基于 CCM3310S 安全芯片的一代 USBKey 设计方案

USBKey 是一种 USB 接口的硬件设备。它内置单片机或智能卡芯片，有一定的存储空间，可以存储用户的私钥以及数字证书，利用 USBKey 内置的公钥算法实现对用户身份的认证。

目前，大多数国内银行均采用 USBKey 作为网络银行的客户端解决方案，使用 USBKey 存放代表用户唯一身份数字证书和用户私钥。在这个基于 PKI 体系的整体解决方案中，用户的私钥是在高安全度的 USBKey 内产生，并且终身不可导出到 USBKey 外部。在网上银行应用中，对交易数据的数字签名都是在 USBKey 内部完成的，并受到 USBKey 的 PIN 码保护。

一代 USBKey 方案介绍

中国工商银行的 U 盾

CCM3310S 安全芯片采用国内具有自主知识产权的 32 位 CPU 安全内核 CS322D 进行设计，具有低功耗、高性能、多功能及高安全性等特点。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。包含了普通 USBKey

所需要的所有功能，可以方便的实现无驱无软，是完美的普通 USBKey 单芯片解决方案。