

北京智芯微电子科技有限公司

芯片传感事业部

项目名称	
项目编号	
文件编号	
文件名称	接口设计

拟制人：

审核人：

批准人：

日期：

1	引言	4
1.1	编写目的.....	4
2	表端套件远程动态库接口说明	4
2.1	会话密钥协商.....	4
2.2	会话密钥协商验证.....	5
2.3	数据抄读.....	5
2.4	电表主动上报.....	6
2.5	钱包操作.....	7
2.6	获取读 ESAM 指令	8
2.7	验证读 ESAM 数据	8
2.8	设置 ESAM 参数	9
2.9	获取下发参数数据.....	10
2.10	密钥更新.....	11
2.11	获取电能表任务数据.....	13
2.12	验证会话数据.....	14
2.13	获取随机数.....	15
2.14	获取广播数据.....	15
2.15	上报数据返回加密.....	16
2.16	软件比对.....	17
2.17	红外查询.....	18
2.18	红外认证.....	18
3	常用操作流程举例说明	19
3.1	密钥更新.....	19
4	附录	19
4.1	操作模式.....	19
4.2	常见错误码.....	19

版 本 历 史

版本号	作者	项目角色	修改日期	修改内容及原因
V1.0	范云龙		20160702	初始版本
V1.1	范云龙		20161207	根据最新文件结构修改 ESAM 文件的读写函数、抄读 上报函数以及密钥更新函数
V1.2	范云龙		20170608	增加红外查询、红外认证流程

北京智芯微电子科技有限公司

1 引言

1.1 编写目的

【阐明编写测试计划的目的，指明读者对象。】

2 表端套件远程动态库接口说明

2.1 会话密钥协商

2.1.1 函数说明

函数名称	int WINAPI Obj_Meter_Test_InitSession(int InKeyState, const char* InEsamId, const char* InAMCTR, const char*ucFLG, char* OutRand1,char* OutSessionData,char* OutMAC)	
参数说明	入参	InKeyState: 电表密钥状态, 0: 测试密钥状态; 1: 正式密钥状态; InEsamId: 当 InKeyState =0 时, Esam 序列号, 当 InKeyState =1 时, 表号 8 字节 InAMCTR: 应用会话协商计数器, 4 字节 ucFLG: 保留
	出参	OutRand1: 会话协商随机数 1 OutSessionData: 会话协商数据, 32 字节 OutMAC:会话协商 MAC, 4 字节
返回值	0: 成功 其他: 错误	

2.1.2 应用举例

InKeyState: 0
InEsamId: "0002D21000000367"
InAMCTR: "000006"
ucFLG: ""
OutRand1: "7284525A3B20582333A21B9CAB8C4B82"
OutSessionData:"8F39FDA670F681A31C5CB932795AB34ED699DB7EBE5B0E48E5EDB2C9448AEA4C"
OutMAC: "C796C2C8"

2.2 会话密钥协商验证

2.2.1 函数说明

函数名称	int WINAPI Obj_Meter_Test_VerifySession(int InKeyState, const char* InEsamId, const char* InRand1, const char* InSessionData, const char* InMAC, char* OutSessionToken)	
参数说明	入参	InKeyState: 电表密钥状态, 0: 测试密钥状态; 1: 正式密钥状态; InEsamId: 当 InKeyState =0 时, Esam 序列号, 当 InKeyState =1 时, 表号, 8 字节 InRand1: 会话协商随机数 1, 来自“会话密钥协商”, 16 字节 InSessionData: 应用会话协商数据, 由电表返回, 48 字节 InMAC: 会话协商 MAC, 由电表返回, 4 字节
	出参	OutSessionIV: 会话密钥初始向量, 177 字节
返回值	0: 成功 其他: 错误	

2.2.2 应用举例

InKeyState: 0

InEsamId: "0002D21000000367"

InRand1: "013F5D368F68A9263751F94C369678E3"

InSessionData: "6339001F27ADE3D06D6227A910B69C4DCDF0E70C4C6AA34EED8B82E788689CB
D486B35777B32E26400567FF99186066F"

InMAC: "C6C43967"

OutSessionIV: "0093506D172ACD4D5D2730731619BC175B61C9BF3230761BF2AAE513E723D2F20
C38CC14C726ACF3B350EFA4E6844EBFA523FE417B8B450D54119CD628E7CB388B3AA42FF1A679
68CDDE63272B8AF792257A669B0E4A0E07DBD571FA0FC95825C1E2DA87689702884CD9C21A6B
9EB1710424FE5808F41D0D9739C1506659868A28EC87EADBFDD2930B7BCFFCE1ADBB5633B62F4
43A53859DCBD53CE7A97243A8FA630D7C6F301812A0BE11FB4CA2BB3FDDA"

2.3 数据抄读

2.3.1 函数说明

函数名称	int WINAPI Obj_Meter_Test_VerifyReadData(int InKeyState, int InOperateMode, const char* InEsamId, const char* InRandHost, const char* InMeterInfo, const char* InMAC, char* OutData)
------	--

参数说明	入参	InKeyState: 电表密钥状态, 0: 测试密钥状态; 1: 正式密钥状态; InOperateMode: 输入数据格式, 具体格式参见附录, 1 字节 InEsamId: 表号, 8 字节 InRandHost:主站随机数, 16 字节 InMeterInfo: 电表文件内容, 长度不固定 InMAC: 4 字节
	出参	OutData:数据明文, 若 InOperateMode =0 则无。
返回值	0: 成功 其他: 错误	

2.3.2 应用举例

InKeyState: 0

InOperateMode:1

InEsamId: "0002D21000000367"

InRandHost: "287A1890F73FA538CC676193AB8AF0D0"

InMeterInfo:"1122334455667788"

InMAC: " "E1D4E722"

OutData:""

2.4 电表主动上报

2.4.1 函数说明

函数名称	int WINAPI Obj_Meter_Test_VerifyReportData(int InKeyState, int InOperateMode, const char* InEsamId, const char * RandAndCTR,const char* InMeterInfo,const char* InMAC ,char * OutData,char * OutRSPCTR)	
参数说明	入参	InKeyState: 电表密钥状态, 0: 测试密钥状态; 1: 正式密钥状态; InOperateMode: 输入数据格式, 具体格式参见附录, 1 字节 InEsamId: 表号, 8 字节 RandAndCTR: 随机数和计数器, 12 字节 InMeterInfo: 电表文件内容, 长度不固定 InMAC:4 字节
	出参	OutData:数据明文, 若 InOperateMode=0, 则无 OutRSPCTR:计数器
返回值	0: 成功 其他: 错误	

2.4.2 应用举例

InKeyState: 0
InOperateMode:2
InEsamId: "0002D21000000367"
RandAndCTR: " 158066F7F296549800000001"
InMeterInfo:99D636ACA9A8386E48935657F1720EB9"
InMAC: "16DBAE94"
OutData: "1122334455667788"
OutRSPCTR: "00000001"

2.5 钱包操作

2.5.1 函数说明

函数名称	int WINAPI Obj_Meter_Test_GetPurseData(int InOperateMode, const char* InEsamId,const char* InSessionIV, int TaskType, const char*InData, char * OutSID,char* OutAttachData, char* OutData,char*OutMAC)	
参数说明	入参	InOperateMode: 操作模式, 具体格式参见附录 InEsamId: Esam 序列号, 8 字节 InSessionIV: 会话密钥初始向量, 177 字节 TaskType: 操作类型: 9 钱包初始化, 10 钱包充值, 11 钱包退费 InData: 数据明文, TaskType=9 时为预置金额, 4 字节, TaskType=10/11 时为购电金额+购电次数+用户编号(6 字节), 14 字节
	出参	OutSID: 安全对象标识, 4 字节 OutAttachData: 安全标识附加数据 OutData: 输出数据 OutMAC: MAC,4 字节
返回值	0: 成功 其他: 错误	

2.5.2 应用举例

InOperateMode: 1
InEsamId: "0002D21000000367"
OutSessionIV:"0093506D172ACD4D5D2730731619BC175B61C9BF3230761BF2AAE513E723D2F20
C38CC14C726ACF3B350EFA4E6844EBFA523FE417B8B450D54119CD628E7CB388B3AA42FF1A679
68CDDE63272B8AF792257A669B0E4A0E07DBD571FA0FC95825C1E2DA87689702884CD9C21A6B
9EB1710424FE5808F41D0D9739C1506659868A28EC87EADBFDD2930B7BCFFCE1ADBB5633B62F4
43A53859DCBD53CE7A97243A8FA630D7C6F301812A0BE11FB4CA2BB3FDDA"
TaskType: 9
InData:" 00000010 "

OutSID: "813E0000"
OutAttachData: "000910"
OutData: "00000010"
OutMAC: "EE85DC16"

2.6 获取读 ESAM 指令

2.6.1 函数说明

函数名称	int WINAPI Obj_Meter_Test_GetESAMData(int InOperateMode,char* OAD, char* OutRandHost,const char * OutSID,char*OutAttachData)	
参数说明	入参	InOperateMode: 操作模式, 具体格式参见附录。 InOAD: 对象属性描述符, 4 字节
	出参	OutRandHost:主站随机数, 4 字节。 OutSID: 安全对象标识, 4 字节 OutAttachData: 安全标识附加数据
返回值	0: 成功 其他: 错误	

2.6.2 应用举例

InOperateMode: 1
InOAD: "40020200"
OutRandHost: "8E540FB9"
OutSID: "802C0001"
OutAttachData: "0009408E540FB90000000D"

2.7 验证读 ESAM 数据

2.7.1 函数说明

函数名称	int WINAPI Obj_Meter_Test_VerifyESAMData(int InKeyState,int InOperateMode, const char* InEsamId,const char* OAD, const char* szInMeterNum, const char* InHostRand,const char* InData,const char * InMAC,char *OutData)	
参数说明	入参	InKeyState: 电表密钥状态, 0: 测试密钥状态; 1: 正式密钥状态; InOperateMode: 操作模式, 具体格式参见附录。 InEsamId: Esam 序列号, 8 字节

		InOAD: 对象属性描述符, 4 字节 szInMeterNum: 表号, 8 字节, 不够 8 字节前面填充 0 InHostRand: 主站随机数 InData:明文或密文, 视 InOperateMode 而定 InMAC:MAC,4 字节
	出参	OutData:明文
返回值	0: 成功 其他: 错误	

2.7.2 应用举例

InKeyState :0
InOperateMode: 1
InEsamId: "0002D21000000367"
InOAD:"40020200"
szInMeterNum: "0000000000000001"
OutRand1:"8E540FB9"
InData:"000000000000000000000000"
InMAC: "16DBAE94"
OutData: "000000000000000000000000"

2.8 设置 ESAM 参数

2.8.1 函数说明

函数名称	int WINAPI Obj_Meter_Test_SetESAMData (int InKeyState, int InOperateMode, const char* InEsamId, const char* InSessionIV,const char* InMeterNum, const char* InESAMRand, const char* InData, char* OutSID,char* OutAttachData, char* OutData, char*OutMAC)	
参数说明	入参	InKeyState: 电表密钥状态, 0: 测试密钥状态; 1: 正式密钥状态 InOperateMode: 操作模式, 具体格式参见附录 (只支持 0 和 2) InEsamId: Esam 序列号, 8 字节 InSessionIV: 会话密钥初始向量, 177 字节 InMeterNum: 表号, 8 字节, 不够 8 字节前面填充 0 InESAMRand:ESAM 随机数 InData: 4 字节 OAD + 1 字节内容 LEN + 内容
	出参	OutSID: 安全标识类型 OutAttachData: 安全标识附加数据 OutData: 输出的数据

	OutMAC: MAC
返回值	0: 成功 其他: 错误

2.8.2 应用举例

```

InKeyState :0
InOperateMode: 3
InEsamId: "0002D21000000367"
InSessionIV: "0093506D172ACD4D5D2730731619BC175B61C9BF3230761BF2AAE513E723D2F20C38CC14C726ACF3B350EFA4E6844EBFA523FE417B8B450D54119CD628E7CB388B3AA42FF1A67968CDDE63272B8AF792257A669B0E4A0E07DBD571FA0FC95825C1E2DA87689702884CD9C21A6B9EB1710424FE5808F41D0D9739C1506659868A28EC87EADBFD2930B7BCFFCE1ADBB5633B62F443A53859DCBD53CE7A97243A8FA630D7C6F301812A0BE11FB4CA2BB3FDDA"
InMeterNum: "0000000000000001"
InESAMRand: "075C51122038FCAA15BC2307F6750FB0"
InData: "000000000101"
OutSID: "811C3110"
OutAttachData: "0017C00000"
OutData: "1F62B4291FE53D73017CBC3CDF819E0F"
OutMAC: "8849D19C"

```

2.9 获取下发参数数据

2.9.1 函数说明

函数名称	int WINAPI Obj_Meter_Test_GetSessionData (int InOperateMode, const char* InEsamId, const char* InSessionIV, int TaskType, const char* InData, char* OutSID, char* OutAttachData, char* OutData, char* OutMAC)	
参数说明	入参	InOperateMode: 操作模式，具体格式参见附录。 InEsamId: Esam 序列号，8 字节 InSessionIV: 会话密钥初始向量,177 字节 TaskType: 4, 安全模式设置、设置会话时效门限; 5, 电价设、电价切换时间、费率时段、定时任务设置; 6, 除拉闸外的控制任务设置; 8, 拉闸任务设置; 3, 除上述操作外的操作。 InData: 参数明文
	出	OutSID: 安全标识类型，4 字节

	参	OutAttachData: 安全标识附加数据 OutData: 输出的数据 OutMAC: MAC, 4 字节
返回值	0: 成功 其他: 错误	

2.9.2 应用举例

InOperateMode: 1

InEsamId: "0002D21000000367"

InSessionIV: "0093506D172ACD4D5D2730731619BC175B61C9BF3230761BF2AAE513E723D2F20C38CC14C726

ACF3B350EFA4E6844EBFA523FE417B8B450D54119CD628E7CB388B3AA42FF1A67968CDDE6327

2B8AF792257A669B0E4A0E07DBD571FA0FC95825C1E2DA87689702884CD9C21A6B9EB1710424

FE5808F41D0D9739C1506659868A28EC87EADBFD2930B7BCFFCE1ADBB5633B62F443A53859DC

BD53CE7A97243A8FA630D7C6F301812A0BE11FB4CA2BB3FDDA"

TaskType: 3

InData: "1122334455667788"

OutSID: "811C3110"

OutAttachData: "000C"

OutData: "1122334455667788"

OutMAC: "1AEB1AD3"

2.10 密钥更新

2.10.1 函数说明

函数名称	int WINAPI Obj_Meter_Test_GetTrmKeyData (int InKeyState, const char* InEsamId, const char* InSessionIV, const char* InMeterNum, const char* KyeType, char* OutSID, char* OutAttachData, char* OutData, char* OutMAC)	
参数说明	入参	InKeyState: 当前密钥状态, 0: 测试密钥状态; 1: 正式密钥状态; InEsamId: Esam 序列号, 8 字节 InSessionIV: 会话密钥初始向量, 177 字节 InMeterNum: 表号, 8 字节 KyeType: 00: 应用密钥, 01: 链路密钥, 电表使用 00, 1 字节
	出参	OutSID: 安全标识类型, 4 字节 OutAttachData: 安全标识附加数据 OutData: 输出的数据 OutMAC: MAC, 4 字节

返回值	0: 成功 其他: 错误
-----	-----------------

2.10.2应用举例

InKeyState: 0

InEsamId: "0002D21000000367"

InSessionIV : "

0093506D172ACD4D5D2730731619BC175B61C9BF3230761BF2AAE513E723D2F20C38CC14C726
ACF3B350EFA4E6844EBFA523FE417B8B450D54119CD628E7CB388B3AA42FF1A67968CDDE6327
2B8AF792257A669B0E4A0E07DBD571FA0FC95825C1E2DA87689702884CD9C21A6B9EB1710424
FE5808F41D0D9739C1506659868A28EC87EADBFD2930B7BCFFCE1ADBB5633B62F443A53859DC
BD53CE7A97243A8FA630D7C6F301812A0BE11FB4CA2BB3FDDA"

InMeterNum: "0000000000000001"

KyeType: "00"

OutSID: "812E0000"

OutAttachData: " 06ED0000000000000000137"

OutData : "

3475640A708A5EDCDE55FCB2A0BE74587064D078F0659C1A30A33D5300B8D81BA1C4FFC73ECE
992B802A530A34BD2F1A8C9E2AB6D3F93FFC24BA7EA8D4C81F39172EBD43C42F885CDDF001A8
46D9CC29080E2D9AD5978C2981EBF8A77BC1E41E5BC92DE0F3827775708BC1CC71955D3B92FC
2332434D7635BEB5E8669899B334E21AFE4EF3FE77B7D8A920BB95E17ABAB75A72AC9C95E67F
10EB57D8B8D32260E807F2726A91FEC87E0988B5F3981A093765423CE976CF126F9109403909A
C200CF93489D81579FC22C4F059D320A5E1CD36B78DA21DA240D7C41E3724AB4A4DA433A73B
C60CEE344F47053BC07E6D47C6A8F126BEB5533E7CDDC40F33016E943D540E8BFE13BE242CC4
F99DECD9EB91B39F0E6B0B2CBE33C9C87952755A70D7DCD45B64E937392DB6F99AF321ED4505
561DF0D220AA78F0A34F196F2D4CDA4EAA1DBF61204F343B972D408058B4A2A423F9ED9FDA8
A48EC59A0A9C7D53621456AD3E5E1D844B2822729AF58C3FE453197121B1DBF4B98F9313B73C
0FE73B191E1DFF8996930EEBBEC5154C95AE3E5A1A8DD6729DBD4A06C92CAB2F47CFC523EB38
02D5B7BF4909017C4AB5BEA2247A59D73F08A3B2B8A60A9BBCDF4AFE43AFDABFC410F15FA6C
A71817B490ECEB99ADF781EF35EFA35B079C03AF07F3C5447CB0F9F019A888363C3085F1AD05B
B0085D4E10EAA8C25188C3675AE502D64D6516F5EF96D14BF3A4ACEC897BBA6A21D1E6FD4CEF
076CD29AAC8C43D8CBE6FCC3E13880E2045ACD68AF121CF170A903DC77026C75344693239070
BFBAEB36975E5F9BFAF2EB0D6135A9A6DD7B1032701EE99BA2B793994D803454DDC499DC95A
FC3FA4D4DCE8FF1F8F4FEDD4D9CFA64D19C87169CE4AEFB8B560984DD343ACE706D2C1B3E91
D5F701A5D58D48946DFF7D312CBB1348C5B56A57E90BA92A118D27143C4261E648C59F7F67FD
871A921235B6E63EE90AC45BF559306E8D0FD02432D49F09E6FF1231D1C155477F78D319718A7
EE933938652C999C1FC0B45012AE555CBBFDFEDC137A35ED33BA9752F6C2EE2893A97D6A7B54
6467F2FA428F437EA1BA5627DDAB165D12F71A16D412C7147E8B3FBAF114DAA20091A6C7FEE6
616C06210DBA4B0B8F2C29997BCA069EC58D1DACD6F835231280BD9C89A2C349475CF9E6F175
54AEC695E885D4896CEBC2D288C6764852D614DDF7CA58B222F721B2B5F5D5C3D0E495356768
F9BA909AF25B7A70AE60252F7211B0FD2317EAC535686AC9EE38E22DC023C18B39CF57FE516E1
F87C7EC82E42F67F2C2200A45E333F451D4D0B50B52F8DBF9BF7B54E97A6EB6688DC954F0F155

B90314ED6503F4C7A376D2359A8CAA755BF11970E8066D00D57E0A1564383B1BE9FC0447444A
38D28C52956823D5B1C2DBEFCE60BD682FA0564F6B1AB5703ACE7C2EEB6DB3A3FF60EAD138D3
1BA7A6171CA9D0197D2CDCEF9FCD3885466E3ABE9055776DB40A1E0938C1AA3D10961F64027
6367419EBC823591D58CE87D46BEA61F81480DD6C1BE90A242516B60591AB7F3FD4C7B788506
8C03B59121FEF03F1DA58727937EA22D530FE9B1404F71F521DC06DF9D50AEF02BECBAE71C6CC
8C9B976C704B2DA815893C2FE8049CEA1C9527445E708DB303AA401C7BE1EBDAE37D10575BDD
9B860772802B34D3DAD371A1C9BBC6B27332BA3F96CA11E1F695F6FE3F2F08F844F12CD93B37
8D2BDEA44C90442F77981696777C15082FF966497756210F06B3DC029369766FD2D1639D103D
1DDB3442FFFF4D5C84165E6F5823C8687AFA76F1B5E69C3586F9DDC1D71403A668F95AFCF93FC
283E2FB4204690E58AA655B45CC35D2ED7029E077B3610C7439E0FB09632B61E3037AC067EDBE
84B9628F16F1FB459C837F0FB2ADD565260166357EEAD1103C56757388623D89DD37A06DB6C9
755908A30B390616F85BF10753216140A2A3870F71B10B6549BB200ACF9139377E37EC8F35C70
F0BD92927825833DF47C2AA186269E35B90A558C959065FAF04EAE068E1A3D7E3FC0DBD23710
58B1DE0C919BD19C120399D8F47F8A222DF50777A3CA17D73CD5E836C46C7D48C8142400FCD
829254CB2F09D53D3882A3AB98C836DD07D57F81E9B3C60090C3DE667BA5D214C708C85BE22
6B95B582D1308C242610EC479DA3DED5559DA9D79E2EBBC6B154BAA7372599D28EE6727F8658
5EB27B2A4BBE515613D35180D993142AD931D1320E94B176DBDED6FE13F90E2168400DC07058
4FA11D0346A14DCBC0E70DF21B92DA5ECC2874BC6371E2F01B23A8224C0158B9EBB6DD87B1EF
FC15B0C638E4D6641D43DD0A2BC65C71512BCB047BE805B5BEC85CE6F592A36E8DE506B1D322
8F5CB53D8FF16F9FE7A013F2BCC2257591D376FB4EC6913C451B1C62358A851C83E8863EF25D7
CA74B9E0469F8CD4C0D00FBDBC8A187C506921F8189695DC05EB44C999C47937B19C37CA1515
AB02D414F29BC78AB585”
OutMAC: "D823A61E"

2.11 获取电能表任务数据

需要进行会话层数据的加密/解密都通过此函数操作。

2.11.1 函数说明

函数名称	int WINAPI Obj_Meter_Test_GetMeterSetData(int InOperateMode, const char* InEsamId, const char* InSessionIV, const char* szData, char* OutSID, char* szOutAttachData, char* szOutData, char* szOutMac)	
参数说明	入参	InOperateMode: 输出数据格式, 具体格式参见附录 InEsamId: ESAM 序列号, 8 字节 InSessionIV: 会话密钥初始向量, 177 字节 szData: 数据明文
	出参	OutSID: 安全标识类型, 4 字节 szOutAttachData: 安全标识附加数据 szOutData: 输出的数据 szOutMac: MAC, 4 字节
返回值	0: 成功 其他: 错误	

2.11.2应用举例

```
InOperateMode: 1
InEsamId:" 0002D21000000367"
InSessionIV                                     :
0093506D172ACD4D5D2730731619BC175B61C9BF3230761BF2AAE513E723D2F20C38CC14C726
ACF3B350EFA4E6844EBFA523FE417B8B450D54119CD628E7CB388B3AA42FF1A67968CDDE6327
2B8AF792257A669B0E4A0E07DBD571FA0FC95825C1E2DA87689702884CD9C21A6B9EB1710424
FE5808F41D0D9739C1506659868A28EC87EADBFD2930B7BCFFCE1ADBB5633B62F443A53859DC
BD53CE7A97243A8FA630D7C6F301812A0BE11FB4CA2BB3FDDA"
szData: "1122334455667788"
OutSID:  "811C3110"
szOutAttachData:  "000C"
szOutData:  "1122334455667788"
szOutMac:  "1AEB1AD3"
```

2.12 验证会话数据

需要进行会话层数据的加密/解密都通过此函数操作。

2.12.1函数说明

函数名称	int WINAPI Obj_Meter_Test_VerifyMeterData(int iKeyState,int InOperateMode, const char * InEsamId,const char* InSessionIV,const char* szData,const char* szInMac,char* szOutData)	
参数说明	入参	iKeyState: 当前密钥状态, 0: 测试密钥状态; 1: 正式密钥状态 InOperateMode: 输出数据格式, 具体格式参见附录 InEsamId: Esam 序列号, 8 字节 InSessionIV: 会话密钥初始向量, 177 字节 szData: 数据明文 szInMac:MAC,4 字节
	出参	szOutData: 输出的数据
返回值	0: 成功 其他: 错误	

2.12.2应用举例

InKeyState :0

```
InOperateMode: 2
InEsamId: "0002D21000000367"
InSessionIV
:
0093506D172ACD4D5D2730731619BC175B61C9BF3230761BF2AAE513E723D2F20C38CC14C726
ACF3B350EFA4E6844EBFA523FE417B8B450D54119CD628E7CB388B3AA42FF1A67968CDDE6327
2B8AF792257A669B0E4A0E07DBD571FA0FC95825C1E2DA87689702884CD9C21A6B9EB1710424
FE5808F41D0D9739C1506659868A28EC87EADBFD2930B7BCFFCE1ADBB5633B62F443A53859DC
BD53CE7A97243A8FA630D7C6F301812A0BE11FB4CA2BB3FDDA"
InData: "D7441205AF9A8BE579588C28E849E0BD"
OutMAC2:"970B15E1"
OutData: " 1122334455667788"
```

2.13获取随机数

2.13.1函数说明

函数名称	int WINAPI Obj_Meter_Test_GetRandHost (char* OutRandHost)	
参数说明	入参	
	出参	OutRandHost: 16 字节随机数
返回值	0: 成功 其他: 错误	

2.13.2应用举例

```
OutRandHost: "287A1890F73FA538CC676193AB8AF0D0"
```

2.14 获取广播数据

2.14.1函数说明

函数名称	int WINAPI Obj_Meter_Test_GetGrpBrdCstData(int iKeyState, int InOperateMode,const char * InEsamId, const char * ucBrdCstAddr, const char* AGSEQ, const char * ucBrdCstData, char* ucOutSID, char* ucOutAttachData,char * ucOutGrpBrdCstData,char* ucOutMac)	
参数	入	InKeyState: 电表密钥状态, 0: 测试密钥状态; 1: 正式密钥状态;

说明	参	InOperateMode: 广播数据类型 1: 明文+Mac 3: 密文+MAC InEsamId: Esam 序列号, 8 字节 ucBrdCstAddr: 组地址; 8 字节,不足 8 字节, 前填充 0 AGSEQ:广播应用通信序列号 4 字节 ucBrdCstData: 广播数据明文; N 字节
	出参	ucOutSID: 安全标识类型, 4 字节 ucOutAttachData: 安全标识附加数据 ucOutGrpBrdCstData: 输出的数据 ucOutMac: MAC,4 字节
返回值	0: 成功 其他: 错误	

2.15 上报数据返回加密

2.15.1 函数说明

函数名称	int WINAPI Obj_Meter_Test_GetResponseData (int InKeyState, int InOperateMode, const char * InMeterNum, const char *InRandHost , const char * InResponseData, char* OutSID,char* szOutAttachData,char* szOutData,char* szOutMac)	
参数说明	入参	InKeyState: 电表密钥状态, 0: 测试密钥状态; 1: 正式密钥状态; InOperateMode: 广播数据类型 0: 明文+Mac 2: 密文+MAC InMeterNum: 表号, 8 字节, 不够 8 字节前面填充 0 InRandHost: 上报随机数; 12 字节 InResponseData: 响应数据明文; N 字节
	出参	OutSID: 安全标识类型, 4 字节 szOutAttachData: 安全标识附加数据 szOutData: 输出的数据 szOutMac: MAC, 4 字节
返回值	0: 成功 其他: 错误	

2.15.2 应用举例

InKeyState:0
 InOperateMode: 2
 InMeterNum: "0000000000000001"
 InRandHost : "158066F7F296549800000001"
 InResponseData: "1122334455667788"
 OutSID: "800C4001"

szOutAttachData : "0020158066F7F29654980000000100000000"
szOutData : "10B1DBC5567A0878E2F8A505542CA6CE"
szOutMac:

2.16 软件比对

2.16.1 函数说明

函数名称	int WINAPI Obj_Meter_Test_VerifyCompareData(int InOperateMode, const char * InKeyID, const char * InComDIV, const char * InIv, const char * InCompareData, const char * InMAC, char * OutData)	
参数说明	入参	InOperateMode: 输出数据格式, 具体格式参见附录 InKeyID: 密钥 ID, 1 字节 InComDIV: 分散因子 InIv: 初始向量 InCompareData: 对比数据密文 InMAC: 对比数据 MAC
	出参	OutData: 明文数据, 若 InOperateMode = 1 为空
返回值	0: 成功 其他: 错误	

2.16.2 应用举例

InOperateMode: 1
InKeyID: "09"
InComDIV: "0000000000000000"
InIv: "8FDAE6E4D3A19CD12933D3936EE029B7"
InCompareData: "1122334455667788"
InMAC: "F3033FFD"
OutData: ""

2.17 红外查询

2.17.1 函数说明

函数名称	int WINAPI Obj_Meter_Test_InfraredRand(char * OutRand1)	
参数说明	入参	
	出参	OutRand1:随机数 R1, 8 字节
返回值	0: 成功 其他: 错误	

2.17.2 应用举例

OutRand1: " 0306B484763FEACD "

2.18 红外认证

2.18.1 函数说明

函数名称	int WINAPI Obj_Meter_Test_InfraredAuth(int InKeyState,const char *InEsamId, const char * InMeterNum, const char * InRand1 ,const char * InRand1Endata,const char* InRand2,char *OutRand2Endata)	
参数说明	入参	InKeyState: 电表密钥状态, 0: 测试密钥状态; 1: 正式密钥状态; InEsamId: Esam 序列号, 8 字节 InMeterNum: 表号, 8 字节, 不够 8 字节前面填充 0 InRand1: 红外查询得到的随机数 R1, 8 字节 InRand1Endata: 芯片返回的 R1 密文, 8 字节 InRand2: 芯片返回的 R2, 8 字节
	出参	OutRand2Endata:随机数 R2 密文, 8 字节
返回值	0: 成功 其他: 错误	

2.18.2应用举例

InKeyState: 1
InEsamId: "0002D2100000032A"
InMeterNum: "0000000000000002"
InRand1: "0306B484763FEACD"
InRand1Endata: "4D1E51D59F06BBB3"
InRand2: "95623FACCA0A4245"
OutRand2Endata: "ED8AFB61714E7A61"

3 常用操作流程举例说明

3.1 密钥更新

操作流程 1 步骤:

- (1) 调用接口 Obj_Meter_Test_GetTrmKeyData()产生 OutData2、OutOAD2、OutAttachData2、OutMAC2
- (2) 调用接口 Obj_Meter_Test_GetMeterSetData () 将第 (1) 步骤的 OutOAD2+OutAttachData2+OutData2+ OutMAC2 和协议层的附加数据作为此接口的 Data 数据明文,再根据需要对其进行 MAC/密文/密文+MAC 的计算并产生 OutData1、OutOAD1、OutAttachData1、OutMAC1

4 附录

4.1 操作模式

操作模式, 长度 1 字节, 用于指定对应文件的操作方式, 如下:
1——明文+MAC
2——密文
3——密文+MAC

4.2 常见错误码

201	获取读卡器列表错误
202	打开读卡器错误
203	复位错误

1501 - 1508	分别代表 1~8 参数长度错误
1601	加密模式不支持, 1,2,3
3020	获取文件信息失败
3021	计算 MAC 错误
3022	加密错误
3023	分散错误
3024	LRC 校验计算错误
3025	解密错误
3026	对比 MAC 错误
3027	计算 HASH 错误
3028	解密出的明文格式不正确
3030	取随机数错误