ICS 27.100
F 22
备案号：50811-2015

DL

中华人民共和国电力行业标准

DL / T 1491 — 2015

智能电能表信息交换安全认证技术规范

Security techniques of information interchange authentication specification for smart electricity meters

2015-07-01发布　　2015-10-01实施

国家能源局　发布

目　　次

前　言

本标准依据 GB/T 1.1—2009 给出的规则起草。

本标准与《智能电能表功能规范》《单相智能电能表技术规范》《三相智能电能表技术规范》《单相智能电能表型式规范》《三相智能电能表型式规范》共同成为智能电能表设计、制造、管理、维护的技术依据。

请注意本文件的某些内容可能涉及专利。文件的发布机构不承担识别这些专利的责任。

本标准由中国电力企业联合会提出。

本标准由电力行业电测量标准化技术委员会归口。

本标准起草单位：中国电力科学研究院、国网河北省电力公司、国网天津市电力公司、国网江西省电力公司。

本标准主要起草人：翟峰、赵兵、章欣、杜蜀薇、杜新纲、葛得辉、彭楚宁、徐英辉、付义伦、刘鹰、吕英杰、李保丰、孙志强、陶鹏、解岩、张卫欣、张春强。

本标准在执行过程中的意见或建议反馈至中国电力企业联合会标准化管理中心（北京市白广路二条一号，100761）。

智能电能表信息交换安全认证技术规范

1 范围

本标准规定了智能电能表的费控功能要求，数据交换安全认证所涉及的数据结构和操作流程，它包括术语定义、安全原则、安全模块和卡片的文件结构、费控功能要求、操作流程和相关功能的检测要求。

本标准适用于电力行业规范智能电能表的设计、制造、订货、验收、使用等环节。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

DL/T 645—2007 多功能电能表通信协议

JR/T 0025—2010 中国金融集成电路（IC）卡规范

国密局函〔2009〕4号 关于请协助做好IC卡系统密码管理工作的函

ISO/IEC 7816 4 识别卡 带触点的集成电路卡 第4部分：行业间交换用命令（Identification cards—Integrated circuit cards Part 4: Organization，security and commands for interchange）

3 术语和定义

下列术语和定义适用于本文件。

3.1

安全模块 ESAM

嵌入在设备内，实现安全存储、数据加/解密、双向身份认证、存取权限控制、线路加密传输等安全控制功能的硬件电路模块。

3.2

密码机 cryptography machine

能够独立完成加/解密和密钥管理功能的设备。

3.3

密码算法 cryptographic algorithm

描述密码处理过程的一组运算规则或规程。

3.4

国密SM1算法 SM1 cryptographic algorithm

经国家密码管理局审批的一个商用密码分组算法。

3.5

认证 certification

验证一个称谓的系统实体身份的过程。

3.6

明文 plain text

待加密的数据。

3.7

密文 cipher text

加密后的数据。

3.8

加密　encryption

对数据进行密码变换以产生密文的过程。

3.9

解密　decryption

加密过程对应的逆过程。

3.10

密钥　key

控制密码变换操作的关键信息或参数。

3.11

主控密钥　master key

处于对称密码系统层次化密钥结构中的最高层，对其他密钥进行加密的密钥。

3.12

消息鉴别码　message authentication code（MAC）

为鉴别消息数据的完整，由密钥参与对其进行运算后产生的代码。

3.13

分散因子　diffusion factor

与本级特征有关的业务代码。

3.14

密钥信息　key information

与密钥相关的一些信息标识。

3.15

CPU 卡　CPU card

配置有存储器和逻辑控制电路及微处理（MCU）电路，能多次重复使用的接触式 IC 卡。

3.16

射频卡　radio frequency card

一种以无线方式传送数据的具有数据存储、逻辑控制和数据处理等功能的非接触式 IC 卡。

3.17

用户购电卡　card for user purchase electric energy

由用户持有的用于电能表与售电系统之间信息交换的 IC 卡。

3.18

参数预置卡　card to set parameter in advance

在生产过程中用于电能表初始化的 IC 卡。

3.19

客户编号　user serial number

用于区别不同用户的具有唯一性的编号。

3.20

表号　meter serial number

电能表出厂时设置的具有唯一性的编号。

3.21

电卡类型　card type

系统运营状态下识别不同卡片种类的标志。

3.22

电子钱包　electronic purse

一种为方便持卡人小额消费而设计的金融 IC 卡应用。

[JR/T 0025—2010，定义 3.11]

3.23

购电金额　money to purchase electric energy

用户在售电系统中缴费买电时所交的电费金额。

3.24

购电次数　times to purchase electric energy

记录自开户之日起用户完成购电交易的总次数，每次购电成功购电次数加一。

3.25

预置金额　money set in meter in advance

在电能表开户前通过参数预置卡预置在电能表内的可使用的用电金额。

3.26

剩余金额　charge balance

在电能表中记录的可供用户使用的电费金额，剩余金额应大于等于零。

3.27

报警金额 1　limiting charge 1

设置在电能表内，采用声光方式提醒用户及时购电的金额限值。

注：报警金额 1 设为零不报警。

3.28

报警金额 2　limiting charge 2

设置在电能表内，采用断电方式提醒用户及时购电的金额限值。

注 1：报警金额 2 设为零时该功能无效。

注 2：报警金额 2 应小于等于报警金额 1。

3.29

透支金额　overdraft

用户已使用但未缴纳电费的金额值，该值小于零。

3.30

参数更新标志位　flag of parameter renovation

用户卡中费率和电价参数是否通过用户卡更新的标志。

3.31

返写　data rewrite to card from meter

用电能表将数据读出并写入 IC 卡的过程。

3.32

非法卡　illegal card insert meter

电能表不能正常识别所插入的介质。

3.33

异常插卡　abnormal card insert meter

电能表对所插入的介质不能完成正常操作的行为，异常插卡包含非法插卡。

注：所有触动卡座触点但操作不成功的行为都属于异常插卡。

3.34

控制命令文件　control command file

用于对控制命令进行明文解析的，以密文方式存储的二进制文件。

3.35

软件比对 software comparison

验证电能表运行程序加密结果与存档源程序加密结果一致性的操作。

4 安全原则

4.1 ESAM

费控电能表应嵌入 ESAM 用于信息交换安全认证。通过固态介质或虚拟介质对费控电能表进行参数设置、预存电费、信息返写和下发远程控制命令操作时，应通过 ESAM 进行安全认证、数据加/解密处理以确保数据传输的安全性和完整性。

4.2 加/解密算法

ESAM 应使用符合国家密码管理政策的国密 SM1 算法。

4.3 关键数据存储

本地费控电能表的剩余金额、购电次数等关键数据应保存在 ESAM 中，并以此作为计量计费依据，电能表内部存储器中的剩余金额应小于等于 ESAM 中的剩余金额，电能表参数设置和状态调整均应采用 ESAM 加密保护。

远程费控电能表本地不计费，不存储和显示与金额、电价、变比、阶梯、购电相关的数据，电能表参数设置和状态调整均应采用 ESAM 加密保护。

4.4 关键数据传输

通过通信端口进行参数修改时，对于 ESAM 中已经定义的、须写入 ESAM 芯片的参数，参照 DL/T 645—2007 定义的协议格式先进行身份认证，认证通过后，以明文+MAC 的方式进行数据的传输和修改；对于 ESAM 中未定义的、写在 ESAM 芯片外部的参数，参照 DL/T 645—2007 定义的协议格式先进行身份认证，认证通过后，以密文+MAC 的方式进行数据的传输和认证，认证通过后，再以明文的方式获取对应的参数，并进行参数设置与存储。身份认证应采用基于国密 SM1 算法的双向挑战应答协议。

4.5 ESAM 扣款说明

本地费控电能表更新 ESAM 中的电子钱包的间隔时间不应小于 15min。当出现掉电、执行插卡操作和远程状态查询命令时，电能表应将存储器中剩余金额和 ESAM 中的剩余金额同步。如果电能表在 15min 内连续收到远程状态查询命令时，后续收到的查询命令不再同步。

远程费控电能表不支持此功能。

5 信息交换模式

电能表根据其费控功能在本地实现与在远程实现区分为本地费控电能表和远程费控电能表。本地费控电能表是在电能表内部实现计量、计费和控制功能的电能表。远程费控电能表是在电能表内部实现计量，远程实现计费和控制的电能表。

本地费控电能表支持本地充值和远程充值两种方式：本地充值方式通过 CPU 卡、射频卡等固态介质（统称为用户卡）进行充值；远程充值方式通过网络等虚拟介质进行远程充值。本地费控电能表支持本地控制和远程控制两种方式：本地控制方式由电能表根据费控功能要求实现本地报警、拉合闸控制；远程控制方式由采集系统主站通过网络等虚拟介质发送报警和跳合闸命令。用户卡、电能表、营销售电系统、银电联网售电系统、用电信息采集系统主站之间进行信息交换的过程如图 1 所示。电能表与用户卡之间、用户卡与售电系统之间，以及电能表与采集系统主站之间应按照流程要求进行安全认证，确保信息交换的安全性。

远程费控电能表不支持本地计费、充值功能，也不支持本地控制功能，只支持远程控制功能。远程控制方式由采集系统主站通过网络等虚拟介质发送报警和跳合闸命令。电能表与用电信息采集系统主站之间、用电信息采集系统与营销售电系统和银电联网售电系统间进行信息交换的过程如图 2 所示。电能

表与采集系统主站之间应按照流程要求进行安全认证，确保信息交换的安全性。

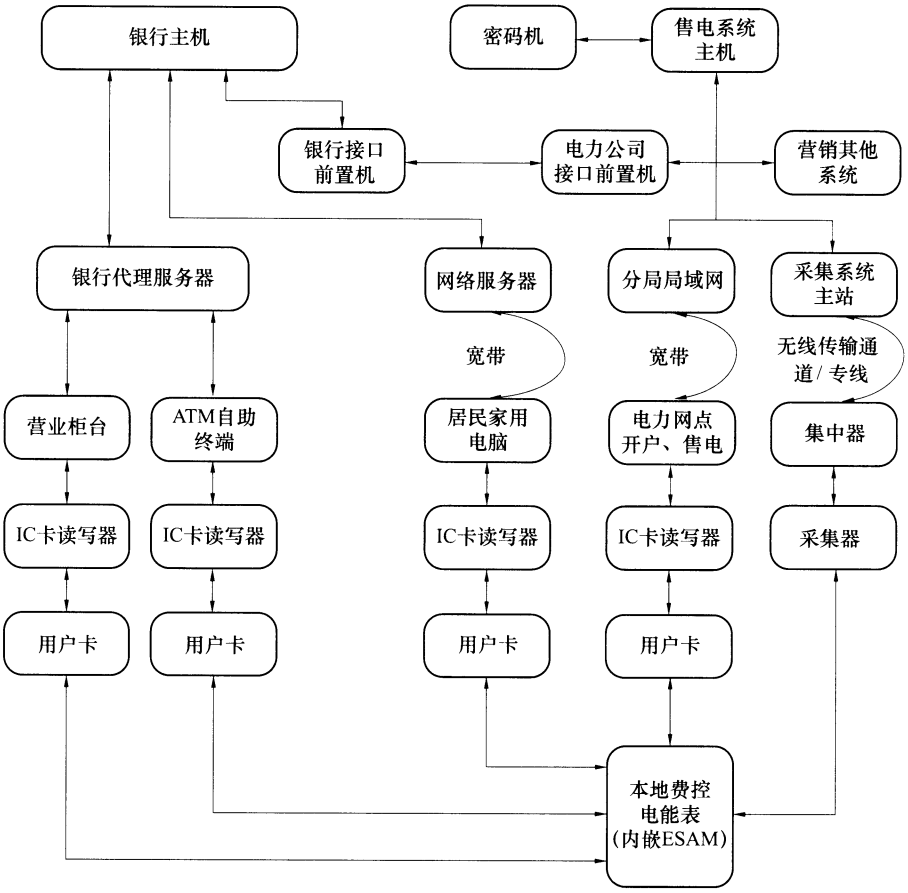

图 1　本地费控电能表信息交换示意图

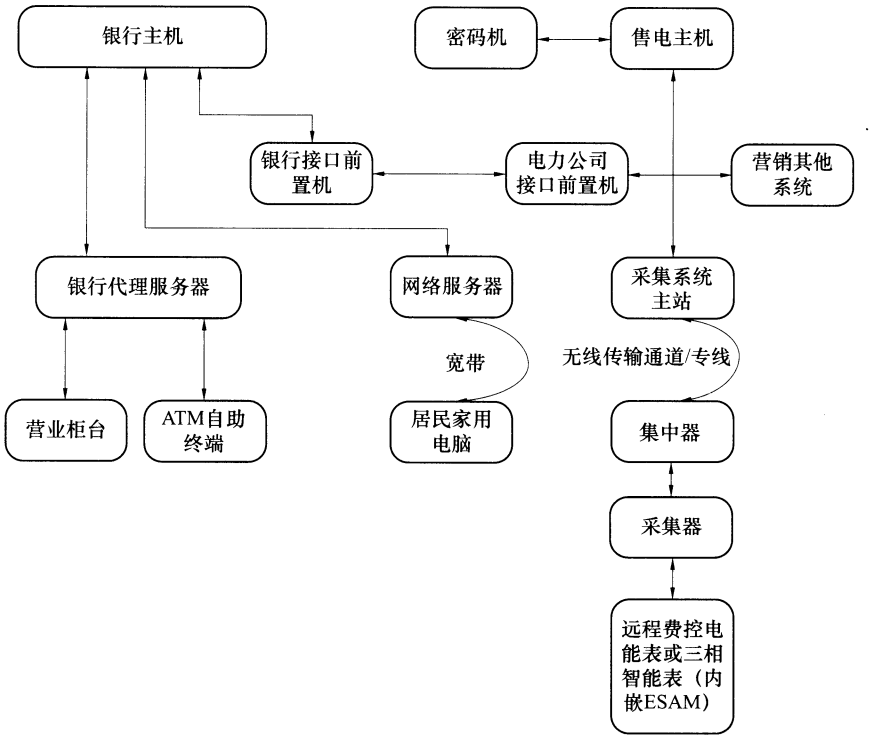

图 2　远程费控电能表信息交换示意图

6 ESAM 与卡片的文件结构

6.1 文件格式

ESAM 与卡片的文件结构相同，应采用不定长格式存放，应采用数据串的形式进行交互，具体格式见表 1。

表 1 文 件 格 式

起始 [a]	命令 [b]	长度 [c]	数据 [d]	校验 [e]	结束 [f]
注：对数据串是否有效的判别依据为：起始、结束字节必须正确；长度与数据区字节数必须相等；校验必须正确。					
a：1 字节，固定为 68H，为数据串的开始标识。 b：1 字节，分高半字节和低半字节，低半字节表示与电能表进行数据交换的 CPU 卡类型，高半字节为 1 表示返写信息文件，为 0 表示原卡片复制的数据。根据命令字可以判断出卡片的类型，然后再根据相应卡片的文件结构确定文件中数据的长度。 c：2 字节，HEX 码，为文件中数据区的长度。 d：字节数不定，为前面介绍数据项的组合，组合方式与命令有关。数据格式为高字节在前低字节在后。 e：1 字节，为命令、长度、数据 3 部分的所有各字节的模 256 的和，即各字节二进制算术和，不计超过 256 的溢出值。 f：1 字节，固定为 16H，代表数据串结束。					

6.2 卡片类型

本地费控电能表所用 CPU 卡包括参数预置卡和用户卡两种类型。用户卡根据应用状态分为开户卡、购电卡和补卡三种类型，卡片类型说明见表 2。

表 2 CPU 卡 片 类 型

序号	卡片类型说明	命令码	备 注
1	参数预置卡	06	用于参数预置和电子钱包初始化
2	用户卡	01	开户卡，用户卡类型为 01，用于电能表开户
			购电卡，用户卡类型为 02，用于正常购电
			补卡，用户卡类型为 03，用于补用户卡

6.3 ESAM 文件结构

6.3.1 文件目录

ESAM 文件目录见表 3。

表 3 ESAM 文 件 目 录

文件	内容说明	标识	权限 1	权限 2
MF	主文件	3F00	主控密钥	主控密钥
MKF	密钥文件	0000	…	主控密钥
EF1	电子钱包文件	0001	自由（扣款）	身份认证＋MAC
EF2	参数信息文件	0002	自由	身份认证＋MAC
EF3	当前套电价文件	0003	自由	身份认证＋MAC
EF4	备用套电价文件	0004	自由	身份认证＋MAC
EF5	密钥状态文件	0005	自由	自由

表 3（续）

文件	内容说明	标识	权限 1	权限 2
EF6	保留	0006	自由	身份认证＋MAC
EF7	运行信息文件	0007	自由	自由
EF8	控制命令文件	0008	自由	身份认证＋密文
EF9	参数更新文件 1	0009	自由	身份认证＋密文＋MAC
EF10	参数更新文件 2	0010	自由	身份认证＋密文＋MAC
EF11	参数更新文件 3	0011	自由	身份认证＋密文＋MAC
EF12	参数更新文件 4	0012	自由	身份认证＋密文＋MAC
EF13	参数更新文件 5	0013	自由	身份认证＋密文＋MAC
EF14	清零命令文件	0014	自由	身份认证＋密文＋MAC
EF18	发行信息文件	0018	自由	签名保护
EF19	记录信息文件 1	0019	自由	签名保护
EF20	记录信息文件 2	0020	自由	签名保护

6.3.2 电子钱包文件

ESAM 中的电子钱包文件见表 4。

表 4 ESAM 中的电子钱包文件

序号	数 据 项	长度 B	说 明
1	剩余金额	4	HEX，单位为元，2 位小数
2	购电次数	4	HEX，无小数位

6.3.3 参数信息文件

ESAM 参数信息文件见表 5。

表 5 ESAM 参数信息文件

序号	数 据 项	长度 B	格式	备 注
1	起始码	1	68H	
2	命令码	1	01H	
3	长度	2	HEX	
4	保留	1	HEX	
5	参数更新标志位	1	HEX	
6	保留	4	HEX	默认 00000000
7	两套分时费率切换时间	5	BCD	年月日时分
8	保留	1	HEX	默认 00
9	报警金额 1	4	BCD	××××××．××
10	报警金额 2	4	BCD	××××××．××

表 5（续）

序号	数 据 项	长度 B	格式	备 注
11	电流互感器变比	3	BCD	×××××
12	电压互感器变比	3	BCD	×××××
13	表号	6	BCD	
14	客户编号	6	BCD	
15	电卡类型	1	BCD	
16	身份认证时效性	2	BCD	分钟
17	校验码	1	HEX	
18	结束码	1	16H	

6.3.4 当前套电价文件

ESAM 当前套电价文件见表 6。

表 6 ESAM 当前套电价文件

序号	数 据 项	长度 B	格式	备 注
1	起始码	1	68H	
2	命令码	1	01H	
3	长度	2	HEX	
4	费率 1	4	BCD	××××. ××××
5	…	…	…	…
6	费率 32	4	BCD	××××. ××××
7	阶梯值 1	4	BCD	××××××. ××
8	…	…	…	…
9	阶梯值 6	4	BCD	××××××. ××
10	阶梯电价 1	4	BCD	××××. ××××
11	…	…	…	…
12	阶梯电价 7	4	BCD	××××. ××××
13	年第 1 结算日	3	BCD	月日时
14	年第 2 结算日	3	BCD	月日时
15	年第 3 结算日	3	BCD	月日时
16	年第 4 结算日	3	BCD	月日时
17	保留	60	HEX	默认为全 00
18	校验码	1	HEX	
19	结束码	1	16H	

6.3.5 备用套电价文件

ESAM 备用套电价文件见表 7。

表 7 ESAM 备用套电价文件

序号	数 据 项	长度 B	格式	备 注
1	起始码	1	68H	
2	命令码	1	01H	
3	长度	2	HEX	
4	费率 1	4	BCD	××××. ××××
5	…	…	…	…
6	费率 32	4	BCD	××××. ××××
7	阶梯值 1	4	BCD	××××××. ××
8	…	…	…	…
9	阶梯值 6	4	BCD	××××××. ××
10	阶梯电价 1	4	BCD	××××. ××××
11	…	…	…	…
12	阶梯电价 7	4	BCD	××××. ××××
13	年第 1 结算日	3	BCD	月日时
14	年第 2 结算日	3	BCD	月日时
15	年第 3 结算日	3	BCD	月日时
16	年第 4 结算日	3	BCD	月日时
17	两套阶梯切换时间	5	BCD	年月日时分
18	保留	55	HEX	默认为全 00
19	校验码	1	HEX	
20	结束码	1	16H	

6.3.6 密钥状态文件

ESAM 密钥状态文件见表 8。

表 8 ESAM 密 钥 状 态 文 件

序号	数 据 项	长度 B	格式	说 明
1	密钥状态	4	HEX	与 DL/T 645—2007 中的密钥 状态位保持一致

6.3.7 运行信息文件

ESAM 运行信息文件见表 9。

表 9 ESAM 运行信息文件

序号	数 据 项	长度 B	格式	备 注
1	起始码	1	68H	
2	命令码	1	11H	
3	数据长度	2	HEX	
4	保留	1	HEX	
5	电流互感器变比	3	BCD	××××××
6	电压互感器变比	3	BCD	××××××
7	表号	6	BCD	
8	客户编号	6	BCD	
9	剩余金额	4	HEX	
10	购电次数	4	HEX	
11	透支金额	4	BCD	××××××. ××
12	保留	4	HEX	默认 00000000
13	非法卡插入次数	3	BCD	
14	返写日期时间	5	BCD	年月日时分
15	校验码	1	HEX	
16	结束码	1	16H	

6.3.8 控制命令文件

ESAM 控制命令文件见表 10。

表 10 ESAM 控制命令文件

序号	数据项	长度 B	格式	备 注
1	密文	××	HEX	长度由密文长度决定

6.3.9 清零命令文件

ESAM 清零命令文件见表 11。

表 11 ESAM 清零命令文件

序号	数据项	长度 B	格式	备 注
1	密文	××	HEX	长度由密文长度决定

6.3.10 发行信息文件

ESAM 发行信息文件见表 12。

表 12　ESAM 发行信息文件

序号	数据项	长度 B	格式	备　注
1	密文	××	HEX	长度由密文长度决定

6.3.11　记录信息文件 1

ESAM 记录信息文件 1 见表 13。

表 13　ESAM 记录信息文件 1

序号	数据项	长度 B	格式	备　注
1	密文	××	HEX	长度由密文长度决定

6.3.12　记录信息文件 2

ESAM 的记录信息文件 2 见表 14。

表 14　ESAM 记录信息文件 2

序号	数据项	长度 B	格式	备　注
1	密文	××	HEX	长度由密文长度决定

6.4　参数预置卡文件结构

6.4.1　文件目录

参数预置卡文件目录见表 15。

表 15　参数预置卡文件目录

文件	内　容　说　明	标识	权限 1	权限 2
MF	主文件	3F00	禁止	禁止
MKF	密钥文件	0000	…	禁止
DF01	电能表应用目录文件	DF01	禁止	禁止
DKF	电能表应用密钥文件	0000	…	禁止
EF1	指令信息文件	0001	自由＋MAC	禁止
EF2	保留	0002	自由＋MAC	禁止
EF3	当前套电价文件	0003	自由＋MAC	禁止
EF4	备用套电价文件	0004	自由＋MAC	禁止
EF5	电子钱包初始化文件	0005	自由＋MAC	禁止

6.4.2　指令信息文件

参数预置卡指令信息文件见表 16，参数更新标志位见表 17。

表 16　参数预置卡指令信息文件

序号	数　据　项	长度 B	格式	备　注
1	起始码	1	68H	
2	命令码	1	06H	
3	长度	2	HEX	
4	保留	1	HEX	
5	参数更新标志位	1	HEX	见表 17
6	保留	4	HEX	默认 00000000
7	两套分时费率切换时间	5	BCD	年月日时分
8	保留	1	HEX	默认 00
9	报警金额 1	4	BCD	××××××．××
10	报警金额 2	4	BCD	××××××．××
11	电流互感器变比	3	BCD	××××××
12	电压互感器变比	3	BCD	××××××
13	校验码	1	HEX	
14	结束码	1	16H	

表 17　参数预置卡参数更新标志位

位	Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
说明	更新当前套费率	更新备用套费率	更新当前套阶梯	更新备用套阶梯				更新其他参数
注 1：当更新当前套费率标志为 1 时，电能表更新当前套费率，不更新两套分时费率切换时间。 注 2：当更新备用套费率标志为 1 时，电能表更新备用套费率，同时更新两套分时费率切换时间。 注 3：当更新当前套阶梯标志为 1 时，电能表更新当前套阶梯值、阶梯电价和年结算日，不更新两套阶梯切换时间。 注 4：当更新备用套阶梯标志为 1 时，电能表更新备用套阶梯值、阶梯电价和年结算日，同时更新两套阶梯切换时间。 注 5：当更新其他参数标志为 1 时，电能表更新未指定的参数。								

6.4.3　当前套电价文件

参数预置卡当前套电价文件见表 18。

表 18　参数预置卡当前套电价文件

序号	数　据　项	长度 B	格式	备　注
1	起始码	1	68H	
2	命令码	1	01H	
3	长度	2	HEX	
4	费率 1	4	BCD	××××．××××
5	…	…	…	…
6	费率 32	4	BCD	××××．××××
7	阶梯值 1	4	BCD	××××××．××
8	…	…	…	…

表 18（续）

序号	数 据 项	长度 B	格式	备 注
9	阶梯值 6	4	BCD	××××××. ××
10	阶梯电价 1	4	BCD	××××. ××××
11	…	…	…	…
12	阶梯电价 7	4	BCD	××××. ××××
13	年第 1 结算日	3	BCD	月日时
14	年第 2 结算日	3	BCD	月日时
15	年第 3 结算日	3	BCD	月日时
16	年第 4 结算日	3	BCD	月日时
17	保留	60	HEX	默认为全 00
18	校验码	1	HEX	
19	结束码	1	16H	

6.4.4 备用套电价文件

参数预置卡备用套文件见表 19。

表 19 参数预置卡备用套电价文件

序号	数 据 项	长度 B	格式	备 注
1	起始码	1	68H	
2	命令码	1	01H	
3	长度	2	HEX	
4	费率 1	4	BCD	××××. ××××
5	…	…	…	…
6	费率 32	4	BCD	××××. ××××
7	阶梯值 1	4	BCD	××××××. ××
8	…	…	…	…
9	阶梯值 6	4	BCD	××××××. ××
10	阶梯电价 1	4	BCD	××××. ××××
11	…	…	…	…
12	阶梯电价 7	4	BCD	××××. ××××
13	年第 1 结算日	3	BCD	月日时
14	年第 2 结算日	3	BCD	月日时
15	年第 3 结算日	3	BCD	月日时
16	年第 4 结算日	3	BCD	月日时
17	两套阶梯切换时间	5	BCD	年月日时分
18	保留	55	HEX	默认为全 00
19	校验码	1	HEX	
20	结束码	1	16H	

6.4.5 电子钱包文件

参数预置卡电子钱包文件见表 20。

表 20 参数预置卡电子钱包文件

序号	数 据 项	长度 B	说 明
1	预置金额	4	HEX，单位为元，2 位小数
2	购电次数	4	HEX，无小数位

6.5 用户卡文件结构

6.5.1 文件目录

用户卡文件目录见表 21。

表 21 用 户 卡 文 件 目 录

文件	内 容 说 明	标识	权限 1	权限 2
MF	主文件	3F00	主控密钥	主控密钥
MKF	密钥文件	0000	…	主控密钥
DF01	电能表应用目录文件	DF01	主控密钥	应用主控密钥
DKF	电能表应用密钥文件	0000	…	应用主控密钥
EF1	参数信息文件	0001	自由＋MAC	明文＋MAC
EF2	电子钱包文件	0002	自由＋MAC	明文＋MAC
EF3	当前套电价文件	0003	自由＋MAC	明文＋MAC
EF4	备用套电价文件	0004	自由＋MAC	明文＋MAC
EF5	返写信息文件	0005	自由	明文＋MAC

6.5.2 参数信息文件

用户卡参数信息文件见表 22。

表 22 用户卡参数信息文件

序号	数 据 项	长度 B	格式	备 注
1	起始码	1	68H	
2	命令码	1	01H	
3	长度	2	HEX	
4	保留	1	HEX	
5	参数更新标志位	1	HEX	
6	保留	4	HEX	默认为全 00
7	两套分时费率切换时间	5	BCD	年月日时分
8	保留	1	00H	
9	报警金额 1	4	BCD	××××××．××
10	报警金额 2	4	BCD	××××××．××

表 22（续）

序号	数 据 项	长度 B	格式	备 注
11	电流互感器变比	3	BCD	××××××
12	电压互感器变比	3	BCD	××××××
13	表号	6	BCD	
14	客户编号	6	BCD	
15	电卡类型	1	BCD	
16	校验码	1	HEX	
17	结束码	1	16H	

6.5.3 电子钱包文件

用户卡电子钱包文件见表 23。

表 23 用户卡电子钱包文件

序号	数 据 项	长度 B	说 明
1	购电金额	4	HEX，单位为元，2 位小数
2	购电次数	4	HEX，无小数位

6.5.4 当前套电价文件

用户卡当前套电价文件见表 24。

表 24 用户卡当前套电价文件

序号	数 据 项	长度 B	格式	备 注
1	起始码	1	68H	
2	命令码	1	01H	
3	长度	2	HEX	
4	费率 1	4	BCD	××××．××××
5	…	…	…	…
6	费率 32	4	BCD	××××．××××
7	阶梯值 1	4	BCD	××××××．××
8	…	…	…	…
9	阶梯值 6	4	BCD	××××××．××
10	阶梯电价 1	4	BCD	××××．××××
11	…	…	…	…
12	阶梯电价 7	4	BCD	××××．××××
13	年第 1 结算日	3	BCD	月日时
14	年第 2 结算日	3	BCD	月日时

表 24（续）

序号	数　据　项	长度 B	格式	备　注
15	年第 3 结算日	3	BCD	月日时
16	年第 4 结算日	3	BCD	月日时
17	保留	60	HEX	默认为全 00
18	校验码	1	HEX	
19	结束码	1	16H	

6.5.5　备用套电价文件

用户卡备用套电价文件见表 25。

表 25　用户卡备用套电价文件

序号	数　据　项	长度 B	格式	备　注
1	起始码	1	68H	
2	命令码	1	01H	
3	长度	2	HEX	
4	费率 1	4	BCD	××××．××××
5	…	…	…	…
6	费率 32	4	BCD	××××．××××
7	阶梯值 1	4	BCD	××××××．××
8	…	…	…	…
9	阶梯值 6	4	BCD	××××××．××
10	阶梯电价 1	4	BCD	××××．××××
11	…	…	…	…
12	阶梯电价 7	4	BCD	××××．××××
13	年第 1 结算日	3	BCD	月日时
14	年第 2 结算日	3	BCD	月日时
15	年第 3 结算日	3	BCD	月日时
16	年第 4 结算日	3	BCD	月日时
17	两套阶梯切换时间	5	BCD	年月日时分
18	保留	55	HEX	默认为全 00
19	校验码	1	HEX	
20	结束码	1	16H	

6.5.6　返写信息文件

用户卡返写信息文件见表 26。

表 26　用户卡返写信息文件

序号	数　据　项	长度 B	格式	备　注
1	起始码	1	68H	
2	命令码	1	11H	
3	数据长度	2	HEX	
4	保留	1	HEX	
5	电流互感器变比	3	BCD	××××××
6	电压互感器变比	3	BCD	××××××
7	表号	6	BCD	
8	客户编号	6	BCD	
9	剩余金额	4	HEX	
10	购电次数	4	HEX	
11	透支金额	4	BCD	××××××. ××
12	保留	4	HEX	
13	非法卡插入次数	3	BCD	
14	返写日期时间	5	BCD	年月日时分
15	校验码	1	HEX	
16	结束码	1	16H	

7　费控相关功能

7.1　费控功能总体要求

电能表费控功能的总体要求如下：

a）　本地费控电能表是在电能表本地实现费控功能的电能表。本地费控电能表支持 CPU 卡、射频卡等固态介质进行充值及参数设置，同时也支持通过虚拟介质远程实现充值、参数设置及控制，即本地预付费与远程预付费是本地费控电能表所应具有的两种预付费方式。本地费控电能表的费控功能都是在电能表内部实现的；

b）　远程费控电能表，本地主要实现计量功能，不支持本地计费功能。计费功能应由远程的主站/售电系统完成，当用户欠费时由远程主站/售电系统发送跳闸命令，给用户断电；当用户充值后，远程主站/售电系统再发送合闸命令，为用户合闸。

7.2　安全认证功能

电能表均应支持安全认证功能，应通过电能表内嵌 ESAM 采用加密保护方式进行身份认证、红外认证、对传输数据进行加密保护和 MAC 验证，做到数据机密性和完整性保护，有效防止重放攻击和非法操作。

7.2.1　身份认证

身份认证包含以下要求：

a）　身份认证功能包括本地身份认证功能和远程身份认证功能；

b）　使用 CPU 卡对电能表进行参数设置或用户充值时，应先进行本地身份认证，认证通过方可进行后续操作；

c） 远程身份认证不通过或身份认证失效后，电能表应不允许进行远程充值、参数设置、密钥更新、数据回抄、远程控制、电能表清零等操作。

7.2.2 红外认证

红外认证包含以下要求：

a） 使用红外通信接口读写关键数据前应先进行红外认证，打开操作权限；红外认证不通过或红外认证失效后，电能表的关键数据不允许读出，所有参数均不允许设置；

b） 红外认证功能只能通过红外通信接口实现；

c） 停电唤醒情况下，电能表应不支持红外认证功能。

7.2.3 数据加密保护

数据加密保护应满足以下要求：

a） 电能表应支持明文＋MAC 和密文＋MAC 设置参数的功能；

b） 电能表应先验证 MAC 校验的有效性，验证通过方可进行后续操作；

c） 电能表应采用解密和验证 MAC 的方式验证数据的有效性，具有防攻击能力。

7.3 初始化功能

本地费控电能表既支持本地初始化功能，又支持远程初始化功能，本地初始化功能通过参数预置卡实现，远程初始化功能通过电子钱包初始化命令实现。远程费控电能表不支持初始化功能。

初始化操作应满足的条件：

a） 电能表内所有密钥均应为测试密钥；

b） 参数预置卡及远程初始化命令中的购电次数为 0。

初始化操作的内容如下：

a） 对电能表内电子钱包文件初始化，不判断囤积金额限值，剩余金额初始化为预置金额，购电次数初始化为 0；

b） 对电能表进行清零操作，同时清本地开户状态、远程开户状态、卡片序列号、非法卡插入次数、远程跳闸状态、远程报警状态，不清客户编号和保电状态；

c） 记录电能表清零记录和购电记录；

d） 购电记录中的购电后总购电次数为 0，购电金额为预置金额，购电前剩余金额为 0，购电后剩余金额和购电后累计购电金额为预置金额；

e） 初始化成功后，如果剩余金额和透支金额限值同时为 0，电能表应处于跳闸状态；否则应处于合闸状态。

7.4 开户功能

开户功能主要用于建立电能表与客户之间的对应关系。本地费控电能表既支持本地开户功能，又支持远程开户功能。本地开户功能通过用户卡建立电能表与客户之间、电能表与用户卡之间的对应关系；远程开户功能通过红外接口、RS-485 接口或载波模块通信接口等以通信方式建立电能表与客户间的对应关系，不能建立电能表与用户卡的对应关系。

开户操作应满足的条件：

a） 购电次数为 0 或 1 的开户卡或远程开户命令；

b） 开户卡中的表号与电能表的表号一致；

c） 对于已开户的电能表，使用本地开户卡开户时，开户卡中的客户编号应与电能表中的客户编号一致；

d） 对于已开户的电能表，使用远程开户命令开户时，命令中的客户编号应与电能表中的客户编号一致。

开户操作的内容：

a） 电能表开户时，如开户命令或开户卡中的购电次数比表内购电次数大 1，应开户并充值，如购

电次数相等，则只开户，不充值；

b） 对于未开户的电能表，插开户卡时，直接开户，开户成功后应保存卡序列号和客户编号，设置电能表为本地已开户状态；

c） 对于未开户的电能表，收到远程开户命令，直接开户，开户成功后应保存客户编号，设置电能表为远程已开户状态；

d） 对于已开户的电能表，插开户卡时，如客户编号一致，则按照本地开户流程操作，同时设置本地已开户状态；

e） 对于已开户的电能表，收到远程开户命令，如客户编号一致，则按照远程开户流程操作，同时设置远程已开户状态；

f） 本地费控电能表客户编号只允许开户时修改，不支持远程修改。

7.5 充值功能

电能表充值功能是在电能表剩余金额的基础上增加购电金额完成的充值操作。电能表应既支持本地充值功能，又支持远程充值功能。

执行充值操作应满足的条件：

a） 未开户电能表不接受充值操作；

b） 电能表充值前应先判断客户编号的一致性；

c） 使用用户卡充值前应判断表号的一致性；

d） 使用购电卡充值前应判断卡片序列号的一致性；

e） 当充值数据帧中的购电次数或用户卡中的购电次数比电能表内的购电次数大 1，并且购电金额加上表内的剩余金额小于等于囤积金额限值（如果囤积金额限值设为 0，在充值时按照 999999.99 处理）时，才可充值；

f） 对于远程开户的电能表，只接受开户卡和补卡操作，不接受购电卡操作；

g） 对于远程开户并远程充值过的电能表，电能表中的购电次数大于 1 时，只接受补卡而不接受开户卡和购电卡操作。

充值操作的内容：

a） 电能表在满足充值操作条件时，对电能表 ESAM 中的电子钱包文件进行充值操作。具体操作应包括将充值金额与 ESAM 中的剩余金额进行累加，购电次数加 1，充值成功后，应保存购电事件记录；

b） 充值操作前，电能表处于合闸状态时，充值成功后，仍保持合闸状态；

c） 充值操作前，电能表处于远程合闸允许、本地跳闸但透支金额未达到透支金额限值时，本地充值成功后，应立即合闸；

d） 充值操作前，电能表处于远程合闸允许、本地跳闸且透支金额达到透支金额限值时，本地充值成功后，只有剩余金额大于合闸允许金额时，方可合闸。

7.6 用户卡返写功能

为方便售电系统判断表内的运行状态，在用户插卡时应返写电能表运行信息。售电系统对用户卡进行开户、售电和补卡操作时，须将返写信息文件清为全 00。

用户卡返写应满足的条件：

a） 插开户卡时，身份认证通过且表号一致；

b） 插购电卡时，身份认证通过且表号、客户编号和卡片序列号均一致；

c） 插补卡时，身份认证通过且表号、客户编号一致。

返写操作的内容：

a） 用户卡中购电次数比表中购电次数大 1 时，执行充值和参数更新功能，然后返写用户卡，并提示成功；

b） 用户卡中购电次数等于表中购电次数时，执行参数更新功能，然后返写用户卡，并提示成功；

c） 用户卡中购电次数小于表中购电次数时，返写用户卡，并提示成功；

d） 用户卡中购电次数比表中购电次数大于等于 2 时，返写用户卡，提示购电次数错误。

7.7 用户卡补卡功能

如用户卡丢失，售电系统应为用户办理补卡业务，新办理的用户卡写为补卡类型。

补卡操作应满足的条件：

a） 电能表已开户；

b） 补卡中的表号和客户编号应与电能表的表号和客户编号一致。

补卡操作的内容：

使用补卡的卡片序列号替换电能表中保存的原卡片序列号，然后进行充值、更新参数，返写等操作。

7.8 卡片操作要求

在参数更新和插卡提示方面，对用户卡操作时间和操作方法应满足如下要求。

a） 参数更新应满足的条件：

1） 插参数预置卡时，电能表应先读出预置卡的全部信息，然后再写 ESAM，所有信息从卡中读出后即可拔卡，如果未读完拔卡，则不预置参数；

2） 与参数预置卡相关的所有操作应在 10s 内完成，否则不预置参数；

3） 插用户卡更新参数时，电能表应先读出用户卡的全部信息，然后再写 ESAM，所有信息从卡中读出后即可拔卡，如果未读完拔卡，则不更新参数；

4） 如用户卡不更新参数，所有操作应在 3s 内完成；如用户卡更新参数，所有操作应在 10s 内完成。

b） 插卡提示如下：

1） 插参数预置卡时，电能表显示“读卡中”，预置成功后显示“读卡成功”，同时显示预置后剩余金额；

2） 插用户卡时，电能表显示“读卡中”，充值成功后显示“读卡成功”，同时显示充值前剩余金额，延时 2s 后显示充值后剩余金额；

3） 电能表插卡时应有声音提示功能，读卡成功蜂鸣器应发出“嘀……”的一声长鸣，读卡失败蜂鸣器应发出“嘀、嘀、嘀”的三声短鸣；

4） 插卡后同时点亮背光，如无操作，60s 后关闭背光。

7.9 密钥更新功能

电能表应支持密钥更新功能，实现密钥状态的切换，包括密钥的下装与恢复，电能表内所有密钥只能通过远程方式更新。

密钥更新操作应满足的条件：

a） 接收的密钥更新报文中的密钥总条数应等于参变量中的密钥总条数；

b） 接收的密钥更新报文中所有密钥的密钥状态必须一致；

c） 接收到的不同密钥编号的密钥条数应等于密钥总条数；

d） 接收的每帧报文 MAC 验证应通过。

密钥更新操作的内容：

a） 密钥密文信息应保存到电能表的内部存储器中；

b） 接收相同密钥编号的数据，应使用新接收的数据覆盖原数据；

c） 接收到不同密钥编号的密钥条数等于密钥总条数时启动密钥更新操作；

d） 密钥更新时按照编号从小到大依次更新；

e） 如更新过程中出现断电重启，重启后应自动补更新；

f） 密钥状态应与密钥更新同步，每成功更新一条密钥同时更新该密钥对应的密钥状态位。

7.10 参数更新功能

电能表应既支持本地参数更新功能，又支持远程参数更新功能。本地参数更新应支持参数预置卡更新和用户卡更新两种方式。

执行参数更新操作应满足的条件：

a） 通过参数预置卡更新参数时，根据参数更新标志位修改对应的参数；

b） 通过用户卡更新参数时，应满足卡内购电次数比电能表的购电次数大 1，或卡内购电次数与电能表的购电次数相等且用户卡返写信息文件为空；

c） 通过载波或 RS-485 通信接口远程更新参数时，应满足远程身份认证通过并在身份认证有效时间内；

d） 通过红外通信接口更新参数时，应先通过红外认证命令打开红外操作权限，然后再进行远程身份认证，认证通过并在身份认证有效时间内方可更新参数。

参数更新操作的内容：

a） 通过参数预置卡更新电能表中的两套电价文件和其他参数，成功后应记录清零记录和购电记录，不记录编程事件记录；

b） 根据参数更新标志位，通过开户卡可更新电能表中的两套电价文件和其他参数，购电卡和补卡仅能更新备用套电价文件，不支持更新当前套电价文件和其他参数，更新成功后应保存编程事件记录；

c） 通过载波、红外或 RS-485 通信方式远程更新参数时，应以 98 级或 99 级加密保护方式进行，更新成功后应保存编程事件记录，具体参见 DL/T 645—2007 及备案文件；

d） 修改表号时，电能表内所有密钥状态均应为测试密钥。

7.11 数据回抄功能

电能表应支持数据回抄功能，具体要求如下：

a） 回抄数据应带 MAC 返回；

b） 抄读电子钱包文件时，剩余金额和购电次数应分别带 MAC 返回；

c） 应支持抄读 ESAM 中的所有文件和数据。

7.12 远程控制功能

电能表应支持远程控制功能，远程控制包括跳闸、合闸允许、直接合闸、跳闸自动恢复、报警、报警解除、保电和保电解除。

远程控制操作的内容：

a） 保电命令优先级高于远程跳闸命令，远程跳闸命令优先级高于本地合闸命令；

b） 电能表在跳闸状态时收到远程跳闸命令，应回正常应答帧；

c） 电能表在执行跳闸命令延时过程中掉电，重新上电后应立即跳闸；

d） 电能表在跳闸状态时收到合闸允许命令等待合闸的过程中掉电，重新上电后应继续停留在等待合闸的合闸允许状态；

e） 电能表在保电状态时收到远程跳闸命令，应返回含未授权信息的错误应答帧；

f） 跳闸自动恢复命令，不受跳闸延时时间限制，直接执行；

g） 电能表在执行跳闸自动恢复命令过程中掉电，重新上电后应立即处于合闸允许或者合闸状态；

h） 远程跳闸、合闸和保电命令优先级高于跳闸自动恢复命令，在跳闸自动恢复过程中收到远程跳闸、合闸或保电命令，原未执行完的跳闸自动恢复操作停止执行；

i） 跳闸自动恢复命令在电能表处于保电、远程跳闸（含延时）、合闸允许、本地达到透支门限跳闸、本地达到报警金额 2 或者过零跳闸时均返回异常应答帧；只有电能表在合闸状态时，才允许执行跳闸自动恢复命令；

j） 跳闸自动恢复时间过程中再次接收到跳闸自动恢复命令，电能表返回正常应答帧，并且以当前

接收命令中延时时间重新开始计时；

k） 远程控制命令应答帧中同时返回控制命令执行状态字或错误状态字。正常应答帧返回控制命令执行状态，异常应答帧中返回错误状态字。

跳合闸事件记录说明：

a） 如继电器发生动作，应记录跳合闸事件记录；

b） 事件记录的操作者代码应为动作命令的发出者，发生时刻应为继电器动作时刻。

7.13 事件记录功能

电能表应具有事件记录功能，具体要求如下：

a） 电能表事件记录说明：

1） 插参数预置卡时应记录电能表清零记录和购电记录；

2） 电子钱包初始化命令应记录电能表清零记录和购电记录；

3） 远程清零命令应记录清零记录；

4） 插用户卡时应记录编程记录、费率表编程记录、阶梯表编程记录和购电记录；

5） 执行远程退费命令应记录退费记录；

6） 插卡出现异常时应记录异常插卡记录；

7） 电能表负荷开关动作时应记录拉、合闸记录；

8） 电能表密钥更新时，应记录密钥更新记录；

9） 远程设置费率电价时，应记录费率表编程记录；

10）远程设置阶梯参数时，应记录阶梯表编程记录。

b） 编程记录说明：

1） 身份认证通过，电能表进入编程状态，出现身份认证时效到、收到身份认证失效命令、再次收到身份认证命令或检测到有卡片插入任意一种情况时，结束该编程状态；

2） 检测到卡片插入，电能表进入编程状态，卡片拔出，结束该编程状态；

3） 在电能表进入编程状态到结束编程状态期间，对电能表进行编程操作，应记录编程记录；

4） 使用卡片设置参数时，编程事件记录中的数据标识为9998＋命令码（卡片格式中）＋更新标志位，操作者代码为卡片序列号的低4字节。

c） 异常插卡记录说明：

1） 异常插卡时，如电能表不能正常读出卡片序列号，记录中的卡序列号应记为全FF；

2） 当操作ESAM或卡片时，异常插卡记录中的命令头记为指令的前5个字节，当未操作ESAM或卡片时，异常插卡记录中的命令头记为全00；

3） 当操作ESAM或卡片时，如ESAM或卡片有应答，则错误响应状态为应答码，其他情况下错误响应状态记为全00。

7.14 清零功能

电能表应具有清零功能，具体要求如下：

a） 本地费控电能表应通过参数预置卡和电子钱包初始化命令实现电能表清零功能，不支持远程电能表清零命令；

b） 远程费控电能表只能通过远程清零命令实现电能表清零功能，不支持电子钱包初始化命令；

c） 清除除电能表清零事件记录以外的所有事件记录，同时保存该次电能表清零事件记录；

d） 清除电能表内电能量、最大需量及发生时间、冻结量、负荷记录、远程跳闸状态、远程报警状态，不清保电状态；电表清零后，电表处于合闸状态。

7.15 软件比对功能

电能表应具有软件比对功能，具体要求如下：

a） 加密保护比对数据的密钥应采用比对因子对ESAM内的密钥进行分散；

b） 比对操作时应采用绝对地址，分多包分别进行；
c） 电能表采用 CPU 个数应不大于 8 个；
d） 允许电能表在程序存储器中最多开辟两个区域存储默认参数；
e） 电能表生产时应将软件备案号固化到电能表中，并能通过通信方式读出。

8 费控相关功能检测

8.1 安全认证功能检测

电能表均应支持安全认证功能，做好机密性和完整性保护，有效防止重放攻击和非法操作。测试安全认证功能时，至少应测试如下内容：

a） 本地身份认证功能和远程身份认证功能；
b） 身份认证时效和身份认证失效的执行；
c） 各种通信接口的红外认证执行；
d） 红外认证时效和红外认证失效的执行情况；
e） 停电唤醒情况下，电能表的红外认证功能执行情况；
f） 电能表解密和 MAC 校验的执行情况；
g） 电能表防攻击能力及电能表挂起功能；
h） 电能表的防伪造卡攻击能力；
i） 频繁通断电对电能表 ESAM 的影响。

8.2 费控功能检测

8.2.1 初始化功能

本地费控电能表应支持初始化功能，远程费控电能表应不支持该功能。测试初始化功能时，至少应测试如下内容：

a） 参数预置卡初始化功能和电子钱包初始化功能；
b） 密钥状态、购电次数、囤积金额限值、合闸允许金额限值等参数对初始化功能的影响；
c） 开户状态、卡片序列号、非法卡插入次数、远程跳闸状态、远程报警状态、客户编号和保电状态等状态信息的清除情况；
d） 参数预置卡的参数更新功能执行情况；
e） 电能表清零记录和购电记录；
f） 电能表的跳合闸状态。

8.2.2 开户功能检测

本地费控电能表应支持该功能，远程费控电能表应不支持该功能。测试开户功能时，至少应测试如下内容：

a） 远程开户功能和本地开户功能；
b） 表号、客户编号、卡片序列号、购电次数、囤积金额限值等参数对开户功能的影响；
c） 开户状态、客户编号、卡片序列号等信息的保存；
d） 用户卡的返写功能执行情况；
e） 参数更新功能执行情况；
f） 购电记录；
g） 未开户电能表，购电卡和补卡的执行情况。

8.2.3 充值功能检测

本地费控电能表应支持该功能，远程费控电能表应不支持该功能。测试充值功能时，至少应测试如下内容：

a） 本地充值功能和远程充值功能；

b） 未开户电能表的充值功能执行情况；
c） 表号、客户编号、卡片序列号、购电次数、囤积金额限值等参数对充值功能的影响；
d） 电能表 ESAM 电子钱包文件的累加；
e） 用户卡的返写功能执行情况；
f） 参数更新功能执行情况；
g） 购电记录；
h） 电能表的跳合闸状态。

8.2.4 补卡功能检测

本地费控电能表应支持该功能，远程费控电能表应不支持该功能。测试补卡功能时，至少应测试如下内容：

a） 本地或远程开户状态下的补卡功能；
b） 未开户电能表的补卡功能；
c） 表号、客户编号、购电次数、囤积金额限值等参数对补卡功能的影响；
d） 电能表 ESAM 电子钱包文件的累加；
e） 用户卡的返写功能执行情况；
f） 参数更新功能执行情况；
g） 卡片序列号等信息的保存；
h） 购电记录；
i） 电能表的跳合闸状态。

8.2.5 费控结算功能检测

本地费控电能表应支持该功能，远程费控电能表应不支持该功能。测试费控结算功能时，至少应测试如下内容：

a） 费率和阶梯的切换和执行情况；
b） 互感器变比对计费功能的影响；
c） 报警金额、透支金额限值、合闸允许金额限值等参数对费控结算功能的影响；
d） 执行过程中的液晶显示和背光提示功能；
e） 电能表的跳合闸状态；
f） 事件记录和冻结记录。

8.3 密钥更新功能检测

电能表均应支持该功能，测试密钥更新功能时，至少应测试如下内容：

a） 密钥更新功能的执行情况；
b） 密钥总条数、密钥状态、密钥编号、MAC 验证等信息对密钥更新功能的影响；
c） 断电重启对该功能的影响；
d） 密钥状态、密钥显示符号等信息的提示功能。

8.4 参数更新功能检测

8.4.1 参数更新

本地费控电能表应支持本地参数更新和远程参数更新，其他类型电能表应支持远程参数更新。测试参数更新功能时，至少应测试如下内容：

a） 本地参数更新应验证参数预置卡、用户卡进行参数更新的执行情况；
b） 本地参数更新应验证密钥状态、参数更新标志位、卡内购电次数、返写信息文件等信息对该功能的影响；
c） 本地参数更新时，验证快速拔卡对参数更新的影响，应保证快速拔卡时所有参数均更新成功；
d） 红外认证功能对远程参数更新的影响；

e） 远程参数更新功能的执行情况；

f） 编程事件记录。

8.4.2 电价切换

本地费控电能表应支持电价切换，包括费率电价切换和阶梯电价切换；其他类型电能表不支持该功能。测试电价切换功能时，至少应测试如下内容：

a） 通过本地参数更新功能进行电价修改的执行情况；

b） 通过数据块方式进行远程电价修改的执行情况；

c） 电价切换执行情况和切换后的计费情况；

d） 电价切换冻结记录；

e） 电能表运行状态字、液晶显示等信息的提示功能。

8.4.3 数据回抄

电能表均应支持该功能，通过数据回抄功能可以读取 ESAM 中的所有数据。测试数据回抄功能时，至少应测试如下内容：

a） ESAM 中的所有文件支持该功能；

b） 回抄数据 MAC 校验应正确。

8.4.4 远程控制功能检测

费控电能表应支持远程控制功能，远程控制功能包括跳闸、合闸允许、直接合闸、跳闸自动恢复、报警、报警解除、保电和保电解除功能。测试远程控制功能时，至少应测试如下内容：

a） 保电命令、远程跳闸命令、远程合闸命令、本地跳合闸命令和跳闸自动恢复命令的优先级执行情况；

b） 电能表命令有效截止时间的执行情况；

c） 电能表执行远程控制命令时，应答帧的响应情况，及应答帧中控制命令执行状态字或错误状态字的情况；

d） 跳合闸命令执行过程中，掉电重新上电的执行情况；

e） 跳合闸事件记录；

f） 跳闸自动恢复命令执行过程中，掉电重新上电的执行情况。

8.4.5 事件记录

电能表均应支持该功能。测试事件记录功能时，至少应测试如下内容：

a） 清零、购电、编程、费率电能表编程、阶梯电能表编程、电子钱包扣减、异常插卡、跳合闸、密钥更新等事件记录的记录情况；

b） 编程记录的发生时刻、操作者代码、数据标识的记录情况；

c） 异常插卡记录的卡片序列号、命令头、错误响应状态等信息的记录情况；

d） 电能表清零记录的永久记录情况。

8.4.6 电能表清零

本地费控电能表应支持参数预置卡和电子钱包初始化命令进行电能表清零，不支持远程电能表清零命令；其他电能表应只支持远程电能表清零命令，不支持电子钱包初始化命令。测试电能表清零功能时，至少应测试如下内容：

a） 本地费控电能表开户状态、卡片序列号、非法卡插入次数、远程跳闸状态、远程报警状态、客户编号和保电状态等状态信息的清除情况；

b） 电能表事件记录的清除情况；

c） 电能表清零事件记录的记录情况；

d） 电能表内电能量、最大需量及发生时间、冻结量、负荷记录等数据的清除。

附 录 A
（规范性附录）
智能电能表费控功能操作流程

A.1 CPU 卡操作流程

A.1.1 身份认证流程

进入身份认证操作流程后，主要操作如下：

a） 读取卡片序列号；
b） 从 ESAM 中取随机数；
c） 电能表使用卡片序列号对 ESAM 内嵌密钥进行分散，产生过程密钥；
d） 使用过程密钥对随机数进行加密得到密文 1；
e） 使用卡片对随机数进行加密得到密文 2；
f） 比较密文 1 和密文 2 是否相等；
g） 相等则认证通过，不相等则置错误标志；
h） 身份认证操作完成。

A.1.2 CPU 卡操作主流程

进入 CPU 卡操作流程后，主要操作如下：

a） 判断电能表是否电压过低，如果电压过低，置错误信息字，跳转到步骤 h)；
b） 电能表显示“读卡中”，同时点亮背光；
c） 对 CPU 卡进行复位；
d） 对 ESAM 进行复位；
e） 选择 CPU 卡应用目录文件；
f） 读取 CPU 卡命令字，根据卡片命令字进入参数预置卡或用户卡处理流程；
g） 对参数预置卡或用户卡进行处理；
h） 若插卡成功，显示“读卡成功”，并根据卡片类型的相关要求显示；若插卡失败，则显示“读卡失败”，并显示异常错误代码；
i） 插卡操作结束。

A.1.3 参数预置卡操作流程

进入参数预置卡操作流程后，主要操作如下：

a） 系统身份认证；
b） 判断所有密钥是否均为测试密钥，如果全为测试密钥继续，否则置错误标志，跳转到步骤 i)；
c） 读参数预置卡指令信息文件，判断文件是否合法，如果不合法，置错误标志，跳转到步骤 i)，如合法继续；
d） 带 MAC 读取参数预置卡中的电子钱包文件，暂存于电能表中；
e） 更新 ESAM 中的电子钱包文件；
f） 根据参数更新标志位带 MAC 读取参数预置卡中的参数，暂存于电能表中；
g） 更新 ESAM 中的参数；
h） 电能表初始化；
i） 参数预置卡操作结束。

A.1.4 用户卡操作主流程

进入用户卡操作流程后，主要操作如下：

a） 对 ESAM 中的电子钱包文件进行扣减；

b） 系统身份认证；

c） 读用户卡指令信息文件，判断文件是否合法，如果不合法，置错误标志，跳转到步骤 h），如合法继续；

d） 用户卡权限外部认证；

e） 判断表号是否一致；

f） 读用户卡电子钱包文件；

g） 根据用户卡类型进入开户卡、购电卡或补卡操作流程；

h） 用户卡操作结束。

A.1.5 开户卡操作流程

进入开户卡操作流程后，主要操作如下：

a） 判断电能表开户状态，如果电能表未开户，跳转到步骤 c），否则继续；

b） 判断客户编号是否一致，如不一致，置错误标志，跳转到步骤 n），否则继续；

c） 判断开户卡中的购电次数是否为 0 或 1，如不为 0 或 1 置错误标志，跳转到步骤 n），否则继续；

d） 判断用户卡与电能表中的购电次数，如果卡内购电次数小于电能表内购电次数，跳转到步骤 l），如果卡内购电次数比电能表内购电次数大 1，跳转到步骤 f），如果购电次数相等继续；

e） 判断用户卡返写信息文件是否为空，如果不为空，判断卡片序列号是否一致，如果一致跳转到步骤 m），如不一致，置错误标志，跳转到步骤 n），如果为空，跳转到步骤 j）；

f） 判断用户卡返写信息文件是否为空，如果不为空，置错误标志，跳转到步骤 m），如果为空继续；

g） 判断剩余金额是否超囤积，如果超囤积，则置错误标志，跳转到步骤 n），否则继续；

h） 带 MAC 读取用户卡中的客户编号和电子钱包文件，暂存于电能表中；

i） 更新 ESAM 中的客户编号和电子钱包文件；

j） 根据参数更新标志位带 MAC 读取用户卡中的参数，暂存于电能表中；

k） 更新 ESAM 中的参数；

l） 保存开户卡的卡序列号，设置电能表本地已开户状态；

m） 返写用户卡返写信息文件；

n） 开户卡操作结束。

A.1.6 购电卡操作流程

进入购电卡操作流程后，主要操作如下：

a） 判断电能表开户状态，如果电能表未开户，则置错误标志，跳转到步骤 l），否则继续；

b） 判断客户编号和卡片序列号是否一致，如不一致，置错误标志，跳转到步骤 l），否则继续；

c） 判断用户卡与电能表中的购电次数，如果卡内购电次数小于电能表内购电次数，跳转到步骤 k），如果卡内购电次数比电能表内购电次数大 1，跳转到步骤 e），如果用户卡中购电次数比电能表中购电次数大于等于 2 时，置错误标志，跳转到步骤 k），如果购电次数相等继续；

d） 判断用户卡返写信息文件是否为空，如果不为空，跳转到步骤 k），如果为空，跳转到步骤 i）；

e） 判断用户卡返写信息文件是否为空，如果不为空，置错误标志，跳转到步骤 k），如果为空继续；

f） 判断剩余金额是否超囤积，如果超囤积，则置错误标志，跳转到步骤 l），否则继续；

g） 带 MAC 读取用户卡中的电子钱包文件，暂存于电能表中；

h） 更新 ESAM 中的电子钱包文件；

i） 根据参数更新标志位带 MAC 读取用户卡中的参数，暂存于电能表中；

j） 更新 ESAM 中的参数；

k） 返写用户卡返写信息文件；

l） 购电卡操作结束。

A.1.7 补卡操作流程

进入补卡操作流程后，主要操作如下：

a） 判断电能表开户状态，如果电能表未开户，则置错误标志，跳转到步骤 m），否则继续；

b） 判断客户编号是否一致，如不一致，置错误标志，跳转到步骤 m），否则继续；

c） 判断用户卡与电能表中的购电次数，如果卡内购电次数小于电能表内购电次数，跳转到步骤 k），如果卡内购电次数比电能表内购电次数大 1，跳转到步骤 e），如果用户卡中购电次数比电能表中购电次数大于等于 2，置错误标志，跳转到步骤 l），如果购电次数相等继续；

d） 判断用户卡返写信息文件是否为空，如果不为空，判断卡片序列号是否一致，如果一致跳转到步骤 l），如不一致，置错误标志，跳转到步骤 m），如果为空，跳转到步骤 i）；

e） 判断用户卡返写信息文件是否为空，如果不为空，置错误标志跳转到步骤 l），如果为空继续；

f） 判断剩余金额是否超囤积，如果超囤积，则置错误标志，跳转到步骤 m），否则继续；

g） 带 MAC 读取用户卡中的电子钱包文件，暂存于电能表中；

h） 更新 ESAM 中的电子钱包文件；

i） 根据参数更新标志位带 MAC 读取用户卡中的参数，暂存于电能表中；

j） 更新 ESAM 中的参数；

k） 保存补卡的卡序列号；

l） 返写用户卡返写信息文件；

m） 补卡操作结束。

A.2 远程操作流程

A.2.1 远程身份认证流程

进入远程身份认证操作流程后，主要操作如下：

a） 读取 ESAM 的序列号；

b） 电能表使用分散因子对 ESAM 内嵌密钥进行分散，产生过程密钥；

c） 使用过程密钥对随机数进行加密得到密文 1；

d） 比较密文 1 与接收报文中的密文是否相等；

e） 相等则认证通过，再从 ESAM 中读取新的随机数 2，返回随机数 2 和 ESAM 的序列号，跳转到步骤 g）；

f） 不相等，置错误标志；

g） 身份认证操作完成。

A.2.2 电子钱包初始化流程

进入电子钱包初始化操作流程后，主要操作如下：

a） 判断是否为本地费控电能表，如不是，置错误标志，跳转到步骤 g）；

b） 判断身份认证时效是否有效，如无效，置错误标志，跳转到步骤 g）；

c） 判断所有密钥是否均为测试密钥，如不是，置错误标志，跳转到步骤 g）；

d） 判断电子钱包初始化命令中的购电次数是否为 0，如不是，置错误标志，跳转到步骤 g）；

e） 对 ESAM 中的电子钱包文件进行预置；

f） 电能表初始化；

g） 电子钱包初始化操作结束。

A.2.3 远程开户流程

进入远程开户操作流程后，主要操作如下：

a） 判断身份认证时效是否有效，如无效，置错误标志，跳转到步骤 i）；
b） 判断电能表是否已开户，如未开户，则跳转到步骤 d）；
c） 判断开户命令与电能表中的客户编号是否一致，如不一致，置错误标志，跳转到步骤 i）；
d） 判断开户命令中的购电次数是否为 0 或 1，如不是，置错误标志，跳转到步骤 i）；
e） 判断开户命令与电能表中的购电次数，如开户命令的购电次数等于电能表内购电次数，跳转到步骤 h），如果开户命令的购电次数比电能表内购电次数大 1，继续，否则置错误标志，跳转到步骤 i）；
f） 判断剩余金额是否超囤积，如超囤积，则置错误标志，跳转到步骤 i）；
g） 对 ESAM 中的电子钱包文件充值；
h） 电能表保存客户编号，并置电能表远程已开户状态；
i） 远程开户操作结束。

A.2.4 远程充值流程

进入远程充值操作流程后，主要操作如下：

a） 判断身份认证时效是否有效，如无效，置错误标志，跳转到步骤 g）；
b） 判断电能表是否已开户，如未开户，则跳转到步骤 g）；
c） 判断充值命令与电能表中的客户编号是否一致，如不一致，置错误标志，跳转到步骤 g）；
d） 判断充值命令与电能表中的购电次数，如充值命令的购电次数比电能表内购电次数大 1 继续，否则置错误标志，跳转到步骤 g）；
e） 判断剩余金额是否超囤积，如超囤积，则置错误标志，跳转到步骤 g）；
f） 对 ESAM 中的电子钱包文件充值；
g） 远程充值操作结束。

A.2.5 远程参数更新流程

进入远程参数更新操作流程后，主要操作如下：

a） 判断电能表是否挂起，如挂起，置错误标志，跳转到步骤 e）；
b） 判断身份认证时效是否有效，如无效，置错误标志，跳转到步骤 e）；
c） 判断解密或 MAC 校验是否正确，如错误，置错误标志，跳转到步骤 e）；
d） 进行参数设置；
e） 远程参数更新操作结束。

A.2.6 密钥更新流程

进入密钥更新操作流程后，主要操作如下：

a） 判断身份认证时效是否有效，如无效，置错误标志，跳转到步骤 h）；
b） 判断密钥内容 MAC 校验是否正确，如错误，置错误标志，跳转到步骤 h）；
c） 判断本条命令的密钥总条数与参数中的密钥总条数是否一致，如不一致，置错误标志，跳转到步骤 h）；
d） 判断本条命令中各条密钥的密钥状态位是否一致，如不一致，置错误标志，跳转到步骤 h）；
e） 根据密钥编号确定密钥保存位置并保存密钥；
f） 根据密钥总条数、密钥编号和密钥状态判断收集到的密钥是否齐全，如果不齐全，则跳转到步骤 h）；
g） 逐条更新 ESAM 中的密钥，同时更新对应密钥的状态位；
h） 密钥更新操作结束。

A.2.7 数据回抄流程

进入数据回抄操作流程后，主要操作如下：

a） 判断身份认证时效是否有效，如无效，置错误标志，跳转到步骤 g）；

b） 判断数据回抄标识是否合法，如不合法，置错误标志，跳转到步骤 g）；
c） 刷新 ESAM 中的电子钱包文件，刷新 ESAM 运行信息文件；
d） 判断是否抄读 ESAM 中的电子钱包文件，如不是，则跳转到步骤 f）；
e） 带 MAC 读取 ESAM 电子钱包文件的剩余金额和购电次数，跳转到步骤 g）；
f） 带 MAC 读取 ESAM 文件数据；
g） 数据回抄操作结束。

A.2.8 远程控制流程

进入远程控制操作流程后，其主要流程如下：
a） 判断电能表是否挂起，如挂起，置错误标志，跳转到步骤 f）；
b） 判断身份认证时效是否有效，如无效，置错误标志，跳转到步骤 f）；
c） 判断解密或 MAC 校验是否正确，如错误，置错误标志，跳转到步骤 f）；
d） 判断电能表当前时间是否超过命令有效截止时间，如超过，置错误标志，跳转到步骤 f）；
e） 执行远程控制操作；
f） 远程控制操作结束。

附 录 B
（资料性附录）
费控功能配置推荐表

序号	功能	智能电能表	远程费控智能电能表	本地费控智能电能表
1	身份认证	•	•	•
2	红外认证	•	•	•
3	初始化			•
4	开户			•
5	充值			•
6	用户卡			•
7	预置卡			•
8	密钥更新	•	•	•
9	参数更新	•	•	•
10	数据回抄	•	•	•
11	远程控制		•	•
12	事件记录	•	•	•
13	远程电表清零	•	•	
14	软件比对	•	•	•
15	保电		•	•
16	费率电价			•
17	阶梯电价			•
18	本地计费			•
19	电价切换			•

中 华 人 民 共 和 国
电 力 行 业 标 准
智能电能表信息交换安全
认 证 技 术 规 范
DL / T 1491 — 2015
*
中国电力出版社出版、发行
（北京市东城区北京站西街 19 号 100005 http://www.cepp.sgcc.com.cn）
北京博图彩色印刷有限公司印刷
*
2015 年 11 月第一版 2015 年 11 月北京第一次印刷
880 毫米×1230 毫米 16 开本 2.25 印张 62 千字
印数 0001—3000 册
*
统一书号 155123 • 2678 定价 **19.00** 元

155123.2678