

▶ DMT-CBS-AD3B

大容量双界面安全芯片

芯片简介

目 录

1	芯片概述.....	2
2	芯片特性.....	3
3	芯片功能框图.....	4
4	芯片认证.....	5
5	芯片开发工具.....	5
6	芯片封装.....	6
7	平台和应用.....	7
8	应用领域.....	7
	版本说明.....	8
	法律声明.....	9
	联系我们(Contact Us).....	9

1 芯片概述

DMT-CBS-AD3B 芯片是为接触式和非接触式应用而设计的双界面智能卡微处理器，符合 ISO7816 和 ISO14443 Type A 和 Type B 协议。射频接口通讯速率可达到 424Kbps，协议选择完全由用户编程控制。

DMT-CBS-AD3B 芯片采用高速低功耗 8052CPU，其比传统 8051 快三倍。该芯片主要用于金融、身份卡、电子商务、交通和数字签名。内置加密协处理器可支持 2048 位 RSA 运算和 256 位 ECC 运算。也支持国密 SSF33、SM1、SM2 和 SM3 加解密算法。

DMT-CBS-AD3B 芯片具有 64KB EEPROM 存储器，可作为数据区或根据应用需要作为程序代码区。

2 芯片特性

■ CPU

- ◆ 8052
- ◆ 系统时钟：
 - 内部时钟：最大 30MHz (支持分频)
 - 外部时钟：1MHz~5MHz

■ 通信接口

- ◆ 接触 ISO/IEC 7816
 - T=0、T=1
 - 支持 PPS 协商
 - 支持多级速率 (最高 97 速率)
- ◆ 非接触 ISO/IEC 14443 TypeA&B
 - 支持多级速率 (最高 424Kbps)
- ◆ Mifare classic (1KB)

■ 电特性

- ◆ 工作电压：2.7V~5.5V
- ◆ 最大工作电流：
 - 小于 20mA @ (5V & 30MHz)
- ◆ 休眠电流：小于 100uA
- ◆ 工作温度：-25°C~+85°C
- ◆ ESD：接触式大于 2000V
- ◆ ESD：非接触式大于 6000V
- ◆ 非接触谐振频率：14.7MHz+/-0.5MHz
- ◆ 谐振电容：52PF+/-2.5

■ 存储器

- ◆ ROM: 128KB
- ◆ EEPROM: 64KB
 - EEPROM 擦写次数 10 万次以上
 - EEPROM 数据保存时间 10 年以上
- ◆ RAM: 6.25KB (4KB 加密专用 RAM)

■ 安全算法

- ◆ 国际算法：
 - 对称算法：DES、3DES、AES
 - 哈希算法：SHA1
 - 非对称算法：
 - RSA (最高 2048bits)、ECC
- ◆ 国产算法：
 - 对称算法：SSF33、SM1、SM4
 - 哈希算法：SM3
 - 非对称算法：SM2

■ 安全特性

- ◆ 低电压、低频率复位
- ◆ 篡改监控、防攻击保护、真随机数发生器、温度探测器
- ◆ 高速 DES 和 3DES 加密引擎，CRC16 引擎兼容 ISO14443-3 CRC
- ◆ 强大的内存管理单元，芯片唯一识别码
- ◆ 支持超级用户模式和普通用户模式
- ◆ 安全、优化的版图设计

3 芯片功能框图

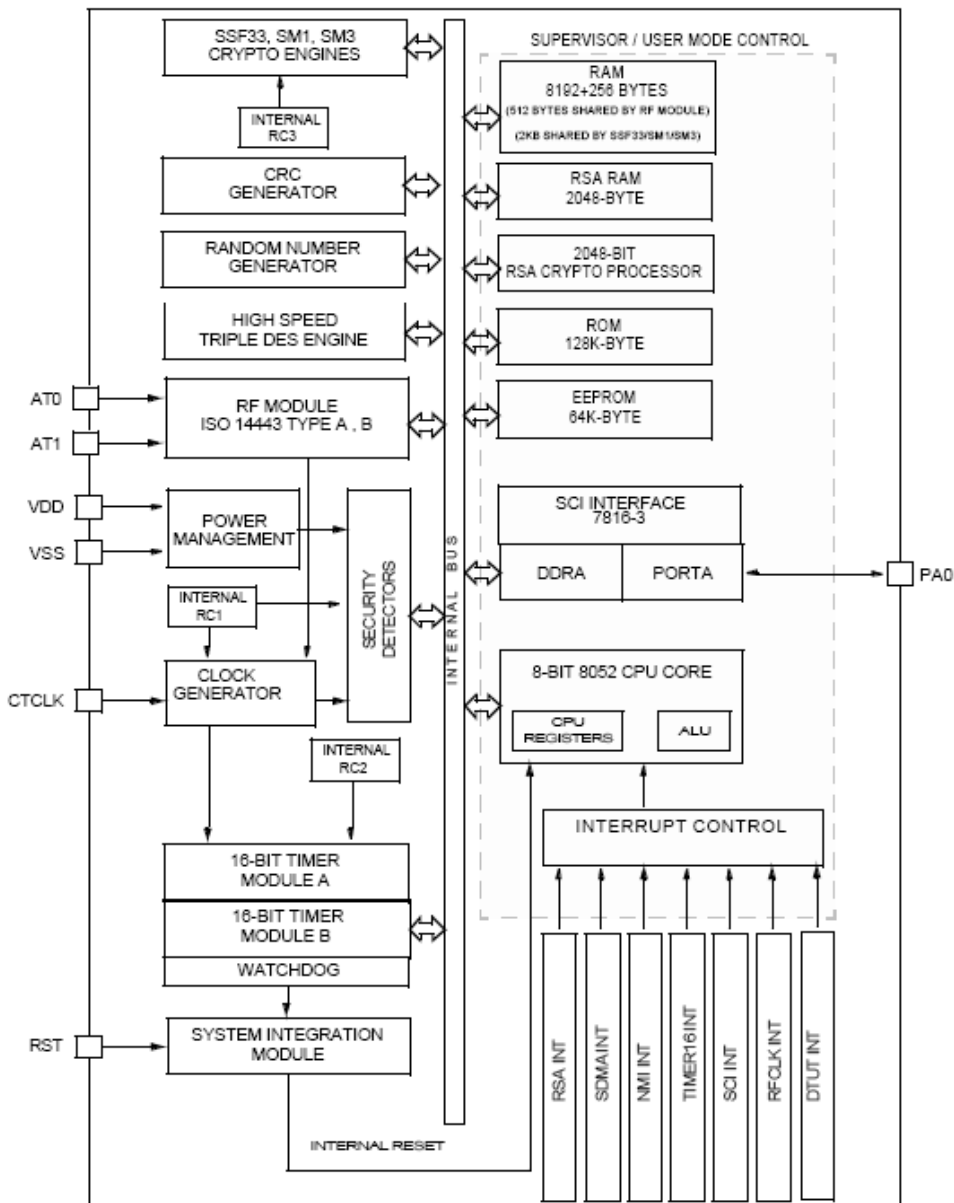


图 3-1: 功能框图

4 芯片认证

- 国家密码管理局商用密码产品型号证书
- 中国信息安全认证中心 EAL4+认证
- 居民健康卡产品备案证书（含生产单位、芯片、COS 备案证书）
- 住建部城市一卡通（含互联互通）芯片备案
- PBOC3.0 借贷记（支持小额支付）检测合格报告
- PBOC3.0 非接触式 IC 支付卡检测合格报告
- PBOC3.0 基于非接触小额支付的扩展应用检测合格报告
- PBOC2.0 金融 IC 卡电子钱包/电子存折检测合格报告
- PBOC 2.0 基于非接触式小额支付的扩展应用
- PBOC 2.0 非接触式 IC 支付卡
- PBOC 2.0 借贷记(支持小额支付)

5 芯片开发工具

- 硬件开发环境（ULINK仿真器、FPGA开发板）
- 软件开发环境（IDE：Keil uVision 4）
- 芯片用户手册和开发环境指导文档
- 算法和驱动API库
- Demo COS和示例程序

6 芯片封装

6.1 产品形态

产品形态	封装形式
Wafer	8吋
Module	接触式模块、非接触式模块、双界面模块
Card	接触式智能卡、非接触式智能卡、双界面智能卡、异形卡

6.2 管脚定义

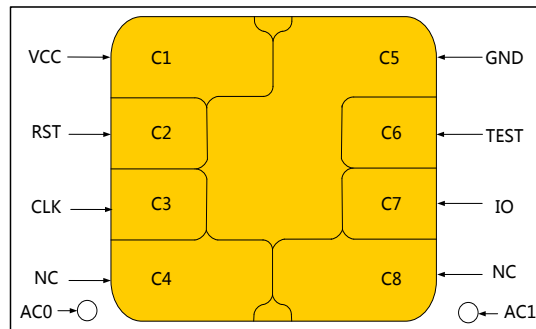


图 6-2 模块封装接线图

符号	功能
VCC	电压
RST	复位
CLK	时钟
GND	接地
PA0(I/O)	数据管脚
AC0	射频信号0
AC1	射频信号1

7 平台和应用

DMT-CBS-AD3B 芯片平台：NATIVE

金融及行业应用支持：

行业		应用
金融类	PBOC3.0 (支持双算法、兼容 PBOC2.0)	1. PBOC2.0/3.0 借贷记 (支持小额支付); 2. PBOC2.0/3.0 非接触式 IC 支付卡 3. PBOC2.0/3.0 基于非接触小额支付的扩展应用; 3. QPBOC; 5. PBOC 2.0 电子钱包/电子存折 (ED/EP); 6. PBOC 2.0 电子钱包/电子存折 (ED/EP) 扩展应用;
行业类		1. 居民健康卡应用; 2. 住建部城市一卡通互联互通应用; 3. 社保应用; 4. 市民卡应用; 5. 客户定制化行业增值应用;

8 应用领域

- 居民健康卡
- 城市一卡通
- 市民卡
- 居住证 IC 卡
- 金融 IC 卡
- 其它行业智能卡应用

版本说明

版本号	发布日期	页数	章节或图表	更改说明
V1.0	2012.12.25	7		首次发布
V1.1	2015.09.24	10		更新文档模板

法律声明

版权所有 © 大唐微电子技术有限公司 2015。保留一切权利。

未经大唐微电子技术有限公司书面同意，任何单位和个人不得擅自摘抄、复制、翻译本芯片说明书内容的部分或全部，并不得以任何形式传播。

联系我们(Contact Us)

公司(Company): 大唐微电子技术有限公司(Datang Microelectronics)
地址(Address): 北京市海淀区永嘉北路6号
邮编(ZIP): 100094
电话(Telephone): +86(10)-58953111
传真(Fax): +86(10)-58953333
网址(Website): www.dmt.com.cn
邮箱(E-mail): market_fs@datang.com