**电动汽车智能支付卡消费交易指令流**

1. 支付卡和充电桩交互流程
   1. 充电桩充电交互流程

| **序号** | **用户（支付卡）** | **充电桩（PSAM、ESAM）** | **说明** |
| --- | --- | --- | --- |
| 1 |  |  | 用户第一次刷卡。 |
| 2 | 复位  返回：ATR信息 + 90 00 |  |  |
| 3 | 发送：00 A4 00 00 02 DF 02  返回：信息数据+ 90 00  FCI信息在返回数据中查找9F0C，获得9F0C{L{FCI}} |  | 选择电动汽车应用目录  返回6A81 表示应用已锁定，交易退出；  用户卡卡号（FCI第11~20字节）；  获取用户卡应用版本（UserVer，FCI第10字节）‘01’为试点密钥版本用户卡，‘02’为全国密钥版本用户卡。  注：此步骤需要保存的数据：用户卡卡号、用户卡用用版本。 |
| 4 | 发送：00B0951804  返回：应用有效日期（4字节） |  | 应用有效日期：  YYYYMMDD  充电桩判断有效日期，过期充电截止，提示相关信息。 |
| 5 | 发送：00B0880001  返回：读验证PIN标识（1字节） |  | 判断是否需要PIN验证。  00：这种方式无需用户输入密码  01：系统默认，需要提供密码 |
| 6 | 发送：00B085000D  返回：电动汽车信息+ 90 00 |  | 1—8（支付卡物理卡号）  9（业务模型）  16 进制转2 进制  第八位为 1 表示充电  第七位为 1 表示换电  10—13（区域编码）  判断支付卡是哪个网省卡片  14—21（计费模型）  判断计费模型使用哪套标准 |
| 7 |  | 复位  返回：信息 + 90 00 |  |
| 8 |  | 发送：00b0960006  返回：Terminalno（6字节） | 获得终端机编号  Terminalno  注：此步骤需要保存 Terminalno和PSAM卡卡号 |
| 9 |  | 发送：00B095000A  返回：PSAMSN（10字节） | 获得PSAM卡卡号PSAMSN  注：此步骤需要保存 Terminalno和PSAM卡卡号 |
| 10 |  | 判断用户卡应用版本  If UserVer==01  发送：00 A4 00 00 02 DF 01  Else if UserVer==02  {发送：00 A4 00 00 02 DF 02  返回：信息数据 + 90 00} | 记录 PSAM卡中“消费密钥索引号”= PKID，在信息数据中，找9F0C{L{FCI}}，FCI的第1字节。  注：此步骤需要保存用户卡应用版本  DF01为上海试点目录 |
| 11 | 发送：00200000+LC+PIN  返回：90 00 |  | 验证PIN  系统默认为“\x12\x34\x56” |
| 12 | 发送：E0 CA 00 00 27  返回：data+90 00 或69 85  Data = 冻结金额（4字节）  +状态字（00无灰锁、01应用已灰锁、10 TAC未读）1字节  +灰锁交易标识（91灰锁、93解扣、95联机解扣）（1字节）  +保留（‘01’）1字节  +ET余额 （4字节）  + ET 交易序号（2字节）  +上次执行的终端机编号（6字节）  +上次执行的日期 （4字节）  +上次执行的时间 （3字节）  +灰锁时的MAC2/上次解扣、联机解扣的交易金额 （4字节）  +灰锁时的GTAC/上次解扣的TAC或联机解扣的MAC3 （4字节）  +终端机交易序号（4字节）  +异常灰锁次数（1字节） |  | 查询灰锁状态  9000判断第一字节 ，6985不用判断，直接跳转到步骤19；  00表示无灰锁  01表示当前应用已灰锁  10表示TAC未读 |
| 13 |  | 根据“异常灰锁次数”判断卡片是否有异常交易记录。  如果异常灰锁次数与状态字都为00时，标识卡片无灰锁记录，执行步骤19（开始当前交易）； |  |
| 14 | E0CA010000 | 如果状态字为10，保存第11步返回的TAC值，形成补充交易包上传。然后发送左边的指令。 |  |
| 15 |  | 如果状态字为01，判断“上次执行的终端机编号”与当前终端机编号一致，在充电桩内查找该条灰记录，进行解扣（步骤26）；如果不一致，执行步骤16（移异常交易记录）。 |  |
| 16 |  | 如果异常灰锁次数为00，执行步骤19（开始当前交易）； |  |
| 17 | 发送：E0 CA 02 00 00  返回：9000 |  |  |
| 18 | 发送：E0 CA 00 01 Le  返回：数据+9000 |  | Le= 0x27\*(异常灰锁次数+1) |
| 19 |  | 比对所有异常灰锁记录的终端及编号，查找与本终端机编号相同的记录，进行解扣。 |  |
| 20 | 发送：E0 CC 00 00 07  返回：可支配金额（前4字节） |  | 读可支配金额。  可支配金额=金额+透支限额 |
| 21 | 发送：E0 7A 08 01 0B +PKID  + terminalno（6字节）+冻结金额（4字节）  返回：  ET余额（4字节）  + ET脱机交易序号（2字节）  + 透支限额（3字节）  + 密钥版本号（1字节）  + 算法标识（1字节）  + 伪随机数（4字节）  + 实际冻结金额（4字节） |  | 灰锁 |
| 22 |  | 发送：E0 40 00 00 20  + 伪随机数（4字节）  + ET脱机交易序号（2字节）  + ET余额（4字节）  + 交易类型标识（‘91’）  + 交易日期(4字节）  +交易时间(3字节）  +密钥版本号(1字节）  +算法标识(1字节）  +冻结金额（4字节）  +支付卡卡号（8字节）  返回：终端交易序号 (4字节）  +终端随机数 (4字节）  +MAC1 (4字节） | 注：此步骤保存ET脱机交易序号、交易日期、交易时间、密钥版本号、算法标识、冻结金额。 |
| 23 | 发送：E0 7C 08 00 13  终端交易序号 (4字节）  +终端随机数 (4字节）  + 交易日期(4字节）  +交易时间(3字节）  +MAC1 (4字节）  返回：GTAC (4字节）  +MAC2(4字节） |  | 注：此步骤保存终端交易序号、GTAC |
| 24 |  | 发送：E0 42 00 00 04  + MAC2  返回：90 00 |  |
| 25 |  |  | 开始充电 |
| 26 |  | 发送：E0 44 00 00 0F  + 交易类型标识（‘93’）  + 用户卡应用序列号（8字节）  + 用户卡脱机交易序号（2字节）  + 交易金额（4字节）  返回：GMAC(4字节)  +SAMTAC(4字节) | 充电完毕后，充电桩应立刻发送该指令给ESAM，并保存相关数据。  注：计算GMAC，保存用户卡应用序列号、用户卡脱机交易序号、交易金额、GMAC和SAMTAC。 |
| 27 | 发送：00 A4 00 00 02 DF02  返回：支付卡公共信息文件  + 90 00 |  | 用户二次刷卡，判断支付卡卡号是否和原卡相同；  充电桩计算交易金额； |
| 28 | 发送：E0 7E 08 01 1C  + 交易金额（4字节）  + 用户卡脱机交易序号（2字节）  + 终端机编号（6字节）  + 终端交易序号（4字节）  + 交易日期（4字节）  + 交易时间（3字节）  + GMAC(4字节)  + ’00’ （如果是异常灰锁记录，此处为1字节异常灰锁记录号）  返回：TAC(4字节) |  | 扣款  注：保存TAC |
| 29 | 发送：E0 CA 01 00 00  返回：90 00 |  | 清除TACUF |
| 30 |  |  | 上传交易 |

交易包说明：

正常交易：用户第二次刷卡成功扣款后，充电桩上传的交易记录中应包括以下数据：交易流水号、终端机编号、终端交易序号、支付卡卡号、交易类型、灰锁金额、消费金额、钱包余额、钱包脱机交易序号、交易日期、交易时间、GTAC、SAMTAC、GMAC、TAC、密钥版本号、算法标识、ESAM序号。

开始充电之前：交易流水号、终端机编号、终端交易序号、支付卡卡号、交易类型、预冻结金额、消费金额、钱包余额、钱包脱机交易序号、交易日期、交易时间、GTAC、密钥版本号、算法标识、ESAM序号。

如果是补充交易，在完成扣款后，应保存下SAMTAC、TAC，与在充电桩中找到的原交易记录合并一条交易记录上传。

1. 充电桩在线交易流程

该流程用于在使用账户扣款时，获取用户卡卡号和认证码，与后台账户进行鉴权。为减少刷卡时等待时间，由充电桩每隔一段时间向主站申请一次随机数（即重复执行第1~3步），当用户刷卡时，使用最新申请的随机数做鉴权。

注：第1~3步为申请随机数的过程，当第3步执行成功后，保存主站下发的随机数。一次充电成功后，应重新申请随机数。直到下一次申请随机数时，更新桩内保存的该随机数。

* 1. 系统认证桩流程：（桩首次上电）

| 序号 | 充电桩 | 运营管理系统连接密码机 |
| --- | --- | --- |
| 桩首次上电，系统比对终端机编号认证 | | |
| 1 | 向ESAM发送指令  发送：00B095000A  返回：ESAM序列号（10字节）  发送：00B0960006  返回：Terminalno（6字节） |  |
| 2 |  | 记录ESAM序列号（后8字节）  terminalno  取主站随机数，下发充电桩 |
| 3 | 选择应用目录，发送：00A4000002DF01  返回：9000  向ESAM发送指令：  0088000108+主站随机数rand  返回：终端鉴权码+9000  向ESAM发送指令：  0084000008  返回：终端随机数  上传终端鉴权码和终端随机数 |  |
| 4 |  | 计算终端鉴权码8字节，与ESAM计算的终端鉴权码比较，是否一致；  一致则计算主站鉴权码，并下发 |
| 5 | 向ESAM发送指令：  0082000108+主站鉴权码  返回：9000 |  |
| 6 | 充电桩上报认证结果 |  |
| 7 |  | 系统判断充电桩认证结果，通过则流程继续。 |
| 8 |  | 读取系统端终端机编号，  比较终端机编号，  发送通过认证指令。  保持心跳。 |

* 1. 在线交易，长链接：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 支付卡 | 充电桩 | 运营管理系统连接密码机 |
| 申请随机数(桩认证系统)（交易使用，提前存在桩内） | | | |
| 1 |  | 向ESAM发送指令：  0084000008  返回：终端随机数（8字节） |  |
| 2 |  |  | 计算主站鉴权码8字节  取主站随机数  返回鉴权码和主站随机数rand |
| 3 |  | 向ESAM发送指令：  0082000108+主站鉴权码  返回：9000 |  |
| 用户一次刷卡，开始鉴权（系统认证卡） | | | |
| 1 |  | 向卡片发送指令：  00A4000002DF02  00b0950A0A |  |
| 2 | 卡片返回：  10字节卡号CardSN |  |  |
| 3 |  | 向卡片发送指令：  0088000108+rand |  |
| 4 | 卡片返回：  8字节认证数据 |  |  |
| 5 |  | 将卡片返回认证信息传递给运营管理系统 |  |
| 6 |  |  | 运营管理系统利用密码机，根据随机数rand和CardSN计算认证数据，与卡片产生的认证数据比对是否一致 |
| 7 |  |  | 如果一致，查找与卡号对应的账户，进行交易。 |
| 8 |  |  | 对充电命令data 算MAC，并加密  返回 ENC(data+MAC) |
| 9 |  | ESAM充电下发数据解密（解密过程见附录），验证MAC，通过则开始充电。 |  |
| 用户二次刷卡 | | | |
| 1 |  | 向卡片发送指令：  00A4000002DF02  00b0950A0A |  |
| 2 | 卡片返回：  10字节卡号CardSN |  |  |
| 3 |  | 充电桩比对是否和第一次刷卡卡号一致，一致进行消费数据统计。（加密数据不超过235字节） |  |
| 4 |  | 对消费数据算MAC：  得到：4字节MAC |  |
| 对消费统计数据data和MAC加密，返回:  Enc{data+MAC} |  |
| 5 |  |  | 对上传数据解密，得到：  消费数据{data+MAC}  配合随机数验证MAC，通过验证则下发交易完成通知。 |

* 1. 密钥更新

在密钥更新前，由主站将所有密钥密文计算完毕后分两部分下传，终端接收齐全后，逐条解密并更新，为避免更新一半时，过程被中断或其他原因导致数据有损。

| 步骤 | 主站下发指令 | 终端 | 描述 |
| --- | --- | --- | --- |
| 1 |  | Reset | 复位 |
| 2 |  | 发送：00B095000A  返回：ESAM序列号（10字节）  发送：00B0960006  返回：Terminalno  （6字节） | 记录ESAM序列号（后8字节）  terminalno  取主站随机数，下发充电桩 |
| 3 |  | 选择应用目录发送：00A4000002DF01  返回：9000  向ESAM发送指令：  0088000108+主站随机数rand  返回：终端鉴权码+9000  向ESAM发送指令：  0084000008  返回：终端随机数  上传终端鉴权码和终端随机数 |  |
| 4 | 计算终端鉴权码8字节，与ESAM计算的终端鉴权码比较，是否一致；一致则计算主站鉴权码，并下发 |  |  |
| 5 |  | 外部认证：  命令：0082000008 + 鉴权数据  返回：9000 |  |
| 6 |  | 充电桩上报认证结果 |  |
| 7 | 充电桩认证通过，则主站发起密钥更新过程。 |  |  |
| 8 |  | 取ESAM 内CardSN （PASMSN）、终端机编号 上传。 |  |
| 9 | 根据 CardSN序列号分散要更新的密钥，下发密钥更新指令数据 |  |  |
| 10 | 使用主站随机数对更新主控公钥指令  {84D4010020+keydata(32字节)}算MAC  得到：4字节MAC  下发更新数据+MAC | 对主站下发MAC进行验证，成功则更新主控密钥 | 更新主控密钥：   1. data= ‘000000’+新主控（16字节） 2. keydata= 旧DF02主控对data进行SM1加密的数据。 3. 以下密钥用新主控加密更新。 4. 对整个报文算MAC验证数据完整。 |
| 11 | 将前5条密钥更新指令做为第一部分更新数据，打包算MAC，得到：  4字节MAC  下发更新数据+MAC | 对主站下发的第一部分数据做MAC验证，成功则保存更新数据。 | data= ‘010100’+新应用维护密钥（16字节） |
| data= ‘000100’+新外部认证密钥（16字节） |
| data= ‘1C0100’+新内部认证密钥（16字节） |
| data= ‘250100’+新用户卡应用维护密钥（16字节） |
| data= ‘220100’+新消费主密钥MPK1（16字节） |
| 将剩余密钥更新指令做为第二部分更新数据，打包算MAC，得到:  4字节MAC  下发更新数据+MAC | 对主站下发的第二部分数据做MAC验证，成功则保存更新数据。 | data= ‘220200’+新消费主密钥MPK2（16字节） |
| data= ‘150100’+新DSTK（16字节） |
| data= ‘1B0100’+新线路保护加解密密钥（16字节）  使用旧线路保护密钥加密。 |
| data= ‘1B0200’+新MAC加解密密钥（16字节）  使用新线路保护密钥加密。 |
| 10 |  | 桩在两部分数据收齐后，发送指令更新所有密钥：  例：  84D4010020+keydata(32字节) |  |

* 1. 参数更新

|  |  |  |  |
| --- | --- | --- | --- |
| 步骤 | 终端ESAM | 主站 | 描述 |
| 参数更新数据下行 | | | |
| 1 |  | 下发参数更新请求 |  |
| 2 | 取随机数、ESAM 内CardSN 、终端机编号 上传。 |  |  |
| 3 |  | 对参数更新数据算MAC，得到  ：4字节MAC  对参数更新数据+MAC 加密，得到：  Enc{data + MAC} |  |
| 4 | 对参数更新密文数据解密，得到参数更新数据data+MAC（解密流程见附录），  验证MAC通过，则参数信息合法。 |  |  |
| 5 | 对更新成功的结果数据，计算MAC，同时将带MAC的数据加密，上传给主站。 |  |  |
| 6 |  | 主站对上传的参数更新结果数据先解密、再验MAC，判断充电桩参数更新的结果是否成功。 |  |

1. 附录1
   1. 数据加密 计算MAC

**加密：**

为保证数据的安全性，充电桩和主站对数据进行加解密处理，ESAM按照如下所示做SM1（e）运算产生密文数据：

步骤一：

发送APDU指令：80 1A 1B 01 00

卡片返回：9000

步骤二：

对数据（data）加密得到相应的密文Enc(data)：

发送APDU指令：80 FA 00 00 LC data

卡片返回：Enc(data)

注：输入源数据为16字节的整数倍，故 ‘10’≤ Lc ≤ ‘F0’（模16）

**MAC运算：**

为验证数据的完整性，并对发送方进行认证，ESAM端按照以下所示做SM1（e）运算产生MAC:

步骤一：

发送APDU指令：80 1A 1B 01 00

步骤二：

对随机数初值、命令数据（data）做MAC运算，得到4字节MAC

送APDU指令：80 FA 05 00 LC data

卡片返回： 4字节MAC

注：：‘20’≤ Lc ≤ ‘F0’（模16）

* 1. 数据解密 验证MAC

**加密：**

ESAM端按照如下所示做SM1（e）运算解密密文数据：

步骤一：

发送APDU指令：801A 1B 01 00

步骤二：

使用得到子密钥对命令数据Enc（data）解密得到相应的明文data：

发送APDU指令：80 FA 80 00 LC Enc(data)

卡片返回： data

注：输入源数据为16字节的整数倍，故 ‘10’≤ Lc ≤ ‘F0’（模16）

**MAC验证:**

使用随机数初值，分散线路保护密钥1B01，做MAC运算，得到的MAC值与报文中的MAC做比较，一致则MAC验证通过