IC卡预付费电能表的安全性

作者：商洛供电局　丁宏林 李小兵

最近在网上看到一则“罕见的特大盗窃国家电力能源案”相关新闻，称一名某电力仪表厂员工，利用其在单位掌握的“写卡程序”，结合单位报废的旧电卡，充入电量后进行非法个人牟利，窃电额度达40万度之巨，天网恢恢终被法办。

预付费电能表的安全性是否存在巨大隐患呢？此案件的发生将有可能引发社会各界对预付费电表安全性的系统思考。

作为一名具有多年电能表行业工作经验的工作者，我认为我们不能因噎废食，因为一棵树木而放弃整个森林，而应有必要、有责任向社会公众介绍IC卡预付费电能表的相关知识，提高社会公众对IC卡预付费电能表的了解，同时也呼吁业内IC卡预付费电能表各生产厂家进行自我反思，防微杜渐，真正做到对企业自身负责、对行业发展负责、对社会负责。

二、IC卡预付费电能表

1、什么是IC卡预付费电能表

简单来说IC卡预付费电能表是以IC卡作为电能量值数据传输介质，在电能表中加入负荷控制部分等功能模块，从而实现电量抄　　收和电量结算的智能型电能表。

2、近几年IC卡预付费电能表发展状态

95年前，主要为电钥匙IC卡，以93C46和24C01为主IC卡为可擦写存储芯片（EEPROM）或一般存储卡，IC卡存储方便、使用简单、价格便宜，安全性不高，存在被破解的可能性，用户以物业小区为主。95年~99年，主要为电话卡式IC卡，以存储卡（24C01）和逻辑加密卡（4442、4428）为主其中逻辑加密卡（4442、4428）的安全性得到进一步提高，内嵌芯片在存储区外增加了控制逻辑，在访问存储区之前需要核对密码，只有密码正确，才能进行操作。用户从单纯物业小区扩展到电力行业管理部门，开始大规模普及使用，98年~至今，主要为金融级IC卡，以CPU卡（CPU卡和SAM模块为加密介质）为主CPU卡内嵌芯片相当于一个特殊类型的单片机，内部除了带有控制器，存储器，时序控制逻辑等外，还带有算法单元和操作系统（芯片操作系统，简称COS），存储容量大，处理能力强，信息存储安全等特性。率先在北京供电局全面推广，并在天津、云南等城市开始推广。

3、如何实现IC卡表的安全性

一般来说IC卡预付费电能表可从生产过程的安全性、软件控制的安全性、用户密码控制的安全性、生物认证信息提供的安全性等四个方面来保证它的安全性，只有四个环节均得到有效控制才能严格保证IC卡预付费电能表的安全性。

三、CPU卡预付费电能表的选用CPU卡和ESAM模块的技术依据

1、安全性

（1） CPU卡采用密钥管理机制，实现了电能表生产和电能表运营管理的分离，认证过程通过加密算法进行动态运算，在实际应用中被破译和攻击的可能性极小。

（2）同时CPU卡电能表中安装有ESAM模块，安全性由CPU卡和ESAM模块进行相互认证，与电能表内的微控制器无关。这样即实现系统的管理性只与发卡方或管理方有关，而与电能表生产厂家无关。

2、 兼容性：CPU卡的数据信息传输方式遵循ISO7816-3国际标准，CPU卡内芯片升级时无需对预付费电能表内的微控制器程序进行改动，这是存储卡和逻辑加密卡所不能实现的。

3、 可扩展性：由于CPU卡采用文件方式对数据进行存储，并采用密钥管理机制，可实

现预付费电能表、预付费水表、预付费燃气表、预付费热量表一卡通。

4、规范性：CPU 卡相关的操作系统满足金融卡规范，故 CPU 卡可很方便的实现收费管理与银行金融系统的接轨。

5、 详细的密钥管理制度：建立了完善的密钥发行管理体系，制订了详细的密钥管理规定。

四、DDSY251 系列单相静止式 CPU 卡预付费电能表基本功能及技术特点

1、DDSY251 系列

DDSY251 系列单相电子式预付费电能表是新近开发的产品，表计内置有 ESAM 模块（小型 CPU，用于数据加密及安全认证，保证表计具有极高的安全性。）该产品采用专用电能转换芯片 ADE7755 进行电能采样后，经专用微电脑计算处理，换算成电度数；并采用智能 CPU 卡，在电能表与售电系统之间双向传递购买电量和使用电量及用电数据，从而实现电能计量与电费预付功能。

2、基本功能

（1）主要特点：

应用计算机管理、先购电后用电；采用光电耦合器采样电能表脉冲的方式自动计量用电量。在额定电流范围内能限制最大使用功率（由供电管理部门限定）；一表一卡，专卡专用，失卡不失电，补卡再用；IC 卡能双向传递数据；电表具有声（可选）、光报警功能，能提供多种声光报警方式；能自动断电警告用户及时购电，当 IC 卡表内的电量为零时，能自动拉闸断电。

（2）电能计量功能：

采用专用数字计量电路，能精确计量单相有功绝对值电量。

（3）过电流保护功能：

对用户负荷进行动态实时监控，在设定的持续时间内，当负荷超过设定阈值后，IC 卡表能自动拉闸断电，用户可选择插卡后立即响应或延时指定分钟后自动恢复供电。

（4）剩余电量报警功能：

电表内设有 2 级报警电量，当剩余电量小於报警电量 2 时，报警指示灯点亮，提醒用户去购电，当剩余电量小于报警电量 1 时，拉闸继电器动作，切断用户用电。用户插卡响应以后，电表可以恢复供电，直至表内的剩余电量为零。

（5）背光控制功能：

家电遥控器点亮液晶背光或插入卡片时，背光点亮，使液晶屏能清晰地显示电表的数据，便于在黑暗环境下观察电表。当显示完相应的内容后，背光熄灭。

（6）脉冲输出功能：

产品有二种脉冲输出方式。一为电表面板上的红外发光管，此脉冲接口主要用于脉冲指示及非接触式验表；二为辅助端子上的脉冲输出，这是经光耦隔离无源输出，此脉冲接口主要用于向负荷控制终端(RTU)、脉冲式集中抄表器提供有功电能脉冲。

2.7 RS485 串口通信功能（可选）：

电表中的部分参数可通过 485 接口读出。RS485 通信协议符合电力行业标准《DL/T 645-1997 多功能电能表通信规约》，另外还可执行一部分自定义协议。

（8） 红外通讯功能：

电表可以通过红外接口与掌上机的红外接口进行通讯。其遵守的协议和 485 所遵守的协议相同。通讯波特率为 1200。红外和 RS485 部分，本表支持读功能，支持写入。修改电表参数时需要用与电表对应的编程卡。

（9） 记忆功能

当供电线路停电时,剩余电能量及其他信息不应丢失。

（10） 辨伪功能

使用非指定 IC 卡或介质时,电能表不应接受或工作。

（11）叠加功能

电能表内预置的剩余电能数与新购电能数应能叠加。

（12）数据返写功能

每次购电卡插入预付费电能表中,预付费电能表不仅能将新购电量写入表内,同时还能将表内用电信息返写到电能卡内,供售电者监督用电情况。返写信息包括：表内剩余电量，使用电量，非法用电标志等。

（13）卡口防攻击功能。

采用特有的保护电路设计，同时强化了预付费电能表卡口防多种攻击的能力（如卡口短路、卡口高压静电、卡口直/交流电压攻击等），与其它同类产品相比，具有较强的抗干扰能力，大幅度降低了受到攻击而损坏的可能性；同时继电器内置/外置可选，电力系统用户可根据自身实际管理需要进行选择，减少了表计正常使用损坏的发生。

（14） 扩充功能

表内留有标准的通讯接口，方便用户定制集抄功能。可通过低压电力线载波、无线、RS485 等多种方式来实现集中抄表功能。

3、技术特点

（1） 表内置微电脑和固化程序，可以自动完成电能采集，电量计算和实时处理，剩余电能显示，电卡读写，断电控制等多种功能。

（2） 电卡采用专用先进的 IC 卡技术，电卡数据采取集成电路结构与密码结合加密方式，数据安全可靠，不可破译并具有长寿命、携带方便的特点，可循环使用十万次以上。配置的卡座可承受十万次以上的插拔动作。

（3）电表使用专用电能计量芯片，其工作方式稳定可靠，抗干扰能力强，可防止潜动产生的误脉冲。

（4）在任何时候电源全部掉电时，所有数据会被存储在表内固态存储器中，数据保持可达十年以上。

（5） 一表一卡，用户电卡只能在自己的表上使用，在其它的表上不起作用。

DDSY251 IC 卡预付费电能表实现了售电的安全性及功能的齐备实用性。为电力部门的收费及抄表带来了极大的方便和收益。随着电力系统的发展和广大电力客户观念的转变，“电是商品”已深入人心，卡式电表有望全面普及，具有广泛的应用前景。