基于 CCM3310S 芯片的 IC 卡互联网终端解决方案

2013 年 2 月 5 日中国人民银行发布并正式实施了《中国金融集成电路（IC）卡规范》（PBOC3.0 规范），在该规范中，原来在 PBOC2.0 规范中降级支持的磁条卡相关内容全部删除了，此举将大大推动金融 IC 卡的发卡进度。为了解决与金融 IC 卡相匹配的个人金融交易终端问题，中国人民银行在 PBOC3.0 规范中增加了第 16 部分《IC 卡互联网终端规范》。 业内所说的三代 USBKey 一般就是指 IC 卡互联网终端，它是指通过互联网渠道、用于与 IC 卡配合共同完成 IC 卡交易的小型读卡设备。

图 1　IC 卡互联网终端照片

IC 卡互联网终端的特征为：具有硬件安全特性，支持安全算法和 PKI 体系，具有接触式和非接触式金融 IC 卡接口，具有大屏幕和全键盘等。

图 2　IC 卡互联网终端外部规格

IC 卡互联网终端支持接触式和非接智能卡读写功能，该设备不仅能够对基于 PBOC 3.0 标准的金融 IC 卡进行充值与脱机余额查询、支付等功能。有的第

三代 USBKey 还支持非接卡读写，OTP 等功能，主要配合网上银行和移动支付使用。

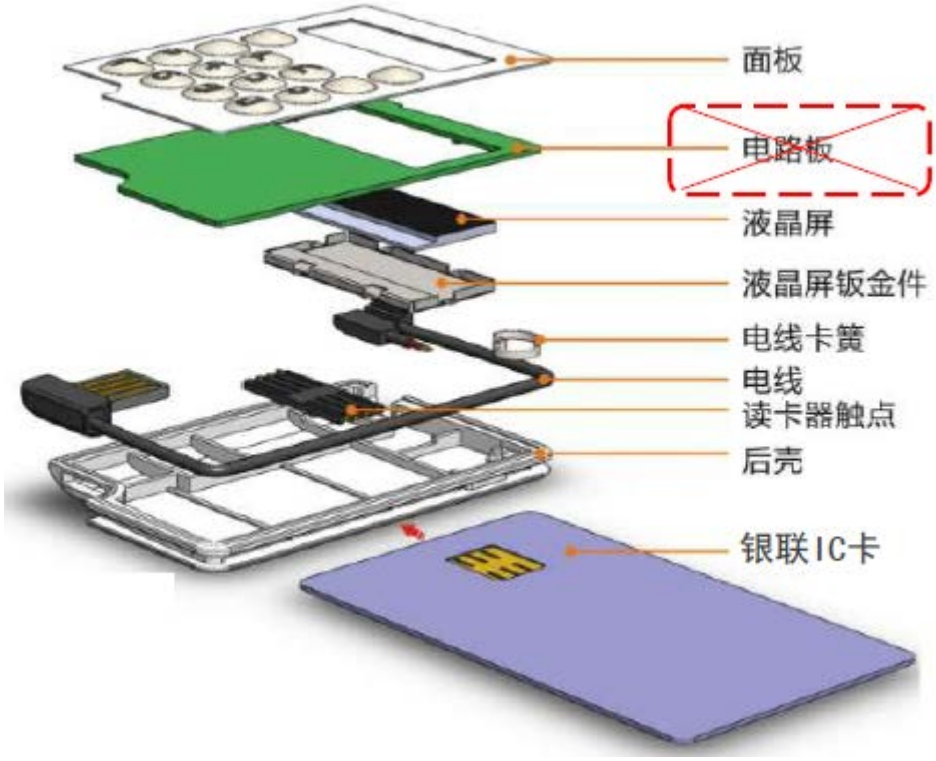

图 3　　典型的 IC 卡互联网终端内部结构

天津国芯 CCM3310S 芯片除可以单芯片实现一、二代 USBKey 的所有控制功能之外，也可以单芯片实现三代 USBKey 的所有标准控制功能，并提供了丰富的接口，可以很方便地添加扩充功能。在基于 CCM3310S 的三代 USBKey 设计方案中，安全芯片主控制器连接着显示屏幕、全键盘和 IC 卡座，它控制着屏幕上的输出显示、获取来自 USB 接口或者 IC 卡部分的通信数据，利用屏幕显示提示用户进行 USBKey 上的相应操作，从而将 PKI 技术应用于普通网银转账业务和 IC 卡充值业务。

CCM3310S 芯片具有 16K 字节 SRAM、16K 字节 ROM 和 256K 字节 EFLASH（512 字节/Page），支持 DES/3DES，RSA，AES，ECC、SHA-1、SHA-256 等国际算法，同时支持 SM1，SM2，SM3，SM4，SSF33 等国密算法，支持 USB2.0 高速模式；拥有 3 个 ISO7816 接口，2 个 SPI 接口（用于连接液晶\字库用 Flash\非接芯片）、I2C 接口、UART 接口（SCI）、I/O 接口（多达 50 个以上，有 8 个支持中断功能的 I/O 可用于连接按键）等多种接口。芯片自带 LDO 电源输出。采用 CCM3310S 设计的三代 USBKey 的框图如下图所示：

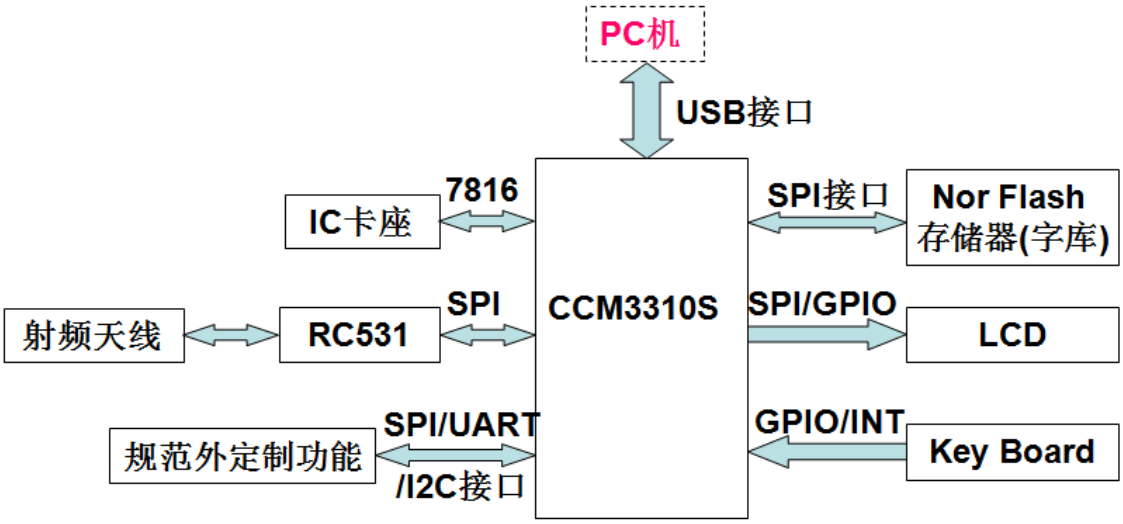

图 4　　典型的 IC 卡互联网终端内部结构

为了方便客户对基于 CCM3310S 芯片的 IC 卡互联网终端方案进行评估，天津国芯设计了基于 CCM3310S 芯片的 IC 卡互联网终端样机板，该样机板可以通过银行卡检测中心的接触式和非接 IC 卡读卡器 Level 1 认证。

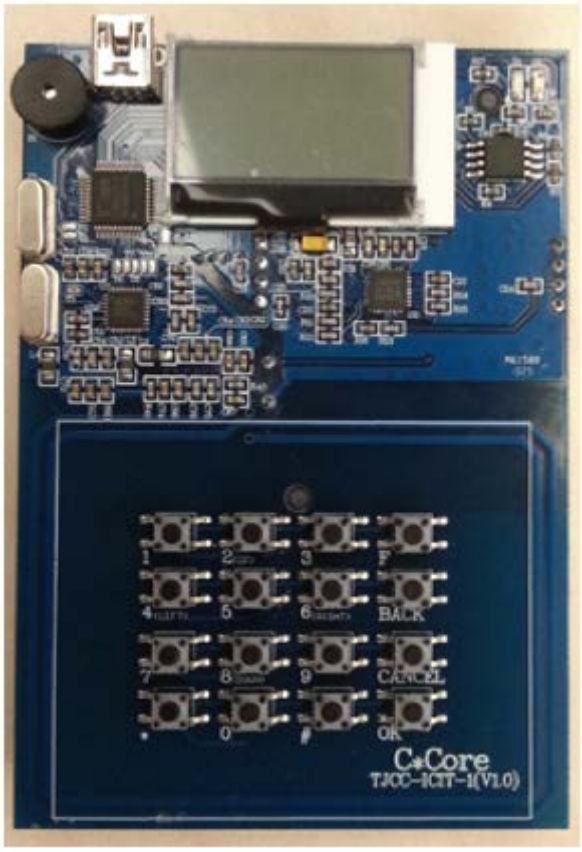

图 5　　天津国芯采用 CCM3310S 芯片设计的 IC 卡互联网终端样机板