



北京云港科技有限公司
Beijing Yungang Technology Co., Ltd

云港配电终端加密单元 使用帮助

版本号	时间日期	制定人	备注
V0.1	2018-06-20		初版
V0.2	2018-11-01		针对新加密单元做了调整

2018-06

目录

- 1 准备工作..... 1
 - 1.1 说明..... 1
 - 1.2 预备工作..... 1
 - 1.3 配置加密单元参数..... 3
- 2 协议配置部分..... 5
 - 2.1 加密无线平衡 101 透传模式..... 5
 - 2.2 加密有线 104 透传模式..... 8
 - 2.3 加密无线平衡 101 协议转换模式..... 11
 - 2.4 加密有线 104 协议转换模式..... 14
- 3 证书管理工具现场运维..... 18
 - 3.1 导出终端原始证书..... 18
 - 3.2 读取终端基本信息..... 22
 - 3.3 导出终端新的证书请求..... 22
 - 3.4 导入主站侧证书到终端..... 23
 - 3.5 调试和正式应用..... 24

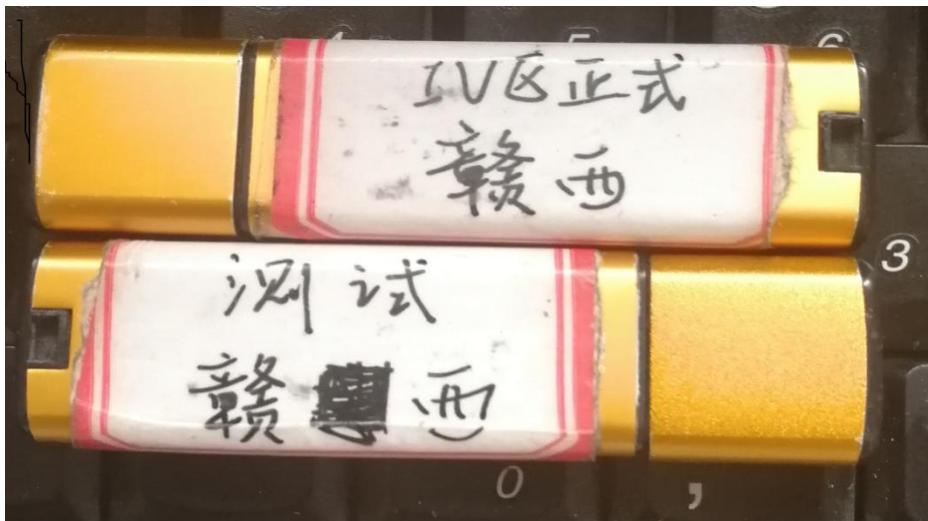
1 准备工作

1.1 说明

本文档会不断根据现场反馈进行更新。如需最新文档，请联系我们。【王工 QQ: 93904133】

1.2 预备工作

- 1、准备一根 USB 转 RS232 的连接线
- 2、准备一根网线，调试笔记本必须具备网口，可以插入网线，如没有请自备【USB 转网口转接线】
- 3、螺丝刀、万用表等工具
- 4、准备一根云港终端加密单元现场运维串口线【MiniUSB 转串口】
- 5、安装云港通讯管理机配置工具，可以从地址【ftp://cloxtec.com/YG-iComManager_setup.exe】
- 6、调试电脑上安装配电终端证书管理工具，可以从地址【<ftp://cloxtec.com/配电终端证书管理工具-安装包/>】下载，建议使用 filezilla 等专业 ftp 工具下载
- 7、到当地供电公司运检部门索要两个 USB Key，如下图：



- 一把标注测试的 Key，是用来导出终端原始证书、制作新的正式证书请求文件【注意，该 USB Key 可以单独向北京智芯微电子厂家购买】

- 一把标注“正式”或“IV区正式”的是导入当地主站证书的【注意，该 USB key 可以由当地供电公司授权向智芯微购买多把，以备不同厂家同时在现场使用】

1.3 配置加密单元参数

打开云港配置工具，第一次安装的时候，需要设定一个工程目录，请自行设定目录。

每一台终端加密单元有一个对应的设备授权码，请跟云港技术支持索取。

1、加密单元配置工具的连接

使用网线连接云港加密单元，可以连接任意网口。注意加密单元的默认 ip 分别为：

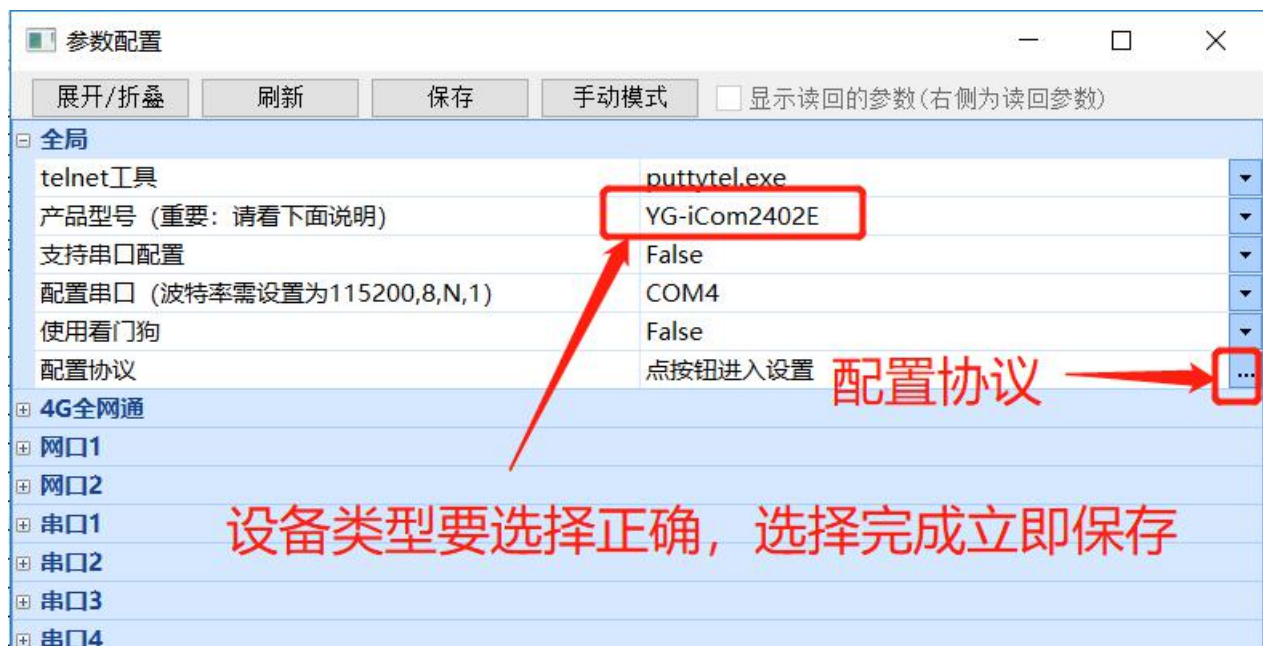
【网口 1:192.168.1.233】

【网口 2:192.168.2.233】

注意：调试电脑的网口 IP 要配置成跟被连接的加密单元网口 IP 在同一个网段。

2、全局部分

进入全局配置以后，首先要根据产品上的型号进行选择，务必选择正确。选择好产品型号以后，立即点保存；保存好产品型号之后，进入协议配置：



3、串口 5 配置

串口 5 是用来跟证书管理工具进行通信，提取证书请求，下载主站证书的，请配置串口 5 的参数如下：

串口5		
串口描述符	/dev/ttyS5	
波特率	115200	▼
校验位	None	▼
数据位	8	▼
停止位	1	▼

注意，证书管理工具的串口参数跟串口 5 参数要一致。

2 协议配置部分

2.1 加密无线平衡 101 透传模式

本模式适用于跟主站是采用加密无线平衡 101 方式通信，终端是标准平衡 101 协议【链路地址、传送原因、公共地址都是 2 个字节长度】。这样的情况下，可以使用透传方式对终端数据进行加密。

在全局中配置协议如下：

协议 1：【采集协议：配网平衡 101 透传协议】【串口】（备注：串口透传到终端设备）

协议 2：【转发协议：配网加密平衡式 101 从站协议（串口透传）】【socket 主动连接】（备注：负责跟主站通信，加解密）

协议 3：【转发协议：配网加密平衡式 101 从站协议】【串口】（备注：用来现场制证、导入主站证书用，且固定使用 COM5）

如下图所示：

报文配置		
配置协议数量：3		
保存 退出		
序号	协议类型	通道类型
1	采集协议：配网平衡101透传协议	串口
2	转发协议：配网加密平衡式101从站协议（串口透传）	Socket主动连接
3	转发协议：配网加密平衡式101从站协议	串口

使用串口 1 跟下面的终端设备连接，则需要配置串口 1 的参数：

串口1		
串口描述符	/dev/ttyS1	
波特率	9600	▼
校验位	None	▼
数据位	8	▼
停止位	1	▼
串口2		
串口3		
串口4		
串口5		

修改串口参数，跟终端串口参数一致

在这种情况下，还需要配置 4G 参数：

全局		
4G全网通		
4G通信功能	True	▼
是否使用用户名和密码登录	False	▼
拨号用户名（不填写使用系统默认用户名）		
拨号密码（不填写使用系统默认密码）		
拨号APN（不填写使用系统默认APN）		需要填写APN
在线状态判断方式	PING	▼
PING对方IP地址（默认8.8.8.8）	8.8.8.8	
使用4G通信的协议号	-1	
网口1		
网口2		
串口1		
串口2		
串口3		

主站如果支持ping通，可以填写主站ip地址

注意当地的 APN 设置，判断 4G 是否在线的方式。下面使用 4G 通信的协议号是用来判断 4G 有无通信数据的来源。如设置的是协议 2，则当协议 2 无任何数据通信时，系统会自动重新拨号连接。

4G全网通		
4G通信功能	True	▼
是否使用用户名和密码登录	False	▼
拨号用户名（不填写使用系统默认用户名）		
拨号密码（不填写使用系统默认密码）		
拨号APN（不填写使用系统默认APN）	xygdzdh.jx	
在线状态判断方式	TCP通信数据	▼
PING对方IP地址（默认8.8.8.8）	8.8.8.8	
使用4G通信的协议号	2	

协议 1 和协议 2 配置如图：

协议1 <采集协议：配网平衡101透传协议>	
协议类型	采集协议：配网平衡101透传协议
转发协议号（用符号‘+’间隔）	2
通道类型	串口
串口号	COM1
协议2 <转发协议：配网加密平衡式101从站协议（串口透传）>	
协议类型	转发协议：配网加密平衡式101从站协议（串口透传）
采集协议号（用符号‘+’间隔）	1
通道类型	Socket主动连接
串口号	COM1
服务器地址	10.37.49.50
服务器端口号	2404
绑定本地网口	不绑定
是否忽略主站安全网关认证	True
是否忽略证书工具认证	False
测试模式（忽略FCB翻转异常）	False
协议3 <转发协议：配网加密平衡式101从站协议>	

填入对方协议号

使用串口1跟终端设备通信

填写主站ip地址和端口

注意：一些主站没有配置安全网关，此处要忽略，否则无法通过认证

协议3是现场制证所用，制证完成，可以从全局中去掉协议3，配置如下图：

协议3 <转发协议：配网加密平衡式101从站协议>	
协议类型	转发协议：配网加密平衡式101从站协议
采集协议号（用符号'+ '间隔）	1
通道类型	串口
串口号	COM5
服务器地址	
服务器端口号	0
绑定本地网口	不绑定
是否线路加密	True
是否忽略主站安全网关认证	True
是否忽略证书工具认证	True
是否忽略主站认证	True
测试模式（忽略FCB翻转异常）	True
链路地址	1
公共地址	1
遥信起始地址	1
遥测起始地址	16385
遥控起始地址	24577
遥调起始地址	25089
电能累计量起始地址	25601
分接头升降档设备起始地址	26113
遥测数据死区千分比	0
是否启用转发点表	False
转发点表配置	点按钮进入设置

串口5	
串口描述符	/dev/ttyS5
波特率	115200
校验位	None
数据位	8
停止位	1

跟证书管理工具通信

都设置为True即可

配置完成，保存参数，退出配置参数窗口。然后到工具主界面上，【连接设备】，连接成功后，【读回设备信息】、【写入设备参数】、【重启设备】。

2.2 加密有线 104 透传模式

本模式适用于跟主站是采用加密有线 104 方式通信，终端是标准 104 协议【链路地址、传送原因、公共地址都是 2 个字节长度】。这样的情况下，可以使用网络透传方式对终端数据进行加密。

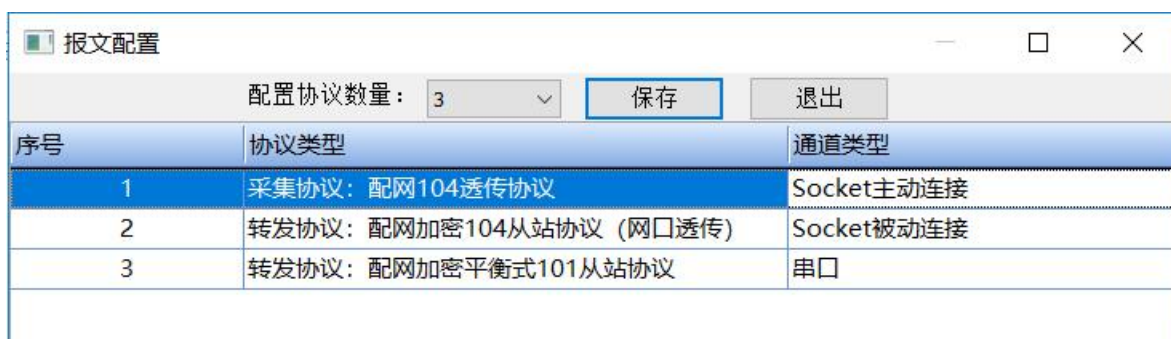
在全局中配置协议如下：

协议 1: 【采集协议: 配网 104 透传协议】【socket 主动连接】（备注: 网口透传到终端设备）

协议 2: 【转发协议: 配网加密 104 从站协议（网口透传）】【socket 被动连接】（备注: 跟主站通信、数据加解密）

协议 3: 【转发协议: 配网加密平衡式 101 从站协议】【串口】（备注: 用来现场制证、导入主站证书用, 且固定使用 COM5）

如下图所示:



报文配置

配置协议数量: 3 [保存] [退出]

序号	协议类型	通道类型
1	采集协议: 配网104透传协议	Socket主动连接
2	转发协议: 配网加密104从站协议 (网口透传)	Socket被动连接
3	转发协议: 配网加密平衡式101从站协议	串口

这种情况下, 4G 模块功能不需要启动, 请设置为 False。

设定网口 1 跟主站通信, 网口 2 跟终端设备通信, 则需要分别配置网口 1 和网口 2 的参数, 见下图:



4G全网通

4G通信功能: False 不使用4G, 设为False

是否使用用户名和密码登录: False

拨号用户名 (不填写使用系统默认用户名):

拨号密码 (不填写使用系统默认密码):

拨号APN (不填写使用系统默认APN):

在线状态判断方式: PING

PING对方IP地址 (默认8.8.8.8): 8.8.8.8

使用4G通信的协议号: -1

网口1

IP地址: 192.168.1.233

子网掩码: 255.255.255.0

网关: 192.168.1.1

设为默认路由: False

网口2

IP地址: 192.168.2.233

子网掩码: 255.255.255.0

网关: 192.168.2.1

设为默认路由: False

串口1

根据主站提供的IP进行设置, 如果主站同步上设备, 请设置为默认路由为True

此处IP设置成跟终端设备网口网段一致

协议 1 和协议 2 的配置如下：

协议 1 <采集协议：配网104透传协议>	
协议类型	采集协议：配网104透传协议
转发协议号（用符号'+ '间隔）	2
通道类型	Socket主动连接
监听端口	2404
服务器地址	192.168.1.100
协议 2 <转发协议：配网加密104从站协议（网口透传）>	
协议类型	转发协议：配网加密104从站协议（网口透传）
采集协议号（用符号'+ '间隔）	1
通道类型	Socket被动连接
服务器端口	2404
最大并发连接数	10
是否忽略主站安全网关认证	True
是否忽略证书工具认证	False
测试模式（忽略帧序号异常）	False

填写对方协议号（指向协议1的转发协议号2和协议2的采集协议号1）

填写终端设备的ip地址和端口（指向协议1的服务器地址192.168.1.100和监听端口2404）

注意主站有没有安全网关，如没有，则忽略，否则通不过认证（指向协议2的“是否忽略主站安全网关认证”为True）

协议 3 是现场制证所用，制证完成，可以从全局中把协议 3 去掉，配置如下图：

协议3 <转发协议：配网加密平衡式101从站协议>	
协议类型	转发协议：配网加密平衡式101从站协议
采集协议号（用符号'+ '间隔）	1
通道类型	串口
串口号	COM5
服务器地址	
服务器端口号	0
绑定本地网口	不绑定
是否线路加密	True
是否忽略主站安全网关认证	True
是否忽略证书工具认证	True
是否忽略主站认证	True
测试模式（忽略FCB翻转异常）	True
链路地址	1
公共地址	1
遥信起始地址	1
遥测起始地址	16385
遥控起始地址	24577
遥调起始地址	25089
电能累计量起始地址	25601
分接头升降档设备起始地址	26113
遥测数据死区千分比	0
是否启用转发点表	False
转发点表配置	点按钮进入设置

跟证书管理工具通信（指向串口号COM5）

都设置为True即可（指向“是否线路加密”、“是否忽略主站安全网关认证”、“是否忽略证书工具认证”、“是否忽略主站认证”均为True）

配置完成，保存参数，退出配置参数窗口。然后到工具主界面上，【连接设备】，连接成功后，【读回设备信息】、【写入设备参数】、【重启设备】。

2.3 加密无线平衡 101 协议转换模式

本模式适用于跟主站通信使用加密平衡 101，但终端设备的通信协议不支持标准平衡 101【标准平衡 101：链路地址、传送原因、公共地址的长度均为 2 个字节】的情况下使用，那么我们要配置 3 路协议：

协议 1：【采集协议：[请选择合适的采集协议](#)】【串口或网口】（备注：跟终端设备通信）

【！注意！：如果终端设备是非标协议，请联系我们技术支持定制协议，以便支持跟终端设备的通信】

协议 2：【转发协议：配网加密平衡式 101 从站协议】【socket 主动连接】（备注：跟主站通信、数据加解密）

协议 3：【转发协议：配网加密平衡式 101 从站协议】【串口】（备注：用来现场制证、导入主站证书用，且固定使用 COM5）

例如，我们跟终端设备使用 Modbus Rtu 协议的情况下，跟主站无线加密通信：

报文配置		
配置协议数量：3 保存 退出		
序号	协议类型	通道类型
1	采集协议：ModbusRtu Master	串口
2	转发协议：配网加密平衡式101从站协议	Socket主动连接
3	转发协议：配网加密平衡式101从站协议	串口

使用串口 1 跟下面的终端设备连接，则需要配置串口 1 的参数：

串口1		
串口描述符	/dev/ttyS1	
波特率	9600	▼
校验位	None	▼
数据位	8	▼
停止位	1	▼
串口2		
串口3		
串口4		
串口5		

修改串口参数，跟终端串口参数一致

在这种情况下，还需要配置 4G 参数：

全局		
4G全网通		
4G通信功能	True	▼
是否使用用户名和密码登录	False	▼
拨号用户名（不填写使用系统默认用户名）		
拨号密码（不填写使用系统默认密码）		
拨号APN（不填写使用系统默认APN）		需要填写APN
在线状态判断方式	PING	▼
PING对方IP地址（默认8.8.8.8）	8.8.8.8	
使用4G通信的协议号	-1	
网口1		
网口2		
串口1		
串口2		
串口3		

主站如果支持ping通，可以填写主站ip地址

注意当地的 APN 设置，判断 4G 是否在线的方式。下面使用 4G 通信的协议号是用来判断 4G 有无通信数据的来源。如设置的是协议 2，则当协议 2 无任何数据通信时，系统会自动重新拨号连接。

4G全网通		
4G通信功能	True	▼
是否使用用户名和密码登录	False	▼
拨号用户名（不填写使用系统默认用户名）		
拨号密码（不填写使用系统默认密码）		
拨号APN（不填写使用系统默认APN）	xygdzdh.jx	
在线状态判断方式	TCP通信数据	▼
PING对方IP地址（默认8.8.8.8）	8.8.8.8	
使用4G通信的协议号	2	

协议 1 和协议 2 的配置：

协议1 <采集协议: ModbusRtu Master>	
协议类型	采集协议: ModbusRtu Master
转发协议号 (用符号'+间隔)	2
通道类型	串口
串口号	COM1
自定义报文设置	点按钮进入设置
轮询间隔 (毫秒)	1000
数据大小端 (以16进制数AABBCCDD为例)	大端字节序 (AABBCCDD)
北海电气测控装置协议支持	False
协议2 <转发协议: 配网加密平衡式101从站协议>	
协议类型	转发协议: 配网加密平衡式101从站协议
采集协议号 (用符号'+间隔)	1
通道类型	Socket主动连接
串口号	COM1
服务器地址	10.37.49.50
服务器端口号	2404
绑定本地网口	不绑定
是否线路加密	True
是否忽略主站安全网关认证	True
是否忽略证书工具认证	False
是否忽略主站认证	False
测试模式 (忽略FCB翻转异常)	False
链路地址	1
公共地址	1
遥信起始地址	1
遥测起始地址	16385
遥控起始地址	24577
遥调起始地址	25089
电能累计量起始地址	25601
分接头升降档设备起始地址	26113
遥测数据死区千分比	0
是否启用转发点表	True
转发点表配置	点按钮进入设置

ModbusRTU
召测和遥控报文设置

字节序

此处填写主站IP和端口

加密功能开关

是否忽略网关认证, 如主站
没有安全网关, 则认证不通
过

注意配置转发点表

协议 3 是现场制证所用, 制证完成, 可以从全局中去掉协议 3, 配置如下图:

协议3 <转发协议：配网加密平衡式101从站协议>	
协议类型	转发协议：配网加密平衡式101从站协议
采集协议号（用符号'+ '间隔）	1
通道类型	串口
串口号	COM5
服务器地址	
服务器端口号	0
绑定本地网口	不绑定
是否线路加密	True
是否忽略主站安全网认证	True
是否忽略证书工具认证	True
是否忽略主站认证	True
测试模式（忽略FCB翻转异常）	True
链路地址	1
公共地址	1
遥信起始地址	1
遥测起始地址	16385
遥控起始地址	24577
遥调起始地址	25089
电能累计量起始地址	25601
分接头升降档设备起始地址	26113
遥测数据死区千分比	0
是否启用转发点表	False
转发点表配置	点按钮进入设置

跟证书管理工具通信

都设置为True即可

配置完成，保存参数，退出配置参数窗口。然后到工具主界面上，【连接设备】，连接成功后，【读回设备信息】、【写入设备参数】、【重启设备】。

2.4 加密有线 104 协议转换模式

本模式适用于跟主站通信使用加密 104，但终端设备的通信协议不支持标准 104 的情况下使用，那么我们要配置 3 路协议：

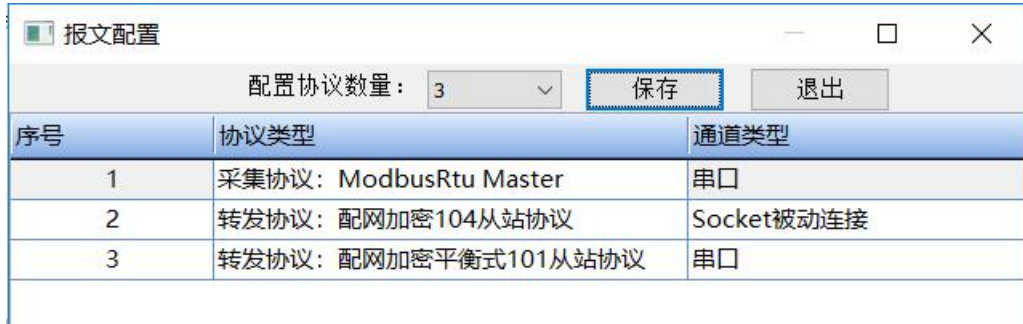
协议 1：【采集协议：请选择合适的采集协议】【串口或网口】（备注：跟终端设备通信）

【！注意！：如果终端设备是非标协议，请联系我们技术支持定制协议，以便支持跟终端设备的通信】

协议 2：【转发协议：配网加密 104 从站协议】【socket 被动连接】（备注：跟主站通信、数据加解密）

协议 3：【转发协议：配网加密平衡式 101 从站协议】【串口】（备注：用来现场制证、导入主站证书用，且固定使用 COM5）

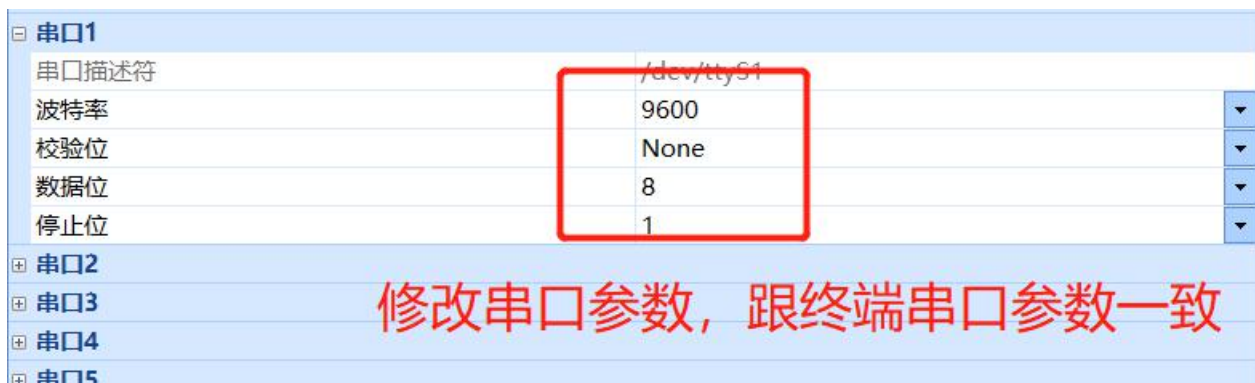
例如，我们跟终端设备使用 Modbus Rtu 协议的情况下，跟主站无线加密通信：



报文配置窗口显示配置协议数量为 3。配置列表如下：

序号	协议类型	通道类型
1	采集协议：ModbusRtu Master	串口
2	转发协议：配网加密104从站协议	Socket被动连接
3	转发协议：配网加密平衡式101从站协议	串口

使用串口 1 跟下面的终端设备连接，则需要配置串口 1 的参数：



串口1配置窗口显示以下参数：

串口描述符	/dev/ttyS1
波特率	9600
校验位	None
数据位	8
停止位	1

修改串口参数，跟终端串口参数一致

在这种情况下，使用网口通信，要关闭 4G 功能：



4G全网通配置窗口显示以下参数：

4G通信功能	False	不使用4G，设为False
是否使用用户名和密码登录	False	
拨号用户名（不填写使用系统默认用户名）		
拨号密码（不填写使用系统默认密码）		
拨号APN（不填写使用系统默认APN）		
在线状态判断方式	PING	
PING对方IP地址（默认8.8.8.8）	8.8.8.8	
使用4G通信的协议号	-1	

网口1配置窗口显示以下参数：

IP地址	192.168.1.233
子网掩码	255.255.255.0
网关	192.168.1.1
设为默认路由	False

根据主站提供的IP进行设置，如果主站同步上设备，请设置为默认路由为True

协议 1 和协议 2 的配置：

协议1 <采集协议: ModbusRtu Master>	
协议类型	采集协议: ModbusRtu Master
转发协议号 (用符号'+ '间隔)	2
通道类型	串口
串口号	COM1
自定义报文设置	点按钮进入设置
轮询间隔 (毫秒)	1000
数据大小端 (以16进制数AABBCCDD为例)	大端字节序 (AABBCCDD)
北海电气测控装置协议支持	False

ModbusRTU 召测及遥控报文配置

协议2 <转发协议: 配网加密104从站协议>	
协议类型	转发协议: 配网加密104从站协议
采集协议号 (用符号'+ '间隔)	1
通道类型	Socket被动连接
服务器端口	2404
最大并发连接数	10
是否线路加密	True
是否忽略主站安全网关认证	True
测试模式 (忽略帧序号异常)	False
t0 (秒)	10
t1 (秒)	30
t2 (秒)	5
t3 (秒)	15
t4 (秒)	8
k (帧数)	12
w (帧数)	8
公共地址	1
遥信起始地址	1
遥测起始地址	16385
遥控起始地址	24577
遥调起始地址	25089
电能累计量起始地址	25601
分接头升降档设备起始地址	26113
遥测数据死区千分比	10
是否启用转发点表	True
转发点表配置	点按钮进入设置

打开加密功能，并注意是否需要忽略网关认证

如主站没有配置网关，则需要忽略，否则认证过程无法通过

注意配置死区值及转发点表

协议 3 是现场制证所用，制证完成，可以从全局中把协议 3 去掉，配置如下图：

协议3 <转发协议：配网加密平衡式101从站协议>	
协议类型	转发协议：配网加密平衡式101从站协议
采集协议号（用符号'+ '间隔）	1
通道类型	串口
串口号	COM5
服务器地址	
服务器端口号	0
绑定本地网口	不绑定
是否线路加密	True
是否忽略主站安全网关认证	True
是否忽略证书工具认证	True
是否忽略主站认证	True
测试模式（忽略FCB翻转异常）	True
链路地址	1
公共地址	1
遥信起始地址	1
遥测起始地址	16385
遥控起始地址	24577
遥调起始地址	25089
电能累计量起始地址	25601
分接头升降档设备起始地址	26113
遥测数据死区千分比	0
是否启用转发点表	False
转发点表配置	点按钮进入设置

跟证书管理工具通信

都设置为True即可

配置完成，保存参数，退出配置参数窗口。然后到工具主界面上，【连接设备】，连接成功后，【读回设备信息】、【写入设备参数】、【重启设备】。

3 证书管理工具现场运维

3.1 导出终端原始证书

第一步：使用运维串口线连接电脑跟加密盒串口 5。

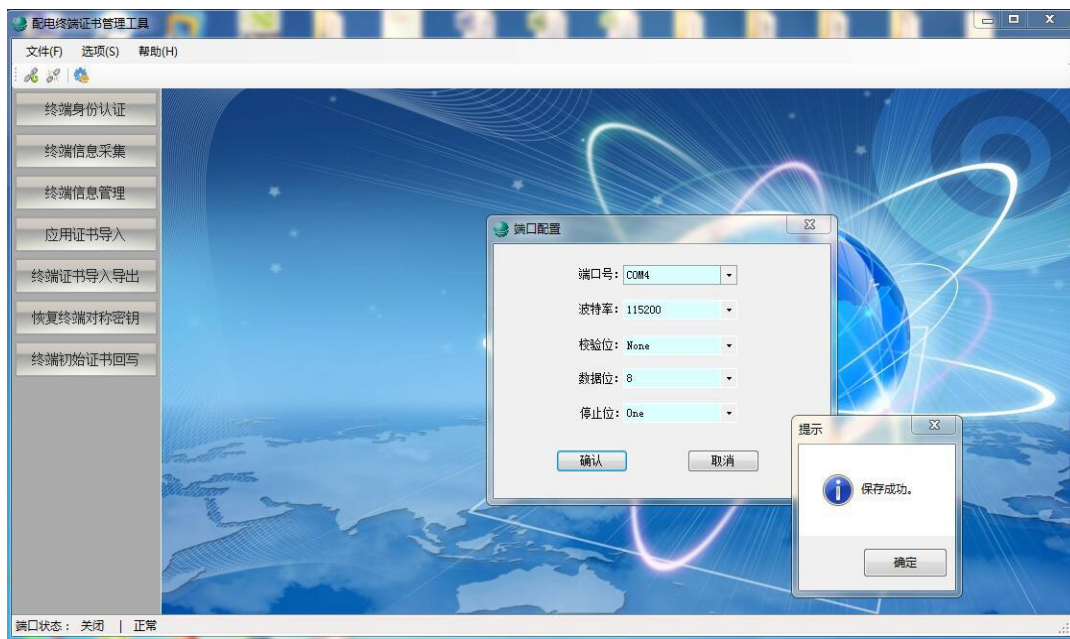
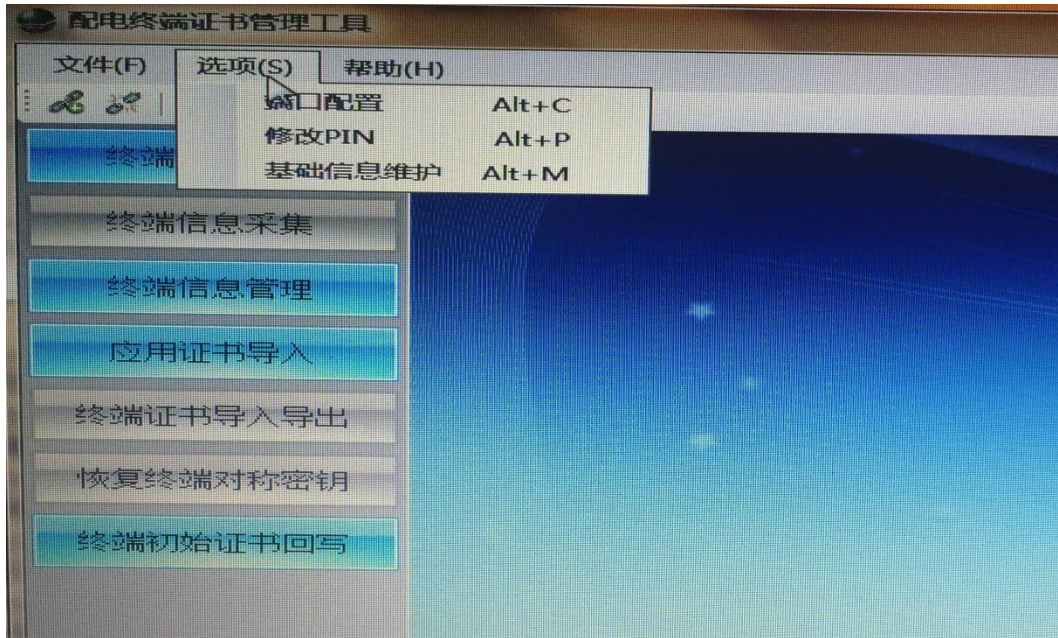
第二步：插入测试 Key



打开配电终端证书管理工具，输入 Key 的登录密码为 123456

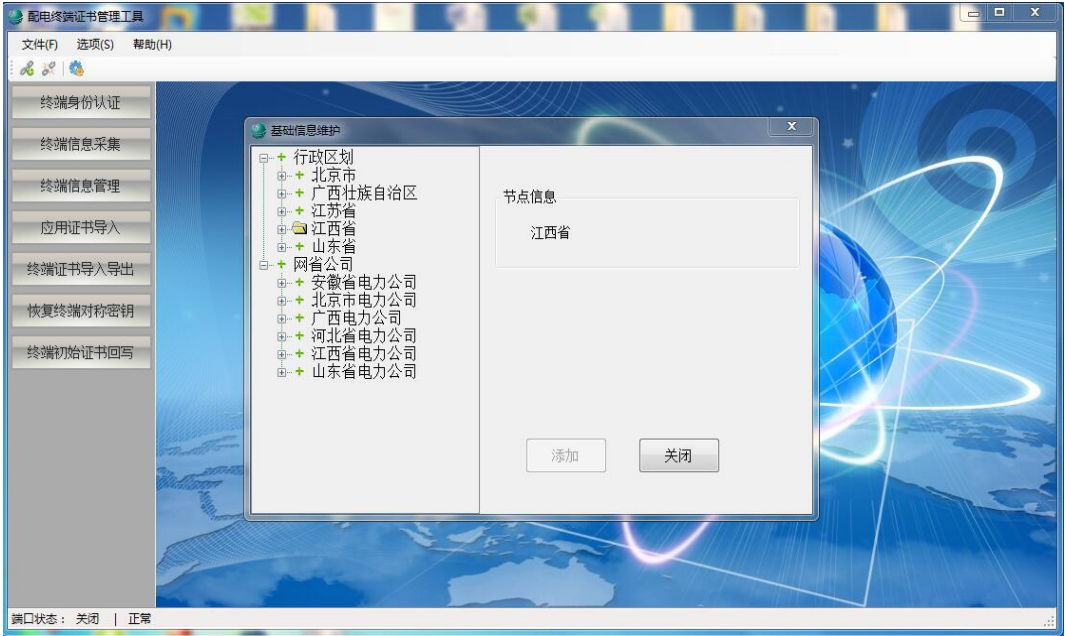


配置连接加密盒串口 1 的串口参数，设置参数为 115200,8, N,1。

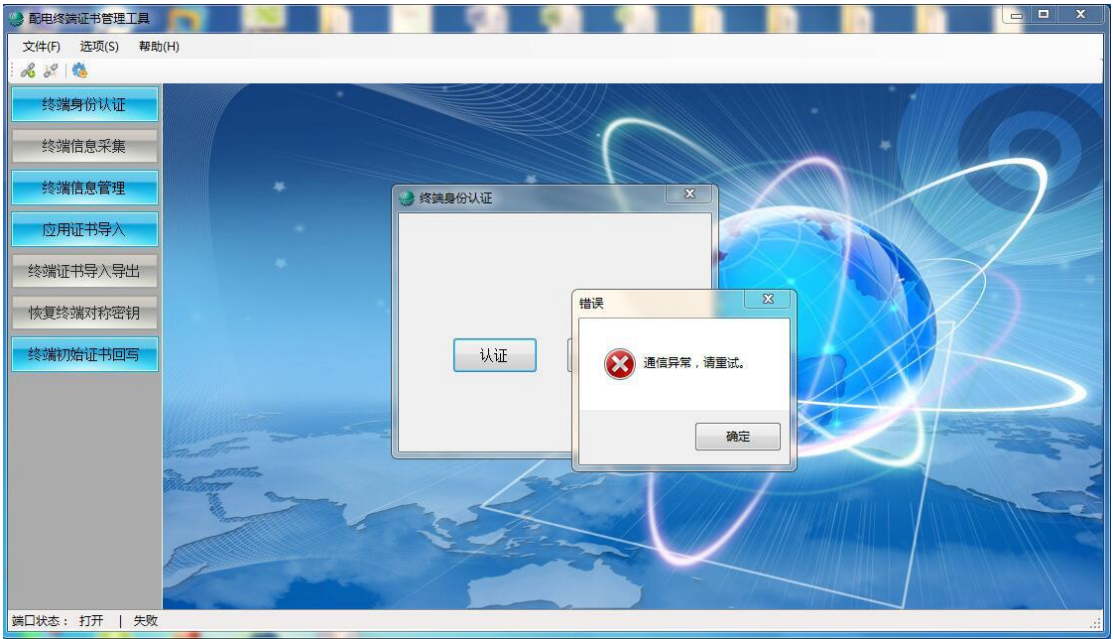


维护证书管理工具基础信息

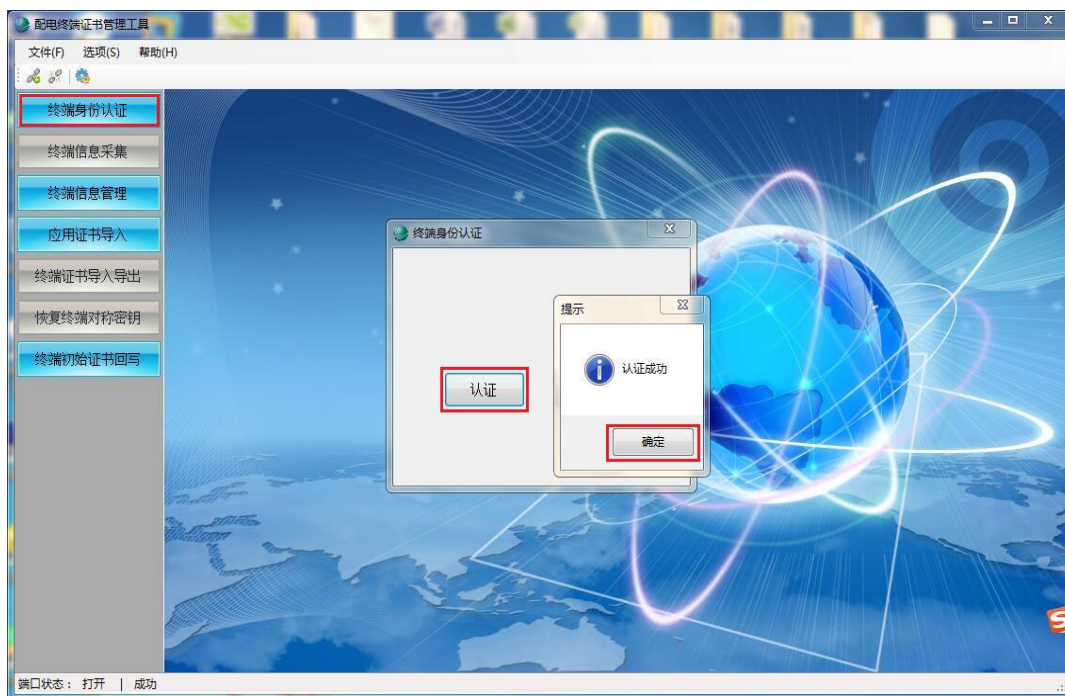
如果有的则增加当地行政区划（省、地、县）和网省公司（省公司、地县公司），如下图：



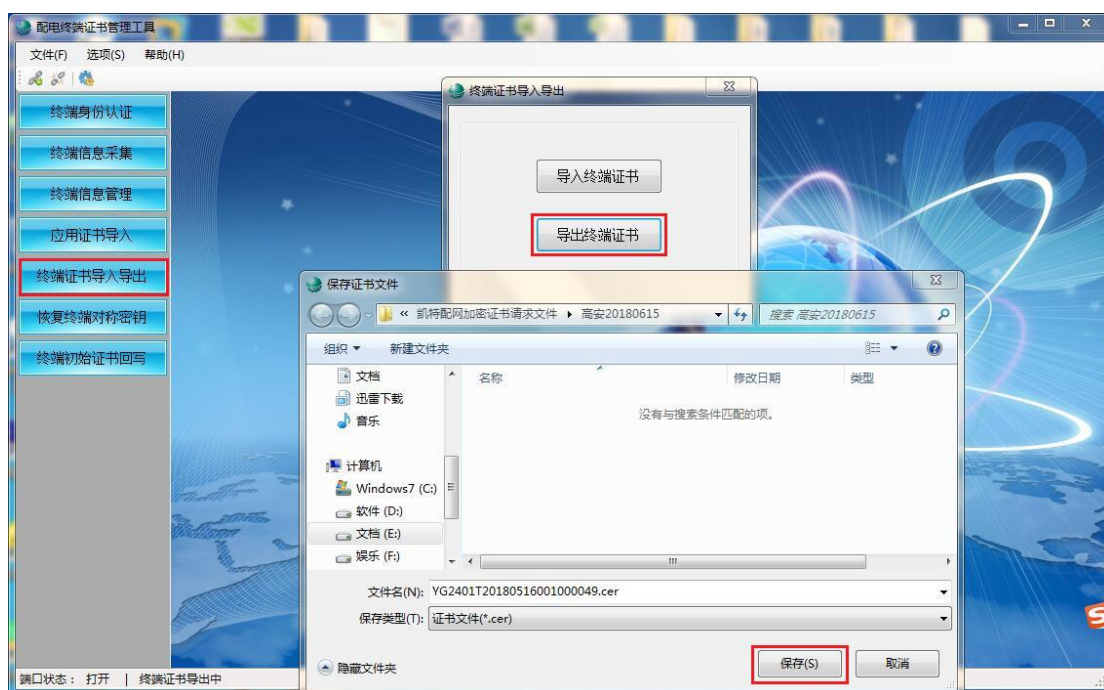
管理工具和终端进行认证，如果有通信异常等提示，则坚持连接线、设备的参数配置等，然后进行重试
认证失败的界面：



认证成功：

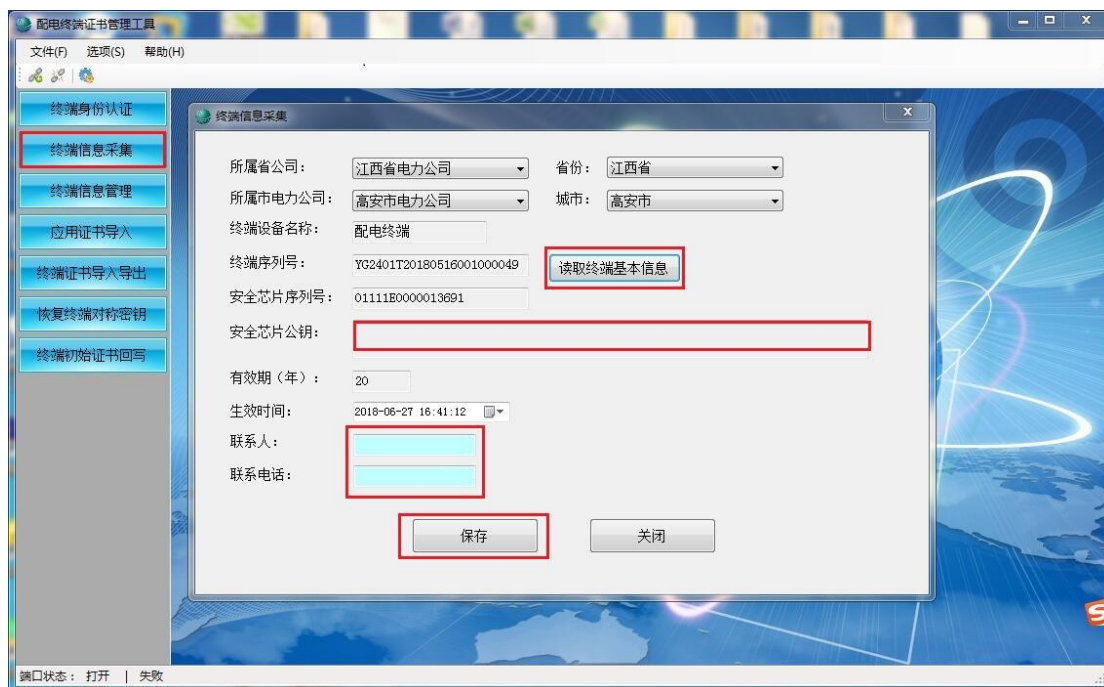


导出终端原始证书。点击终端证书导入导出，点击导出终端证书，会生成一个 cer 结尾的文件夹并保存到合适的文件夹，这个文件是要给主站的，联调的时候要用。



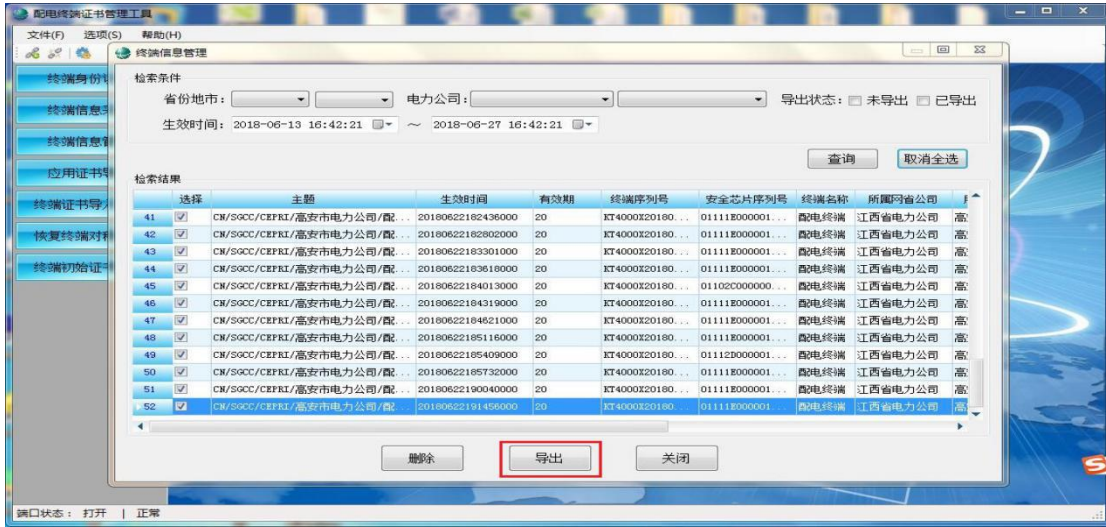
3.2 读取终端基本信息

在上一节的基础上，点击证书管理工具上的“终端信息采集”，在弹出的界面上行，点“读取终端基本信息”，填写好相应地县供电公司相应的联系人和联系电话，然后保存。



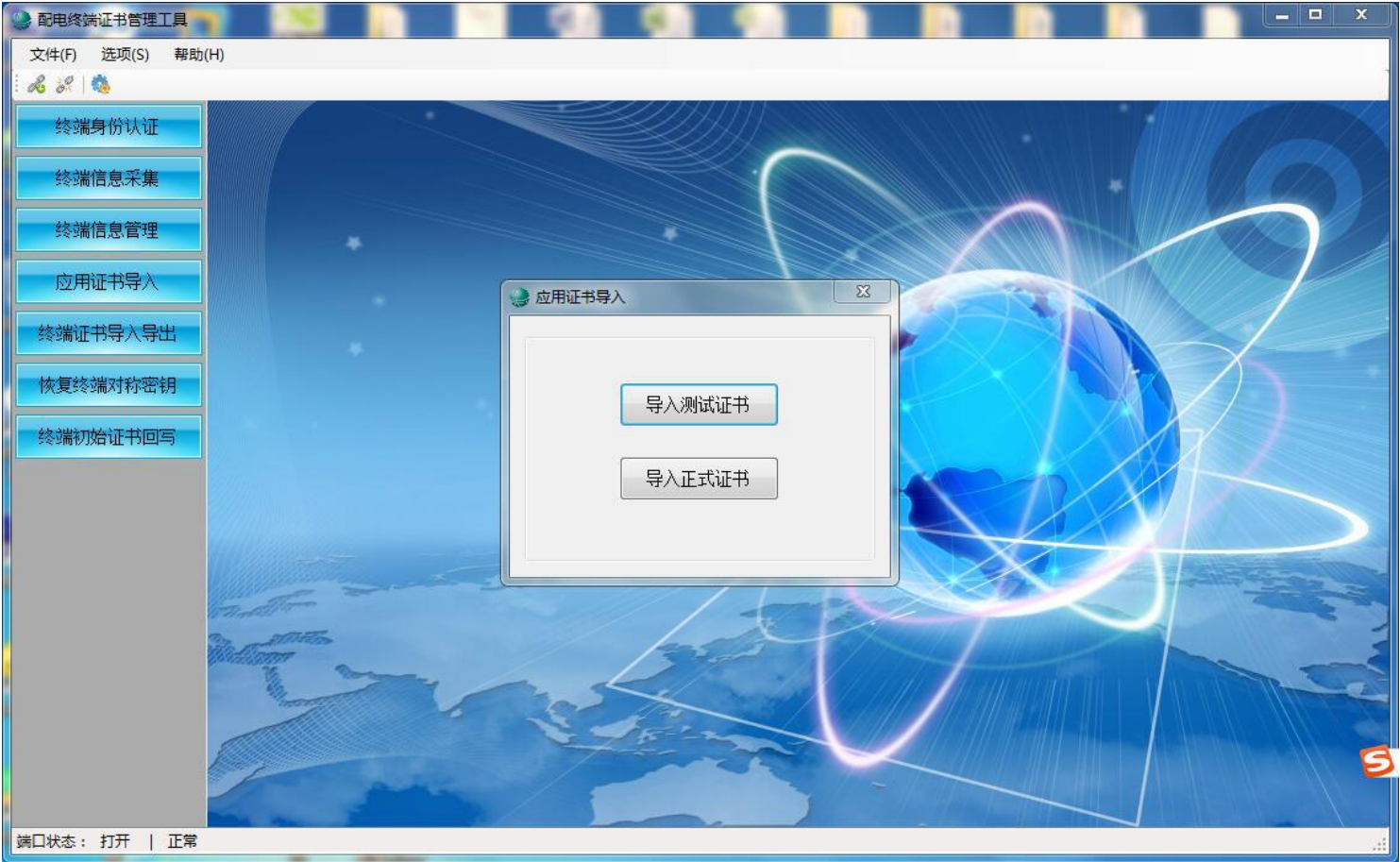
3.3 导出终端新的证书请求

在证书管理工具界面上点左侧的“终端信息管理”，弹出终端信息维护列表，在此界面上，勾选未导出的证书请求文件，保存到一个固定目录中，随后将此目录打压缩包，发送给地县公司相关联系人，此请求文件会进一步发送到电科院申请终端新的证书。



3.4 导入主站侧证书到终端

关闭证书管理工具，拔出“测试” Key，随后插入“正式” Key，在界面上直接点击“导入应用证书”，在弹出的窗口中，选择“导入正式证书”，将 Key 内保存的主站侧证书导入到加密盒中：



3.5 调试和正式应用

把前面导出的终端原始证书提供给主站，加密盒插入地县工地提供的 SIM 卡，将卡号绑定的 IP 地址提供给主站运维人员，随后就可以上电进行数据通信测试了。

在调试成功的基础上，等电科院的终端正式证书下来之后，将电科院提供的新的终端证书发送给主站运维人员，替换原来的终端原始证书，则新证书会自动导入的加密盒设备，随后便会使用新的证书进行加密通信了。