SJJ1507

服务器密码机

用户使用手册

北京江南天安科技有限公司

2015 年 3 月

江南天安

SJJ1507 服务器密码机

用户使用手册

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

SJJ1507 服务器密码机用户使用手册 V1.0

最新发行日期：2015 年 3 月

声明

本手册由北京江南天安科技有限公司编写，仅随密码机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。

本手册适用于 SJJ1507 服务器密码机。

北京江南天安科技有限公司

二〇一五年三月

手册目录

图表目录

1. 熟悉 SJJ1507 服务器密码机

1.1. 产品概述

密码技术是保障信息安全的关键核心技术，必须确保密码算法的安全、自主、可控。现在普遍应用的国际密码算法 DES/3DES、RSA 等已不安全，开发国产密码算法产品，推进国产密码算法的普遍应用，逐步平滑代替国际密码算法，是保障我国信息安全的必由之路。

北京江南天安科技有限公司开发的服务器密码机，是支持国产密码算法（SM1、SM2、SM3、SM4、ZUC）的密码设备，能够支持国家重点信息系统由使用国际密码算法向使用国家自主密码算法的平滑过渡，在这些重要的信息系统中推广国产密码算法，可以有利于保障国家重要信息系统的安全性，保障这些重要行业信息系统的安全运行，加强国家自主的信息安全保障。

服务器密码机使用自主研制的 SJK1322 密码卡，可以提供多种国产密码算法，并能够保证密钥和密码算法安全性，具有很高的安全性和实用价值。符合 GM/T 0018-2012，《密码设备应用接口规范》，可以安全、灵活、方便的集成到各类安全应用系统中。

服务器密码机针对安全性高，高速、高性能的应用环境而研制开发，功能完善、算法性能高、并发工作量大。作为高端商用基础密码产品，他可以为信息安全传输系统提供高性能的数据加解密服务，又可以作为主机数据安全存储系统、身份认证系统以及对称、非对称密钥管理系统的主要密码设备和核心构件，具有广泛的系统应用潜力。可广泛的应用与银行、保险、证券、交通、邮政、电子商务、移动通信等行业的安全业务应用系统。

服务器密码机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、安全报文形式导入导出密码机；

- 数据加密，对称 SM1/SM4/ZUC 算法加解密和非对称 SM2/RSA 算法的数据加解密；
- 签名验签，非对称 SM2/RSA 算法的签名验签运算；
- MAC 运算，对称密钥（SM1/SM4/ZUC）的 MAC 运算；
- 摘要算法，SHA1/SHA256/SM3 摘要算法；

SJJ1507 服务器密码机主要用作加密服务端。密码机采用 LINUX 操作系统，稳定可靠；采用密码芯片实现密码算法；采用客户端控制，通过网口或串口对密码机进行维护管理和配置，简单方便。

典型的应用与管理拓扑图：

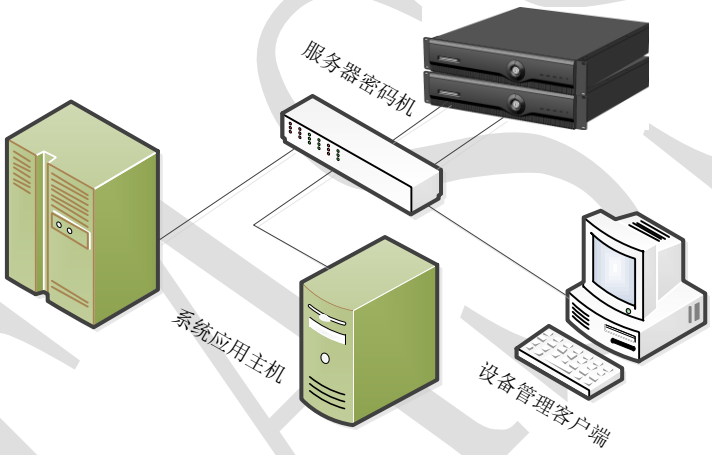


图 1-1 密码机应用演示拓扑图

1.2. 系统构成

1.2.1. 硬件配置

表 1-1 密码机硬件配置

项目	SJJ1507 服务器密码机
串行接口	标准 RS-232 串行接口 2 个
并行接口	1 个
网口	10M/100M/1000M 自适应 2 个
IC 卡插口	1 个
LED 指示灯	电源、工作、安全、IC 卡、报警
状态模式锁	常规模式、安全模式
蜂鸣器	1 个
IC 卡	10 张
通用密码模块	多个（根据具体配置不同）

1.2.2. 软件配置

1) LINUX 内核 2.6.18
2) TASS 密码运算嵌入式软件 V1.0
3) TASS SJJ1507 服务器密码机嵌入式系统软件 V1.0

1.3. 密码机外形结构

1.3.1. 设备实物图

图 1-2 密码机实物图

1.3.2. 前面板说明

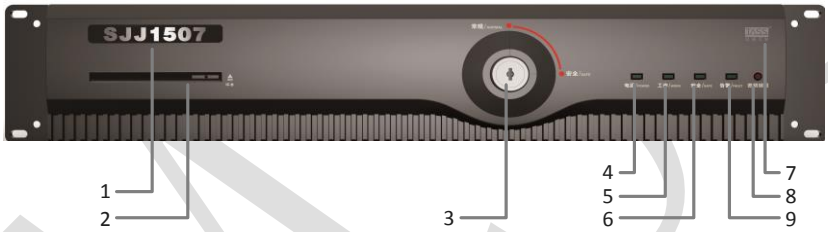


图 1-3 密码机前视图

1. 设备型号
2. IC 卡读写器（芯片面朝上）
3. 状态控制锁（常规/安全）
4. 电源指示灯
5. 工作指示灯（处理业务时忙碌时闪）
6. 安全状态指示灯
7. 设备厂商 LOGO
8. 密钥销毁按钮
9. 告警指示灯

1.3.3. 后面板说明

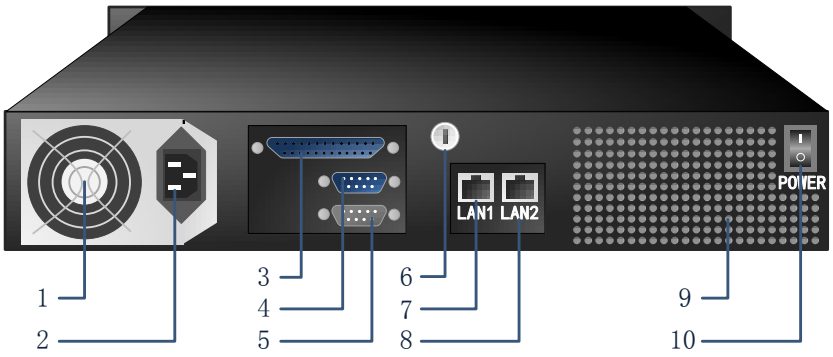


图 1-4 密码机后视图

1. 电源散热孔
2. 电源插头
3. 打印并口
4. 打印串口
5. 管理串口
6. 机箱锁
7. TCP/IP 设备管理端口
8. TCP/IP 主机服务端口
9. 机箱散热孔
10. 电源开关

1.4. 密码机物理及电气指标

表 1-2 密码机物理及电气指标

指标项目		SJJ1507 服务器密码机
物理特性	实际尺寸	87mm(高)×425mm(宽)×480mm(深)
	包装尺寸	650mm(长)×580mm(宽)×245mm(高)
	净重量	19KG
	颜色	亚黑色
	外壳机构	高强度金属机箱
电器特性	工作电压	220V±20%
	工作电流	0.8A
	频率	50±3Hz
	最大功耗	176W
环境参数	工作环境温度	0℃～60℃
	工作相对湿度	5%～90%，非凝结
	存储环境温度	-20℃～60℃
	存储相对湿度	5%～90%，非凝结
平均无故障时间		≥30000 小时

1.5. 产品随机配件

表 1-3 密码机随机配件表

序号	配件名称	单位	数量	备注
1	电源线	根	1	1.2 米
2	状态锁钥匙	把	2	
3	IC 卡	张	10	
4	网线	根	1	3 米
5	串口管理线	根	1	2 米
6	串口转接头	个	1	USB 转串口
7	光盘	张	1	设备管理客户端软件 操作手册 用户手册
8	快速部署说明	份	1	彩色折页版
9	装箱单	份	1	A4 纸
10	保修卡	份	1	
11	合格证	份	1	

2. 快速使用 SJJ1507 服务器密码机

2.1. 密码机的安装启动

SJJ1507 服务器密码机作为主机密码安全服务器，应安装在本地网络内部，且必须是一个安全可控的环境。

使用随机附带的电源线连接到密码机后面板的电源接口上，打开后面板的电源控制开关，即可启动密码机。

密码机上电后可以听到“嘀”的一声，开机后有一个系统引导和初始化的过程，然后系统自动启动一系列服务软件，此过程中前面板的工作指示灯处于持续闪灭交替状态，大约 3 分钟后，密码机以“嘀--”长响 1-2 秒、工作灯灭状态提示服务启动完成，此时对外提供密码运算服务和管理服务。

2.2. 密码机的管理配置

密码机正常启动后，设备管理人员需要对密码机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。

2.2.1. 连接设备管理端口

首先将作为管理终端的 windows 主机正确连接到密码机的设备管理端口上。SJJ1507 服务器密码机支持使用串行端口和网络端口做为密码机的设备管理口。

1) 串口方式连接

在密码机的后面板有标注“管理串口”字样的端口，使用随机附带的终端管理线连接该端口和管理终端主机上的串口。

如管理终端没有串口，可以使用随机附带的 USB 转接头，并安装驱动程序。

2) TCP/IP 方式连接

密码机的后面板设置有两个网络端口，当使用网络方式进行设备管理时，需使用标注为“LAN2”的网口。

通过网线将密码机的管理服务端口连接到本地网络中。

2.2.2. 运行登录设备管理客户端

正确连接管理端口后，在管理客户端系统主机上运行随机光盘中的设备管理客户端软件 HsmManager.exe，点击“串口连接”或“TCP/IP 连接”登录到密码机。

1) 串口连接

在初始未知密码机 IP 地址的情况下，需使用串口连接方式登录，查看或重置密码机管理服务端口的属性设置。

密码机的出厂默认管理串口的属性：

波特率：38400

数据位：8

奇偶校验：无

停止位：1

数据流控制：无

2) TCP/IP 连接

使用 TCP/IP 连接模式，需输入一个登录口令，以验证操作人员的合法性，密码机出厂时默认的 TCP/IP 管理登录口令为“12345678”。

密码机的出厂默认管理网口属性：

管理服务 IP 地址：192.168.20.20

端口号：8020

设备管理的详细功能和操作说明参见本文“SJJ1507 密码机设备管理操作详述”部分内容。

2.2.3. 设备初始化

密码机出厂时，内部装有测试主密钥，无授权控制机制，无开机卡模式。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。

当密码机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、制作开机卡、设置授权机制、制作授权卡。

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 位开机卡管理人员、1 或 3 或 5 位设备授权控制人员；
- 每人格式化一张 IC 卡，设定卡片访问口令，详见 3.4.2IC **卡操作**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

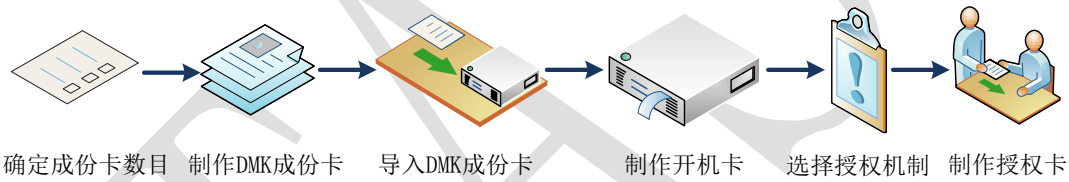


图 2-1 设备原始初始化流程

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。

2.2.4. 设备属性配置

通过专用的设备管理客户端软件成功登录密码机后，需要正确配置密码机的主机端口属性、管理端口属性和可信客户端列表。

更新设备配置需要获取“设备配置更新”操作类别的授权许可，授权操作参见 3.3.2 **授权管理**章节说明。

1) 设置主机端口属性

该配置对应密码机后面板的“LAN1”端口的属性，用于对业务系统提供主机密码服务。

表 2-1 主机端口属性表

属性项	参数范围	备注说明
主机服务 IP	有效的 IP 地址	主机密码服务的 IP 地址
端口号	1 - 65535	端口号，默认为 8019
子网掩码	有效的子网掩码	
网关地址	有效的网关地址	
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
IP 地址访问控制机制	启用/禁用	启用，仅限可信客户端访问； 禁用，不限客户端来源；

需要根据用户的实际应用需求，正确配置上述参数。

对开发环境和测试环境下的密码机，“IP 地址控制机制”可以设置为“禁用”项，方便系统的开发调试；对生产环境下的密码机，该项必须设置为“启动”项，以确保密码机使用的安全可控。

2) 设置管理端口属性

该配置对应密码机后面板的“LAN2”端口的属性，用于对管理客户端提供设备管理服务。

表 2-2 管理端口属性表

属性项	参数范围	备注说明
管理服务 IP	有效的 IP 地址	设备管理服务的 IP 地址
端口号	1 - 65535	端口号，默认为 8020
子网掩码	有效的子网掩码	

网关地址	有效的网关地址	

需要根据用户的实际应用需求，正确配置上述参数。

说明：

主机密码服务对业务应用系统提供主机指令集服务，设备管理服务对设备管理客户端提供管理配置的服务，两者的服务对象不同，在物理端口和逻辑 IP 地址上应独立分开。密码机后面板的 LAN1 端口对应主机密码服务，LAN2 端口对应设备管理服务，二者的 IP 地址必须位于不同子网中，否则 LAN2 网口将被禁用。

3) 可信客户端设置

当主机服务端口的“IP 地址访问控制机制”项设置为“启用”时，密码机则仅接受预先配置的可信客户端发来的连接请求，此时需要将合法客户端主机 IP 地址添加到可信客户端列表中。具体操作参见 3. 3. 1 **设备配置**章节说明。

若主机服务端口的“IP 地址访问控制机制”项设置为“禁用”，则可信客户端设置无效。

【注意】完成密码机的基础管理配置后，请重启密码机以使新设置生效。

2.3. 使用密码机的主机密码服务

2.3.1. 连接主机服务端口

SJJ1507 服务器密码机通过标准的以太网接口与业务主机进行网络通讯，其后面板的“LAN1”端口是密码机的主机密码服务端口；

通过网线连接密码机服务端口到业务系统网络中。

2.3.2. 访问主机密码服务

完成对密码机的正确连接和配置后，系统主机可通过调用 SDF 接口向密码机请求密码安全服务，SDF 接口使用 TCP/IP 协议与密码机进行交互，详见密码机随机光盘中的《SJJ1507 服务器密码机应用开发手册》。

密码机的快速使用流程

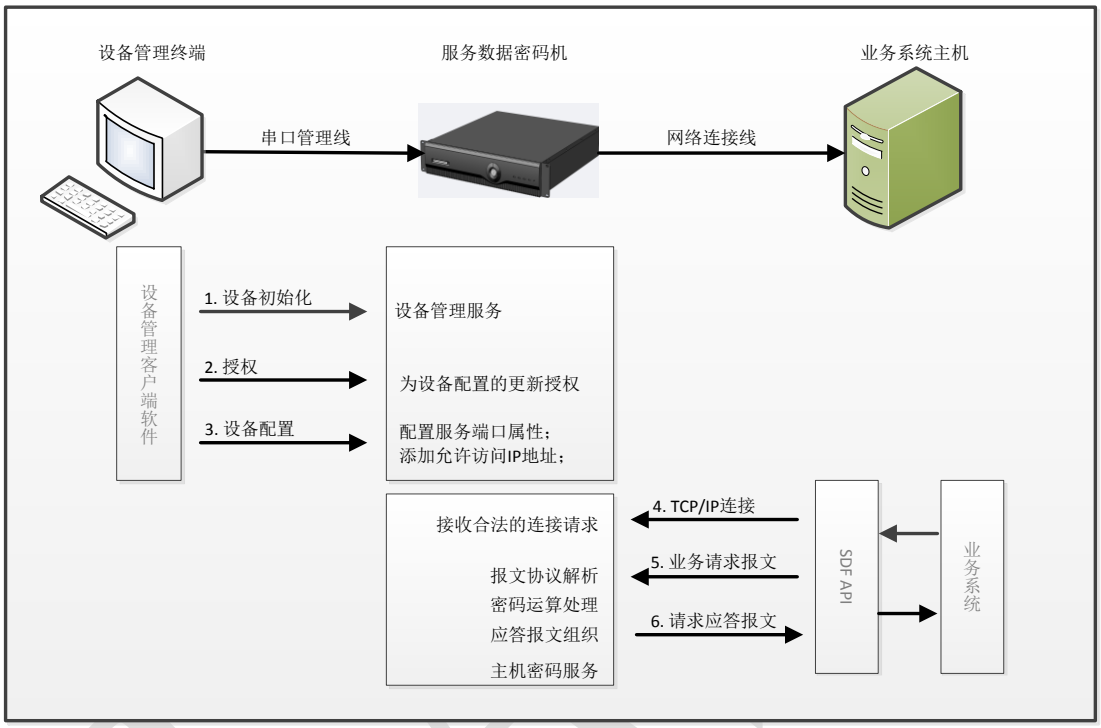


图 2-2 密码机的快速使用流程图

3. SJJ1507 密码机设备管理操作详述

密码机的管理采用 C/S 模式进行。密码机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。

在服务器密码机开机启动后 1 – 2 分钟后，在管理客户端所在的系统主机上双击运行 PKIManager.exe（从随机附带的光盘中获取），其主界面如下：

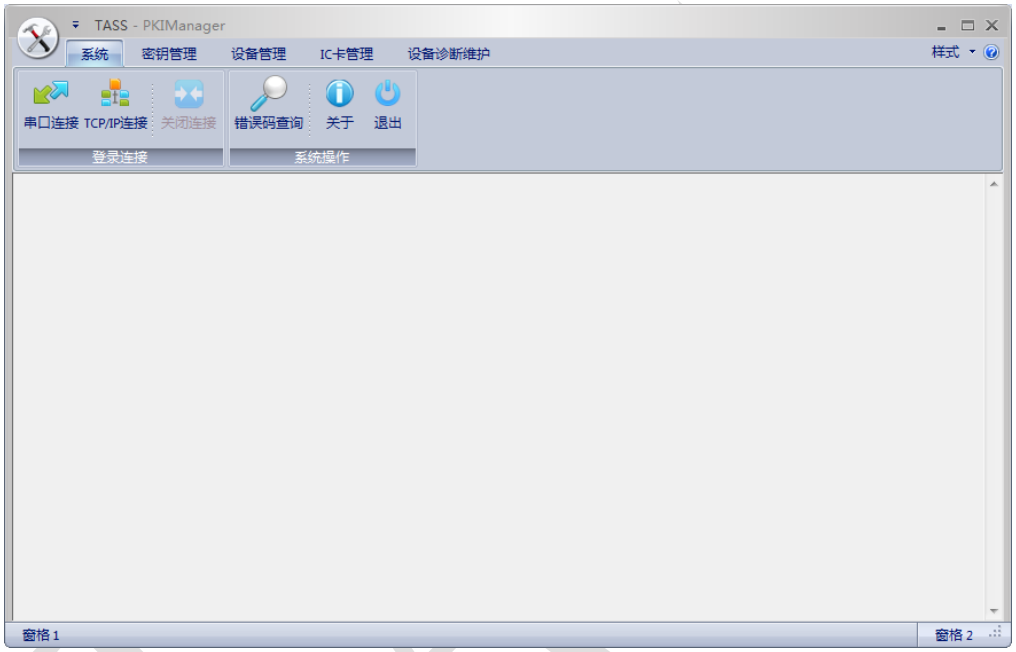


图 3-1 密码机设备管理客户端软件主界面

该客户端软件提供的管理操作包括：

- 系统操作，串口或 TCP 登录连接，关闭连接，错误码查询和退出；
- 密钥管理，设备主密钥的原始/恢复初始化，应用密钥管理、备份和恢复；
- 设备管理，服务端口、可信客户端、设备时间的配置，授权管理，TCP 登录口令管理；
- IC 卡管理，IC 卡的格式化、复制、修改口令；
- 设备诊断，日志的配置与导出，设备运行状态信息的获取，系统维护；

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，若是直接执行光盘上的 HsmManager.exe，则不记录日志文件。

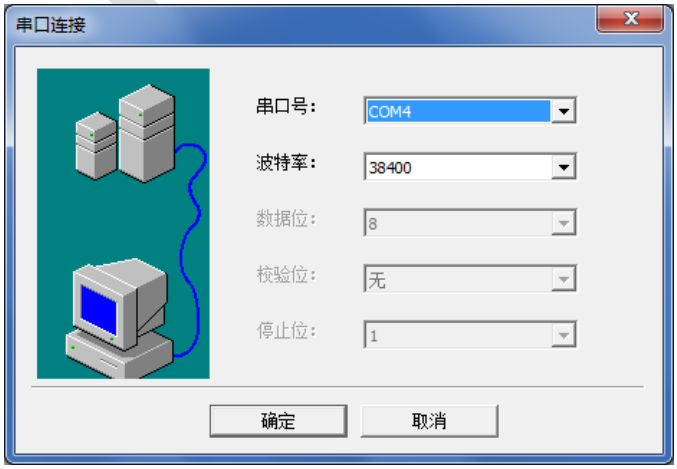
3.1. 系统操作

在进行管理配置操作前，首先需要通过该软件登录密码机，支持两种连接登录方式：串口连接、TCP/IP 连接。

图 3-2 设备管理客户端的登录连接

3.1.1. 串口连接

点击“串口连接”按钮，系统弹出串口参数设置对话框：



选择管理客户端上连接密码机的本机串口号，波特率保持默认的 38400 不变，点击“确定”后，管理软件的视图会提示连接登录结果。

3.1.2. TCP/IP 连接

点击“TCP/IP 连接”按钮，系统弹出 TCP/IP 连接参数设置对话框：

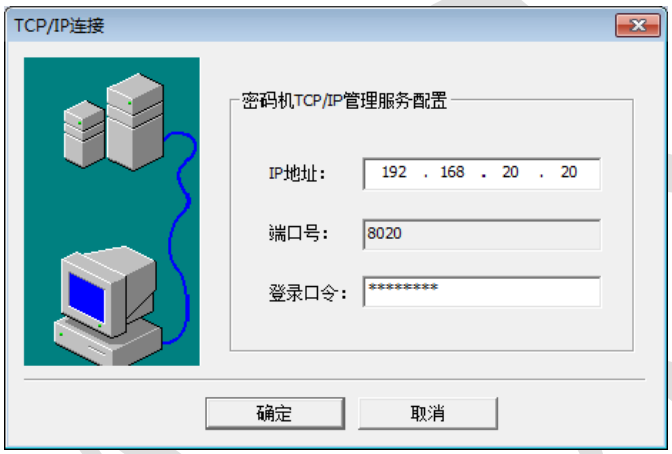


图 3-3 TCP/IP 连接登录密码机

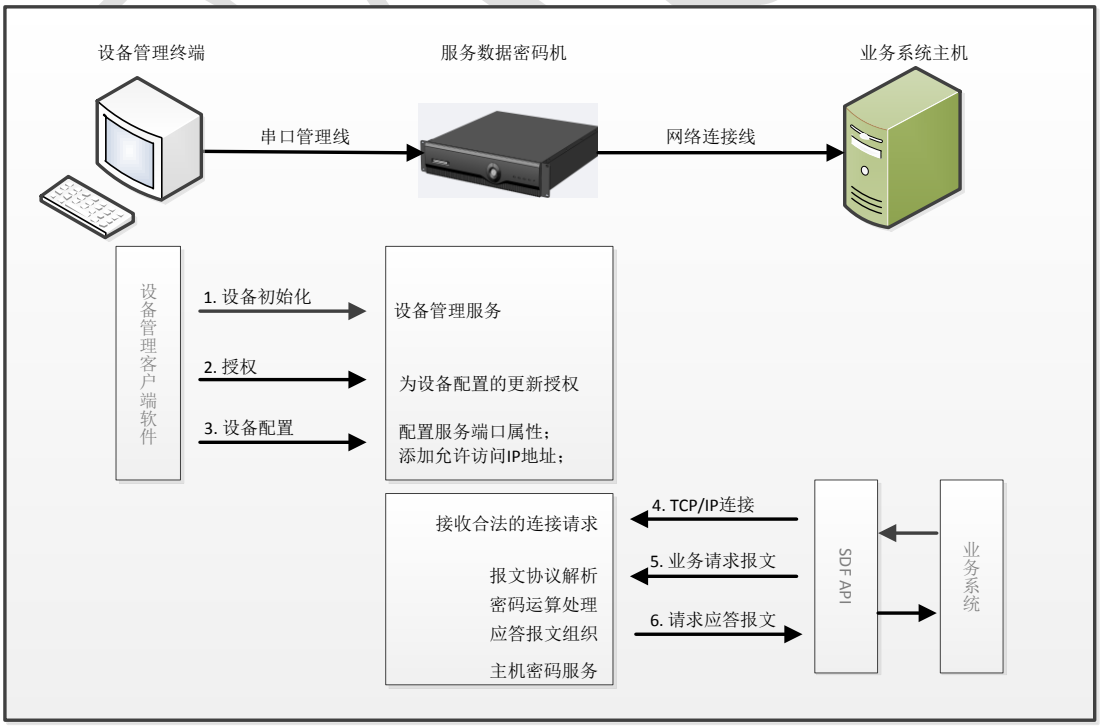


图 3-4 串口连接登录密码机

输入目标密码机的管理服务 IP 地址（密码机的出厂默认管理 IP 地址为：192.168.20.20）与登录口令，点击“确定”后，软件的视图会提示连接登录结果。

其中登录口令用于验证 TCP/IP 连接登录人员的合法性，密码机出厂默认口令为“12345678”，该口令可在登录后进行修改或重置（重置仅限串口连接模式下许可）。

3.2. 密钥管理

图 3-5 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；
- 应用密钥管理，对称、非对称密钥管理和密钥的备份与恢复；

3.2.1. 原始初始化

密码机出厂时装载有标准的测试主密钥，方便用户的开发调试用，当密码机要投入生产环境时，必须正确的完成生产初始化操作，流程包括产生 DMK 成份卡、导入合成 DMK、制作开机卡、确定授权机制、制作授权卡。

点击“原始初始化”按钮，系统弹出警告提示框：

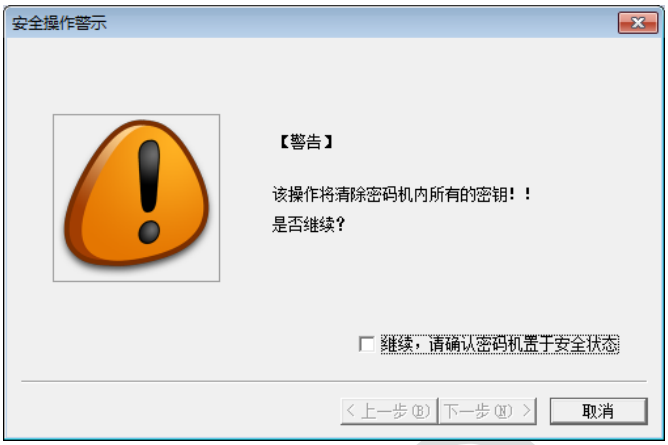


图 3-6 设备管理的安全警示

该操作将清除设备内的全部密钥，若要继续则拨动密码机前面板的状态锁到“安全”模式下，勾选继续，点击“下一步”：

图 3-7 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）确定成份卡数目并输入，点击“下一步”进入第二步：

图 3-8 原始初始化第二步

在原始初始化第二步中，将依次制作 n 张成份卡。

制作成份卡时，由成份卡持有人两次输入预定义的秘密值（8-32 个任意字符），插入要制作的成份 IC 卡并输入卡片口令，点击“产生成份卡”按钮，密码机将计算得到的成份数据写入 IC 卡；

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

图 3-9 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 张成份卡导入到密码机内。按照提示插入一张成份卡并输入口令，点击“导入成份卡”按钮，密码机将读取卡片内的成份数据；

同上导入 n 张成份卡，成份卡的导入次序无关，但不能将同一张成份卡多次导入。点击“下一步”进入第四步：

图 3-10 原始初始化第四步

原始初始化的第四步，制作开机卡。开机启动时必须插入正确的开机卡密码机才能提供正常的密码安全服务。开机卡为一机一卡。

依照提示，插入要制作的开机卡，输入卡片口令，点击“下一步”完成开机卡的制作，进入第五步：

图 3-11 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 张授权卡由 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 张授权卡认证通过。

选定授权控制机制后，点击“下一步”进入第六步：

图 3-12 原始初始化第六步

原始初始化的第六步，制作授权卡。按照系统提示依次插入 n 张 IC 卡，完成授权卡的制作。点击“完成”按钮结束原始初始化操作，请将安全状态锁拨回工作模式。

初始化操作完成后，密码机内已设置了新的生产主密钥，需重启密码机或重启主机密码服务以使新密钥生效。

3.2.2. 恢复初始化

当多机备份时，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，可完成多台密码机的设备主密钥同步。流程包括导入 DMK、制作开机卡、同步授权信息或制作新的授权卡。

点击“恢复初始化”按钮，系统弹出警示框（如图 3-6）；类同原始初始化，该操作将清除设备内的全部密钥，若要继续则拨动密码机前面板的状态锁到“安全”模式下，勾选继续，点击“下一步”：

图 3-13 恢复初始化第一步

在恢复初始化第一步中，输入 DMK 成份卡数目，点击“下一步”：

图 3-14 恢复初始化第二步

在恢复初始化第二步中，依次插入 n 张成份卡并输入 IC 卡口令，点击“导入成份卡”按钮，密码机将读取卡片内的成份数据；

成份卡的导入次序无关，但不能将同一张成份卡多次导入。点击“下一步”进入第三步：

图 3-15 恢复初始化第三步

恢复初始化的第三步，制作开机卡。依照系统提示，插入要制作的开机卡并输入 IC 卡口令，点击“下一步”完成开机卡的制作，进入第四步“确定授权机制”：

图 3-16 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卡。

1. 多机备份的密码机若共用一套授权卡，则选择“同步授权信息”，点击“下一步”：

图 3-17 恢复初始化第五步 - 1

插入有效授权卡输入口令，点击“完成”后结束恢复初始化流程；

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

图 3-18 恢复初始化第五步 - 2

依次制作 n 张新的授权卡，操作类同原始初始化的第六步，点击“完成”结束恢复初始化流程；

然后按照系统提示，请将安全状态锁拨回工作模式。重启密码机或重启主机密码服务以使新密钥生效。

3.2.3. 出厂初始化

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，在测试主密钥下，密码机内使用公开通用的 LMKs 密钥，见用户开发手册 1.4 章节内容。

点击“装载测试主密钥”按钮，系统弹出警示框（如图 3-6）；类同原始初始化，该操作将清除设备内的全部密钥，若要继续则拨动密码机前面板的状态锁到“安全”模式下，勾选继续，点击“下一步”：

图 3-19 出厂初始化第一步

使用测试主密钥时，密码机将使用无开机卡模式。点击“下一步”后类同原始初始化的步骤，确定授权控制机制，完成授权卡的制作。

【说明】原始初始化、恢复初始化或出厂初始化操作，需在安全状态下进行，将清除设备内的全部密钥，如有需要，请在该类操作前进行应用密钥的备份。

3.2.4. 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，如下：

```
[2014-11-17 15:35:51] 【获取DMK校验值，成功】
# DMK校验值: 08D7B4FB629D0885
```

3.2.5. 对称密钥管理

系统提供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“对称密钥管理”，系统将列举当前已存在的密钥状态：

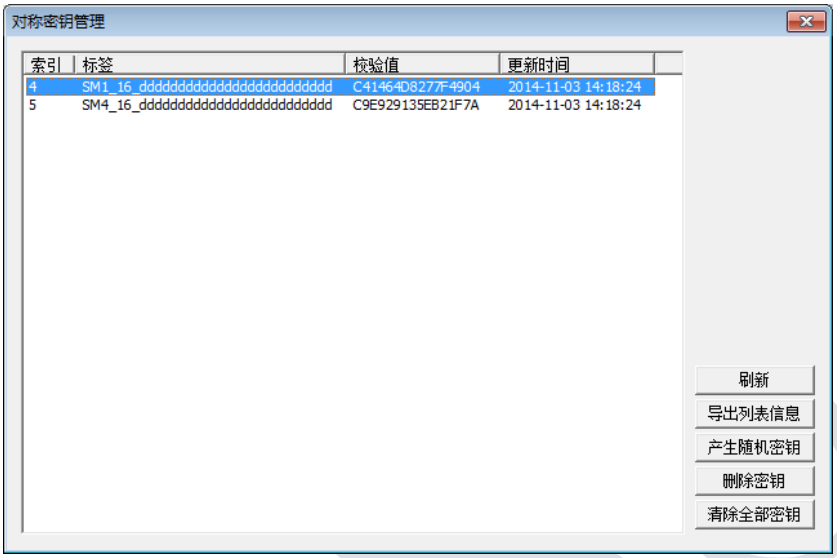


图 3-20 对称密钥管理

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、删除密钥和清除全部密钥。

【注意】密码机内部密钥的变更需获取“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：

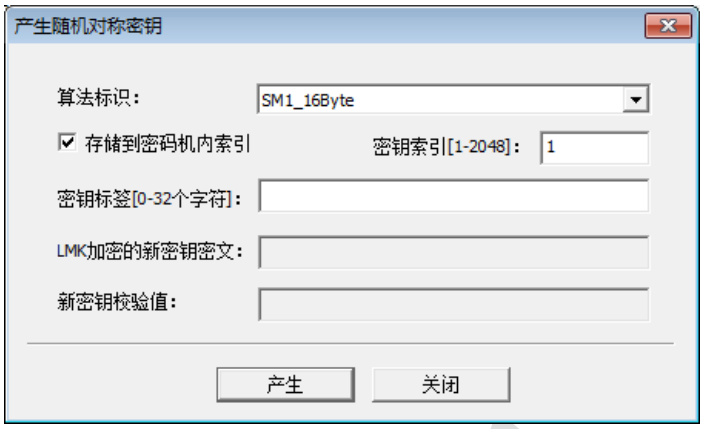


图 3-21 产生随机对称密钥

用户可根据需要选择要产生密钥的密钥类型、算法标识、是否存储在密码机内，输入密钥索引、密钥标签，点击“产生”，密码机将产生新的随机密钥并输出显示密文和校验值；若勾选了“存储到密码机内索引”，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”，密码机将删除选定的密钥，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”，密码机将清除全部对称密钥，并提示操作结果；

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：

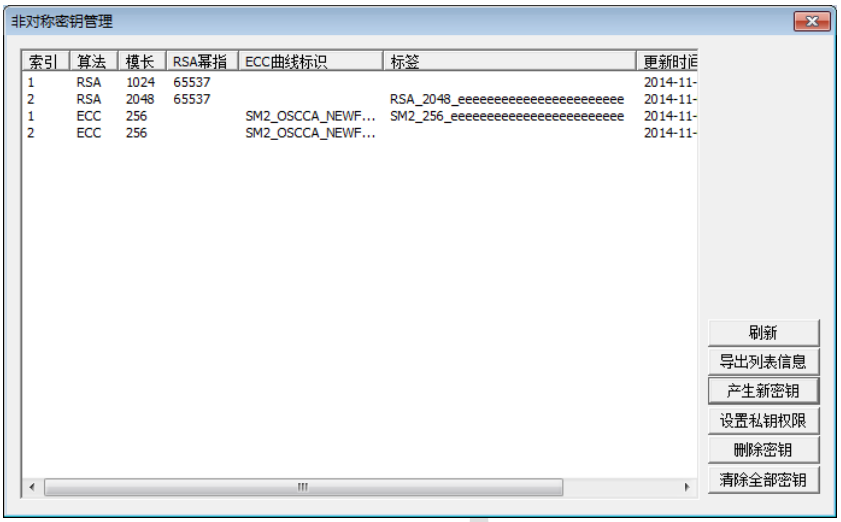


图 3-22 非对称密钥管理

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，密码机该版本仅支持 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。

1） **产生随机密钥**

点击“产生新密钥”按钮，系统弹出对话框：

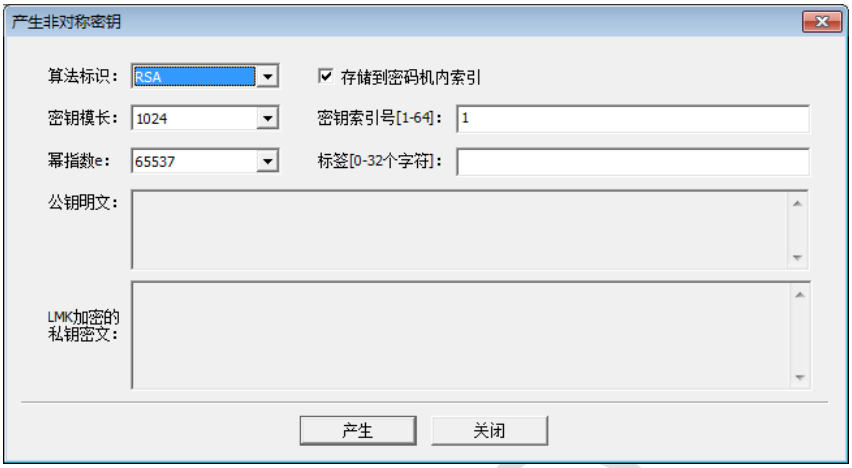


图 3-23 产生非对称密钥

用户可根据需要选择要产生密钥的算法标识、是否存储在密码机内，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”，密码机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“存储到密码机内索引”，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”，密码机将删除选定的密钥，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”，密码机将清除全部对称密钥，并提示操作结果；

3.2.7. 密钥备份与恢复

密钥备份，是将密码机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。

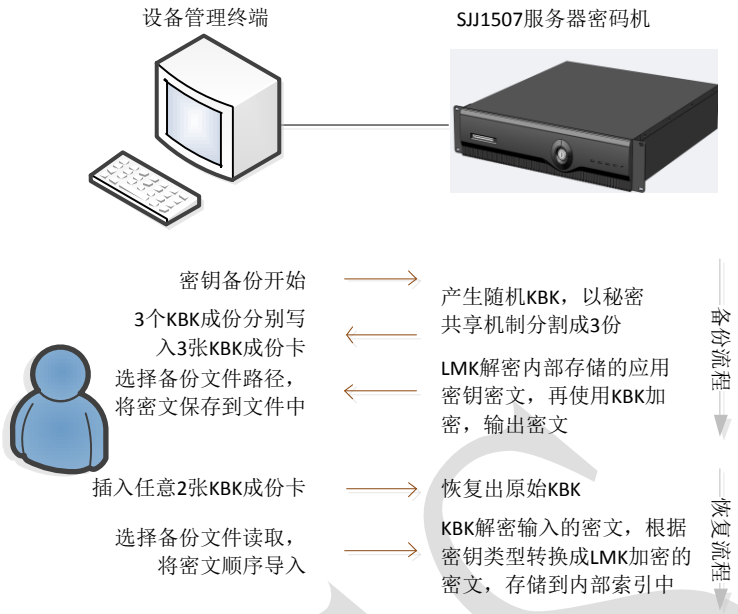


图 3-24 密钥备份恢复流程

1） 密钥备份

密钥备份将制作 3 张 KBK 卡，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卡：

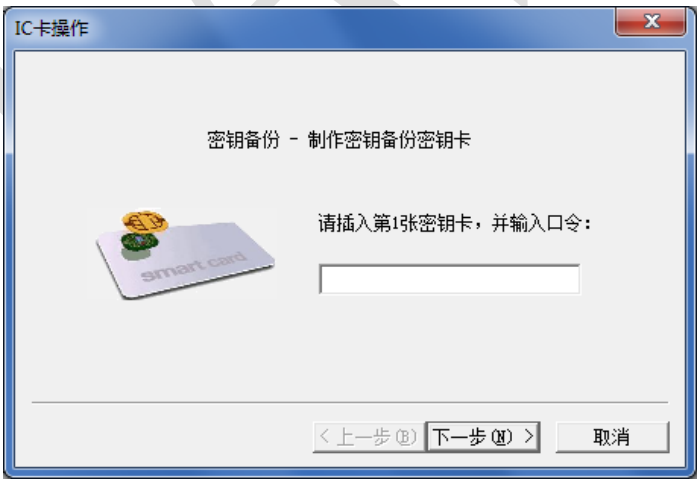


图 3-25 密钥备份–制作 KBK 卡

按照系统提示插入空白 IC 卡并输入口令，点击“下一步”，密码机将依次制作出 3 张 KBK（密钥备份密钥）卡，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：

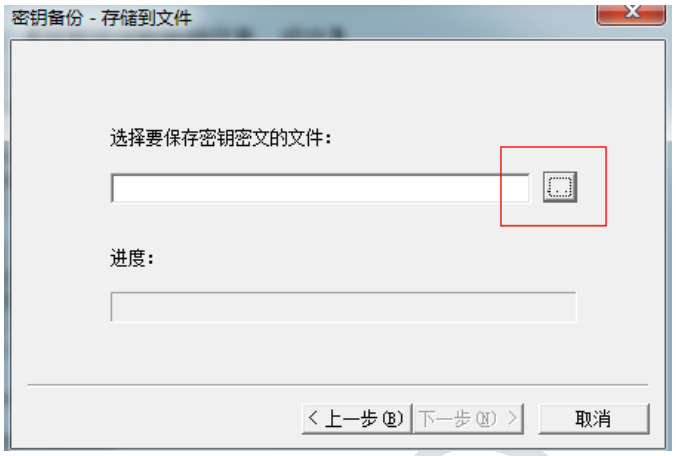


图 3-26 密钥备份–选择文件

按提示选择文件名，点击“下一步”，密码机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：

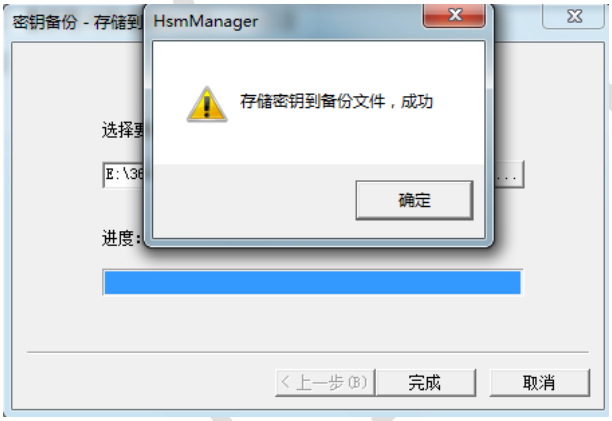


图 3-27 密钥备份–完成

点击“完成”结束密钥备份流程。3 张 KBK 卡和备份文件需妥善保管，待密钥恢复时使用。

2） 密钥恢复

密钥恢复需使用备份时制作的任意 2 张 KBK 卡和密钥备份文件。

点击“密钥恢复”，系统提示读取密钥备份密钥卡：

图 3-28 密钥恢复–读取 KBK 卡

按照系统提示，插入任意 2 张备份时产生的 KBK 卡并输入口令，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：

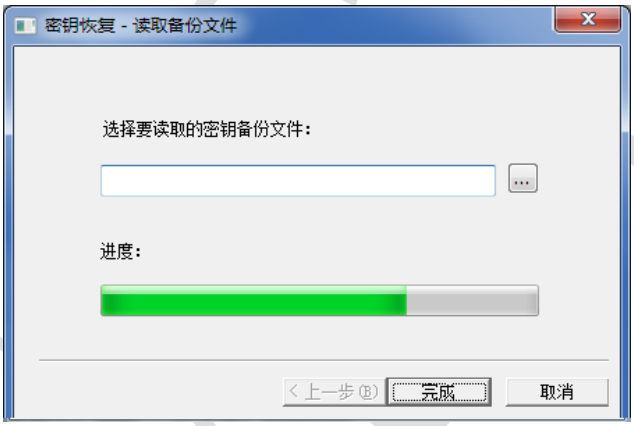


图 3-29 密钥恢复–选择备份文件

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”结束密钥恢复操作。

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 3-30 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，可信客户端管理、主机端口/管理端口、设备时间的获取与重置，配置卡的制作和导入；
- 授权管理，为某些操作授权和查看当前的授权状态；
- TCP 登录口令管理，修改与重置；

3.3.1. 设备配置

密码机需完成正确的属性配置后，业务系统才能正常连接使用密码机。

- 可信客户端，即允许访问的客户端 IP 地址，列举与添加、删除；
- 主机端口属性，主机密码服务端口属性配置的获取与重置。
  对应密码机后面板的 LAN1 端口，密码机通过该端口对业务系统提供密码运算服务。
- 管理端口属性，设备管理服务端口属性配置的获取与重置。
  对应密码机后面板的 LAN2 端口，密码机通过该端口对设备管理客户端软件提供配置管理服务。
  【注意】为保证设备的管理与应用的安全性，管理端口的 IP 地址与主机端口的 IP 地址必须处于不同的子网中，否则 LAN2 端口被禁用。
- 设备时间，获取与重置；
- 配置卡的应用，配置卡用于备份密码机的配置信息，并可导入恢复到新的密码机以同步配置信息；

上述属性的更新需获取“设备配置更新”操作类别的授权许可，且某些属性被重置后需重启主机密码服务或重启密码机后方可生效。

1） 可信客户端配置

点击“可信客户端”，系统将显示当前已配置的允许访问客户端 IP 地址列表：

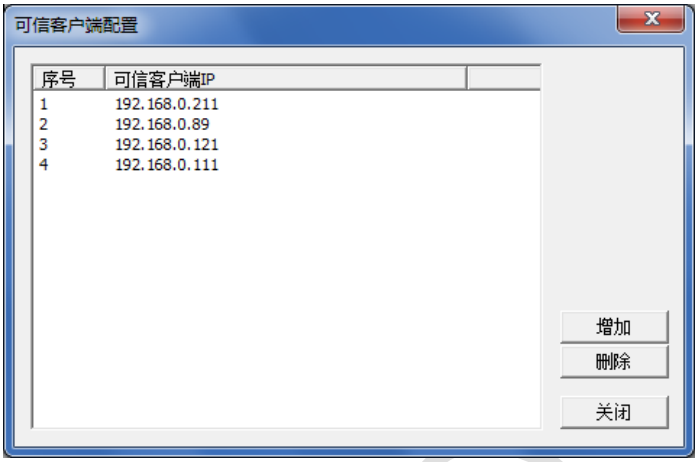


图 3-31 可信客户端配置

可根据实际应用需求进行增加和删除操作，即时生效。

a) 增加可信客户端

点击“增加”按钮，系统弹出输入对话框：

图 3-32 增加可信客户端

输入有效的可信客户端 IP 地址，点击“确定”将新的客户端 IP 添加到允许访问地址列表中，每个增加操作最多可添加 6 个可信客户端。

b) 删除可信客户端

在可信客户端列表中，选择要删除的 IP 地址，一个或多个，点击“删除”按钮，密码机将删除选定的客户端 IP，并弹出操作结果；

2） 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：

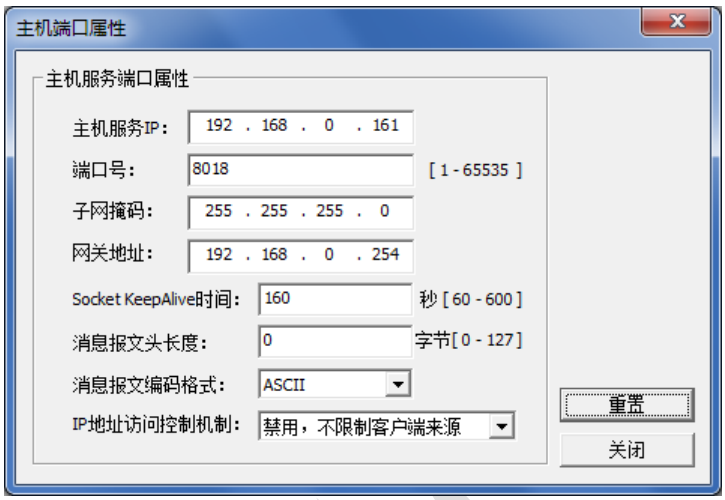


图 3-33 主机端口属性配置

主机端口属性项及说明详见**表 2-1 主机端口属性表**内容。

若主机服务 IP、子网掩码、网关地址被更新重置，则重启密码机后生效；

若端口号、KeepAlive 时间、报文头长、编码格式被更新重置，则重启主机密码服务后生效；

若 IP 地址访问控制机制被更新重置，则即时生效；

3） 管理端口属性配置

点击“管理端口属性”，系统将显示当前的设备管理服务端口属性值：

图 3-34 管理端口属性配置

管理端口属性项及说明详见**表 2-2 管理端口属性表**内容。

上述属性若被更新重置，则重启密码机后生效；

【注意】为保证设备的管理与应用的安全性，管理端口的 IP 地址与主机端口的 IP 地址必须处于不同的子网中，否则 LAN2 端口被禁用。

4） 设备时间配置

点击“设备时间”，将显示出当前的设备时间配置：

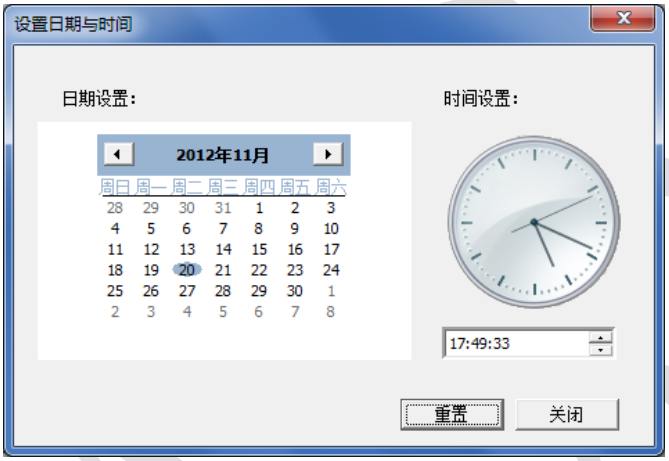


图 3-35 设备时间配置

用户可根据实际情况重新选择日期和时间，点击“重置”则为密码机设定新的设备时间，即时生效。

5） 配置卡的应用

图 3-36 配置卡应用

备份设备配置信息，选择“导出配置信息到 IC 卡”，然后按照系统提示插入一张配置 IC 卡并输入口令，密码机将自身的设备配置信息备份存储到配置卡上；

恢复设备配置信息，选择“从 IC 卡导入配置信息”，然后按照系统提示插入配置卡，密码机将读取卡上的配置信息导入到设备配置中。

设备配置信息包括主机端口属性、管理端口属性和可信客户端列表，不包括设备时间。

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；密码机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。

- IC 卡授权机制

  通过验证授权 IC 卡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 8 类，通过授权卡验证后，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、管理服务端口； 增加删除可信客户端； 重置设备时间；
	应用密钥管理	随机产生内部存储的密钥； 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；
	TCP 登录口令管理	重置 TCP 管理模式的登录口令；

	日志管理	重置日志配置；

1） 授权操作

点击“操作授权”，系统提示要验证授权卡：

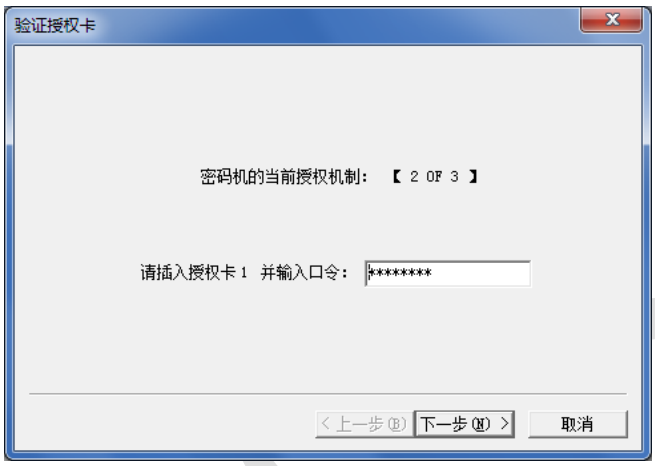


图 3-37 授权–验证授权卡

按照系统提示，插入授权卡并输入口令，点击“下一步”，密码机将验证授权卡的有效性，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卡验证通过（授权卡的验证次序无关，但重复验证无效），然后弹出授权类别对话框：

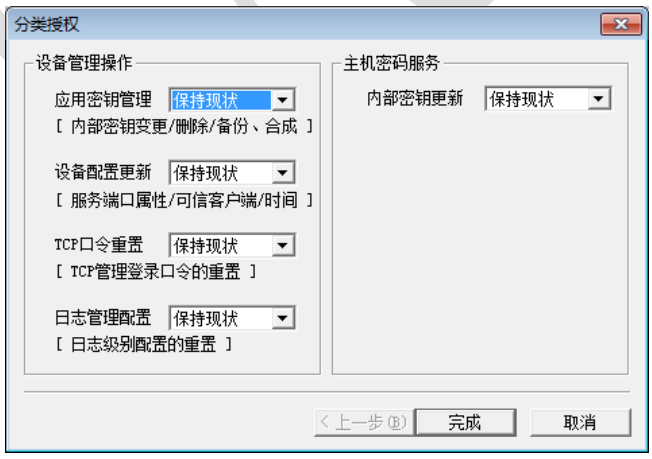


图 3-38 授权–选择类别和时间

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），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。

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：

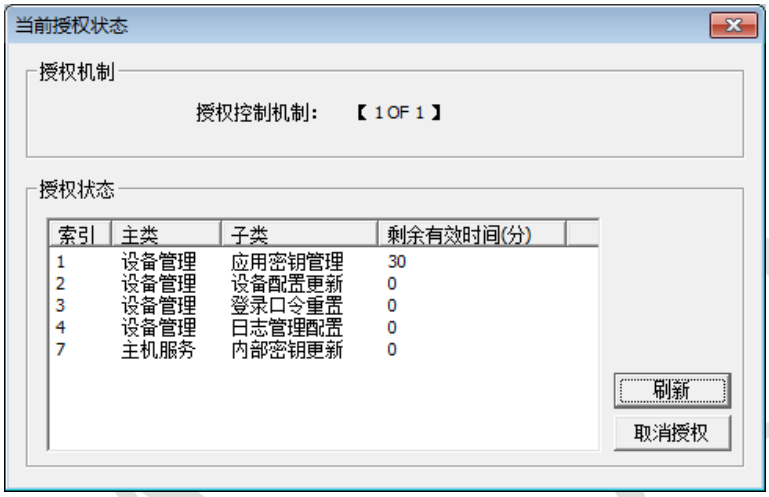


图 3-39 获取当前授权状态

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”，密码机将取消这些类别的授权许可。

当密码机配置为“无授权控制机制”时，所有的操作均不受限，且取消授权操作无效。

3.3.3. TCP 登录口令管理

TCP 登录口令，用于对通过 TCP/IP 连接方式登录设备管理时的用户合法性控制。密码机出厂时的默认的登录口令为“12345678”，该口令可修改和重置，但重置操作仅限串口登录后允许执行。

1） 修改口令

点击“修改口令”：

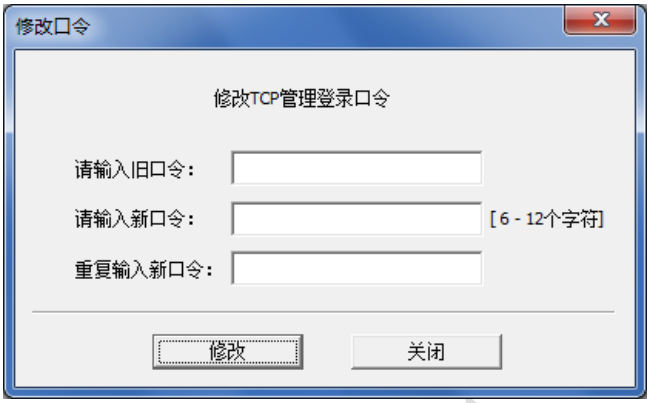


图 3-40 修改 TCP 管理登录口令

输入旧口令和要修改的新口令（两次输入确保无误），点击“修改”按钮完成口令的更新。TCP 登录口令必须是 6 – 12 个可见 ASCII 字符。

2） 重置口令

仅当串口连接模式登录设备管理后，“重置口令”按钮可用，点击后系统弹出：

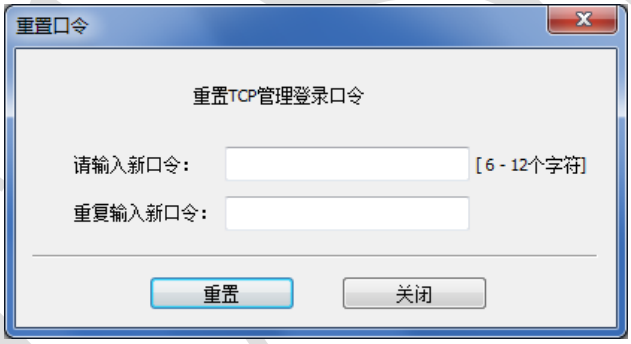


图 3-41 重置 TCP 管理登录口令

无需旧口令，直接两次输入口令（6 – 12 个 ASCII 字符），点击“重置”按钮，完成新口令的设置，新口令即时生效。

3.4. IC 卡管理

图 3-42 IC 卡管理功能

3.4.1. IC 卡管理说明

密码机采用智能 CPU 卡辅助完成设备管理过程中的身份认证或机密数据的存储，大大提高密码机的操作管理安全。IC 卡分为几类：

表 3-2 IC 卡分类表

	卡片类别	卡片内容	卡片用途
1	主密钥成份卡	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	授权卡	保存设备授权信息数据	用于授权管理的身份验证
3	开机卡	保存开机掩码因子	用于开机时恢复 DMK，一机一卡
4	密钥备份密钥卡	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 张恢复原 KBK
5	配置卡	保存设备的配置参数	用于备份存储设备的配置信息

用户可根据系统的安全需求制定相应的 IC 卡管理规则，定义卡片持有人和卡片类型，为卡片进行格式化（个人化）操作：重置卡片的生成日期、用户标识、发卡机构标识、保护口令等。所有的 IC 卡在使用时，均需要输入保护口令。

3.4.2. IC 卡操作

1） 格式化 IC 卡

密码机随机附带多张空白智能 IC 卡，在使用前应先进行格式化，为卡片设置一个访问口令，卡片口令应有持卡人自行选定并严格保管。

点击“格式化 IC 卡”，系统弹出对话框：

图 3-43 格式化 IC 卡

按照提示，输入卡片新口令（必须是 6 – 12 个数字），二次确认输入，输入持有人标识或名称、发行者标识（可以是用户单位名称），插入要格式化的 IC 卡后点击“确定”，等待片刻系统将提示操作结果。

2） 获取 IC 卡信息

插入 IC 卡，点击“获取 IC 卡信息”，系统将读取并在视图上显示出卡片的基础信息，包括卡号、类型、制卡时间、持有人标识等，如下图：

```
[2012-11-16 16:13:46] 【获取IC卡信息，成功】
# IC卡号     : 117440512
# 卡片类型   : 授权卡
# 格式化时间: 2102-10-04 10:18:05
# 制卡时间   : 2102-11-16 15:56:07
# 持有人ID   : Ella
# 发行者ID   : TASS Technology
# 授权卡标识: 1
# DMK校验值  : 08D7B4FB629D0885
```

3） 复制 IC 卡

密码机支持 IC 卡复制功能，用于备份各类功能卡片。

点击“复制 IC 卡”，系统弹出读取源卡对话框：

图 3-44 复制 IC 卡–读取源卡

按照提示，插入要复制的源 IC 卡并输入访问口令，点击“下一步”：

图 3-45 复制 IC 卡–写目标卡

按照提示，插入要复制的目标 IC 卡并输入访问口令，点击“下一步”完成 IC 卡复制操作。

4） 修改 IC 卡口令

点击“修改 IC 卡口令”，系统弹出对话框：

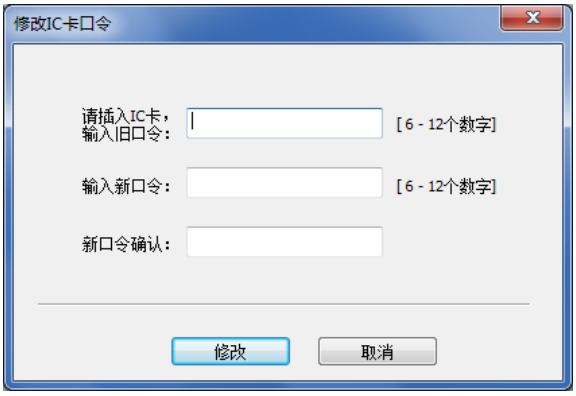


图 3-46 修改 IC 卡口令

按照提示插入要修改口令的 IC 卡，输入其旧口令，两次输入新口令（必须是 6 – 12 个数字），点击“修改”按钮，系统将提示操作结果。

3.5. 设备诊断

图 3-47 设备诊断功能

如图所示，设备诊断功能包括：

- 日志管理：日志的导出、清除与配置；
- 设备运行状态：设备基础信息、网络状态、设备自检、主机服务情况、PING 测试、资源信息；
- 系统维护：设备服务升级功能及切换超级维护终端；

3.5.1. 日志管理

密码机支持日志分类配置机制，分为错误日志和业务日志。

用户可根据需要启用或关闭某类日志类型，可导出或清除日志内容。其中业务日志支持外发功能，密码机将接收处理的所有业务动作和操作结果发送到预先配置的用户系统的 syslog 服务器上，以供查询审计。

开启日志记录对设备的运行性能有一定的影响，建议在生产环境中关闭日志功能。若开启了日志记录，务必及时导出并清除日志。

1） 日志配置

日志配置的变更重置，需要获取“日志管理配置”操作类别的授权许可。

点击“日志配置”，系统获取显示当前的配置属性：

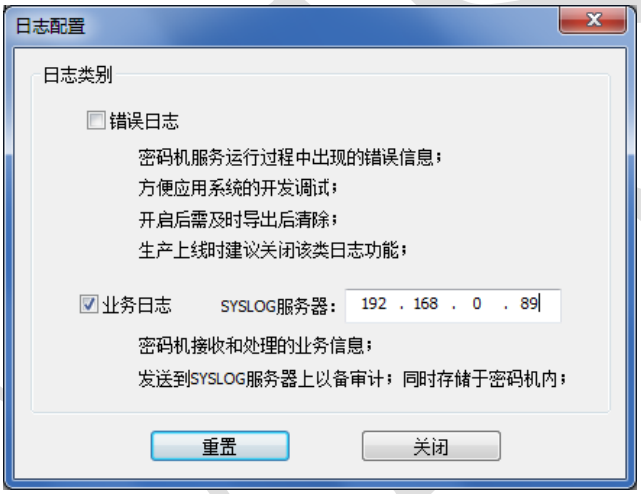


图 3-48 日志配置

用户根据实际情况，选择开启或关闭两类日志，若开启业务日志需正确设置外部的 SYSLOG 服务器地址。

点击“重置”更新日志配置，该项更新即时生效。

2） 日志导出

点击“导出日志”，系统弹出对话框：

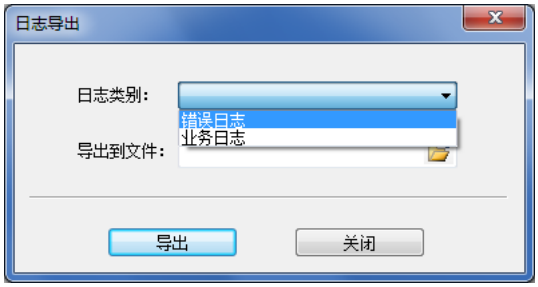


图 3-49 日志导出

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。

3） 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。

3.5.2. 设备运行状态

- 设备基础信息，获取服务软件的版本信息
- 网络状态，获取密码机上的网络连接情况
- 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
- PING 测试，PING 测试网络状况
- 设备资源信息，获取查看密码机的当前资源使用率

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等：

```
[2012-11-16 17:18:50] 【获取设备基础信息，成功】
# 设备主密钥校验值: 08D7B4FB629D0885
# 主机服务版本号   : H1.08.00
# 管理服务版本号   : M1.09.00
# 加密卡版本号     : CS00-025
# 设备序列号       : 201207000155
```

2） 网络状态

点击“网络状态”，系统获取显示密码机当前的网络连接情况：

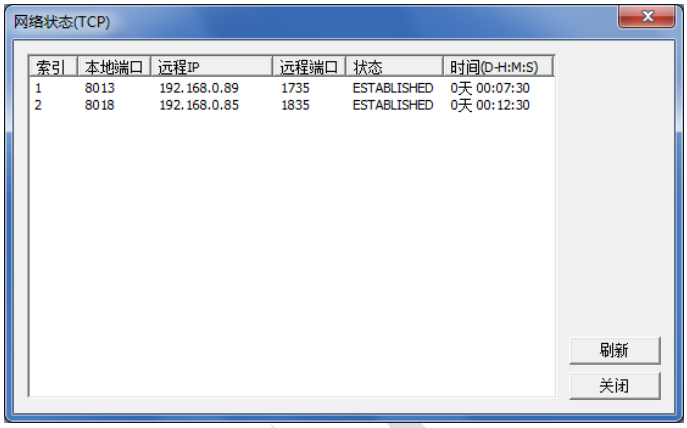


图 3-50 网络连接状态信息

3） 设备自检

点击“设备自检”，系统的视图上显示密码机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：

```
[2013-03-27 16:07:56] 【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
```

4） 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：

```
[2012-11-16 17:20:50] 【获取服务连接状态，完成】
# 主机服务: 正常
# 支持的最大连接数: 2048
# 当前已使用连接数: 0
# 剩余可用连接数   : 2048
```

5） PING 测试

点击“PING 测试”，弹出对话框：

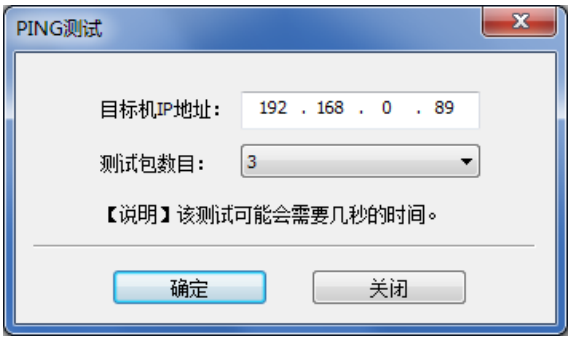


图 3-51 PING 测试

输入要测试的外部目标主机 IP 地址，选择测试包数目（1 – 5），点击“确定”后等待测试结束，系统将弹出测试结果提示框；

6） 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：

```
[2012-11-16 17:22:55] 【获取密码机资源占用信息，成功】
# 内存占用率: 3.96%
# CPU占用率 : 0.00%
```

3.5.3. 系统维护

1） 服务升级

密码机提供方便安全的服务升级功能。

服务升级前需做好设备的备份，包括配置和密钥。

升级服务时，需要厂商支持人员持专用的维护卡和服务升级包文件，然后在该客户端软件上完成服务的升级替换。

升级后需重启密码机以使新版服务生效。

4. 设备维护与疑难解答

4.1. 密码机的升级

SJJ1507 服务器密码机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/安装的密码机进行系统升级。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。

升级方法参见本文“3.5.3 系统维护”章节内容。

4.2. 常见问题 Q&A

一般情况下，服务器密码机出现故障，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） **设备无法启动**

- 请确认密码机已经连接电源，再重新启动；

2） **管理客户端软件的串口连接失败**

- 请确认正确使用管理线连接了密码机的管理端口（COM1）和终端主机的串口；
- 请确认终端软件选择了正确的串口号，已按照说明正确配置了串口属性；
- 确认密码机处于加电运行状态；

3） **管理客户端软件的TCP/IP连接失败**

- 请确认客户端与密码机的LAN2端口网络连接正常；
- 请确认登录界面中输入正确的密码机IP地址；
- 请确认输入了正确的TCP登录口令；

- 请确认客户端IP地址与密码机管理服务IP地址在一个网段内；

4) 管理客户端软件的菜单变灰无法使用

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

5) IC卡访问失败

- 请确认卡片被正确插入（IC卡状态灯亮）；
- 请确认输入了正确的卡片口令；

网络通讯

6) 密码机与主机系统网络通讯失败

- 请正确配置密码机的服务端口属性，应划入同一网段、接入同一VLAN；

7) 密码机与主机系统应用通讯失败

- 将密码机与应用服务器划分在同一网段、接入同一VLAN，正确配置；
- 将连接密码机的主机或服务器的IP地址添加到密码机的可信客户端列表中；

设备指示灯、蜂鸣器状态说明

8) 工作灯

- 密码机加电开机后的工作灯持续闪烁，标识设备处于开机过程中，大约3-4分钟密码机启动成功，则工作灯变更为灭状态；
- 若密码机加电开机超过5分钟工作灯仍持续闪，且外部没有访问密码机的业务请求，则说明密码机启动失败，请立即与我公司销售或支持人员联系；
- 密码机成功启动后，在外部有访问密码机的业务请求时，工作灯闪烁，标识当前的业务处理繁忙情况；

9) 告警灯

- 告警灯灭状态，标识设备正常；
- 密码机加电启动成功后，告警灯闪，说明设备自检失败，可能存在内部密

码模块故障，请立即与我公司销售或支持人员联系，根据实际情况对设备进行维修、更换；

- 密码机加电启动成功后，告警灯常亮，说明密码机无DMK或没有插入正确的开机卡；

10）蜂鸣器

- 加电开机后3-4分钟，’嘀—‘长响1-2秒标识启动完成；
- 设备启动完成后，’嘀，嘀，嘀’持续响，说明有服务未启动成功；
- 设备初始化过程中销毁密钥时，’嘀’一声响标识密钥销毁完成；
- 设备运行时，按住前面板的“密钥销毁按钮”不动，蜂鸣器将由慢到快的’嘀，嘀，嘀’持续响，警示即将销毁内部所有密钥；10秒后将’嘀—‘长响2秒标识已完成密钥销毁工作；

硬件故障

可能存在的硬件故障：

- 由于 CPU、内存导致加密机无法启动；
- 由于网卡故障导致通讯中断；
- 由于密钥卡故障导致密钥管理失败；
- 由于 IC 卡、读卡器故障导致密钥导入、导出失败；

上述现象发生后需即时与我公司人员联系，根据实际情况对设备进行维修、更换。

4.3. 错误码说明

4.3.1. 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
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	IC卡上电失败
0xE0000C02	IC卡格式化失败
0xE0000C03	IC卡验证PIN失败
0xE0000C04	IC卡更新PIN失败

0xE0000C05	读取IC卡失败
0xE0000C06	写入IC卡失败
0xE0000C07	IC卡不允许拷贝
0xE0000C10	IC卡类型错误
0xE0000C15	IC卡序号重复
0xE0000C17	DMK卡成份无效
0xE0000C18	读取DMK卡失败
0xE0000C19	写入DMK卡失败
0xE0000C20	IC卡读取的DMK成份无效
0xE0000C30	授权卡验证失败
0xE0000C31	授权卡序号无效，小于1或大于当前的授权机制
0xE0000C32	授权机制无效
0xE0000C40	KBK卡序号无效
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：mmj@tass.com.cn

5. 总体规格与需知

5.1. 总体规格

- **硬件规格**

  参见本文“1.4 密码机物理及电气指标”部分内容。

- **通信协议**

  网络通信：TCP/IP 协议

  控制端口：串行通信 RS232 标准

- **产品支持**

  支持的操作系统：WINDOWS 9X/NT/2000/XP/7、Linux、UNIX、HP Unix

  密码算法：SM1、SM2、SM3、SM4、ZUC、RSA、SHA1、SHA256

- **管理客户端软件的系统要求**

  操作系统：Windows 2000/XP/VISTA/7 等

  硬件要求：CPU 主频 600 MHz 以上；512M 内存

5.2. 重要安全需知

请仔细阅读安全须知。保存安全须知以备参考。

1、 请遵照产品上的警告标志与说明。
2、 清洁表面时，先拔下电源插头。切勿使用化学清洁剂。请以湿布擦拭即可。
3、 切勿将产品靠近水源。

4、 切勿将产品放于不稳定的推车、椅子或桌面上，以免产品滑落而损毁。

5、 使用本产品时，请留意标签上注明的电压类型。如果您无法确定，请洽询经销商或当地电力公司。

6、 请勿放置任何物品于电源线上，更勿将电源线放在出入口，以免遭到踩踏。

7、 使用延长线时，请注意其电源负荷度。插在同一延长线的电器总用电数不可超过延长线的电流负荷度。同时，同一插座的耗电量不可超过保险丝的负荷量。

8、 切勿将任何其他物品插入本产品的槽内，以免误触电路，造成短路、起火。同时，请勿泼洒任何液体到产品上。

9、 请勿自行维修产品。因为不当的拆卸，可能会导致触电或其他不良后果。因此，有任何维修问题，请接洽合格技术服务人员。

10、遇到下列状况时，请将电源插头拔掉，并寻求合格维护人员协助：

a) 电源线或插头有破损时；

b) 液体侵入机身时；

c) 依照指示操作，而产品仍无法正常运作时，您只能调整操作步骤中所提及的控制，因为如果调整不当，可能导致计算机受损，而且这些控制方式需要合格的技术人员，才能将计算机恢复到原来状况；

d) 产品不小心掉落地面或外壳有任何损伤时；

e) 产品功能明显改变，指明需要维修时；

SJJ1507 服务器密码机

用户使用手册

江南天安

地址：北京市海淀区马甸桥东路 17 号金澳国际大厦 1110 室

电话：010-82326383

传真：010-82328039

网址：http://www.tass.com.cn