北京南瑞智芯微电子科技有限公司
BEIJING NARI SMARTCHIP MICROELECTRONICS TECHNOLOGY COMPANY LIMITED

费控电能表安全模块
远程功能函数动态库
接口说明

目　录

版 本 历 史

版本号	修改日期	修改内容
V1.0.0	2015-01-27	1. 初版
	2015-04-14	2. 更新了部分描述，增加了出参长度说明
	2015-07-23	3. 费控模式切换接口说明，去掉“仅正式密钥状态下可以做此操作”

简介

本程序适用于南方电网表端套件相关应用程序开发，可用于电能表厂家调试远程相关功能。

本程序需要使用的读卡器为 DKQ-05 读卡器，使用的 cpu 卡片为模拟主站加密卡。使用时，模拟主站加密卡插入主卡座。下面接口的使用，有一定的顺序性，常用顺序为：连接设备器 -> 其他接口。

1. 连接设备

功能描述

连接设备。

函　　数

Int OpenDevice(int ReaderType)

参数说明

ReaderType	读卡器类型，整型，0：DKQ-05 读卡器（目前只支持该类型读卡器）

参数范例:

无

函数返回:

0	成功
其他	失败，见错误代码表

2. 关闭连接设备

功能描述

关闭设备。

函　　数

Int CloseDevice()

参数说明

无。

参数范例:

无

函数返回:

0	成功
其他	失败，见错误代码表

3. 身份认证

- **功能描述：**

获取随机数以及密文,用于远程身份认证。

- **函　　数：**

int IdentityAuthentication(int Flag,char *PutDiv,char *OutRand,char *OutEndata)

- **参数说明：**

Flag	表示电表密钥状态，整型，0：测试密钥状态；1：正式密钥状态；
PutDiv	表示输入的分散因子,字符型,8 字节，“0000”+表号；
OutRand	输出的随机数,字符型,8 字节（因追加了’\0’,上位机软件调用时，出参长度至少应为 17 个字符）；
OutEndata	输出的密文,字符型,8 字节（因追加了’\0’,上位机软件调用时，出参长度至少应为 17 个字符）；

- **参数范例：**

Flag	0
PutDiv	"0000555555555555"

- **函数返回：**

0	成功
其他	失败，见错误代码表

4. 远程控制

- **功能描述：**

远程拉闸、合闸、报警等控制数据计算。

- **函　　数：**

int UserControl(int Flag,char *PutRand,char *PutDiv,char *PutEsamNo, char *PutData, char *OutEndata)

- **参数说明：**

Flag	表示电表密钥状态，整型，0：测试密钥状态；1：正式密钥状态；

PutRand	表示输入的随机数,字符型,4 字节，电表身份认证成功后返回；
PutDiv	表示输入的分散因子,字符型,8 字节，“0000”+表号；
PutEsamNo	表示输入的电表安全模块序列号，字符型，8 字节；
PutData	表示拉闸、合闸、报警等控制命令明文,字符型,8 字节；
OutEndata	输出的数据长度，字符型，20 字节（因追加了’\0’,上位机软件调用时，出参长度至少应为 41 个字符）。

- **参数范例：**

Flag	0
PutRand	"271789B1"
PutDiv	"0000000000000001"
PutEsamNo	"0001111100000032"
PutData	"1A00140730104001"

- **函数返回：**

0	成功
其他	失败，见错误代码表

5. 参数信息更新

- **功能描述：**

用于参数信息计算。

- **函　　数：**

int ParameterUpdate (int Flag,char *PutRand,char *PutDiv,char *PutApdu,char *PutData, char *OutData)

- **参数说明：**

Flag	表示电表密钥状态，整型，0：测试密钥状态；1：正式密钥状态；
PutRand	表示输入的随机数,字符型,4 字节，电表身份认证成功后返回；
PutDiv	表示输入的分散因子,字符型,8 字节，“0000”+表号；
PutApdu	写电表安全模块命令头，字符型，5 字节；
PutData	表示输入的参数信息明文,字符型；

OutData	输出的数据和 MAC（出参长度至少应为 512 字符）。

- **参数范例：**

Flag	0
PutRand	"B4C8C420"
PutDiv	"0000555555555555"
PutApdu	"04D6811008"
PutData	"00002209"

- **函数返回：**

0	成功
其他	失败，见错误代码表

6. 当前套电价参数更新

- **功能描述：**

用于当前套电价参数计算。

- **函　　数：**

int PricelUpdate(int Flag,char *PutRand,char *PutDiv,char *PutApdu,char *PutData, char *OutData)

- **参数说明：**

Flag	表示电表密钥状态，整型，0：测试密钥状态；1：正式密钥状态；
PutRand	表示输入的随机数,字符型,4 字节，电表身份认证成功后返回；
PutDiv	表示输入的分散因子,字符型,8 字节，“0000”+表号；
PutApdu	写电表安全模块命令头，字符型，5 字节；
PutData	表示输入的当前套电价参数明文,字符型；
OutData	输出的数据和 MAC（出参长度至少应为 512 字符）。

- **参数范例：**

Flag	0
PutRand	"B4C8C420"
PutDiv	"0000555555555555"
PutApdu	"04D6830484"

PutData

″0001000300110000002100000031000000020000000207000002000000020700000200000002000000020777000255000002000000020000000200000002000000020000000200000002000000020000000200000002000000020000000200000002000000020000000200000000200000002000000020000000200000000000000000000″

- **函数返回:**

0　　　　　成功

其他　　　　失败，见错误代码表

7. 备用套电价参数更新

- **功能描述：**

用于备用套电价参数计算。

- **函　　数:**

int Price2Update (int Flag, char *PutRand, char *PutDiv, char *PutApdu, char *PutData, char *OutData)

- **参数说明：**

Flag　　　　表示电表密钥状态，整型，0：测试密钥状态；1：正式密钥状态；

PutRand　　表示输入的随机数，字符型，4 字节，电表身份认证成功后返回；

PutDiv　　　表示输入的分散因子，字符型，8 字节，“0000”+表号；

PutApdu　　写电表安全模块命令头，字符型，5 字节；

PutData　　表示输入的备用套电价参数明文，字符型；

OutData　　输出的数据和 MAC（出参长度至少应为 512 字符）。

- **参数范例:**

Flag　　　　0

PutRand　　″B4C8C420″

PutDiv　　　″0000555555555555″

PutApdu　　″04D6840484″

PutData

″00010003001100000021000000310000000200000002070000020000000207000002

0000000200000002077700025500000020000000200000002000000020000000200000
002000000020000000200000002000000020000000200000002000000020000000200
000002000000020000000200000002000000000000000000000000″

函数返回:

0　　成功

其他　　失败，见错误代码表

8. 二类参数更新

功能描述:

用于远程二类参数设置计算。

函　　数:

```
int ParameterElseUpdate (int Flag,char *PutRand,char *PutDiv,char *PutApdu,char *PutData, char *OutEndata)
```

参数说明:

Flag	表示电表密钥状态，整型，0: 测试密钥状态；1: 正式密钥状态；
PutRand	表示输入的随机数，字符型，4 字节，电表身份认证成功后返回；
PutDiv	表示输入的分散因子，字符型，8 字节，“0000”+表号；
PutApdu	写电表安全模块的 APDU 指令头，字符型，5 字节；
PutData	表示输入的二类参数明文，字符型；
OutEndata	输出的密文和 MAC，字符型（出参长度至少应为 512 字符）。

参数范例:

Flag	0
PutRand	″B4C8C420″
PutDiv	″0000555555555555″
PutApdu	″04D6880014″
PutData	″0400100400230000″

函数返回:

0　　成功

其他　　失败，见错误代码表

备注：

PutApdu 参数中 LC 的计算方法：明文数据长度+3 字节后，补成模 16 的倍数，再加 4 字节，将密文写入到电表安全模块后存储格式为：L 明文数据长度 + 明文数据 DATA。

PutApdu 参数中 P1 的计算方法：利用数据标识的 DI2 模 5 的结果，判断采用哪个参数更新文件。

数据标识 DI2 模 5 = 0：采用参数更新文件 1；（P1 即 88）

数据标识 DI2 模 5 = 1：采用参数更新文件 2；（P1 即 89）

数据标识 DI2 模 5 = 2：采用参数更新文件 3；（P1 即 90）

数据标识 DI2 模 5 = 3：采用参数更新文件 4；（P1 即 91）

数据标识 DI2 模 5 = 4：采用参数更新文件 5。（P1 即 92）

9. 远程开户/充值

- **功能描述：**

用于远程钱包开户/充值，仅正式密钥状态下可以做此操作。

- **函　　数：**

int IncreasePurse(int Flag,char *PutRand，char*PutDiv，char*PutData,char *OutData)

- **参数说明：**

Flag　　表示电表密钥状态，整型，　1：正式密钥状态；

PutRand　　表示输入的随机数,字符型,4 字节，电表身份认证成功后返回；

PutDiv　　表示输入的分散因子,字符型,8 字节，“0000”+表号；

PutData　　表示输入的参数明文,包含：购电金额+购电次数+客户编号，共 14 字节，金额、次数均为 HEX 码；

OutData　　输出的数据，购电金额+购电次数+MAC1+客户编号+MAC2，共 22 字节（因追加了’\0’,上位机软件调用时,出参长度至少应为 45 个字符）。

- **参数范例：**

Flag　　1

PutRand　　″B4C8C420″

PutDiv　　"0000555555555555"

PutData　　"000000C8000000021122334455 66"

- **函数返回:**

0　　成功

其他　　失败，见错误代码表

10. 钱包初始化

- **功能描述:**

用于钱包初始化 MAC 计算，仅测试密钥状态下可以做此操作。

- **函　　数:**

int InitPurse(int Flag,char *PutRand, char*PutDiv, char*PutData,char *OutData)

- **参数说明:**

Flag　　表示电表密钥状态，整型，0: 测试密钥状态;

PutRand　　表示输入的随机数,字符型,4 字节，电表身份认证成功后返回;

PutDiv　　表示输入的分散因子,字符型,8 字节，“0000”+表号;

PutData　　表示输入的数据明文，包含预置金额，4 字节，HEX 码;

OutData　　输出的数据,预置金额+MAC1+“00000000”+MAC2, 共 16 字节(因追加了'\0',上位机软件调用时,出参长度至少应为 33 个字符)。

- **参数范例:**

Flag　　0

PutRand　　"B4C8C420"

PutDiv　　"0000555555555555"

PutData　　"000000C8"

- **函数返回:**

0　　成功

其他　　失败，见错误代码表

11. 密钥更新

- **功能描述：**

用于电能表远程密钥更新时，获取密钥信息、密钥密文及 MAC。

- **函　　数**

int KeyUpdateV2 (int PutKeySum ,char *PutKeyState,char *PutKeyId,char *PutRand ,char *PutDiv,char *PutEsamNo,char *OutData)

- **参数说明：**

PutKeySum	密钥总条数，最大值 17；
PutKeyState	目标密钥状态，要更新成正式密钥时传“01” ；要更新成测试密钥时传“00”；
PutKeyId	指密钥编号，从“00”开始，到“10”结束，编号格式为 HEX 码，每次最多输出 4 条密钥，如"00010203"指需要输出“00”、“01”、“02”、“03”四条密钥密文，调用函数时密钥编号从“00”开始，顺序输入；
PutRand	4 字节随机数，电表身份认证成功后返回；
PutDiv	8 字节分散因子，“0000”+表号；
PutEsamNo	8 字节电表安全模块序列号；
OutData	输出的数据，N*(4 字节密钥信息+32 字节密钥密文)+4 字节 MAC，N 不大于 4。（出参长度至少应为 512 字符）

- **参数范例：**

PutKeySum	17
PutKeystate	"01"
PutKeyid	"0001020A"
PutRand	"B6382720"
PutDiv	"0000555555555555"
PutEsamNo	"0001111100000032"

- **函数返回：**

0	成功
其他	失败，见错误代码表

12. 清零

- **功能描述**

用于生成电能表清零命令的密文。

- **函　　数**

int DataClear1(int Flag,char *PutRand,char *PutDiv,char *PutData,char *OutData)

- **参数说明**

Flag	表示电表密钥状态，整型，0：测试密钥状态；1：正式密钥状态；
PutRand	4 字节随机数，电表身份认证成功后返回；
PutDiv	8 字节分散因子，“0000”+表号；
PutData	清零数据明文，8 字节或 12 字节；
OutData	输出的数据，20 字节（因追加了’\0’,上位机软件调用时，出参长度至少应为 41 个字符）。

- **参数范例:**

Flag	0
PutRand	"B4C8C420"
PutDiv	"0000555555555555"
PutData	"1900140903111011"

- **函数返回:**

0	成功
其他	失败，见错误代码表

13. 红外认证查询

- **功能描述**

用于产生红外认证查询所需的随机数。

- **函　　数**

int　InfraredRand(char *OutRand1)

- **参数说明**

OutRand1	输出的 8 字节随机数（因追加了'\0',上位机软件调用时，出参长度至少应为 17 个字符）。

- **参数范例：**

无

- **函数返回：**

0	成功
其他	失败，见错误代码表

14. 红外认证

- **功能描述：**

用于获取红外认证密文和随机数。

注意：红外认证前必须先进行红外认证查询。

- **函　　数：**

int InfraredAuth(int Flag,char *PutDiv,char *PutEsamNo,char *PutRand1,char *PutRand1Endata,char *PutRand2,char *OutRand2Endata)

- **参数说明：**

Flag	电表密钥状态，整型，0：测试密钥状态；1：正式密钥状态；
PutDiv	8 字节分散因子，“0000”+表号；
PutEsamNo	8 字节电表安全模块序列号，电能表红外认证查询命令返回；
PutRand1	8 字节随机数，红外认证查询函数返回；
PutRand1Endata	8 字节随机数 1 密文，电能表红外认证查询命令返回，密文是由电表返回的字符型数据；
PutRand2	8 字节随机数 2，电能表红外认证查询命令返回；
OutRand2Endata	返回 8 字节随机数 2 密文（因追加了'\0',上位机软件调用时，出参长度至少应为 17 个字符）。

- **参数范例：**

Flag	0
PutDiv	"0000000000000001"
PutEsamNo	"0001111100000032"

PutRand1　　"271789B1271789B1"

PutRand1Endata　　"B89467F6980DA078"

PutRand2　　"98C1FFAFFA314BEC"

- **函数返回:**

0　　成功

其他　　失败，见错误代码表

备注：

红外认证的流程如下：

主站
调用：红外认证查询函数
返回：随机数Rand1

↓

电能表
发送：红外认证查询命令
返回：表号
　　ESAM序列号
　　随机数1密文K1
　　随机数Rand2

↓

主站
调用：红外认证函数
输入：表号
　　ESAM序列号
　　随机数Rand1
　　随机数1密文K1
　　随机数Rand2
返回：随机数Rand2的密文K2

注：函数加密随机数1，加密结果与K1进行比较，不相同则返回错误代码，相同则继续，加密Rand2得到密文K2

↓

电能表
发送：红外认证命令
返回：认证结果

15. 数据回抄

- **功能描述**

用于验证回抄数据(包含状态查询数据)MAC 的正确性。

- **函　　数**

int MacCheck(int Flag, char *PutRand, char *PutDiv, char *PutApdu,char *PutData, char *PutMac)

- **参数说明**

Flag	表示电表密钥状态，整型，0：测试密钥状态；1：正式密钥状态；
PutRand	4 字节随机数，身份认证函数返回随机数的前 4 字节；
PutDiv	8 字节分散因子，“0000”+表号；
PutApdu	5 字节 APDU 指令头，固定格式为 04D686P2LC，其中 P2 为起始地址，LC = DATA 长度+MAC 长度+分散因子长度；
PutData	回抄的数据；
PutMac	回抄的 MAC。

- **参数范例：**

Flag	0
PutRand	"447034E1"
PutDiv	"0000555555555555"
PutApdu	"04D6860016"
PutData	"04000106000000000000"

- **函数返回：**

0	成功
其他	失败，见错误代码表

注：所有文件都支持回抄。

16. 记录信息文件 1 更新

- **功能描述**

用于对需要发送给电表安全模块的明文数据，进行 MAC 的计算。

- **函　　数**

int MacWrite(int Flag ,char *PutRand,char *PutDiv,char *PutEsamNo,char *PutFileID,char *PutDataBegin,char *PutData,char *OutData)

- **参数说明**

Flag	表示电表密钥状态，整型，0：测试密钥状态；1：正式密钥状态；
PutRand	4 字节随机数，电表身份认证成功后返回；
PutDiv	8 字节分散因子，“0000”+表号；
PutEsamNo	8 字节电表安全模块序列号；
PutFileID	1 字节文件标识；
PutDataBegin	2 字节起始字节；
PutData	明文数据,文件最大 0x95 字节；
OutData	输出的明文数据+4 字节 MAC 数据(出参长度至少应为 512 字符)。

- **参数范例：**

Flag	0
PutRand	"690AF9B6"
PutDiv	"0000000000000001"
PutEsamNo	"00021199000000B1"
PutFileID	"17"
PutDataBegin	"0000"
PutData	"11223344"

- **函数返回：**

0	成功
其他	失败，见错误代码表

17.　记录信息文件 2 更新

- **功能描述**

用于对需要发送给电表安全模块的明文数据，进行密文+MAC 的计算。

- **函　　数**

int EncMacWrite(int Flag ,char *PutRand,char *PutDiv,char

*PutEsamNo,char *PutFileID,char *PutDataBegin,char *PutData,char *OutData)

- **参数说明**

Flag	表示电表密钥状态，整型，0：测试密钥状态；1：正式密钥状态；
PutRand	4 字节随机数，电表身份认证成功后返回；
PutDiv	8 字节分散因子，“0000”+表号；
PutEsamNo	8 字节电表安全模块序列号；
PutFileID	1 字节文件标识；
PutDataBegin	2 字节起始字节；
PutData	明文数据，文件最大 0x95 字节；
OutData	输出的密文和 MAC 数据（出参长度至少应为 512 字符）。

- **参数范例:**

Flag	0
PutRand	"F5A307BE"
PutDiv	"0000000000000001"
PutEsamNo	"00021199000000B1"
PutFileID	"18"
PutDataBegin	"0000"
PutData	"1122334455"

- **函数返回:**

0	成功
其他	失败，见错误代码表。

18. 程序比对数据计算

- **功能描述**

用于生成程序比对数据的密文。

- **函　　数**

int EncForCompare(char *PutKeyid, char *PutDiv, char *PutData,char *OutData)

参数说明

PutKeyid　1 字节密钥索引，本套件中支持的密钥索引为 05-0a，通信规约中与函数中输入索引需统一；

PutDiv　8 字节分散因子；

PutData　比对数据块，64 字节；

OutData　输出的密文，64 字节（因追加了'\0',上位机软件调用时，出参长度至少应为 129 个字符）。

参数范例:

PutKeyid　"06"

PutDiv　"0000000000000001"

PutData

"0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000"

函数返回:

0　成功 ；

其他　失败，见错误代码表。

备注：

1）数据解释：

- 比对密钥索引：05-0a；
- 分散因子：8 字节，从比对因子起始地址开始，在程序存储器中顺序取 16 个字节，前 8 字节与后 8 字节异或，结果作为分散因子；
- 比对数据：从比对数据起始地址开始取 256 个字节，以 64 字节为单位分成四个数据块(Data1、Data2、Data3、Data4),然后对数据块进行处理(Data1^Data2^Data3^Data4=Data,其中^代表异或运算符)，得到 64 个字节的加密单元数据 Data；如待加密数据字节数不足指定长度时（待加密数据 256 字节，比对因子为 16 字节），先补结束符 0x80，剩余字节补 0x00。比对因子和待加密数据均遵循此规则；
- 比对数据密文：64 字节，电表代码指定区间代码加密结果由多个 EncData 组成，以 64 字节为数据项上送。

19. 钱包退费计算

- **功能描述：**

用于对退费数据进行计算，只是正式状态下可以做此操作。

- **函　　数：**

int DecreasePurse(int Flag,char *PutRand,char *PutDiv, char *PutData, char *OutEndata)

- **参数说明：**

Flag	电表密钥状态，整型， 1：正式密钥状态；
PutRand	输入的随机数,字符型,4 字节，电表身份认证成功后返回；
PutDiv	输入的分散因子,字符型,8 字节，“0000”+表号；
PutData	输入的 4 字节退费金额,字符型，HEX 码；
OutEndata	输出的密文和 MAC,字符型，20 字节（因追加了’\0’,上位机软件调用时，出参长度至少应为 41 个字符）。

- **参数范例：**

Flag	1
PutRand	"B4C8C420"
PutDiv	"0000555555555555"
PutData	"000000C8"

- **函数返回：**

0	成功
其他	失败，见错误代码表

注：购电次数每变化一次，仅允许退费一次；退费功能不修改购电次数。

20. 费控模式切换

- **功能描述：**

用于费控模式切换。

- **函　　数：**

int SwitchChargeMode(int Flag,char *PutRand,char*PutDiv,char*PutData,

char *OutData)

- **参数说明：**

Flag　　电表密钥状态，整型，0：测试密钥状态；1：正式密钥状态；

PutRand　　输入的随机数,字符型,4 字节，电表身份认证成功后返回；

PutDiv　　输入的分散因子,字符型,8 字节，“0000”+表号；

PutData　　输入的参数明文,字符型,包含费控模式状态字+购电金额+购电次数,金额、次数均为 HEX 码；

OutData　　输出的数据，费控模式状态字+MAC1+购电金额+购电次数+MAC2，共 17 字节（因追加了'\0',上位机软件调用时，出参长度至少应为 35 个字符）。

- **参数范例：**

本地切远程范例：

Flag　　1

PutRand　　"B4C8C420"

PutDiv　　"0000555555555555"

PutData　　"010000000000000000"

远程切本地范例：

Flag　　1

PutRand　　"B4C8C420"

PutDiv　　"0000555555555555"

PutData　　"020000000500000001"

- **函数返回：**

0　　成功

其他　　失败，见错误代码表

21. 错误代码表

代码	意义		代码	意义
202	打开读卡器错误		1501	参数 1 错误
203	关闭读卡器错误		1502	参数 2 错误

301	芯片复位错误		1503	参数 3 错误
302	芯片选择错误(非主站加密卡)		1504	参数 4 错误
			1505	参数 5 错误
			1506	参数 6 错误
			1507	参数 7 错误
			1508	参数 8 错误

声明：

本文件已经过反复核对，内容与所述软件相符。虽然我们已尽力将文档描述准确，但我们还是不能保证不出现错误或纰漏，敬请各位读者不吝赐教。我们将对内容定期审查，在下一版中进行修正并发布。