存储到用户选定的密钥备份文件中。 • **保存到UKEY内**：备份密钥保存在密钥存储UKEY中。

4. 制作3份密钥备份密钥UKEY（KBKUKEY），单击**下一步**。

   a) PC插入空UKEY。

   b) 在**UKEY操作**中，单击**下一步**。

c) 选择空UKEY，单击**确定**，输入UKEY口令。

d) 根据步骤*4.a*~步骤*4.c*，依次制作3份KBKUKEY。

3份KBKUKEY分给3位密钥管理员保存。

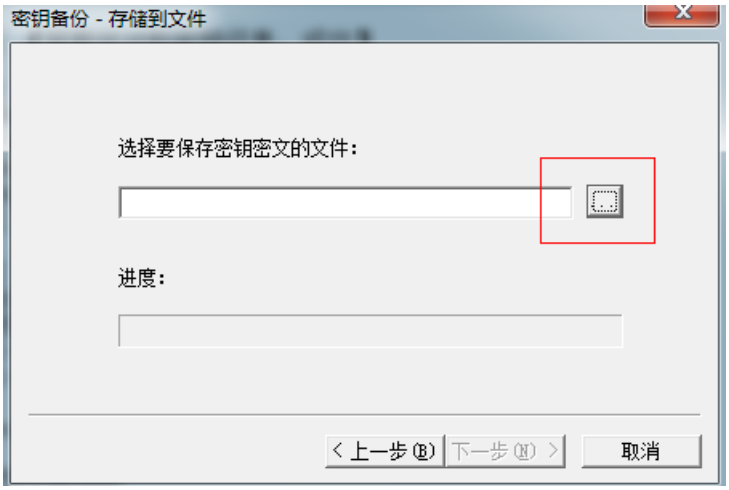
根据保存类型，选择下一步操作。

- 如果是**保存到文件**，跳转到步骤*5*。
- 如果是**保存到UKEY内**，跳转到步骤*6*。

5. （可选）备份密钥保存到文件。

备份密钥数据选择**保存到文件**使用本步骤。

a) 设置密钥备份文件的路径和名称。



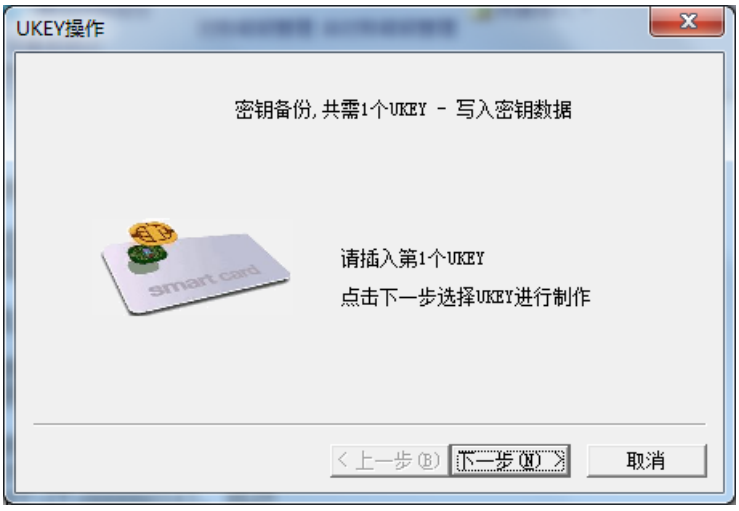
b) 单击**完成**。

进度条显示备份进度情况，完成后系统显示结果。

6. （可选）备份密钥保存到密钥存储UKEY内。

备份密钥数据选择**保存到UKEY内**使用本步骤。

a) 插入空UKEY，单击**下一步**。



b) 选择空UKEY，单击**确定**，输入UKEY口令。

c) 单击**完成**，结束密钥备份。

1.4.2.8.2 恢复密钥

该章节介绍了如何恢复密钥。

操作步骤

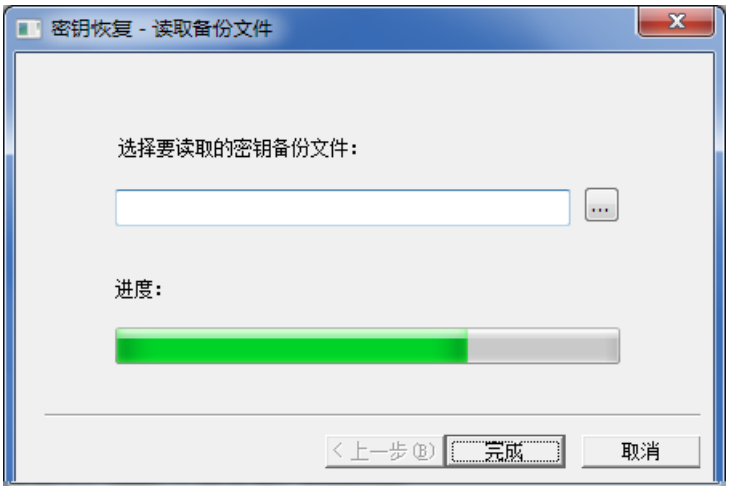
1. 登录*VsmManager*管理工具。
2. 单击**密钥管理** > **恢复导入**。
3. 选择恢复来源。
   - 从密钥备份文件中恢复，跳转到步骤*4*。
   - 从密钥存储UKEY中恢复，跳转到步骤*5*。
4. 从密钥备份文件中恢复密钥。

   密钥恢复需使用备份时制作的任意2个KBKUKEY和密钥备份文件。

   a) 单击**从文件中恢复密钥**。

   b) 插入任意2个KBKUKEY，输入口令，单击**下一步**。

   c) 选择需要恢复的密钥备份文件。



d) 单击**完成**。

5. 从密钥存储UKEY中恢复密钥。

a) 单击**从UKEY中恢复**。

b) 插入任意2个KBKUKEY，输入口令，单击**下一步**。

c) 插入密钥存储UKEY，恢复密钥。

1.4.3 设备管理

1.4.3.1 配置主机端口属性

该章节介绍如何配置主机端口属性。

背景信息

密码机和ECS之间的服务通讯方式出厂默认配置为明文通讯。

若要配置为密文通讯，则主机端口属性需要设置为密文通讯，同时还需要在TACSP安全代理软件进行相应的配置，以保证应用能够正常调用密码服务。密文通讯服务配置，参见配置密文通讯。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备管理** > **主机服务端口属性**。
3. 设置主机端口属性。

> **说明**：
> 需要根据实际需求正确配置主机端口属性。

表 1-9: 主机端口属性

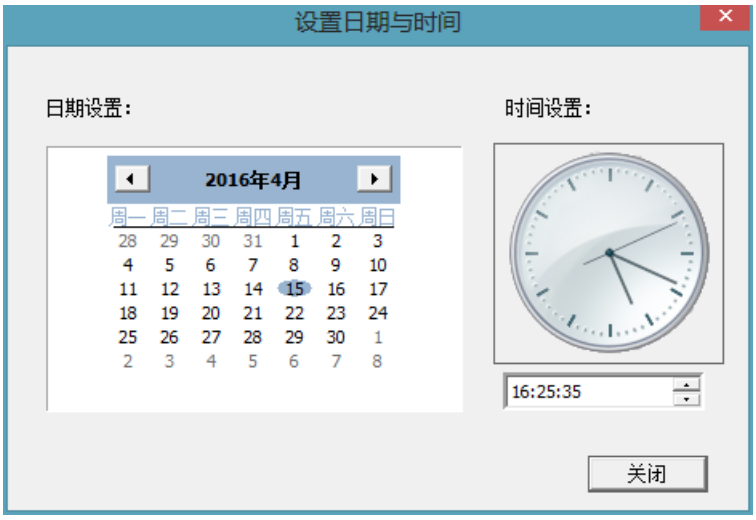
属性	说明
Socket KeepAlive时间	TCP连接保活探测时间，单位：秒。 取值范围：60~600
消息报文头长度	主机报文消息头长度，单位：字节。 取值范围：60~600
消息报文编码格式	主机报文的编码格式。 • ASCII • EBCDIC
主机服务通讯方式	• 明文通讯：与主机服务间的通讯为明文。 • 密文通讯：与主机服务间的通讯为密文。

1.4.3.2 配置设备时间

该章节介绍如何配置设备时间。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备管理** > **设备时间**。
3. 设置时间和日期。



1.4.3.3 授权管理

1.4.3.3.1 授权操作

该章节介绍如何进行授权。

背景信息

部分设备管理操作和主机指令应用需要获取授权许可，密码机支持严格灵活的授权管理控制。授权具有以下优点：

- 授权机制可配置

  支持1选1、3选2、5选3和无授权控制机制。授权控制机制需在初始化的过程中设置，完成初始化后不允许被修改。

- UKEY授权机制

  通过验证授权UKEY完成对授权人员的身份识别，安全可靠。

- 分类分时授权控制

  通过授权UKEY验证后，可选择本次授权的操作类别及给予授权的时间，当某类操作授权的时效过期后，其授权许可将自动失效。

说明：
初始化时，如果**授权机制**配置为无授权控制机制，所有的操作均不受限。则本章节不需要设置。

操作步骤

1. 登录*VsmManager*管理工具。

2. 单击**设备管理 > 操作授权。**
3. 根据提示依次插入授权UKEY，输入口令，单击**下一步。**

   系统将根据授权机制要求半数以上的授权UKEY验证通过。授权UKEY的验证次序无关，但重复验证无效。
4. 配置授权操作信息。

   可同时为多个类别授权不同的时限。

表 1-10: 授权类别说明

主类	子类	操作范围说明
设备管理	设备配置更新	重置端口属性，包括主机服务端口。
	应用密钥管理	• 随机产生内部存储的密钥。 • 成份形式合成对称密钥。 • 删除内部对称或非对称密钥。 • 清除内部对称或非对称密钥。 • 内部密钥备份导出。
主机服务	账户PIN解密	使用BA/NG主机命令。
	产生公钥MAC	使用EO/TQ主机命令。
	内部密钥更新	• KR/KD/KI/SI/TW/TY，内部存储模式的对称密钥的产生或导入。

主类	子类	操作范围说明
		• EI/EK/EJ/TS，内部存储模式的RSA密钥对的产生或导入。 • E0/E1/TU，内部存储模式的SM2密钥对的产生或导入。

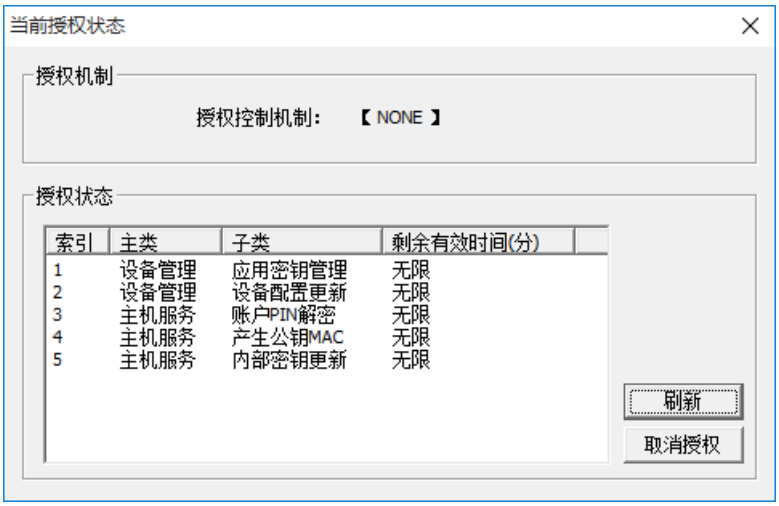
5. 单击**完成**。

1.4.3.3.2 获取授权状态

该章节介绍如何获取授权状态。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备管理** > **当前授权状态**。
3. 查看授权状态信息。



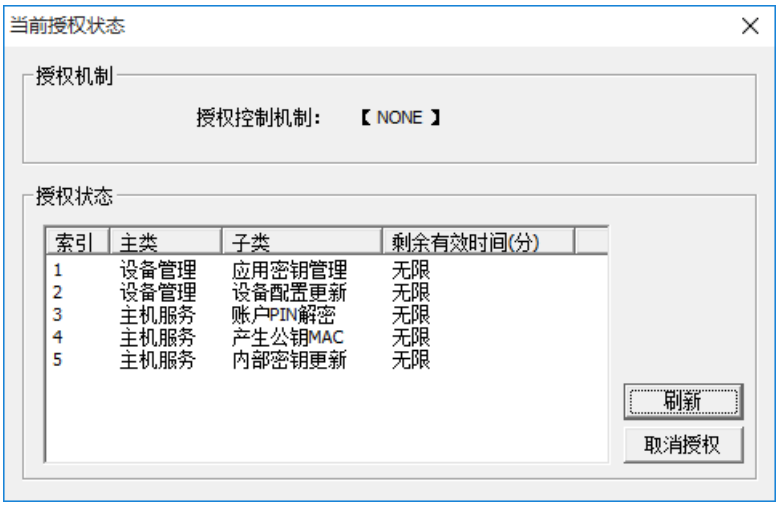
4. 单击**刷新**。

1.4.3.3.3 取消授权

该章节介绍如何取消授权。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备管理** > **当前授权状态**。
3. 在**授权状态**中选择授权类型。



4. 单击**取消授权**。

1.4.3.3.4 签发应用许可

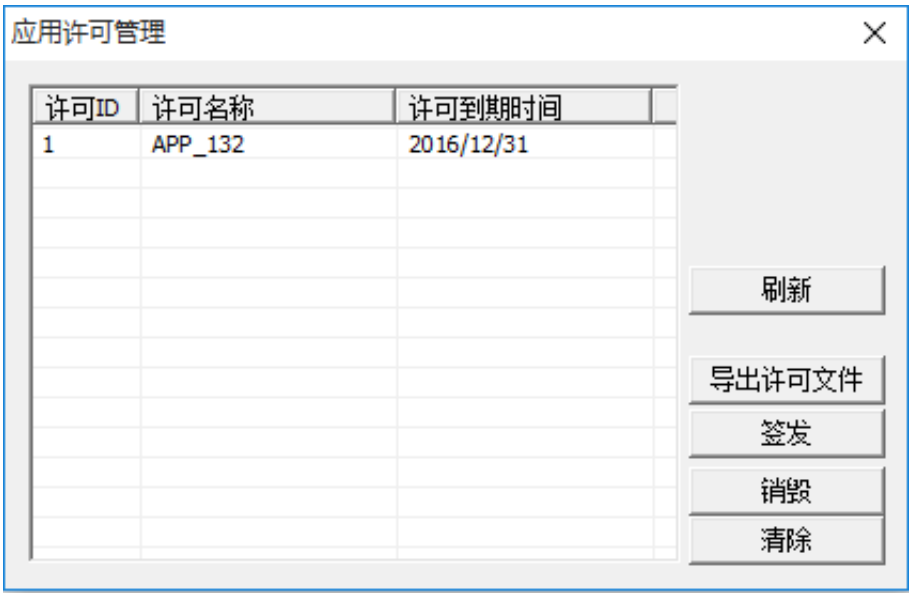
该章节介绍如何签发应用许可。

背景信息

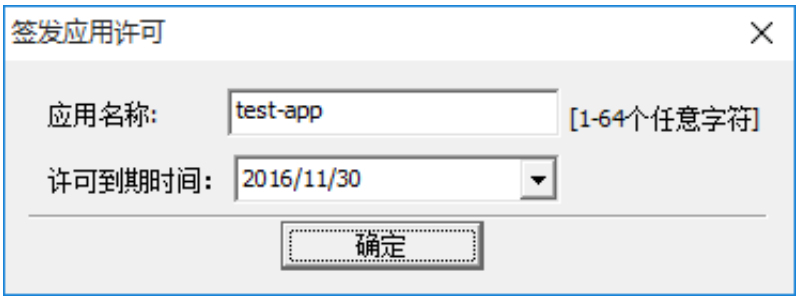
配置密文通讯时，需要为TACSP签发应用许可。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备管理** > **应用许可管理**。
3. 单击**签发**。



4. 设置应用名称和到期时间。



5. 单击**确定**。

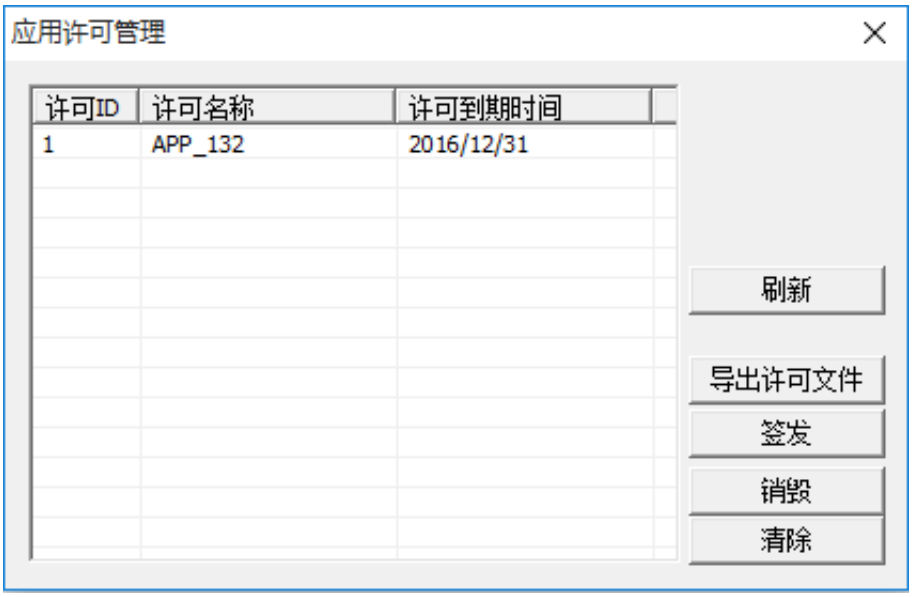
   生成应用许可文件（*.license*后缀的文件），并自动导出到VsmManager管理工具所在目录。

1.4.3.3.5 管理应用许可

该章节介绍如何管理应用许可。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备管理** > **应用许可管理**。
3. 查看应用许可列表。



4. 管理应用许可。

   - **导出许可文件**

     选择列表中已有的应用许可，单击**导出许可文件**，应用许可文件导出到VsmManager管理工具所在目录。

   - **销毁**

选择列表中已有的应用许可，单击**销毁**，应用许可文件将失效。

- **清除**

  单击**清除**，所有应用许可文件将失效。

1.4.3.4 UKEY管理

1.4.3.4.1 概述

该章节介绍UKEY的管理规则和分类。

UKEY管理操作不需要登录密码机即可执行，用户可根据系统的安全需求制定相应的UKEY管理规则，例如：

- 定义UKEY持有人和UKEY类型。
- UKEY进行格式化（个人化）操作。
- 重置用户标识。

UKEY分类说明参见表 *1-11: UKEY分类说明*。所有的UKEY在首次使用时，均需要输入保护口令。

表 1-11: UKEY分类说明

UKEY类别	说明	用途
主密钥成份UKEY	保存用户输入的设备主密钥DMK成份数据。	用于合成设备主密钥。
授权UKEY	保存设备授权信息数据。	用于授权管理的身份验证。
密钥备份密钥UKEY	保存密钥备份密钥KBK以秘密共享算法（2 of 3）分割后的秘密成份。	恢复密钥时使用任意2个恢复原KBK。
密钥存储UKEY	存储备份的密钥。	存储备份的密钥。
管理员UKEY	存储平台公钥，加密机信息等。	用户开机，协商通讯，以及整个管理工具与密码机通讯运算。

1.4.3.4.2 添加管理员

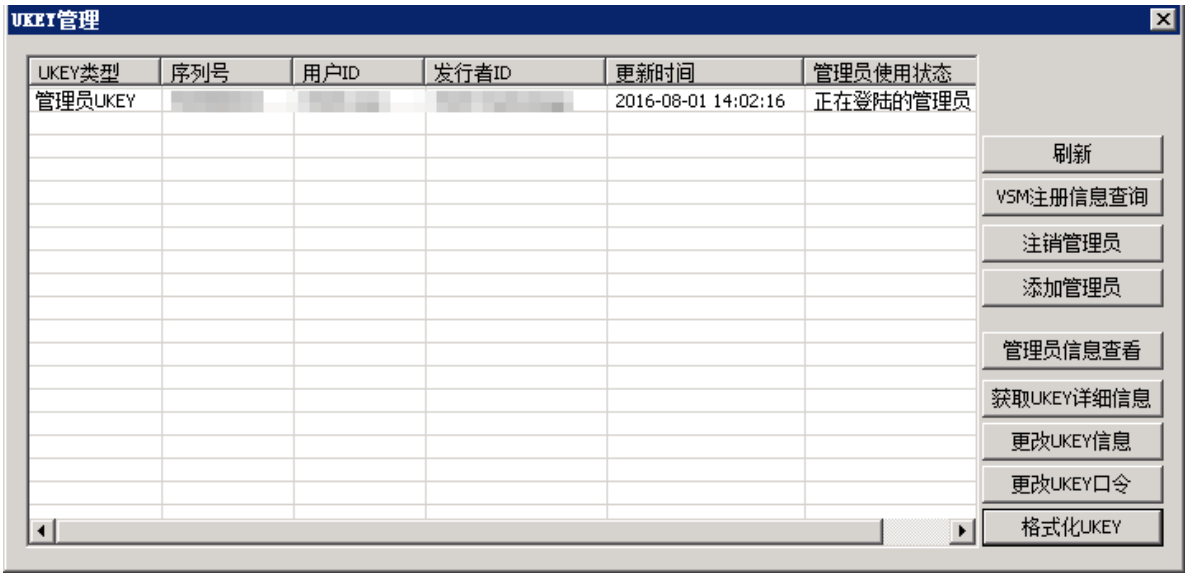
该章节介绍如何添加管理员。

背景信息

首次注册管理员请参考注册管理员*UKEY*。为了防止管理员UKEY丢失，建议另外添加几把管理员UKEY。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备管理** > **UKEY管理**。
3. PC插入空UKEY。
4. 在左侧列表中，选中空UKEY。



5. 单击**添加管理员**。

1.4.3.4.3 注销管理员

该章节介绍如何注销管理员。

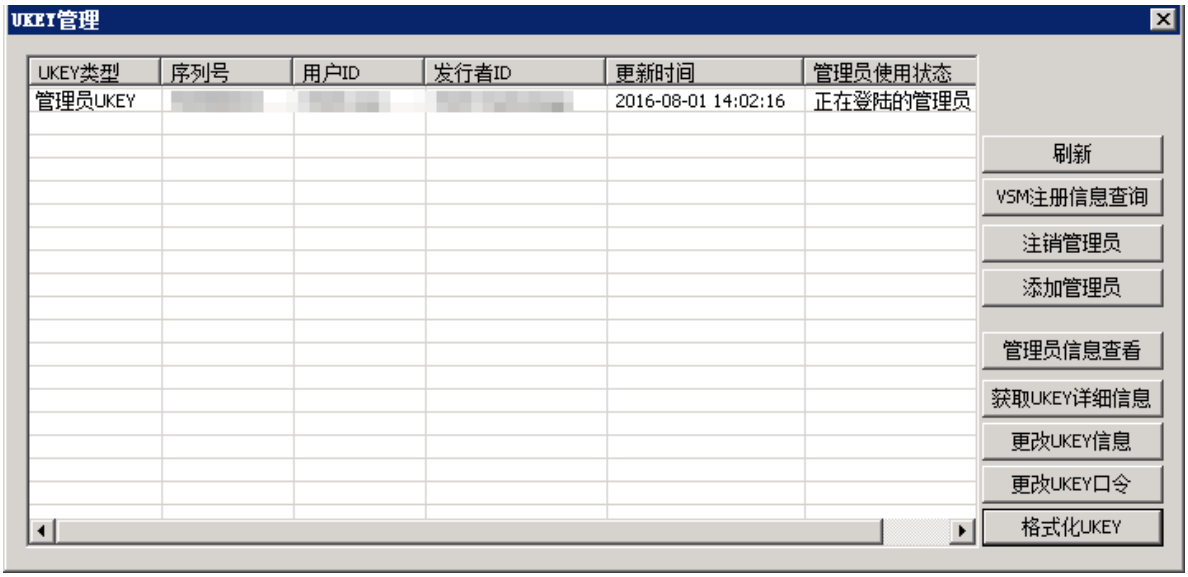
背景信息

说明：

只有选择正在登录的管理员UKEY，**注销管理员**操作才能生效。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备管理** > **UKEY管理**。
3. 在左侧列表中，选中正在登录的管理员UKEY。



4. 单击**注销管理员**。

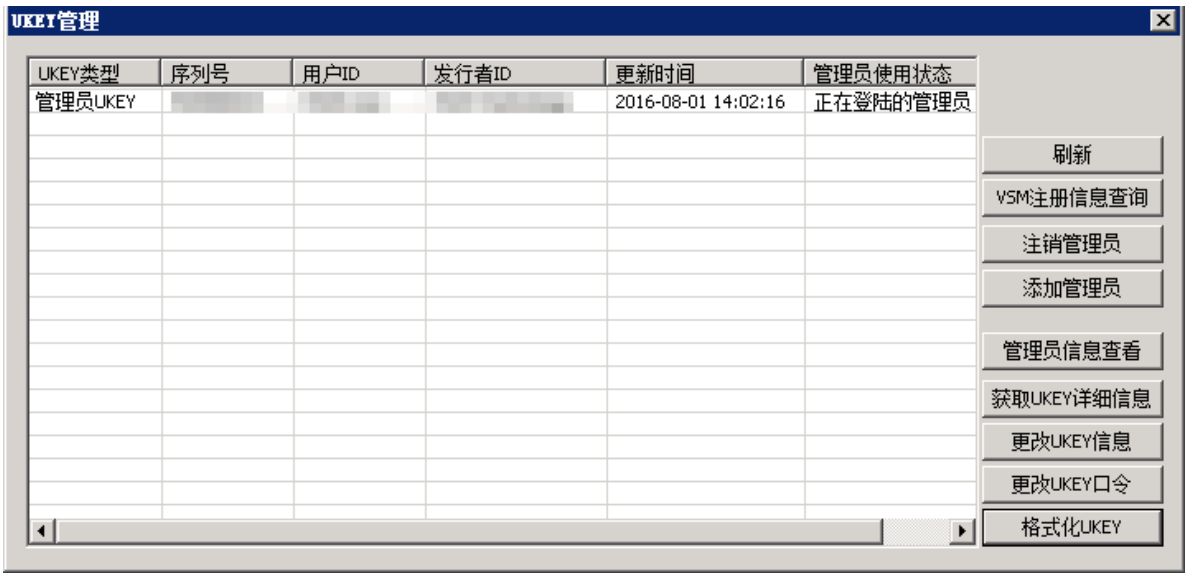
   注销成功后，VsmManager管理工具自动退出。

1.4.3.4.4 查询已注册的管理员UKEY信息

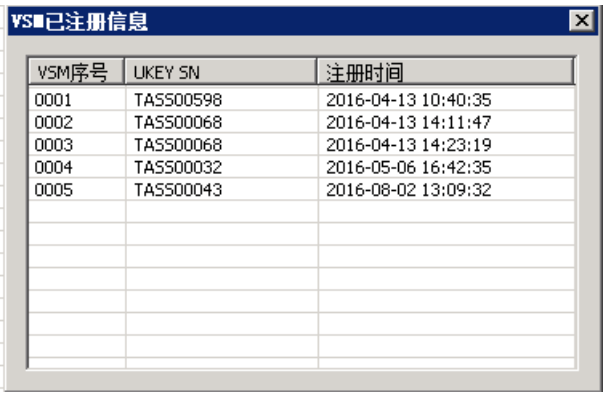
该章节介绍如何查询已注册的管理员UKEY信息。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备管理** > **UKEY管理**。
3. 单击**VSM注册信息查询**。



4. 查看已注册的管理员UKEY信息。

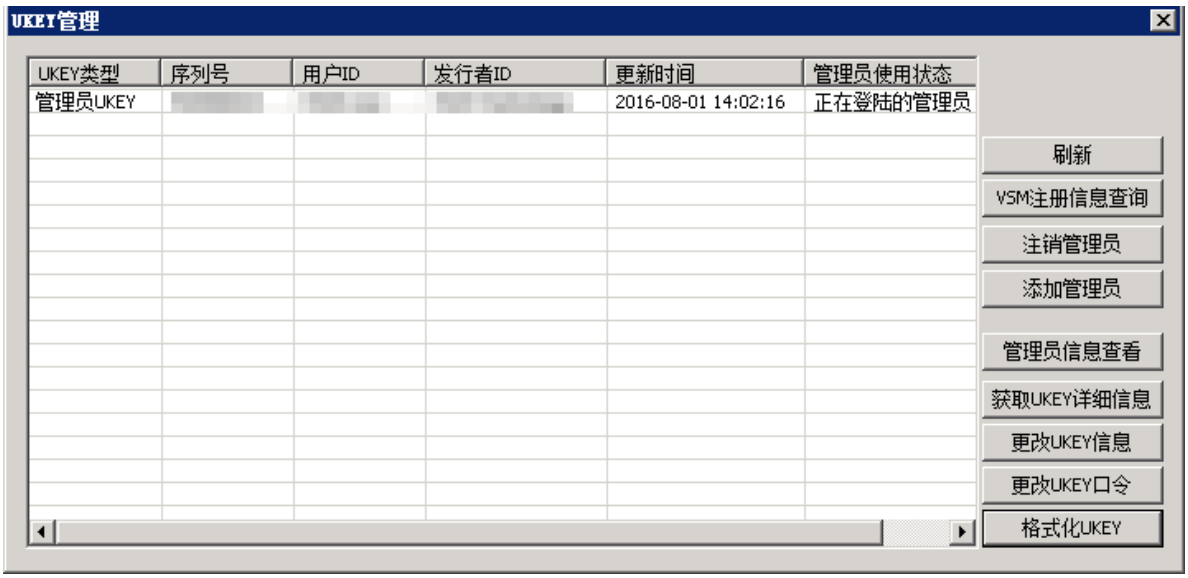


1.4.3.4.5 获取UKEY详细信息

该章节介绍如何获取UKEY详细信息。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备管理** > **UKEY管理**。
3. 在左侧选择UKEY，单击**获取UKEY详细信息**。



4. 查看UKEY详细信息。

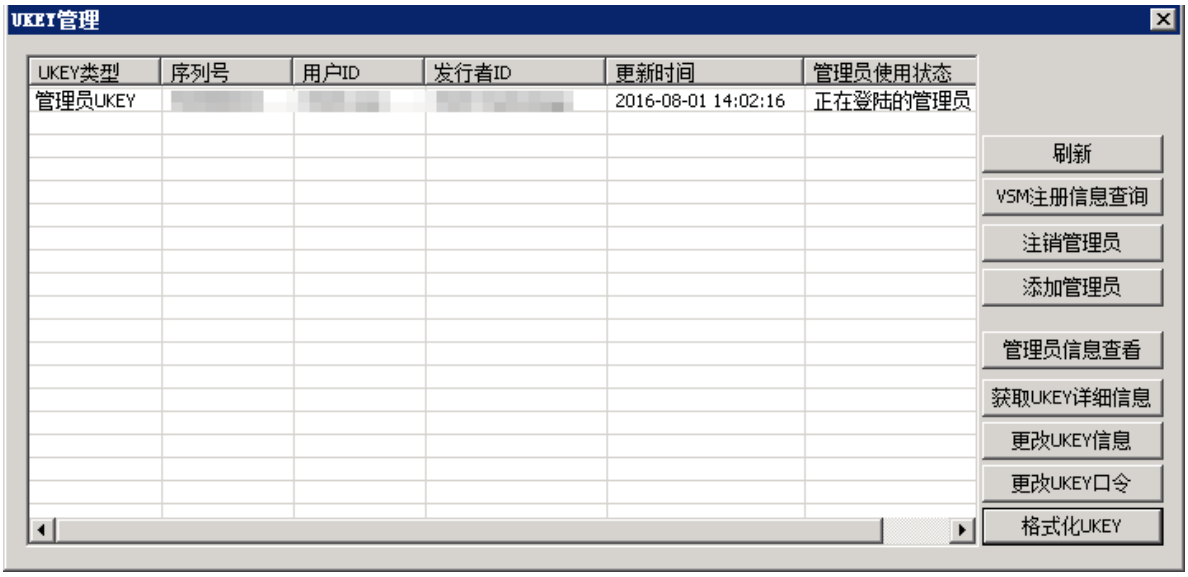
```
[2015-03-04 17:59:47] 【获取UKEY信息,
# UKEY序号  : T-00000015
# UKEY类型  : 密钥存储UKEY
# 格式化时间: 2015-02-09 17:18:00
# 制UKEY时间: 2015-03-04 17:01:20
# 持有人ID  : TASS_MXL
# 发行者ID  : TASS_TECHNOLOGY
# 密钥存储UKEY标识 : 0
```

1.4.3.4.6 更改UKEY信息

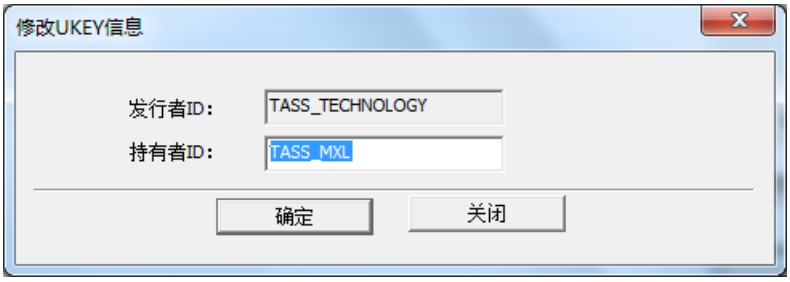
该章节介绍如何更改UKEY信息。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备管理** > **UKEY管理**。
3. 在左侧选择UKEY，单击**更改UKEY信息**。



4. 修改**持有者ID**。



5. 单击**确定**。

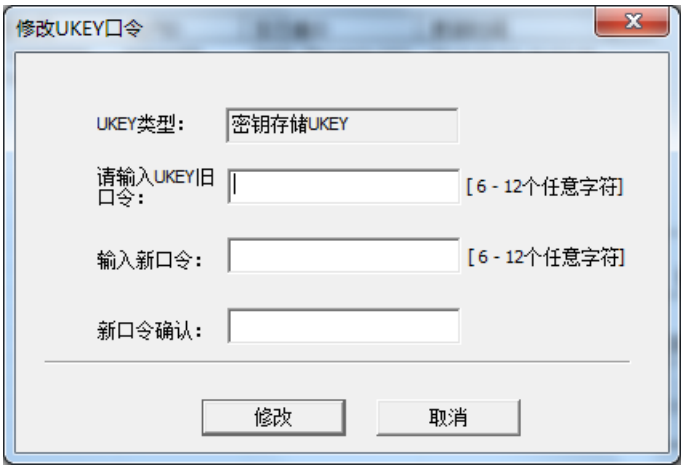
1.4.3.4.7 更改UKEY口令

该章节介绍如何更改UKEY口令。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备管理** > **UKEY管理**。
3. 在左侧选择UKEY，单击**更改UKEY口令**。

4. 修改UKEY口令。



5. 单击**修改**。

1.4.3.4.8 格式化UKEY

该章节介绍如何格式化UKEY。

背景信息

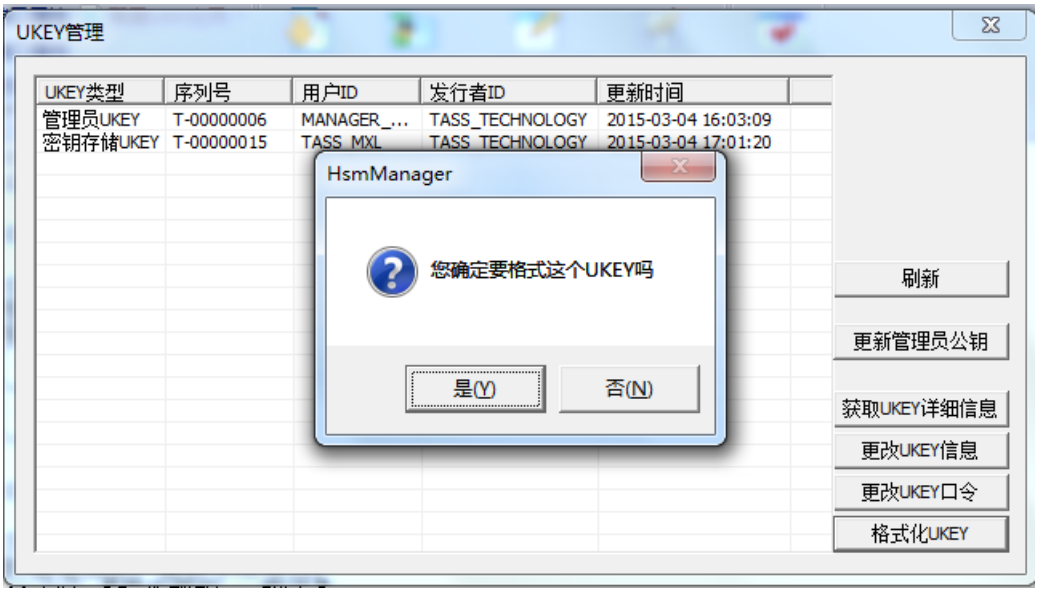
说明：

管理员UKEY不允许格式化。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备管理** > **UKEY管理**。

3. 在左侧选择UKEY，单击**格式化UKEY**。



4. 在确认提示框中，单击**是**。

   格式化后，UKEY内容重置为默认值（空UKEY）。

1.4.3.5 设备诊断维护

1.4.3.5.1 导出日志

该章节介绍如何导出日志。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备诊断维护** > **导出日志**。
3. 设置日志导出信息。

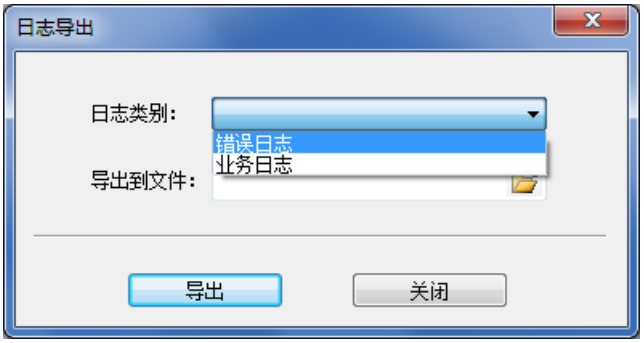


表 1-12: 日志导出

参数	说明
日志类别	导出日志类别： • 错误日志 • 业务日志
导出到文件	选择导出日志保存在本地的路径和文件名。

4. 单击**导出**。

1.4.3.5.2 清除日志

该章节介绍如何清除日志。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备诊断维护** > **清除日志**。
3. 在确认提示框中，单击**是**。

   操作完成后，密码机将清除全部日志。

1.4.3.5.3 查看设备基础信息

该章节介绍如何查看设备基础信息。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备诊断维护** > **设备基础信息**。
3. 查看设备基础信息。

```
[2016-04-14 17:22:01] 【获取设备基础信息，成功】
# 设备主密钥校验值: DF0ED66BFA4DC70F
# 主机服务版本号   : H1.24.06
# 管理服务版本号   : M1.17.00
# 加密卡版本号     : C1.16.09
```

1.4.3.5.4 设备自检

该章节介绍如何进行设备自检。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备诊断维护** > **设备自检**。
3. 检测关键单元情况。

```
[2016-04-14 17:22:22] 【设备自检，成功】
# 物理噪声源检测   : OK
# SM2算法单元检测 : OK
# SM3算法单元检测 : OK
# SM4算法单元检测 : OK
# 密钥库完整性检测: OK
```

1.4.3.5.5 查看主机服务状态

该章节介绍如何查看主机服务状态。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备诊断维护** > **主机服务状态**。
3. 查看主机服务状态。

```
[2016-04-14 17:22:44] 【获取服务连接状态，完成】
# 主机服务: 正常
# 支持的最大连接数: 64
# 当前已使用连接数: 10
# 剩余可用连接数   : 54
```

1.4.3.5.6 查看设备资源信息

该章节介绍如何查看设备资源信息。

操作步骤

1. 登录*VsmManager*管理工具。
2. 单击**设备诊断维护** > **设备资源信息**。
3. 查看设备资源信息。

```
[2016-04-14 17:23:15] 【获取密码机资源占用信息，成功】
# 内存占用率: 7.84%
# CPU占用率 : 0.25%
```

1.5 TACSP管理

1.5.1 配置TACSP

该章节介绍如何配置TACSP安全代理软件。TACSP安全代理软件基于密码机的安全应用而设计开发的安全代理软件，是集多机热备、负载均衡功能为一体的密码机应用平台。

前提条件

ECS和密码机在同一个VPC网络中。

背景信息

TACSP安全代理软件支持的操作系统和加密方式如下。

- 操作系统：支持Linux、AIX、HP-UNIX等类UNIX操作系统。
- 加密方式：支持以Socket方式提供密码安全服务，应用程序通过socket方式访问安全代理软件。

操作步骤

1. 通过FTP软件上传TACSP安全代理软件到业务ECS。
2. 通过SSH登录业务ECS。
3. 进入TACSP所在路径。
4. 配置*tacsp_cfg.ini*。

   *tacsp_cfg.ini*配置文件内容如下：

```
[TACSP_IPC]
COMMAND_QUEUE_KEY           = 130
RESPONSE_QUEUE_KEY          = 131
SHARED_MEMORY_KEY           = 132
LOG_LEVEL                   = 1

[TACSP_SERVERINFO]
LISTEN_IP_FLG               = 0
LISTEN_PORT                 = 9999
HSM_LOADSIZE                = 2
HSM_LOADSELF                = 0

[TACSP_HSMINFO]
HSM_COUNT                   = 0
TOTAL_TIMEOUT               = 6
SINGLEHSM_TIMEOUT           = 2

[TACSP_HSM00]
HSM_TYPE                    = SJJ1310
HSM_IP                      = 192.168.19.51
HSM_PORT                    = 8018
HSM_WEIGHT                  = 10
HSM_ENC_COMM                = 0

[TACSP_HSM01]
```

```
HSM_TYPE                = SJJ1310
HSM_IP                  = 192.168.119.102
HSM_PORT                = 8018
HSM_WEIGHT              = 10
HSM_ENC_COMM            = 1
```

表 1-13: 配置说明

节点	键名	说明
TACSP_IPC	-	TACSP使用的IPC相关ID。
	COMMAND_QUEUE_KEY	TACSP使用2个队列和1个共享内存。 此处配置的队列ID和共享内存ID，必须确保与当前系统中的相关ID不冲突。 取值范围：1~65537
	RESPONSE_QUEUE_KEY	
	SHARED_MEMORY_KEY	
	LOG_LEVEL	日志级别： • *0*：不记录任务日志。 • *1*：记录错误日志。 • *2*：记录连接信息。 • *3*：记录调试信息日志。
TACSP_SERVERINFO	-	对外提供socket服务配置信息。
	LISTEN_IP_FLG	• *0*：默认值，监听127.0.0.1 • *1*：监听0.0.0.0
	LISTEN_PORT	负载热备对外提供的监听端口。 取值范围：1025~65535
	HSM_LOADSIZE	头部中表示报文长度的字节数。
	HSM_LOADSELF	头部表示报文长度中是否包含自身长度： • *0*：不包含 • *1*：包含
TACSP_HSMINFO	-	密码机相关信息
	HSM_COUNT	密码机数量。 取值范围：1~20
	TOTAL_TIMEOUT	每次socket通讯总的超时时间，单位：秒。

节点	键名	说明
		建议取值：加密机个数 * 单台加密机通讯超时 + 2
	SINGLEHSM_TIMEOUT	每台加密机每次socket通讯的超时时间，单位：秒。
TACSP_HSM*xx*	-	某索引密码机的信息，有n个密码机，必须有n个节配置。 *xx*取值范围：00~（n-1）
	HSM_TYPE	密码机类型
	HSM_IP	密码机的IP地址
	HSM_PORT	密码机的端口号
	HSM_WEIGHT	密码机的工作权重，即安全代理软件和此台加密机有多少个socket连接。 取值范围：1~65
	HSM_ENC_COMM	和密码机的通讯模式： • *0*：明文通讯 • *1*：密文通讯

5. （可选）配置环境变量TACSPCFG和CLUSTERDEBUG环境变量。

> **说明**：
> 如不配置TACSPCFG，则配置文件必须在TACSP安全代理软件所在的路径下；如不CLUSTERDEBUG配置，则日志将默认输出在TACSP安全代理软件所在的路径下。

a) 编辑*/etc/profile*。

```
# vi /etc/profile
```

b) 在*/etc/profile*中添加变量。

```
export TACSPCFG=tacsp_cfg.ini所在目录
```

```
export CLUSTERDEBUG=日志存储目录
```

c) 使环境变量立即生效。

```
source /etc/profile
```

1.5.2 配置密文通讯

该章节介绍如何配置密文通讯。

背景信息

密文通讯方式是指应用主机与密码机之间的通讯采用加密的方式，能够在专有云的环境下提供更安全更可靠的加密服务。

操作步骤

1. 配置主机端口属性。

   主机服务通讯方式修改为密文通讯。

2. 签发应用许可证。

   应用许可的内容包括VSM设备公钥、TACSP公私钥、应用名称、签发时间、到期时间及设备私钥对前述内容的签名。

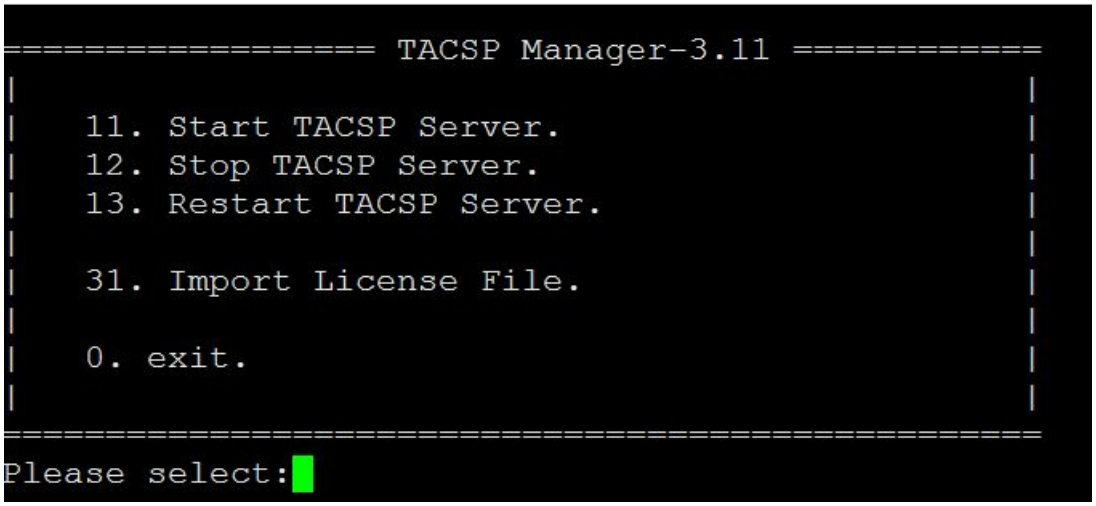
   说明：
   如果有多个密码机，分别导出应用许可证。

3. 应用许可证通过FTP上传到TACSP安全代理软件所在路径。

4. 导入应用许可证。

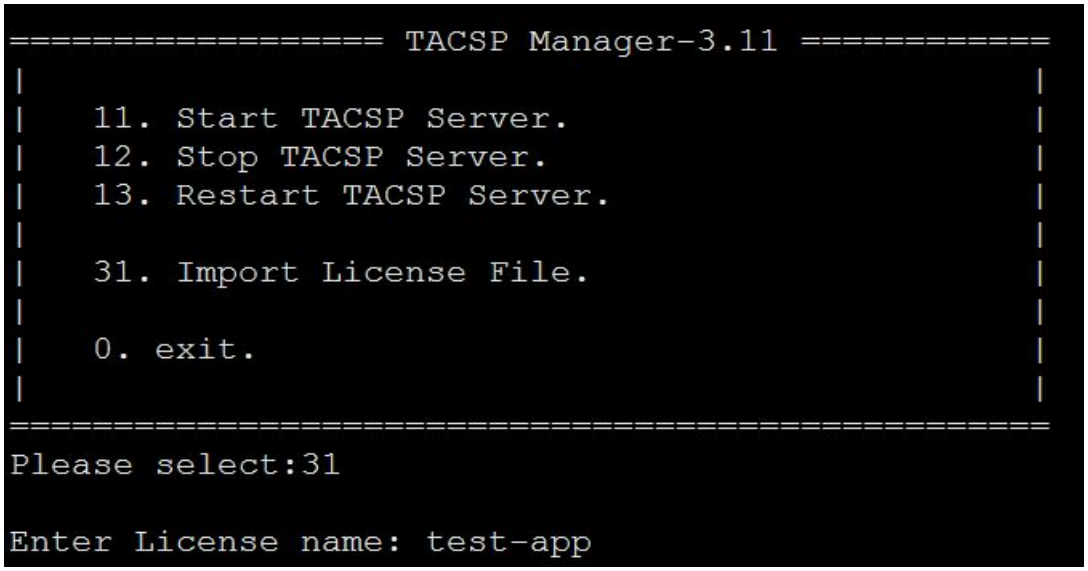
   a) SSH登录ECS并进入TACSP安全代理软件所在路径。

   b) 执行**./keyMng**。



c) 输入*31*，按回车键（Enter）。

开始导入应用许可证。



d) 输入许可证名称，按回车键（Enter）。

e) （可选）重复步骤*4.c*~步骤*4.d*，导入其他加密机的应用许可证。

如果有多台密码机，则需要依次导入其他密码机的应用许可证。

f) 输入*11*，启动TACSP安全代理软件。

如果TACSP已经启动，则输入*13*，重启TACSP。

1.5.3 启动TACSP

该章节介绍如何启动TACSP。

操作步骤

1. 通过SSH软件登录ECS。

2. 进入TACSP所在路径。
3. 执行**./keyMng**。
4. 输入*11*，按回车键（Enter）。

1.5.4 重启TACSP

该章节介绍如何重启TACSP。

操作步骤

1. 通过SSH软件登录ECS。
2. 进入TACSP所在路径。
3. 执行**./keyMng**。
4. 输入*13*，按回车键（Enter）。

1.5.5 停止TACSP

该章节介绍如何停止TACSP。

操作步骤

1. 通过SSH软件登录ECS。
2. 进入TACSP所在路径。
3. 执行**./keyMng**。
4. 输入*12*，按回车键（Enter）。

1.5.6 设置TACSP日志级别

该章节介绍如何设置TACSP日志级别。

背景信息

修改TACSP日志级别：

- 未启动TACSP，修改LOG_LEVEL参数值，具体参考配置*TACSP*。
- 已启动TACSP，可以按照本章节修改。

操作步骤

1. 通过SSH软件登录ECS。
2. 进入TACSP所在路径。
3. 执行**./setlog** *log_level*。

*log_level*取值如下：

- *0*：不记录任务日志。
- *1*：记录错误日志。
- *2*：记录连接信息。
- *3*：记录调试信息日志。

1.5.7 停止连接密码机

该章节介绍TACSP如何停止连接密码机

背景信息

在TACSP已经启动成功的情况下，可以单独停止连接某台密码机。此功能适用情况：

- 需要确认密码机无处理中的业务。
- 仅用于替换密码机时使用。

操作步骤

1. 通过SSH软件登录ECS。
2. 进入TACSP所在路径。
3. 执行**./keyMng stop** *ip*。

   *ip*为密码机IP地址。

   通过查看*tacsplog*日志文件，确认执行结果是否成功。

1.5.8 启动连接密码机

该章节介绍TACSP如何启动连接密码机。

背景信息

在TACSP已经启动成功的情况下，停止连接某台密码机后，可以进行重新连接。此功能适用情况：

- 确认新连接的密码机已经写入配置文件，且TACSP和密码机之间通讯畅通。
- 仅用于动态增加密码机时使用。

操作步骤

1. 通过SSH软件登录ECS。
2. 进入TACSP所在路径。
3. 执行**./keyMng start** *ip*。

*ip*为密码机IP地址。

通过查看*tacsplog*日志文件，确认执行结果是否成功。

1.6 调用加密实例

1.6.1 创建Demo实例

该章节介绍如何创建Java的Demo实例。

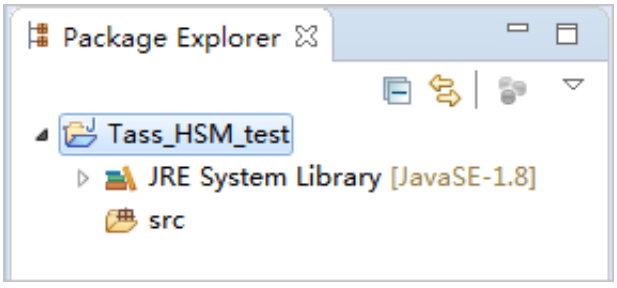
背景信息

VsmManager管理工具和密文通讯方式配置完成后，您就可以通过调用API接口，使用加密服务。

本章节创建JAVA的Demo实例后，您可以通过JAVA源文件了解如何调用加解密的API接口，实例说明参见*Demo*实例说明。

操作步骤

1. 在Eclipse中新建Java工程。
   a) 单击**File** > **New** > **Java Project**。
   b) 在**Project name**中输入工程名称。
   c) 单击**Finish**。
   创建Java工程实例如下所示。



2. 导入jar包。
   加密服务需要的3个jar包：
   - *TassHsmApihsmGeneralFinance_1.47.2529.jar*
   - *TassHsmDriver_SJJ1310_3.83.2529.jar*
   - *TassHsmFrame_2.57.2526.jar*

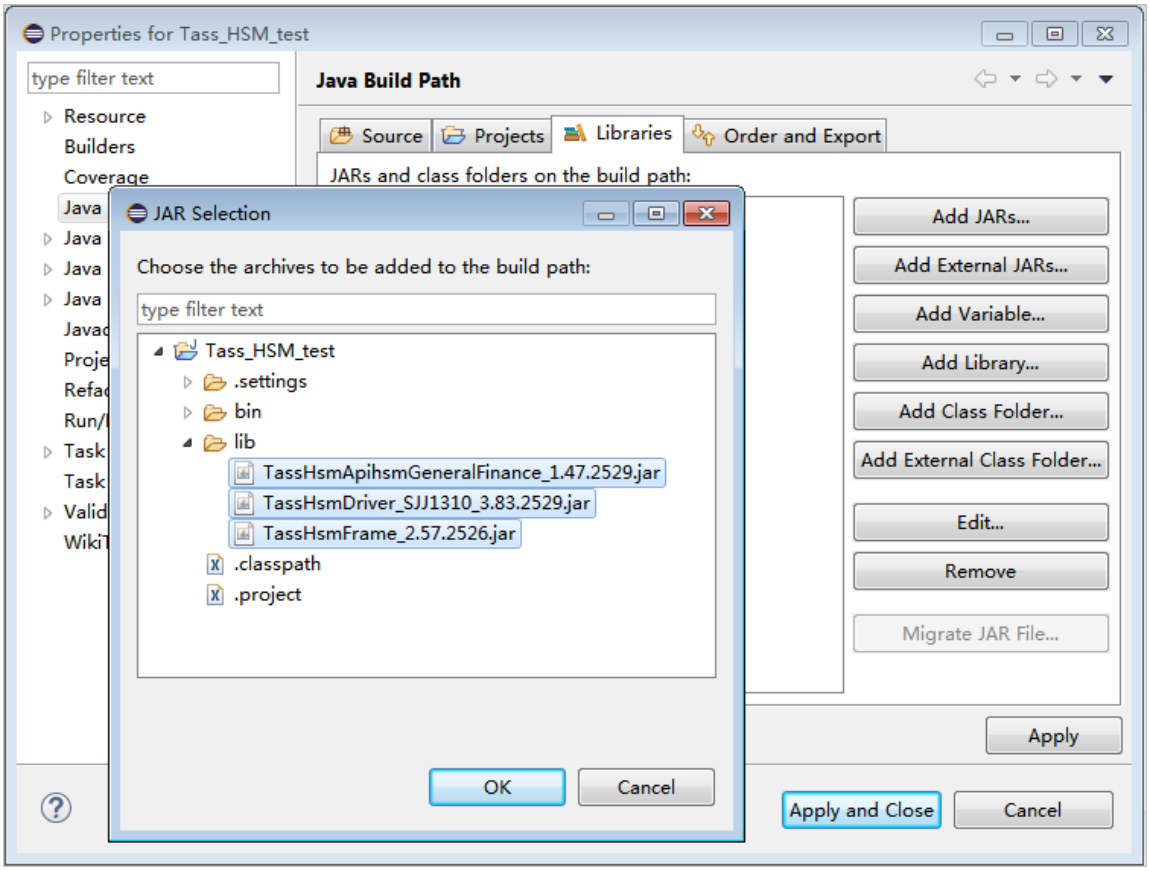
   a) 右键单击工程名称，选择**New** > **Folder**。
   b) 在**Folder name**中输入*lib*，单击**Finish**。

c) 复制*TassHsmApihsmGeneralFinance_1.47.2529.jar*、*TassHsmDriver_SJJ1310_3.83.2529.jar*、*TassHsmFrame_2.57.2526.jar*包。

d) 右键单击**lib**，选择**Paste**。

e) 右键单击工程名称，选择**Build Path** > **Configure Build Path**。

f) 选择**Libraries**页签，单击**Add JARs**。



g) 选择*lib*中的3个jar包，单击**OK**。

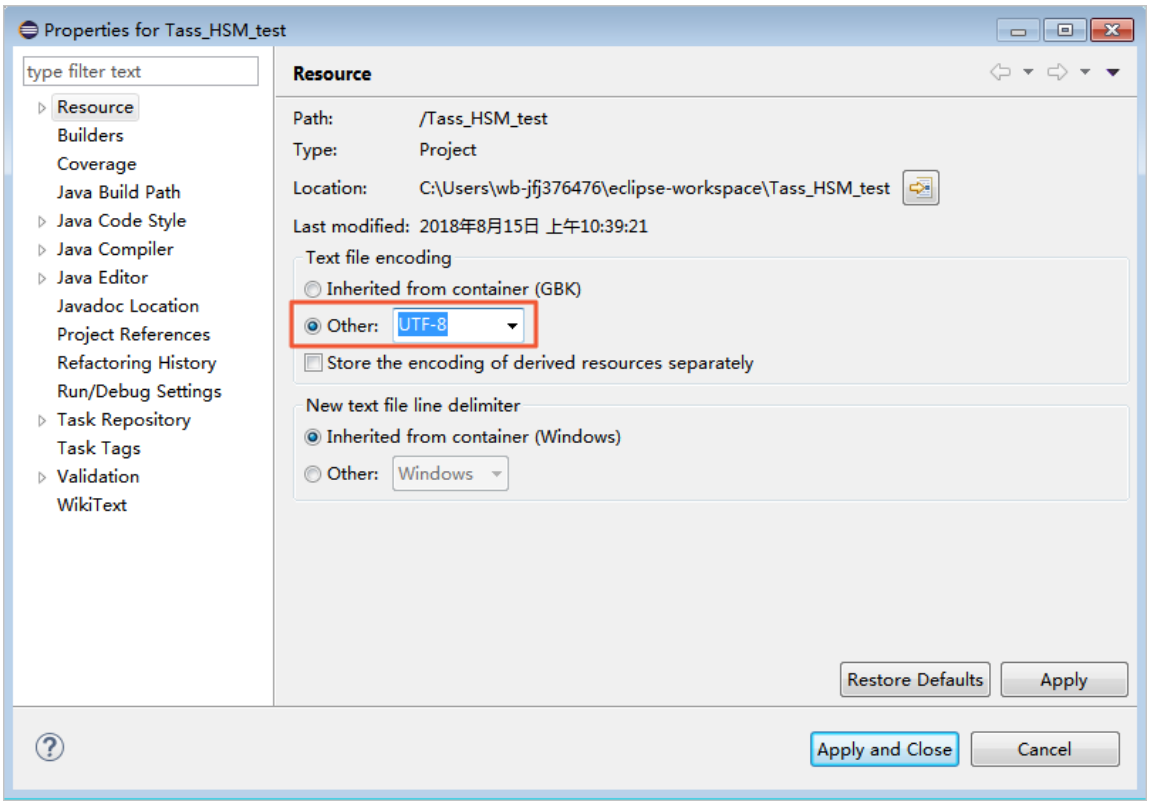
h) 单击**Apply and Close**。

3. 修改编码格式为*UTF-8*。

a) 右键单击工程名称，选择**Properties**。

b) 单击**Resource**。

c) 在**Text file encoding**中选择**Other**，并在下拉菜单中选择*UTF-8*。



d) 单击**Apply and Close**。

4. 复制Java实例文件到工程中。

   Java demo文件：*test_hsmGeneralFinance.java*。

   a) 复制*test_hsmGeneralFinance.java*。

   b) 右键单击*src*目录，选择**Paste**。

1.6.2 Demo实例说明

该章节介绍Demo实例。

实例化接口

以配置文件形式实例化接口，代码如下：

```
hsmGeneralFinance hgf = hsmGeneralFinance.getInstance("F:\\cacipher.ini");
```

*cacipher.ini*文件说明如下：

```
[LOGGER]
logsw          =      error,info
logPath        =      F://error
[HOST 1]
hsmModel       =      SJJ1310
linkNum        =      1
host           =      192.168.19.132
```

```
port          =     8018
timeout       =     15
encodetype    =     0
msgheadlength =     0
```

表 1-14: 配置说明

配置项		说明
[LOGGER]	logsw	输出日志的类型。
	logPath	输出日志的路径。
[HOST 1]	hsmModel	密码机型号：*SJJ1310*。
	linkNum	连接数，取值范围：1~64。
	host	密码机的IP。
	port	端口，固定为8018端口。
	timeout	设置为默认值。
	encodetype	设置为默认值。
	msgheadlength	设置为默认值。

对称加解密

对称加解密代码如下：

```
int algType = 0;
  String keyType = "00A";
  int symmKey = 1;
  String disperFactor = null;
  int sessionType = 0;
  String sessionFactor = null;
  int padFlag = 1;
  byte [] inData = mm.getBytes();
  String IV = "1111111111111111";
  byte [] symmEnc = hgf.generalDataEnc(algType, keyType, symmKey, disperFactor,
sessionType, sessionFactor, padFlag, inData, IV);
  System.out.println("16进制字符串输出对称加密结果"+Forms.byteToHexString(symmEnc));

  byte [] symmDec = hgf.generalDataDec(algType, keyType, symmKey, disperFactor,
sessionType, sessionFactor, padFlag, symmEnc, IV);
  System.out.println("字符串输出解密结果"+new String (symmDec));
```

- 对称加解API为generalDataEnc，具体说明参见《云盾*API*》中的generalDataEnc章节。
- 对称解密API为generalDataDec，具体说明参见《云盾*API*》中的generalDataDec章节。

RSA非对称加解密

RSA非对称加解密代码如下：

```
padFlag = 1;
  byte [] indata = mm.getBytes();
  int RSAkeyPair = 1;
  byte[] RsaPublicKeyEnc = hgf.RsaPublicKeyEnc(padFlag, indata, RSAkeyPair);
  System.out.println("16进制字符串输出RSA公钥解密结果"+Forms.byteToHexString(RsaPublicK
eyEnc));

  byte[] RsaPrivateKeyDec = hgf.RsaPrivateKeyDec(padFlag, RSAkeyPair, RsaPublicKeyEnc);
  System.out.println("输出RSA私钥解密结果"+new String(RsaPrivateKeyDec));
```

- RSA非对称加解API为RsaPublicKeyEnc，具体说明参见《云盾*API*》中的RsaPublicKeyEnc章节。
- RSA非对称解密API为RsaPrivateKeyDec，具体说明参见《云盾*API*》中的RsaPrivateKeyDec章节。