云加密服务—
EVSM 管理工具用户使用手册
（专业版）V1.3

北京江南天安科技有限公司

2017 年 11 月

要了解更多关于我们的产品，服务和支持信息，请访问：http://www.tass.com.cn

云加密服务—EVSM 管理工具用户使用手册 V1.2

最新发行日期：2016 年 11 月

声明

本手册由北京江南天安科技有限公司编写，仅随 VSM 配送给用户和合作伙伴参阅。本公司保留有对本手册进行重新修订的权利，随时可能对手册中出现的错误、与最新资料不符之处等做必要的修改和升级，且不另行通知，但全部编入新版用户手册中。

本公司依中华人民共和国著作权法，享有及保留对本手册的所有权和解释权，任何公司和个人未经允许，不得擅自使用、复制、修改、传播本手册的内容。

此手册适用于 EVSM1.25.11 以上的版本，对应的 VSM 管理工具版本为 1.2.2.6，tacsp 版本为 3.11 。

北京江南天安科技有限公司

二〇一六年十一月

手册目录

图表目录

1. 江南天安金融数据 VSM 简述

江南天安金融数据 VSM（简称：EVSM）是以现代密码技术为核心的主机安全模块，具有自主密钥管理机制，能将密码运算过程封装在其内部完成，为业务系统提供安全的应用层密码服务，包括密钥管理、消息验证、数据加密、签名的产生和验证等，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。

作为传统密码设备的升级换代产品，在支持原有金融业务安全需求的基础上，扩展了 SM1、SM2、SM3、SM4 国产密码算法在金融领域中的应用支持，符合 PBOC1.0/2.0/3.0、GP、EMV2000 等应用规范，以及社保、建设部、交通等行业规范。在金融领域支持网上银行、业务前置系统、主机系统、发卡系统、密钥管理等业务系统上的应用，同时支持能源、社保、交通等一卡通应用领域。

金融数据 VSM 为业务系统提供密码安全服务，包括：

- 密钥管理，密钥的安全存储和使用、分散产生子密钥、安全报文形式导入导出 EVSM；
- 数据加密，对称 SM1/SM4/DES/AES 算法加解密和非对称 SM2/RSA 算法的数据加解密；
- 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；
- 签名验签，非对称 SM2/RSA 算法的签名验签运算；

2. 快速使用 EVSM

江南天安 EVSM 作为主机密码安全服务器，应部署在 VPC 网络内部，且必须是一个安全可控的环境。

EVSM 正常启动后，设备管理人员需要对 EVSM 进行必要的正确配置管理，包括设备的初始化和属性设置等操作。

2.1. 登录

- **直接登录**

打开 VsmManager.exe 文件，点击“系统——VSM 登录管理”，如下图：

图 2-1 系统登录

在弹出的页面中，输入 EVSM 的 IP 地址及端口号（端口号固定为 8013）。点击“登录”即可登录 VSM 管理系统，如下图

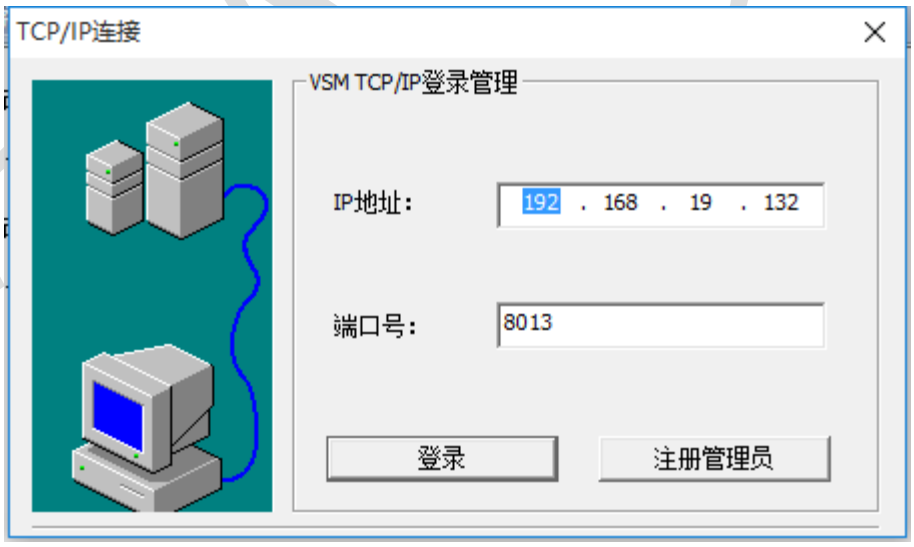

图 2-2 系统登录

当弹出下面界面后，证明登录成功。

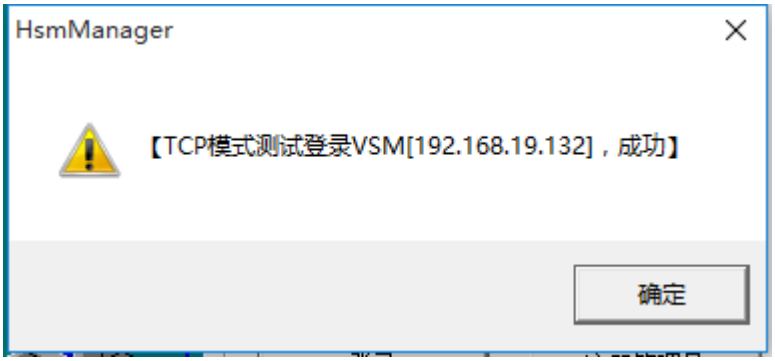

图 2-3 系统登录成功

注：在没有注册管理员的情况下直接登录系统，不可以对 EVSM 进行原始初始化和恢复初始化工作，即，不可以更改 EVSM 的主密钥，仅可以在测试主密钥的环境下进行密钥管理。

- **注册管理员**

打开 VsmManager.exe 文件，点击“系统——VSM 登录管理”，在弹出的页面中，输入 EVSM 的 IP 地址及端口号（端口号固定为 8013），如下图：

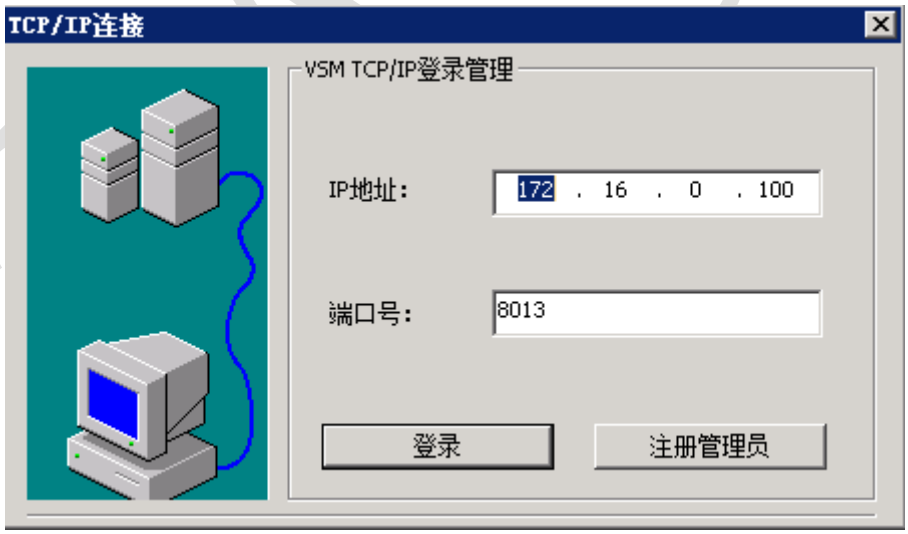

图 2-4TCP/IP 连接

插入 UKEY，点击“注册管理员”，在弹出的页面中，选择插入的 UKEY 并确定，如下图：

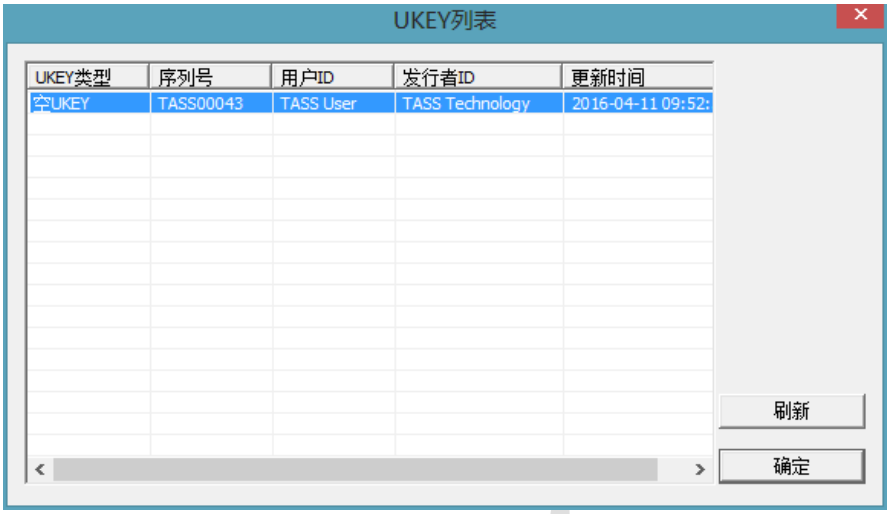

图 2-5 注册管理员

输入口令点击“确定”完成管理员的注册。EVSM 出厂时默认的 UKEY 管理登录口令为“12345678”。

- 登录系统

点击“登录”，在 KEY 列表中选择管理员 KEY 并确定，如下图：

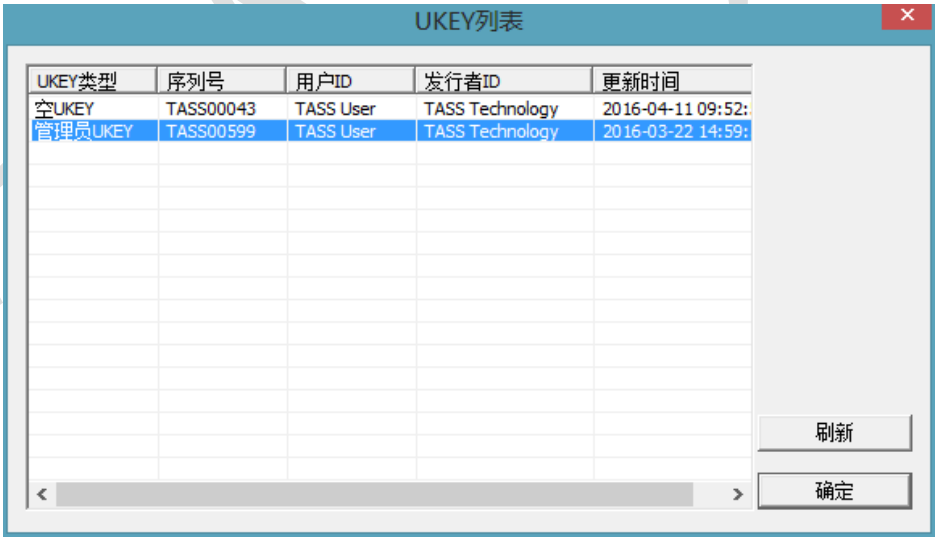

图 2-6 选择管理员

在弹出的对话框中输入 UKEY 的口令，点击“确定”即可登录，如下图：

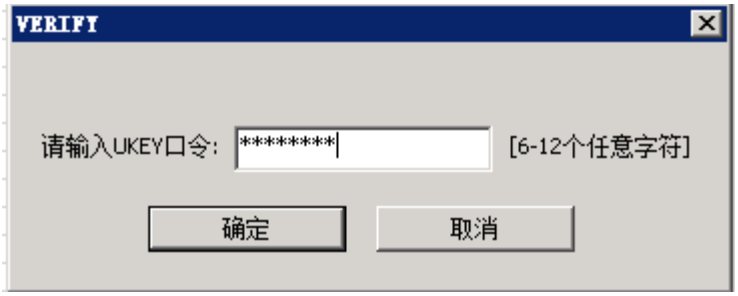

图 2-7 系统登录

如果登录成功会弹出登录成功对话框，点击“确定”登录系统。如下图：

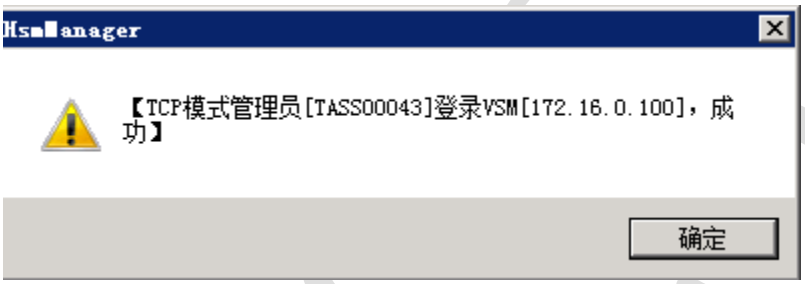

图 2-8 系统登录成功

2.2. EVSM 初始化

EVSM 启动后默认完成了出厂初始化的工作，内部装有测试主密钥，无授权控制机制。适用于业务系统的测试开发环境下的开发调试，仅需正确配置设备的服务端口属性即可。

当 EVSM 要安装到正式的生产环境时，必须对设备进行原始初始化操作，流程包括重置设备主密钥、设置授权机制、制作授权 UKEY。

原始初始化准备工作

- 设定 2–8 位设备主密钥 DMK 管理人员、1 或 3 或 5 位设备授权控制人员；
- 每人格式化一个 UKEY，设定 UKEY 访问口令，详见 3.3.3 UKEY 管理章节内容；
- 每个 DMK 管理人员预定义一份自己的秘密值（8 - 32 个任意字符）；

原始初始化流程

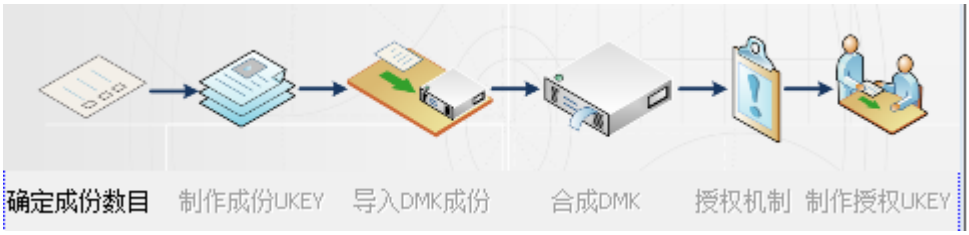

图 2-9 设备原始初始化流程

设备原始初始化的具体操作步骤，详见 3.2.1 **原始初始化**章节内容。

2.3. 设备属性配置

通过专用的设备管理客户端软件成功登录 EVSM 后，需要正确配置 EVSM 的主机端口属性。点击“设备管理——主机端口属性”进行设置，如下图：

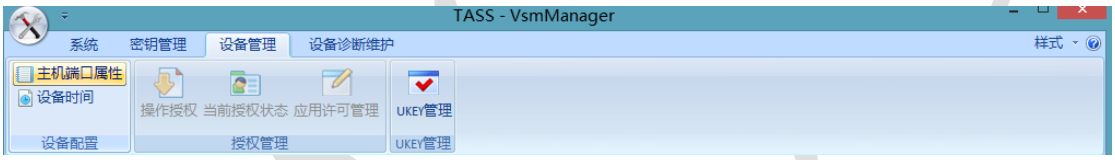

图 2-10 设备属性配置

主机端口属性列表如下：

表 2-1 主机端口属性表

属性项	参数范围	备注说明
Socket KeepAlive 时间	60 - 600	秒数，TCP 连接保活探测时间
消息报文头长度	0 - 127	字节数，主机报文消息头长度
消息报文编码格式	ASCII/EBCDIC	主机报文的编码格式
主机服务通讯方式	明文通讯/密文通讯	明文：与主机服务间的通讯为明文 密文：与主机服务间的通讯为密文

需要根据用户的实际应用需求，正确配置上述参数。

主机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，则需要在 TACSP 安全代理软件上进行相关的配置，以保证应用能够正常调用密码机的密码服务。

2.4. 操作授权

设备初始化完成后，需要对设备管理及主机密码服务进行授权后才能正常使用密钥管理的功能。详细操作过程见 3.3.2 授权管理章节。

3. EVSM 设备管理操作详述

EVSM 的管理采用 C/S 模式进行。EVSM 提供专用的设备管理客户端软件，可以运行于任意 windows 系统主机上，界面友好操作方便。

在 EVSM 启动后 3 – 4 分钟后，在做为管理客户端的系统主机上双击运行 VsmManager.exe，其主界面如下：

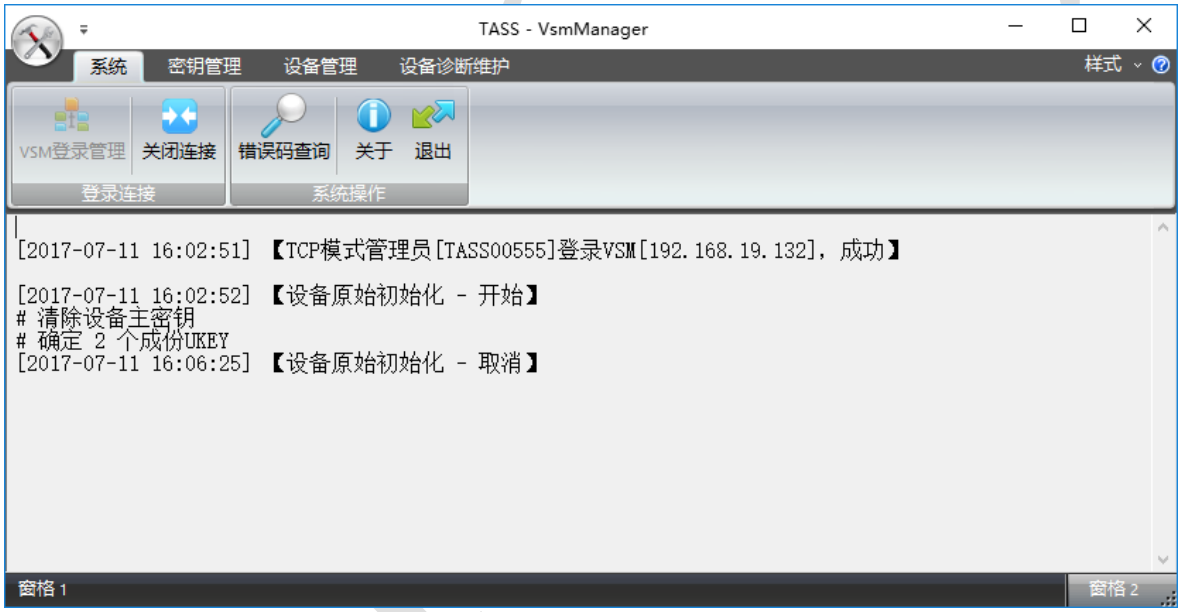

图 3-1 EVSM 设备管理客户端软件主界面

该客户端软件提供的管理操作包括：

- 系统操作，VSM 登录管理，关闭连接，错误码查询，关于和退出；
- 密钥管理，设备主密钥的原始/恢复初始化，出厂初始化，获取 DMK 校验值，导出 DMK 成分，对称/非对称密钥的管理，备份导出和恢复导入；
- 设备管理，主机端口属性，设备时间，授权操作，当前授权状态，应用许可管理，UKEY 管理；

- 设备诊断维护，导出日志，清除日志，设备基础信息，设备自检，主机服务状态，设备资源信息；

在管理客户端软件上的所有操作，均会在软件的视图上显示操作过程和结果，若是操作失败将显示出错误码，错误码的意义说明可通过点击“错误码查询”按钮进行查询。

软件退出时自动将本次登录后的管理操作过程记录到日志文件中，日志文件的路径为软件同级目录下 log/ HsmManagerLog_*time*.txt。

在进行管理配置操作前，首先需要通过该软件登录 VSM，

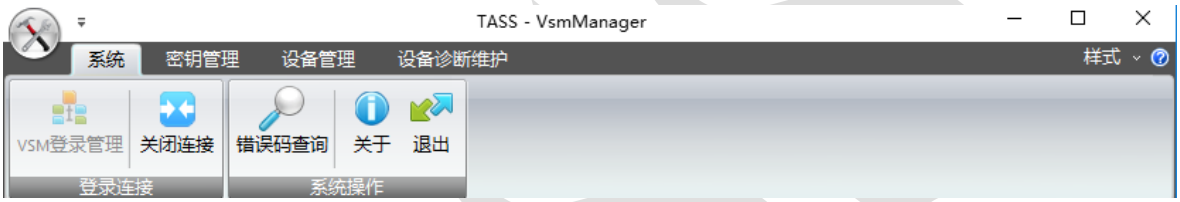

图 3-2 设备管理客户端的登录连接

3.1. TCP/IP 连接

在点击“VSM 登录管理”按钮之前需要确认好管理员 UKEY 是否插好，点击按钮，系统弹出提示，确定后会显示 TCP/IP 连接参数设置对话框：

图 3-3 TCP/IP 连接登录 VSM

第一次使用时需要注册管理员，其详细操作方法见 2.1 章节。

注册管理员完成后，输入目标 VSM 的管理服务 IP 地址与端口号，点击“登录”，在弹出的对话框中选择管理员 key，点击“确定”后，在新弹出的对话框中输入 UKEY 口令完成系统登录。登录口令用于验证 TCP/IP 连接登录人员的合法性，EVSM 出厂默认管理口令为“12345678”，该口令可在登录后 UKEY 管理内进行修改或重置。

3.2. 密钥管理

图 3-4 管理客户端的密钥管理功能

如图所示，密钥管理分为两类：

- 设备主密钥管理，原始初始化、恢复初始化、出厂初始化和获取主密钥校验值、导出 DMK 成份；
- 应用密钥管理，对称、非对称密钥管理和密钥的备份导出与恢复导入；

3.2.1. 原始初始化

当 EVSM 要投入生产环境时，必须正确的完成生产初始化操作，流程包括产生 DMK 成份 UKEY、导入合成 DMK、确定授权机制、制作授权 UKEY。

点击“原始初始化”按钮，系统弹出警告提示框：

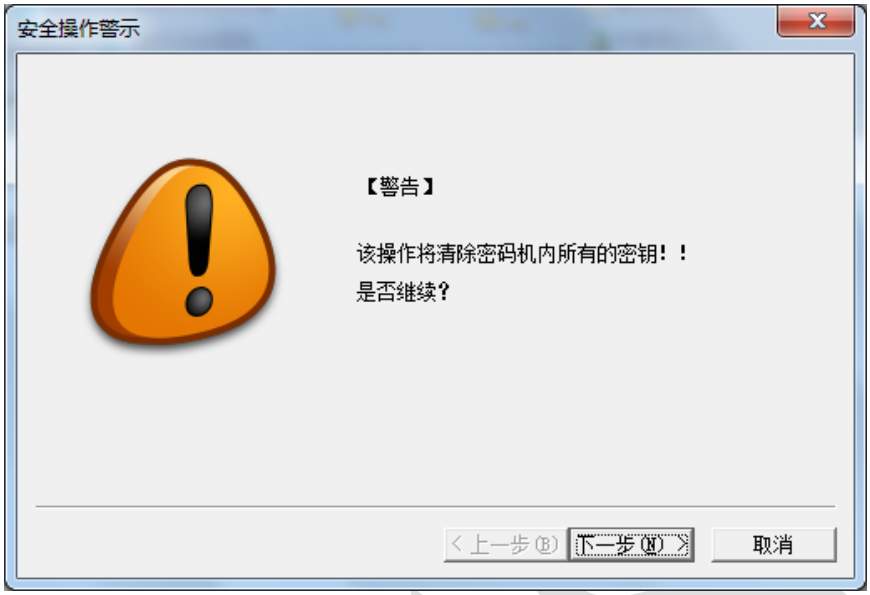

图 3-5 设备管理的安全警示

该操作将清除设备内的全部密钥，点击“下一步”：

图 3-6 原始初始化第一步

在原始初始化第一步中，根据 DMK 成份管理员人数（2－8 人）确定成份 UKEY 数目并输入，点击“下一步”进入第二步：

图 3-7 原始初始化第二步

在原始初始化第二步中，将依次制作 n 个成份 UKEY。

制作成份 UKEY 时，由成份 UKEY 持有人两次输入预定义的秘密值（8-32 个任意字符）,或者点击“随机秘密值”按钮，产生随机的 32 个字符秘密值。

插入要制作的成份 UKEY 并输入 UKEY 口令，点击“产生成份 UKEY”按钮，弹出 UKEY 列表，选择要制作的 UKEY 输入口令并点击“确定“，通过计算得到的成份数据写入 UKEY；

同上步骤制作 n 个（在第一步中确定的数目）成份 UKEY 后，点击“下一步”进入第三步：

图 3-8 原始初始化第三步

在原始初始化第三步中，将成功制作的 n 个成份 UKEY 导入到 EVSM 内。按照提示选择一个成份 UKEY 并输入口令，点击“导入成份 UKEY”按钮，EVSM 将读取 UKEY 内的成份数据；

同上导入 n 个成份 UKEY，成份 UKEY 的导入次序无关，但不能将同一个成份 UKEY 多次导入。点击“下一步”进入第四步：

图 3-9 原始初始化第四步

原始初始化的第四步合成 DMK，点击“下一步”完成，进入第五步：

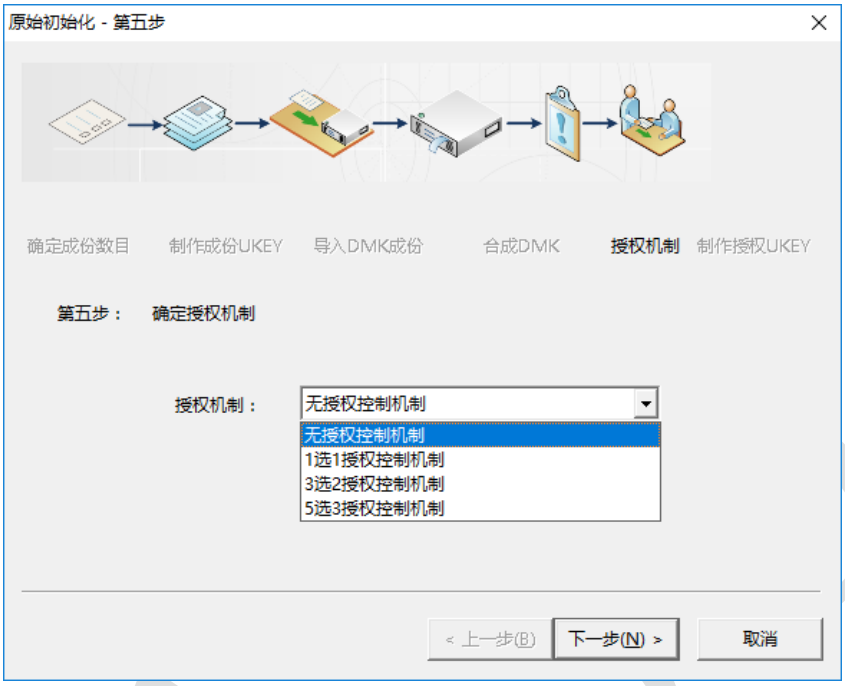

图 3-10 原始初始化第五步

原始初始化的第五步，选择授权机制：

- 无授权控制机制
- 1 选 1 授权控制机制
- 3 选 2 授权控制机制
- 5 选 3 授权控制机制

说明：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。

选定授权控制机制后，点击“下一步”进入第六步：

图 3-11 原始初始化第六步

原始初始化的第六步，制作授权 UKEY。按照系统提示依次插入 n 个 UKEY，完成授权 UKEY 的制作。点击“完成”按钮结束原始初始化操作

初始化操作完成后，EVSM 内已设置了新的生产主密钥

当多 EVSM 备份时，则在第一台设备上完成原始初始化后，对其他的设备进行恢复初始化操作，可完成多台 EVSM 的设备主密钥同步。

恢复初始化流程包括导入 DMK、同步授权信息或制作新的授权 UKEY。

点击“恢复初始化”按钮，系统弹出警示框（如图 3-5）；类同原始初始化，该操作将清除设备内的全部密钥，点击“下一步”：

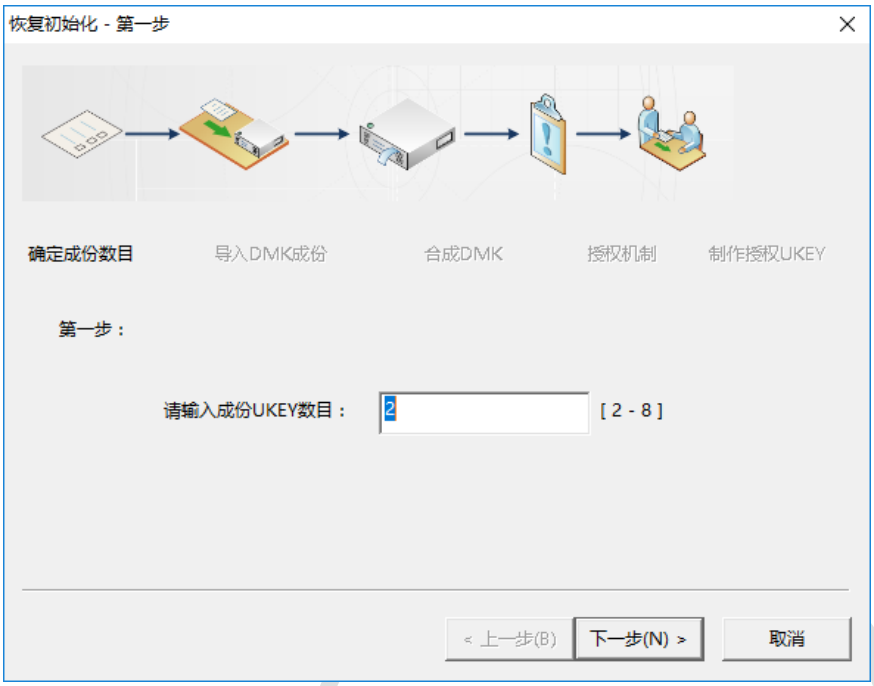

图 3-12 恢复初始化第一步

在恢复初始化第一步中，输入 DMK 成份 UKEY 数目，点击“下一步”：

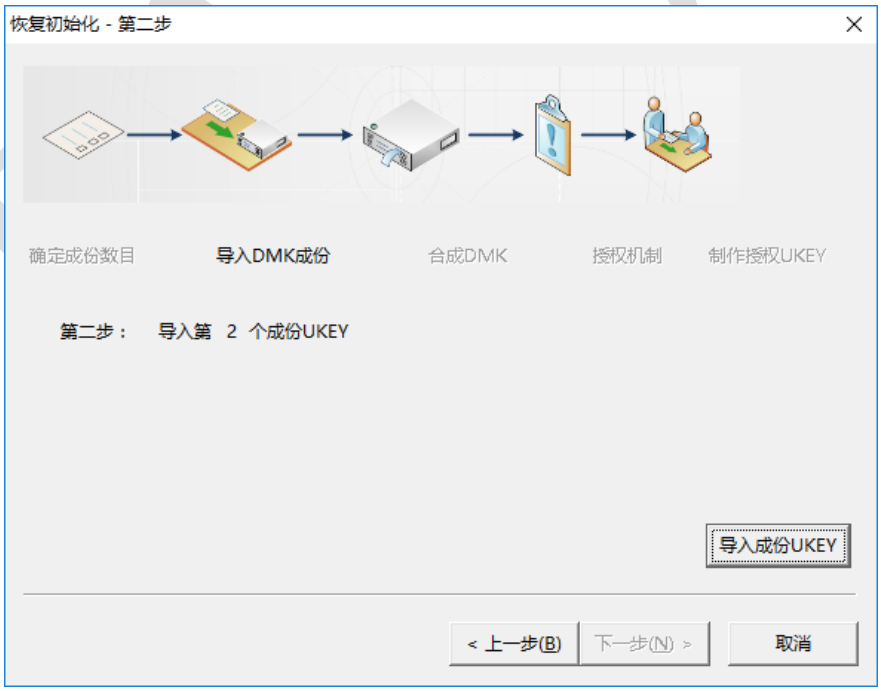

图 3-13 恢复初始化第二步

在恢复初始化第二步中，依次插入 n 个成份 UKEY 并输入 UKEY 口令，点击“导入成份 UKEY”按钮，EVSM 将读取 UKEY 内的成份数据；

成份 UKEY 的导入次序无关，但不能将同一个成份 UKEY 多次导入。点击“下一步”进入第三步：

图 3-14 恢复初始化第三步

恢复初始化的第三步，合成 DMK。依照系统提示，点击“下一步”完成，进入第四步“确定授权机制”：

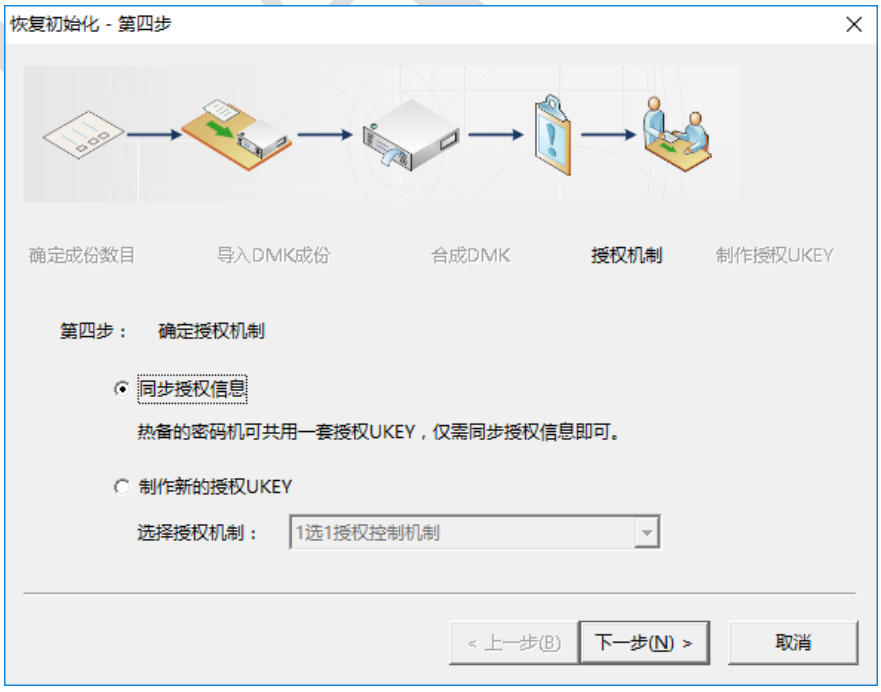

图 3-15 恢复初始化第四步

恢复初始化的第四步中，用户可选择同步授权信息或制作新的授权 UKEY。

1. 多机备份的 EVSM 若共用一套授权 UKEY，则选择“同步授权信息”：

图 3-16 恢复初始化第五步 - 1

插入有效授权 UKEY 输入口令，点击“完成”后结束恢复初始化流程；

2. 用户若需要每台 EVSM 使用独立的授权 UKEY，则选择“制作新的授权 UKEY”且确定新的授权控制机制，点击“下一步”：

图 3-17 恢复初始化第五步 - 2

依次制作 n 个新的授权 UKEY，操作类同原始初始化的第六步，点击“完成”；

3.2.2. 出厂初始化

用户在进行系统开发或调试时，可以为 EVSM 进行出厂初始化，内部自动装载测试主密钥，EVSM 内使用公开通用的 LMKs 密钥，见用户开发手册 1.4 章节内容。

点击“出厂初始化”按钮，系统弹出警示框（如图 3-5）；类同原始初始化，该操作将清除设备内的全部密钥，点击“下一步”：

图 3-18 出厂初始化第一步

使用测试主密钥时。点击“下一步”后类同原始初始化的步骤，确定授权控制机制，完成授权 UKEY 的制作。

3.2.3. 获取 DMK 校验值

点击“获取 DMK 校验值”，系统会在界面控件显示当前设备主密钥的校验值：

```
[2012-11-16 11:09:35] 【获取DMK校验值，成功】
# DMK校验值: 08D7B4FB629D0885
```

图 3-19 校验值

3.2.4. 导出 DMK 到成份 UKEY

该系列 EVSM（M1.14.00 以上版本）支持将 DMK 导出到多个成份 UKEY 中，该功能为原 EVSM 的成份 UKEY 丢失或损坏做 DMK 的备份用，可保证能够重新合成出与原 EVSM 同样的 DMK，但不保证 DMK 成份 UKEY 中内容与原制作的成份 UKEY 完全相同。

点击“导出 DMK 成份”，系统弹出提示界面：

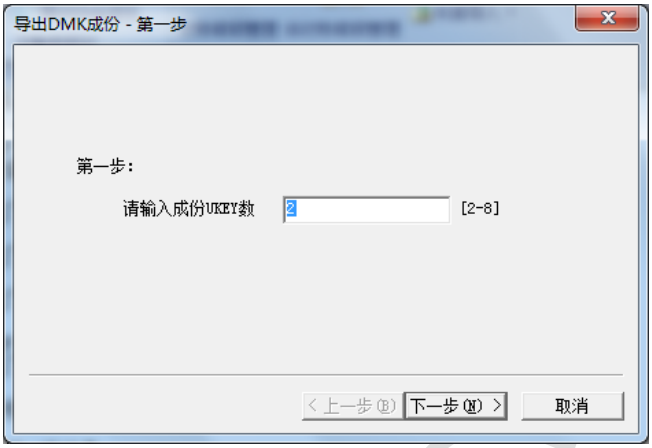

图 3-20 导出 DMK 成份第一步

按提示输入要导出的成份 UKEY 的数目（2-8），点击“下一步”：

图 3-21 导出 DMK 成份第二步

按系统提示，点击下一步选择 UKEY 将依次导出写入到 n 个 DMK 成份 UKEY 中。

3.2.5. 对称密钥管理

系统提供对称密钥的随机产生、合成产生、删除和列举当前设备内密钥的功能。点击“对称密钥管理”，系统将列举当前已存在的密钥状态：

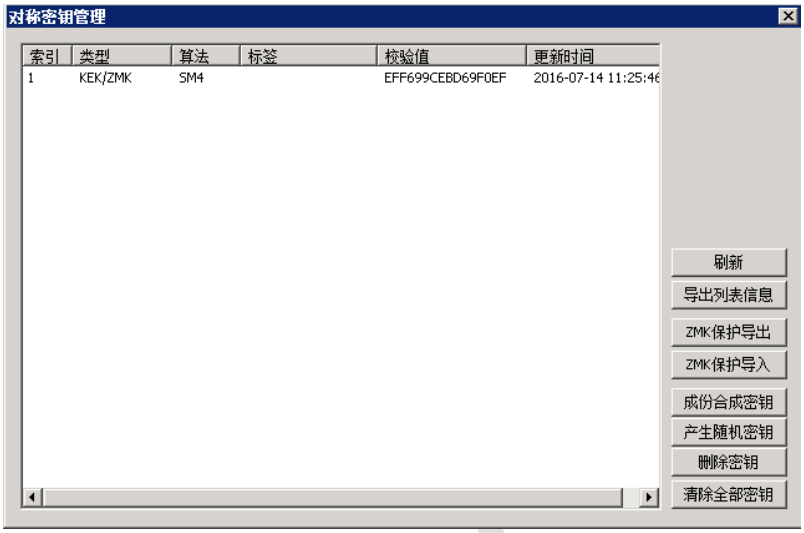

图 3-22 对称密钥管理

密钥状态信息包括：

- 密钥索引号，对称密钥索引号范围 1 – 2048；
- 密钥类型，参考《用户开发手册》中的 2.2.1 章节内容；
- 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；
- 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；

密钥管理操作包括：产生随机密钥、成份合成密钥、删除密钥、清除全部密钥和由 ZMK 保护导入导出应用密钥、产生并打印密钥成分，支持将密钥列表信息导出到本地文件中。

【注意】EVSM 内部密钥的变更和成份合成密钥需获取“密钥管理”类别的授权许可，详见 3.3.2 授权管理章节内容。

1） 产生随机密钥

点击“产生随机密钥”按钮，系统弹出对话框：

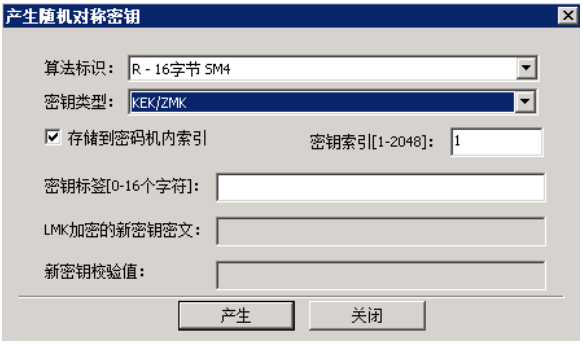

图 3-23 产生随机对称密钥

用户可根据需要选择要产生密钥的密钥类型、算法标识、是否存储在 EVSM 内，输入密钥索引、密钥标签，点击“产生”，EVSM 将产生新的随机密钥并输出显示密文和校验值；若勾选了“存储到 VSM 内索引”，则自动存储到指定索引中覆盖；

2） 成份形式合成密钥

点击“成份合成密钥”按钮，系统弹出对话框：

图 3-24 成份合成对称密钥第一步

合成第一步，用户可根据需要选择要新密钥的密钥类型、算法标识、成份数目、是否存储在 EVSM 内，输入密钥索引、密钥标签，点击“下一步”：

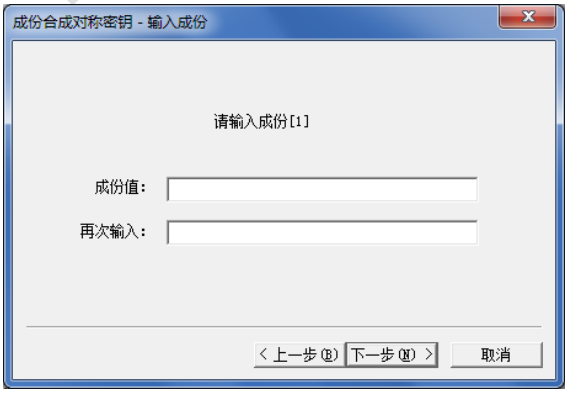

图 3-25 成份合成对称密钥第二步

按照系统提示，依次输入 n 个密钥成份，每个成份输入两遍以确认，输入全部的成份后，完成密钥合成，系统弹出结果信息框：

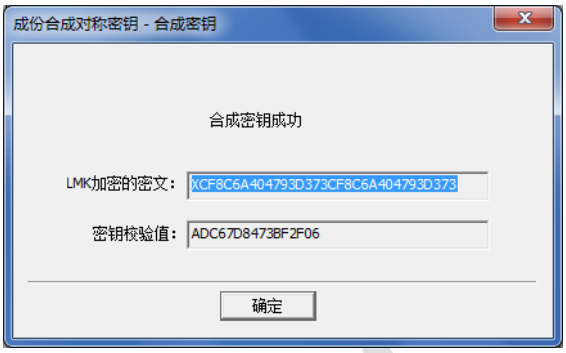

图 3-26 成份合成对称密钥结果

EVSM 将合成新的密钥并输出显示密文和校验值;若勾选了“存储到 VSM 内索引”，则自动存储到指定索引中，覆盖原内容；

3） 删除密钥

在密钥列表中选择要删除的密钥，一条或多条，点击“删除密钥”按钮，系统将弹出操作确认提示框，确认删除则点击“是”，EVSM 将删除选定的密钥，并提示操作结果；

4） 清除全部密钥

点击“清空全部密钥”按钮后，将弹出操作确认提示框，确认全部清除则点击“是”，EVSM 将清除全部对称密钥，并提示操作结果；

5） 导出密钥列表内容到文件

1.1.1.2 版本之后的客户端管理工具支持该功能。

点击“导出列表信息”按钮，管理工具将把对称密钥列表中的所有信息导出写入到本地文件 keylist.txt（管理工具可执行程序所在目录下），采用追加模式写入；

6） ZMK 保护导出密钥

该系列 EVSM（M1.14.00 以上版本）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。

选中某个密钥，点击“ZMK 保护导出”按钮，将使用选择的加密机内存储的 ZMK 或导出选中的密钥：

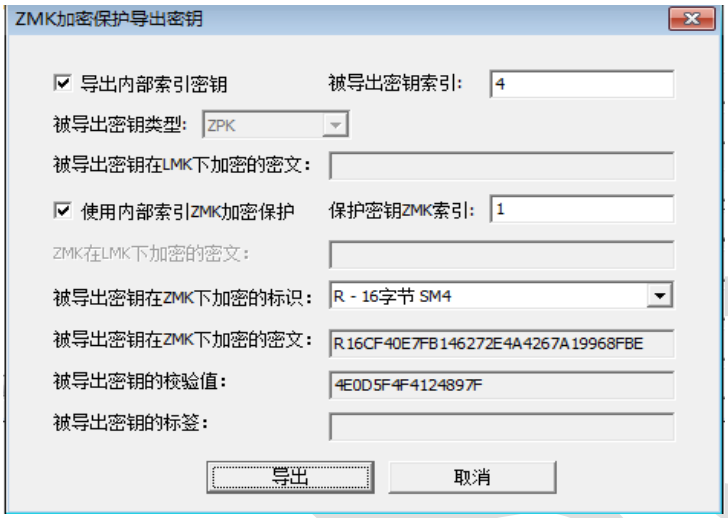

图 3-27 ZMK 加密保护导出密钥

也可以使用外部输入的 ZMK 在 LMK 下加密的密文去保护导出在 LMK 下加密的密钥密文：

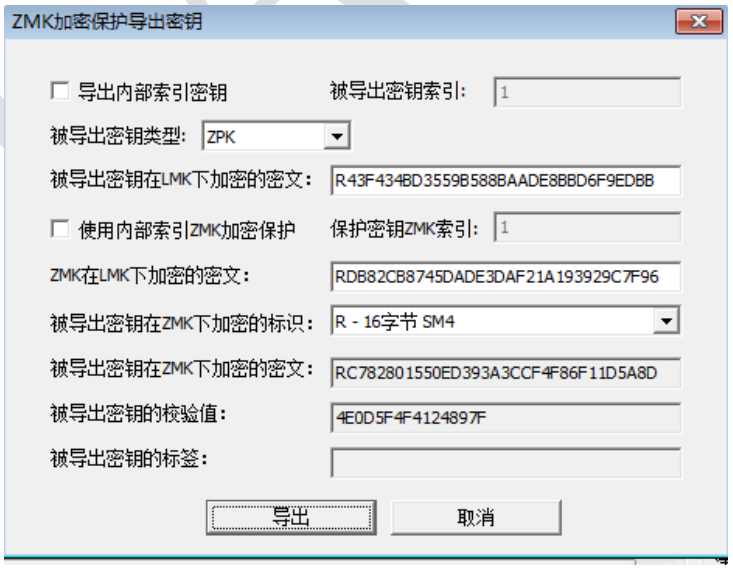

图 3-28 外部输入 ZMK 加密保护导出密钥

7） ZMK 保护导入密钥

该系列 EVSM（M1.14.00 以上版本）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加密机内：

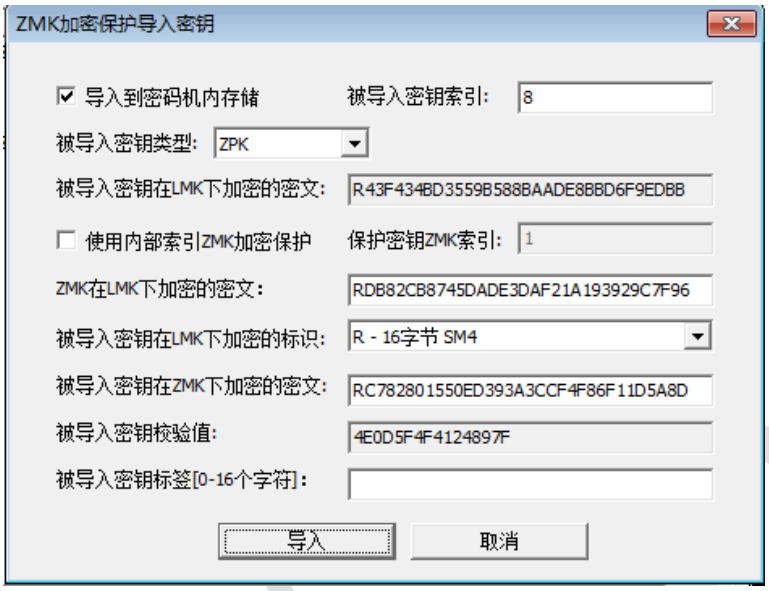

图 3-29 ZMK 加密保护导入密钥

3.2.6. 非对称密钥管理

系统提供非对称密钥的随机产生、删除和列举当前设备内密钥的功能。点击“非对称密钥管理”，系统将列举当前已存在的密钥状态：

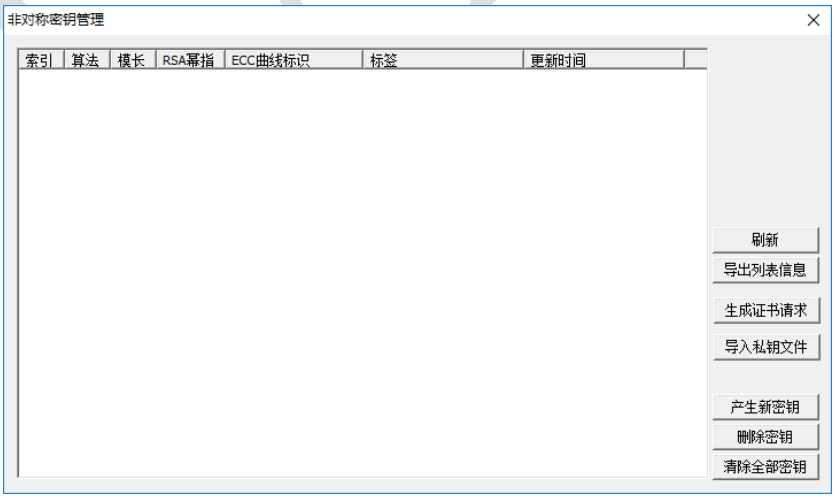

图 3-30 非对称密钥管理

密钥状态信息包括：

- 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；
- 算法，RSA 或 ECC；
- 模长，对 RSA 算法模长支持 1024、1152、1408、1912、2048 位；对 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，EVSM 该版本仅支持 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，密钥产生的时间；

密钥管理操作包括，产生随机密钥、删除密钥和清除全部密钥，支持将密钥列表信息导出到本地文件中。

1） **产生随机密钥**

点击“产生新密钥”按钮，系统弹出对话框：

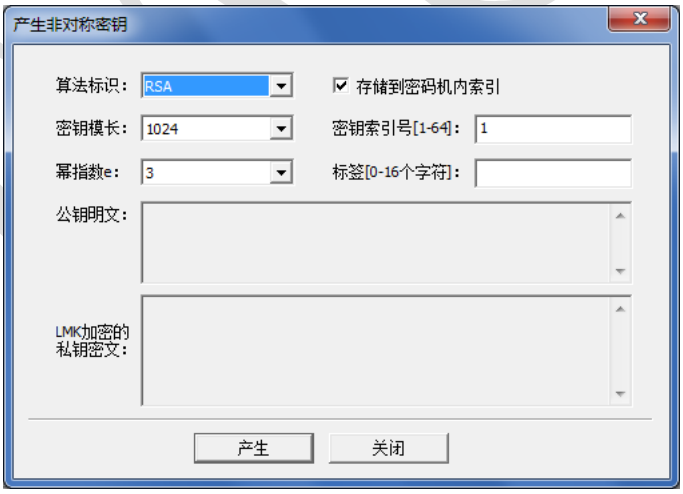

图 3-31 产生非对称密钥

用户可根据需要选择要产生密钥的算法标识、是否存储在 EVSM 内，输入密钥索引、密钥标签，若产生 RSA 密钥则需选择模长和幂指数；点击“产生”，EVSM 将产

生新的非对称密钥并输出显示公钥明文和私钥密文;若勾选了“存储到 VSM 内索引”，则自动存储到指定索引中，覆盖原内容；

2） 删除密钥

在密钥列表中选择要删除的密钥，一条或多条，点击“删除密钥”按钮，系统将弹出操作确认提示框，确认删除则点击“是”，EVSM 将删除选定的密钥，并提示操作结果；

3） 清除全部密钥

点击“清空全部密钥”子菜单后，将弹出操作确认提示框，确认全部清除则点击“是”，EVSM 将清除全部对称密钥，并提示操作结果；

4） 导出密钥列表内容到文件

1.1.1.2 版本之后的客户端管理工具支持该功能。

点击“导出列表信息”按钮，管理工具将把非对称密钥列表中的所有信息导出写入到本地文件 keylist.txt（管理工具可执行程序所在目录下），采用追加模式写入。

5） 生成证书请求

1.2.2.10 版本及之后版本的客户端管理工具支持该功能。

输入合法的主题：如/CN=XXX，选择私钥，支持加密机内部私钥索引，也支持外部输入 LMK 加密的私钥密文，点击“确定”按钮，完成证书请求生成。

6） 导入私钥文件

可导入 RSA 密钥的 pfx 和 pem 文件到密码机保存。选择私钥文件,输入证书口令，点击“确定”完成私钥的导入。

3.2.7. 密钥备份与恢复

密钥备份，是将 EVSM 内部存储的全部应用密钥（包括对称、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 EVSM 中。可用于做多机密钥同步或设备误操作后恢复应用密钥。

该系列 EVSM（M1.14.00 以上版本）支持将密钥备份到 UKEY 内。

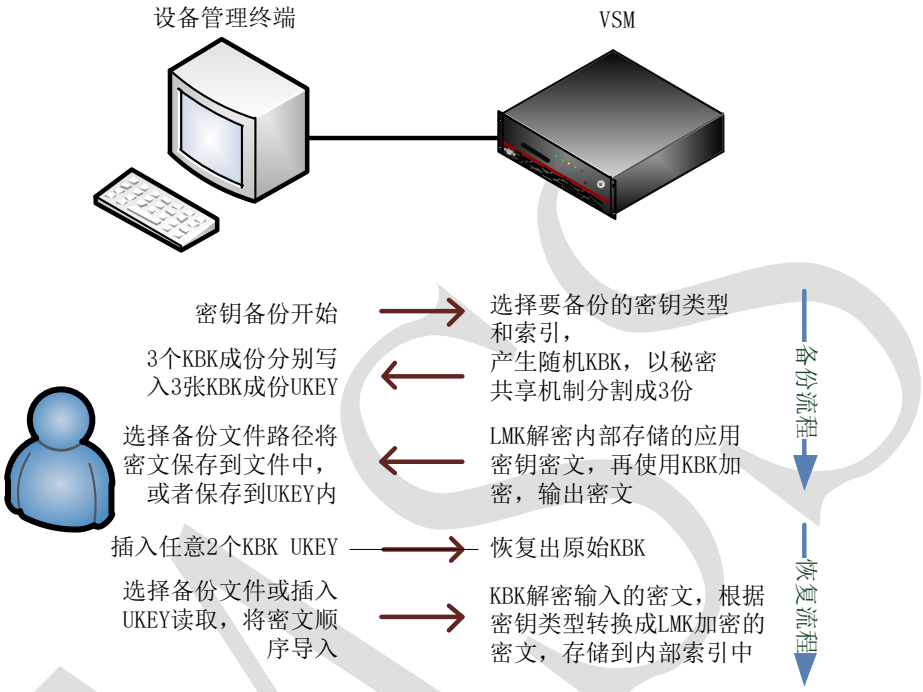

图 3-32 密钥备份恢复流程

1） 密钥备份

选择需要备份的密钥类型和索引，支持保存到文件或 UKEY 内：

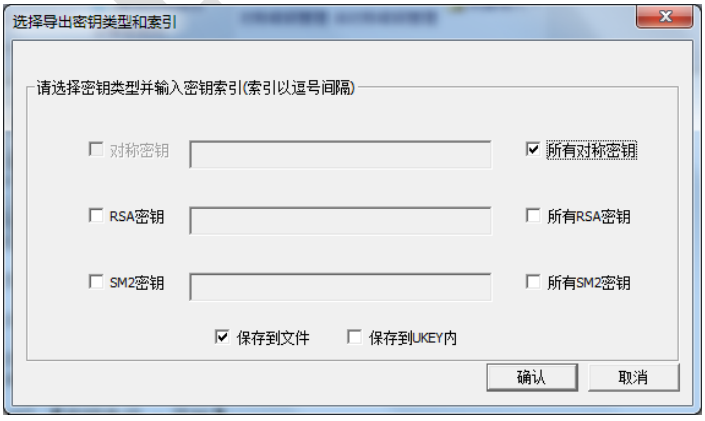

图 3-33 选择密钥类型和索引

支持选择全部密钥或者输入指定索引，索引格式为：num,num-num，比如 1，2，4-7，等同于 1，2，4，5，6，7。

密钥备份将制作 3 个 KBKUKEY，备份导出密钥密文存储到用户选定的密钥备份文件中。密钥备份需获取“应用密钥管理”类别的授权许可。

点击“密钥备份”，系统提示制作密钥备份密钥 UKEY：

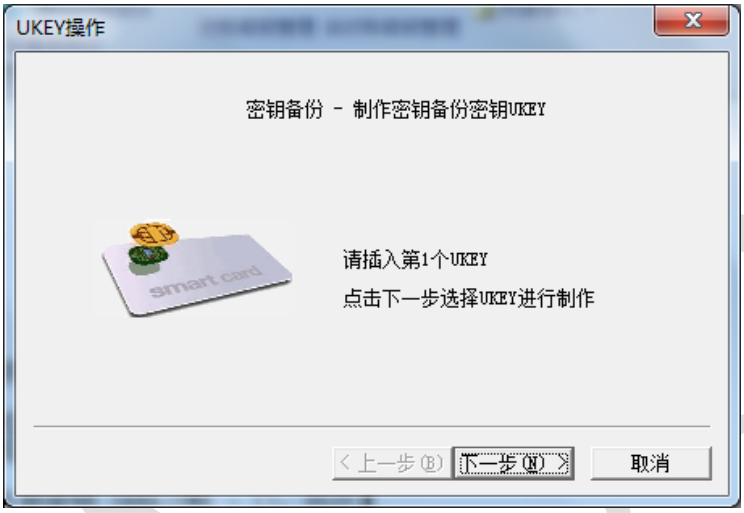

图 3-34 密钥备份 – 制作 KBKUKEY

按照系统提示插入空白 UKEY 并输入口令，点击“下一步”，EVSM 将依次制作出 3 个 KBK（密钥备份密钥）UKEY，由 3 个密钥管理员分别保管；然后系统将提示用户选择密钥备份文件名：

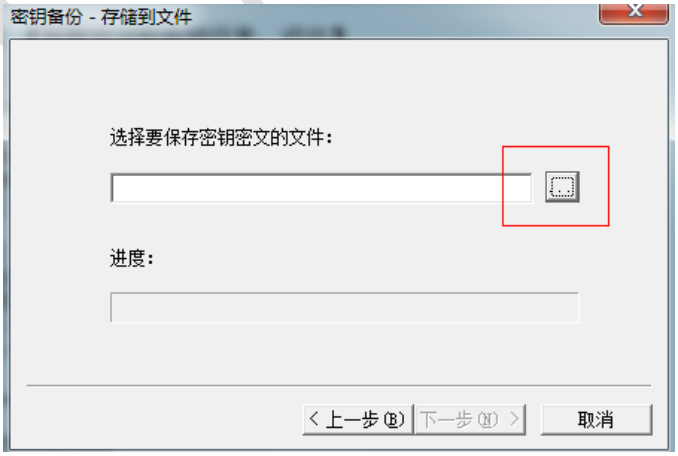

图 3-35 密钥备份 – 选择文件

按提示选择文件名，点击“下一步”，EVSM 将逐步的备份导出全部应用密钥，进度条显示备份进度情况，完成后系统显示结果。

点击“完成”。3 个 KBKUKEY 和备份文件需妥善保管，待密钥恢复时使用。

或者保存到 UKEY 内：

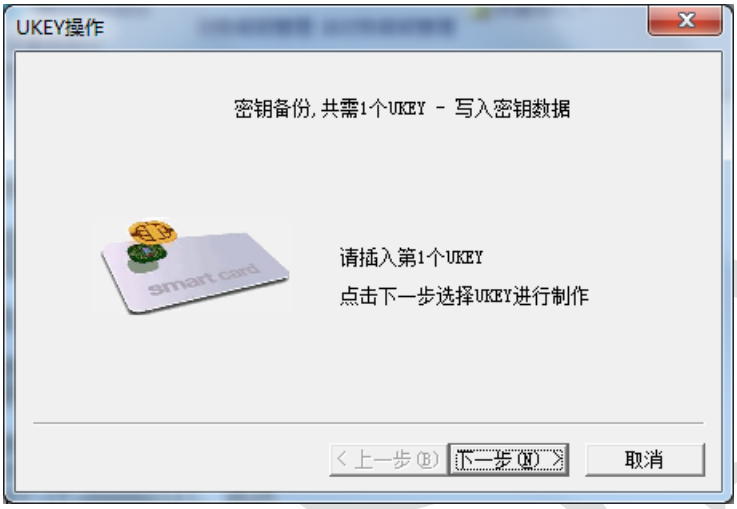

图 3-36 密钥备份 – 写入 UKEY

2） 密钥恢复

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。

点击“恢复密钥”，“从文件中恢复密钥”，系统提示读取密钥备份密钥 UKEY：

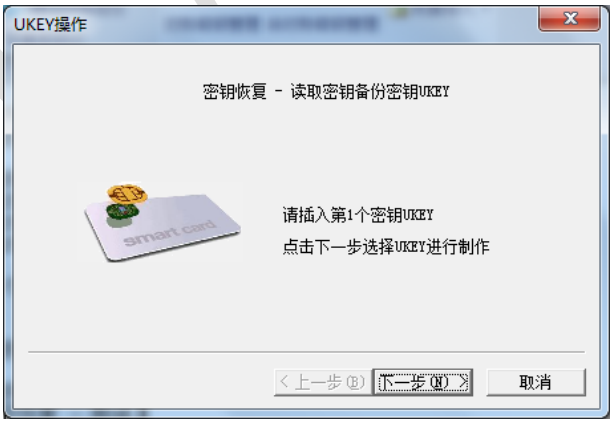

图 3-37 密钥恢复 – 读取 KBKUKEY

按照系统提示，插入任意 2 个备份时产生的 KBKUKEY 并输入口令，还原出备份密钥，点击“下一步”，系统提示用户选择要恢复的密钥文件：

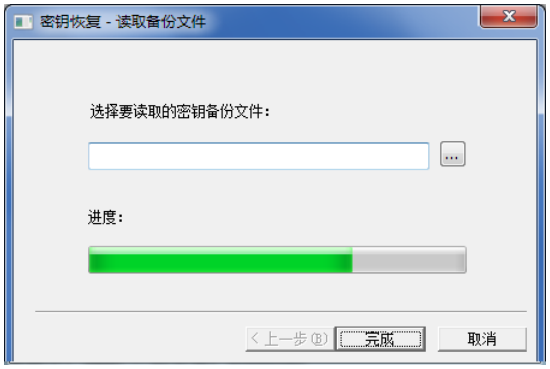

图 3-38 密钥恢复 – 选择备份文件

选择密钥备份文件，等待系统完成应用密钥的恢复。点击“完成”。

也可以选择“恢复密钥”，“从 UKEY 中恢复”。

密钥恢复后，可通过对称密钥管理和非对称密钥管理查看密钥信息是否正确。

3.3. 设备管理

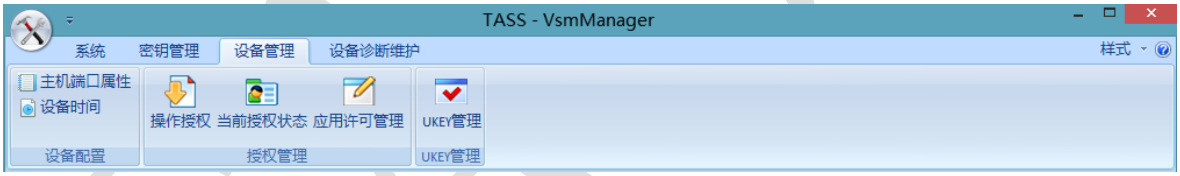

图 3-39 管理客户端的设备管理功能

如图所示，设备管理功能包括：

- 设备配置，主机端口属性配置、设备时间的获取与重置；
- 授权管理，为某些操作授权和查看当前的授权状态，应用许可管理；
- UKEY 管理；

3.3.1. 设备配置

EVSM 需完成正确的属性配置后，业务系统才能正常连接使用 EVSM。

1） **主机端口属性配置**

点击“主机端口属性”，系统将显示当前的主机密码服务端口属性值：

图 3-40 主机端口属性配置

主机端口属性项及说明详见**表 2-1 主机端口属性表**内容。

若 KeepAlive 时间、报文头长、编码格式、主机服务通讯方式被更新重置，则重启主机密码服务后生效；

2） **设备时间**

点击“设备时间”，将显示出当前的设备时间配置：

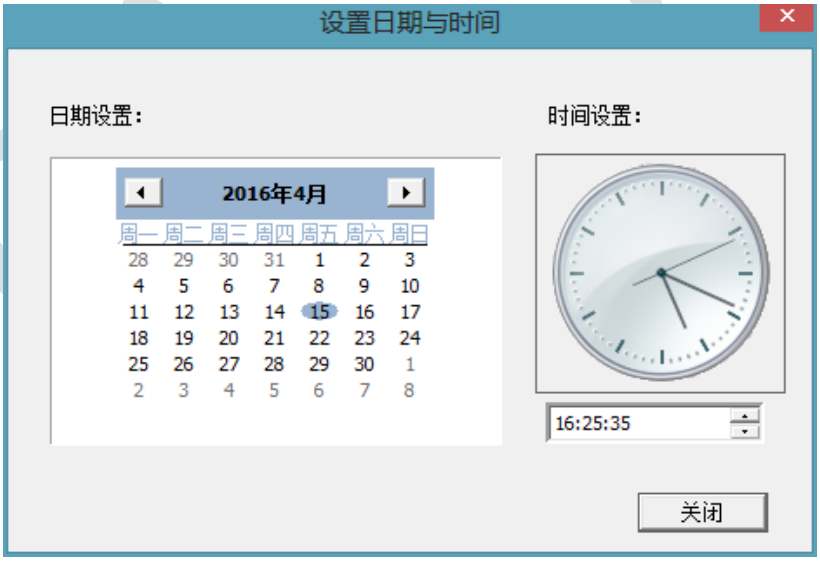

图 3-41 设备时间配置

3.3.2. 授权管理

部分设备管理操作和主机指令应用需要获取授权许可后方可使用；EVSM 支持严格灵活的授权管理控制：

- 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；

  授权控制机制需在设备初始化的过程中正确设置，完成设备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

  涉及授权控制的操作分为 5 类，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；

表 3-1 授权类别说明表

主类	子类	授权控制的操作范围说明
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	LMK 加密解密 PIN	使用 BA/NG 主机命令
	计算公钥 MAC	使用 EO/TQ 主机命令
	产生内部存储的密钥或导入到内部存储	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；

1） 授权操作

点击“操作授权”，系统提示要验证授权 UKEY：

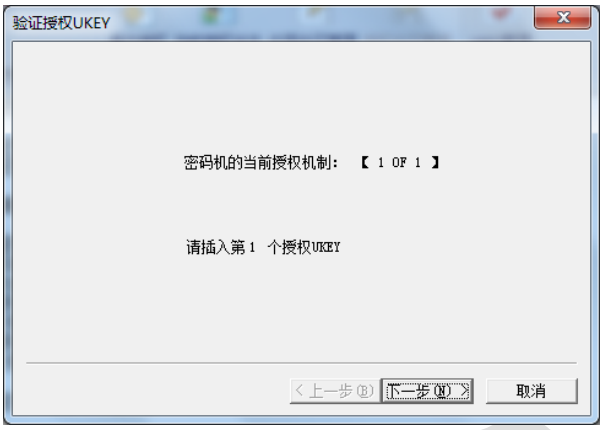

图 3-42 授权 – 验证授权 UKEY

按照系统提示，插入授权 UKEY 并输入口令，点击“下一步”，EVSM 将验证授权 UKEY 的有效性，弹出结果提示框；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），然后弹出授权类别对话框：

图 3-43 授权 – 选择类别和时间

根据应用需求，选择要授权许可的操作类别和授权时限（10 分、30 分、1 小时、12 小时、24 小时、授权至关机及授权至永久），可同时为多个类别授权不同的时限。点击“完成”结束授权操作。

其中“授权至永久”，EVSM 关机重启后该类别操作仍处于授权许可状态，直至被取消授权或变更授权时限；其他时限的授权，在到达时限或关机/重启时自动失效。

2） 获取授权状态和取消授权

点击“当前授权状态”，系统将显示授权状态列表：

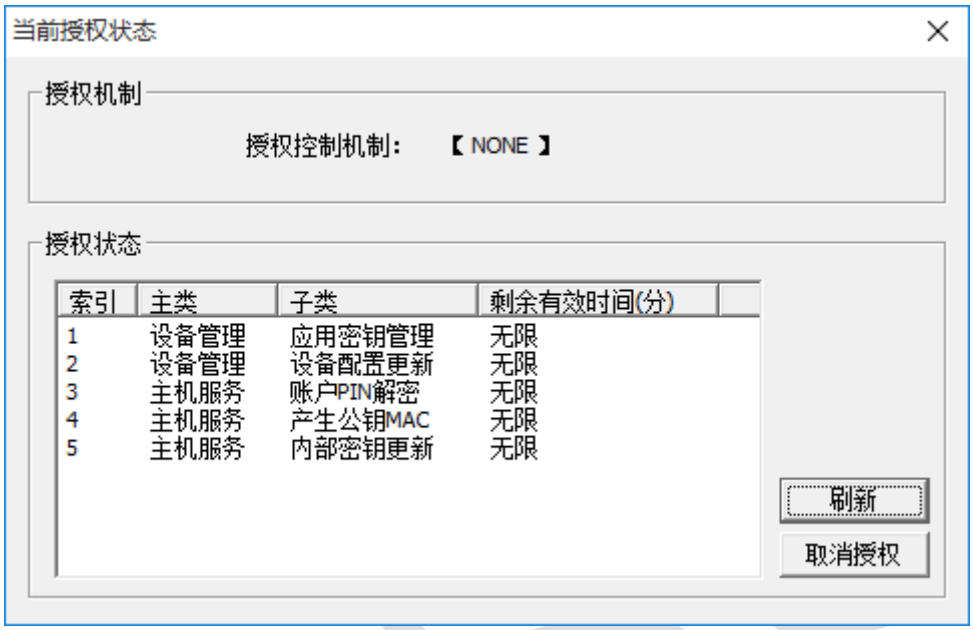

图 3-44 获取当前授权状态

选择要取消授权许可的操作类别（一个或多个），点击“取消授权”，EVSM 将取消这些类别的授权许可。

当 EVSM 配置为“无授权控制机制”时，所有的操作均不受限。

3） 应用许可管理

包括签发应用许可，销毁应用许可，清除应用许可和导出许可文件等操作，点击“应用许可管理”按钮如下：

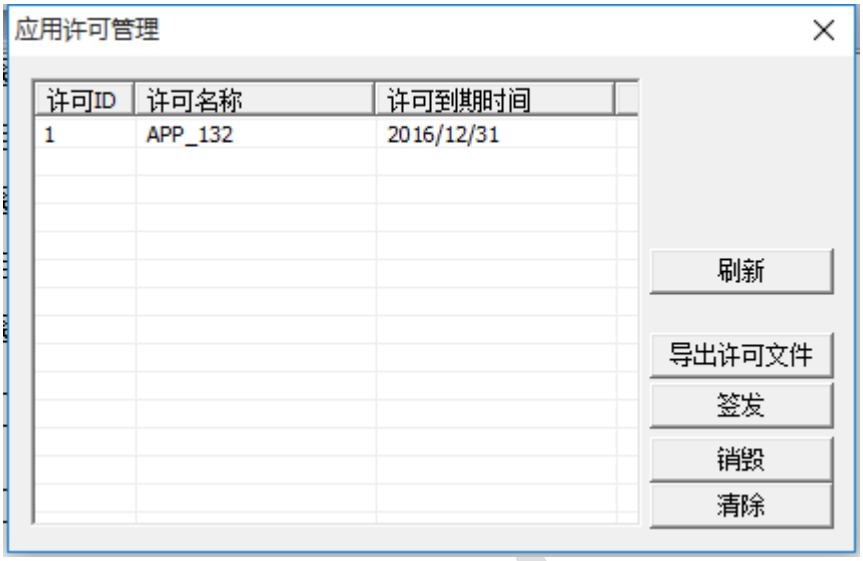

图 3-45 应用许可管理

点击“签发”按钮，如下：

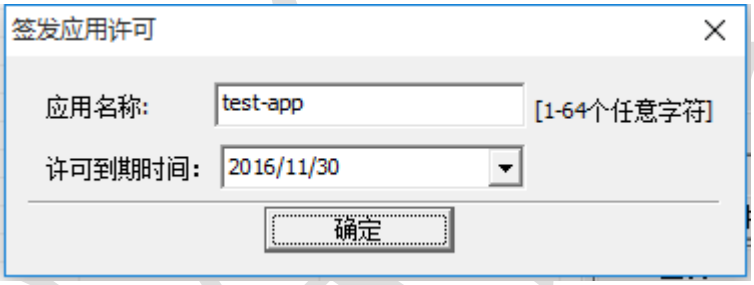

图 3-46 生成应用许可

输入应用名称，选择许可到期时间，点击“确定”按钮，生成应用许可文件并自动导出存储在工具同级目录下(应用名_VSM 序列号.license)。

选中列表内某一个应用许可，点击“导出许可文件”按钮，该应用许可文件将被导出存储在工具同级目录下。

选中列表内某一个应用许可，点击“销毁”按钮将使该应用许可失效。

点击“清除”按钮将使 EVSM 内所有的应用许可失效。

3.3.3. UKEY 管理

点击“UKEY 管理“将显示如下列表,该操作可在 TCP/IP 未登录 EVSM 情况下执行。

图 3-47 UKEY 管理功能

- EVSM 注册信息查询

点击“VSM 注册信息查询”在弹出的对话框中可以查看此台 EVSM 注册管理员的 UKEY 信息，包括 UKEY SN 和注册时间，如下图：

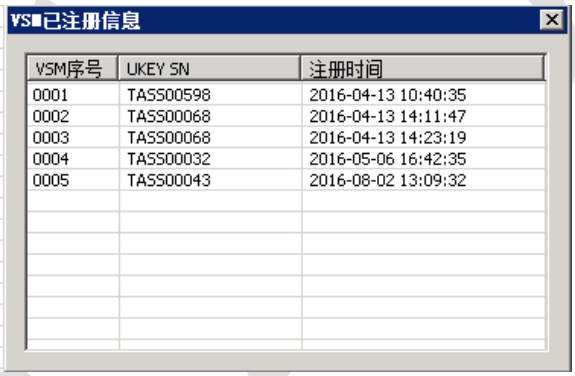

图 3-48 注册信息查询

- 注销管理员

选中正在登录的管理员 UKEY，点击“注销管理员”按钮可以注销管理员，只能选择正在登录的管理员进行注销，注销成功后，工具自动退出。

- 添加管理员

为了防止管理员 UKEY 丢失，建议另外添加几把管理员 UKEY。选中一把空 UKEY，点击“添加管理员”完成管理员 UKEY 添加。

UKEY 分为如下几类：

表 3-2 UKEY 分类表

	UKEY 类别	UKEY 内容	UKEY 用途
1	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
2	授权 UKEY	保存设备授权信息数据	用于授权管理的身份验证
3	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
4	密钥存储 UKEY	存储备份的密钥	存储备份的密钥
5	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 EVSM 通讯运算

UKEY 管理不需要登录 EVSM 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，定义 UKEY 持有人和 UKEY 类型，为 UKEY 进行格式化（个人化）操作：重置用户标识。所有的 UKEY 在首次使用时，均需要输入保护口令。

UKEY 操作：

1） 获取 UKEY 详细信息

选择 UKEY 点击“获取 UKEY 详细信息”按钮:

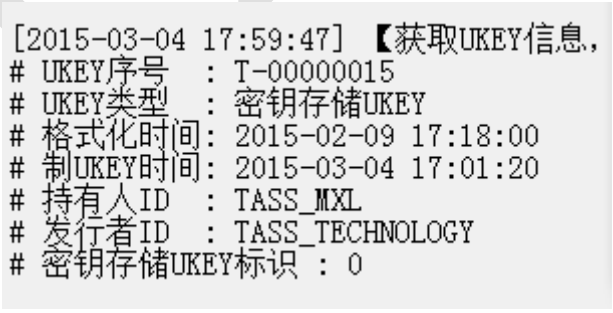

图 3-49UKEY 详细信息

2） 更改 UKEY 信息

点击“更改 UKEY 信息”，系统弹出对话框：

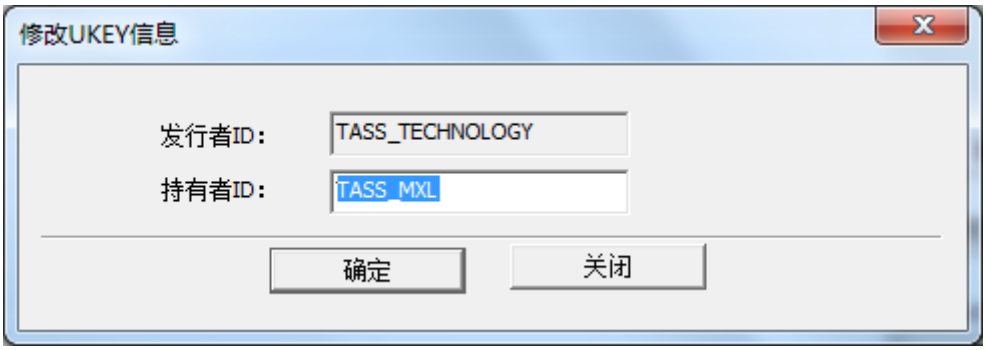

图 3-50 修改 UKEY 口令

可以修改持有者 ID 信息，点击“确定”按钮，系统将提示操作结果。

3） 修改 UKEY 口令

点击“修改 UKEY 口令”，系统弹出对话框：

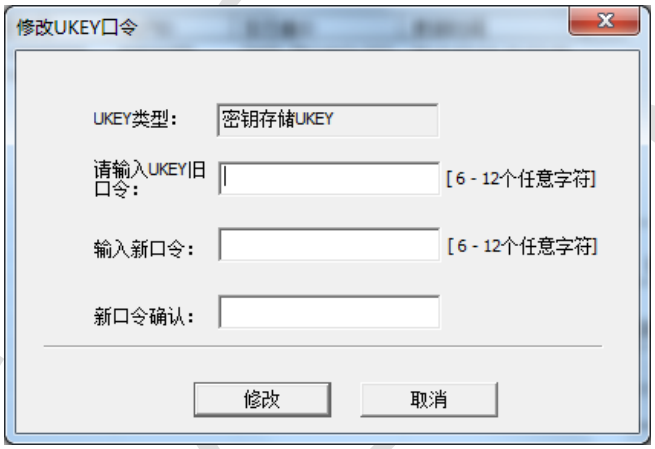

图 3-51 修改 UKEY 口令

按照提示插入要修改口令的 UKEY，输入其旧口令，两次输入新口令（必须是 6 – 12 个人任意字符），点击“修改”按钮，系统将提示操作结果。

4） 格式化 UKEY

点击“格式化 UKEY”，将 UKEY 内容重置为默认值(空 UKEY)：

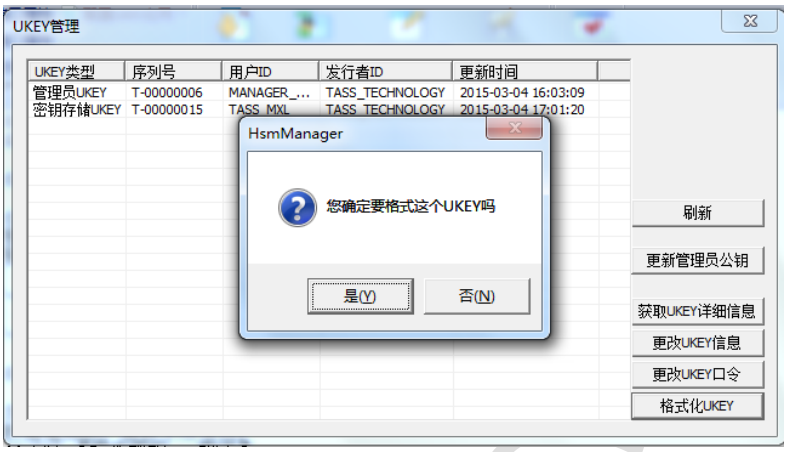

图 3-52 格式化 UKEY

管理员 UKEY 不允许格式化。

3.4. 设备诊断维护

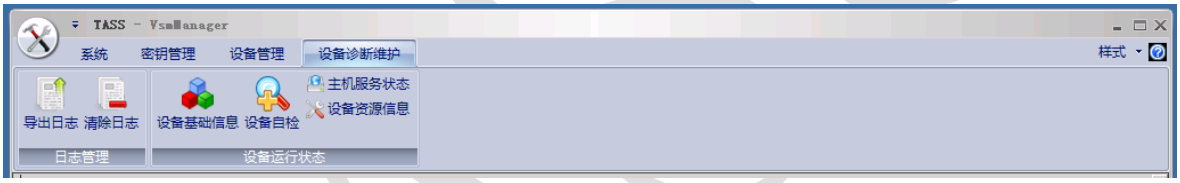

图 3-53 设备诊断功能

如图所示，设备诊断功能包括：

- 日志管理：导出日志，清除日志。
- 设备运行状态：设备基础信息、设备自检、主机服务情况、设备资源信息；

3.4.1. 日志管理

加密机支持日志导出和清除功能。

- 日志导出

点击“导出日志”，系统弹出对话框：

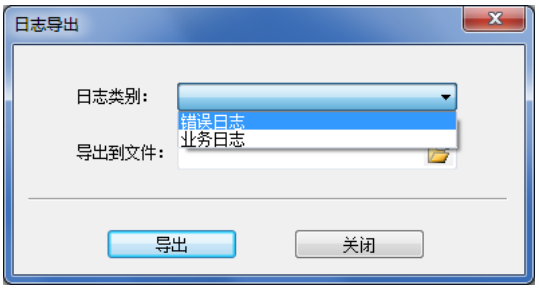

图 3-54 日志导出

选择要导出的日志类别和保存导出日志内容的文件名，点击“导出”按钮，系统将从密码机获取指定的日志内容并存储到文件中。

注：日志类别分为错误日志和业务日志。

- **日志清除**

点击“清除日志”，系统将弹出操作确认提示框，若用户确定清除密码机内的全部日志则点击“是”，系统将提示清除操作的结果。

3.4.2. 设备运行状态

- 设备基础信息，获取服务软件的版本信息
- 设备自检，进行内部关键密码单元的检测
- 主机服务状态，获取主机服务连接数状态
- 设备资源信息，获取查看 EVSM 的当前资源使用率

1） 设备基础信息

点击“设备基础信息”，系统的视图上将设备的版本信息及设备网 UKEYMAC 地址：

```
[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
```

2） 设备自检

点击“设备自检”，系统的视图上显示 EVSM 内关键单元的自检情况，包括物理噪声源检测、密码算法自检、密钥库自检：

```
[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
```

3） 主机服务状态

点击“主机服务状态”，系统的视图上显示主机密码服务的状态：

```
[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
```

4） 设备资源信息

点击“设备资源信息”，系统的视图上将显示当前设备的资源使用情况：

```
[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%
```

4. 设备维护与疑难解答

4.1. EVSM 的升级

江南天安 EVSM 支持快速客户化功能定制，在实现了客户新增功能后，需对已送货/安装的 EVSM 进行系统升级。通常情况下，该操作由我公司专业人员进行现场服务，本部分内容仅供用户参考，仅在必要的情况下同时在技术支持人员的电话指导下由用户自行操作。

4.2. 常见问题 Q&A

一般情况下，EVSM 出现故障，请尽快与我们联系，用户可以在我们的技术人员的指导下，排除故障。不能排除的，我们会依照有关保修和售后服务的有关条款，尽快予以解决。

设备管理

1） **管理客户端软件的TCP/IP连接失败**

- 请确认登录界面中输入正确的EVSM IP地址；
- 请确认管理员UKEY是否插好
- 请确认输入了正确的管理员登录口令；
- 请确认客户端IP地址与EVSM管理服务IP地址在一个网段内；

2） **管理客户端软件的菜单变灰无法使用**

- 请确认已成功登录EVSM；
- 部分功能尚未开放；
- 部分功能需要特定的EVSM状态前提；

3） **UKEY访问失败**

- 请确认UKEY被正确插入；
- 请确认输入了正确的UKEY口令；

网络通讯

4） **EVSM与主机系统网络通讯失败**

- 请正确配置EVSM的服务端口属性，应划入同一网段、接入同一VLAN；

5） **EVSM与主机系统应用通讯失败**

- 将EVSM与应用服务器划分在同一网段、接入同一VLAN，正确配置；

4.3. 错误码说明

4.3.1. 主机密码服务的应答错误码说明

代　码	描　述

01	验证错误或密钥奇校验错
02	算法的密钥长度不符合
03	无效的算法模式
04	无效的密钥类型代码
05	无效的密钥长度标识
06	无效的密钥成份个数或非法的偏移量
07	密钥校验值比对失败
08	输入数据类型无效
09	导出的密钥个数无效
10	源密钥奇校验错
12	用户存储区内容无效。复位、重启或覆盖
13	LMK 错误
14	LMK组003-005 下加密的PIN无效
15	无效的输入数据 (无效的格式，无效的字符，或输入的数据长度不够)
16	控制台或打印机没有准备好/没有连接
17	加密机没有在授权状态，或不允许输出明文PIN
18	文档格式定义没有加载
19	指定的 Diebold 表无效
20	PIN数据块没有包含有效的值
21	无效的索引值，或索引/数据长度数溢出
22	无效的帐号
23	无效的PIN数据块格式代码
24	PIN 的长度不到4位或超过12位
25	十进制转换表不正确
26	密钥标识错
27	密钥长度错
28	无效的密钥类型
29	密码功能不允许
30	无效的用户参考号
31	PIN申请函批处理空间不足
32	输入类型无效，RSA算法标识、MAC报文块模式，ICV模式，交易模式等
33	LMK密钥交换存储区有故障
34	mac算法模式无效
35	mac取值方式无效
36	密钥分散级数无效
37	会话密钥类型无效
38	会话密钥算法类型错误
39	非法的数据padding类型
40	无效的固件校验值

41	内在的硬件/软件错误。RAM损坏，无效的错误代码等
42	密码运算失败
43	DER解码失败
45	密钥不存在
49	密钥错误
51	无效的消息头
52	非对称密钥密钥用法（签名、加密）错误
53	非对称密钥长度非法（RSA 512-2048. ECC 256）
54	DER编码类型非法
55	密钥索引超限
56	RSA密钥指数非法
57	非对称密钥数据非法
58	ECC密钥曲线标识错误
65	交易密钥标识设置为NULL
67	命令码没有授权
68	命令码禁用
69	PINBLOCK禁用
70	无效的密文数据，解密后去PADDING失败；或密钥头验证失败
74	摘要hash模式不支持
75	单长度的密钥用作双长度或三长度
76	公钥长度错误
77	明文数据块错误
78	密文密钥长度错误
79	哈希算法对象标识符错误
80	报文数据长度错误
81	无效的证书头
82	无效的校验值长度
83	密钥格式错误
84	密钥校验值错误
85	无效的OAEP掩码产生算法
86	无效的OAEP掩码产生算法的摘要算法
87	OAEP参数错
90	EVSM接受的请求数据校验错误
91	纵向冗余校验(LRC) 字符和通过输入数据计算的值不匹配
92	命令/数据域中的计数值不正确或不在规定的范围内
93	公钥标识验证失败
94	公钥摘要值验证失败
96	密钥标签长度错
97	内部参数错，如会话密钥模式与源密钥类型冲突

98	报文封装错
99	内部运算错误

4.3.2. 设备管理终端的错误码说明

代　码	描　述
0XD0000001	参数非法，指针空
0XD0000003	参数非法，超出有限范围
0XD0000011	打开COM端口失败
0XD0000012	连接TCP端口失败
0XD0000013	通讯失败
0XD0000014	发送数据失败
0XD0000015	接收数据失败
0XD0000016	COM通讯接收数据失败，无ETX
0XD0000017	接收数据失败, 2-byte长度错误
0XD0000018	连接数非法，大于2048
0XD0000020	TCP管理，会话密钥校验值验证失败
0XD0000030	密钥管理，密钥个数不合法
0XD0000040	口令长度无效
0XD0000041	口令包含非法字符
0XD0000050	数据包含非法字符
0xE0000017	管理操作未处于授权状态
0xE0000600	报文中内容非法
0xE0000601	管理终端未合法登录
0xE0000602	命令码不支持，EVSM服务版本低
0xE0000603	报文长度错误
0xE0000605	登录口令错误
0xE0000606	摘要运算错误
0xE0000607	加解密运算失败
0xE0000608	DMK无效
0xE0000609	密钥索引错误
0xE0000704	无效的字符
0xE0000706	数据包含非十进制字符
0xE0000707	数据包含非十六进制字符
0xE0000708	数据长度超出预期
0xE0000709	数据去PADDING失败
0xE000070A	数据比较失败，不一致
0xE000070B	malloc失败，内存错误
0xE0000801	可信客户端IP地址已存在

0xE0000802	非法的IP地址
0xE0000A00	服务进程启动失败
0xE0000B02	日志文件读失败
0xE0000B03	日志文件不存在
0xE0000B04	日志文件内容为空
0xE0000C00	UKEY上电失败
0xE0000C02	UKEY格式化失败
0xE0000C03	UKEY验证PIN失败
0xE0000C04	UKEY更新PIN失败
0xE0000C05	读取UKEY失败
0xE0000C06	写入UKEY失败
0xE0000C07	UKEY不允许拷贝
0xE0000C10	UKEY类型错误
0xE0000C15	UKEY序号重复
0xE0000C17	DMKUKEY成份无效
0xE0000C18	读取DMKUKEY失败
0xE0000C19	写入DMKUKEY失败
0xE0000C20	UKEY读取的DMK成份无效
0xE0000C30	授权UKEY验证失败
0xE0000C31	授权UKEY序号无效，小于1或大于当前的授权机制
0xE0000C32	授权机制无效
0xE0000C40	KBKUKEY序号无效
0xE0000C42	密钥恢复时的KBK验证标识错误
0xE0000C43	密钥恢复时的密钥校验失败
0xE0000D00	清除DMK失败

4.4. 支持与服务

如果您在安装、使用本产品时遇到困难或有任何问题，您可以随时拨打下面电话或上网查询：

公司总机：010-82326383

公司网址：http://www.tass.com.cn

支持邮箱：wangguoqiang@tass.com.cn