基于 CCM3310S 安全芯片的
三代 USB Key 设计方案

三代 USBKey 方案介绍

银盾思创设计的三代 USBKey

第三代 USBKey 从安全角度主要是解决了交易密码的泄露问题，其交易密码采用 USBKey 自带的全键盘来输入，此外，第三代 USBKey 还支持智能卡读写功能，该设备不仅能够完成网上银行的基本功能，而且可以同时通过网银对基于 PBOC 3.0 标准的 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。

CCM3310S 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(用于连接液晶和字库用 Flash)、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：