基于 CCM3310S 安全芯片的
二代 USB Key 设计方案

二代 USBKey 方案介绍

中国工商银行的二代 USBKey

在国内 USBKey 市场快速增长的同时，安全性更高、功能更完善的二代 USBKey 也逐步取代传统的一代 USBKey。易用性好、稳定性高、安全性强、支持网上银行新增值应用等特性是二代 USBKey 相较一代 USBKey 所具备的新特点，在表现形式上需具有按键语音或按键显示等人机交互功能。

二代 USBKey 在一代 USBKey 的基础上增加了液晶显示和按键，使用过程仅仅增加了一个用户按键确认动作，简单易用。二代 USBKey 基本上解决了一代 USBKey 的安全漏洞，安全级别得到了质的提升，适合对网上交易安全要求较高的用户。具体如下：

1. 待签名的敏感信息在二代 USBKey 的液晶上进行显示，达到所见及所签的效果，杜绝了黑客篡改信息所带来的安全漏洞；

2. 交易需要用户按二代 USBKey 的按键进行确认，达到交易过程为用户可控状态。

CCM3310S 可以单芯片实现二代 USBKEY 的所有控制功能，是理想的二代 USBKey 单芯片解决方案。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 设计的二代 USBKey 的框图如下图所示：