产品简介

华大 CIU98_B 安全 SE 产品

CIU98_B 安全 SE 产品采用 ARM 32bit CPU 核，提供 7816、SPI 接口，提供硬件 3DES、AES、SM1、SM2、SM3、SM4、PKE 协处理器、硬件 CRC、WDT、真随机数发生器。芯片提供灵活的存储器管理、安全管理机制，支持异常及事件等多种中断机制，提供了多种复位方式和时钟配置方式，并支持低功耗模式。面向移动支付、安全 SE 等安全领域的应用。

CPU 特性

ARM SC000 RISC 处理器

处理器	
CPU	ARM 32bit CPU
系统时钟	36MHz
支持	大端模式，Thumb/Thumb2 指令集
低功耗	支持低功耗模式
产品特性	
FLASH	10 年数据保持时间,10 万次数据擦写; 用户空间 256KB
RAM	40KB
产品特性	支持唯一设备标识
	支持安全密钥存储
	支持对称体系、非对称体系等安全认证
	支持对称加解密、MAC 运算
	支持非对称加解密、HASH 计算等运算
	支持访问数据的线路保护、权限设置等
	支持数据安全存储
	支持安全访问控制
接口	
ISO/IEC7816	兼容 ISO/IEC 7816 T＝0 协议
	支持外部时钟 1~5MHz
SPI	符合 SPI 接口规范，最高支持 18MHz
GPIO	6 个

接口特性

符合 ISO/IEC 7816-3 T=0 协议，支持 SPI 接口

安全特性	
存储器数据加密、存储器地址加扰	√
支持存储器访问权限保护机制	√
电压检测/温度检测/频率检测等安全传感器	√
多种防 SPA/DPA/DFA 攻击设计	√
有源屏蔽层	√
多安全算法 DES、3DES、AES、RSA、ECC、SM1、SM2、SM3、SM4、SHA-n	√
电气特性	
工作电压	1.62~5.5V
工作电流	正常电流：小于 10mA
低功耗模式	Standby：小于 200uA @5.5V,1MHz
ESD	4KV（HBM）
工作温度	-40℃~85℃
应用领域	
移动支付安全 SE	√
TBOX 安全 SE	√
开发环境	
提供 SDK 开发包	√
封装形式	
DFN8(5*6*0.75)	√
QFN32(5*5*0.75)	√