Product Preview

µ**T83RFC12864**

Dual Interface SmartCard MCU with 64KB E^{2}PROM and 2048-bit Crypto Co-Processor

The µT83RFC12864 is a dual interface smart card microcontroller (MCU) designed for contact and contactless applications which requires more flexibility to interface with different built-up infrastrutures. It complies with ISO7816 and ISO14443 Type A and B standards. The RF front-end can support data rate up to 424Kbps. The selection of protocol is fully under user program control.

µT83RFC12864 features a high speed low power 8052 CPU which is typically three times faster than traditional 8051.

It is targetting for high security applications such as Banking, Identity Card, E-commerce, transportation and Document Digital Signature. The built-in crypto co-processor can speed up cryptographic calculation with up to 2048 bits modulo exponetiation (A^B mod N) and other similar calculations such as Elliptic Curve Cryptography (ECC). It supports up to 2048-bit RSA and 256-bit ECC calculation

µT83RFC12864 features 64KB E^{2}PROM which can be used for DATA area or program code extension area according to application requirement.

Typical Crypto Functions Performance:

Function	Typical Time (ms)@30MHz
RSA 1024 bits signature with CRT*	43
RSA 1024 bits signature without CRT	120
RSA 1024 bits verification (e=10001)	1.6
Triple DES	3us
ECC 256 bits key generation	46
ECC 256 bits signature	24
ECC 256 bits verification	104

GENERAL FEATURES

• High speed 8052 compatible CPU core

• 128k-byte user ROM

• Total 64k-byte user E^{2}PROM
  – 64 byte per page
  – configurable for data or program area

• Total 3.25K-byte user RAM and 2K-byte Crypto RAM

• Two 16-bit programmable timer with precaler

• SCI interface with ISO7816 T=0 support

• 40MHz Internal Oscillator RC1

• CPU clock divider (divide by 1,2,4 or 8) and selectable clock source

• Maximum standby current during stop: 500µA (no external clock)

• ESD protection at least 4KV (HBM) for contact pads and 2KV (HBM) for antenna pads.

• Operation temperature range: -25C to +85C

CONTACTLESS MODE FEATURES

• Operating Frequency: 13.56MHz

• Support ISO14443 Type A and B

• Support 106, 212 and 424Kbps in both Type A and B mode

• Software switch between contact and contactless mode

• Support mixed modes (contact and contactless) operation

*CRT : Chinese Remainder Theorem

µT83RFC12864/PR — rev. 1.0

SECURITY FEATURES

- Low Voltage Reset and Low Frequency Reset
- Tamper Monitor
- Protection Features Against Security Attacks
- True Random number generator
- High Speed single DES and Triple DES engine
- High Speed 2048-bit Crypto Co-processor
- CRC 16 Engine per ISO 13239 and compatible with ISO14443-3 CRC requirement
- Powerful Memory Management Unit (MMU)
- Support supervisor mode and user mode
- Temperature detector
- Optimized layout for security
- Unique identification code

SUPPORT STANDARDS

- ISO/IEC 7816
- ISO/IEC 14443
- EMV 2000

μT83RFC12864/PR — rev. 1.0

1. GENERAL OVERVIEW

The µT83RFC12864 is a dual interface smart card MCU for high security level smart card applications and also best fit for banking and ID applications. The block diagram of the µT83RFC12864 is shwon in Figure1.
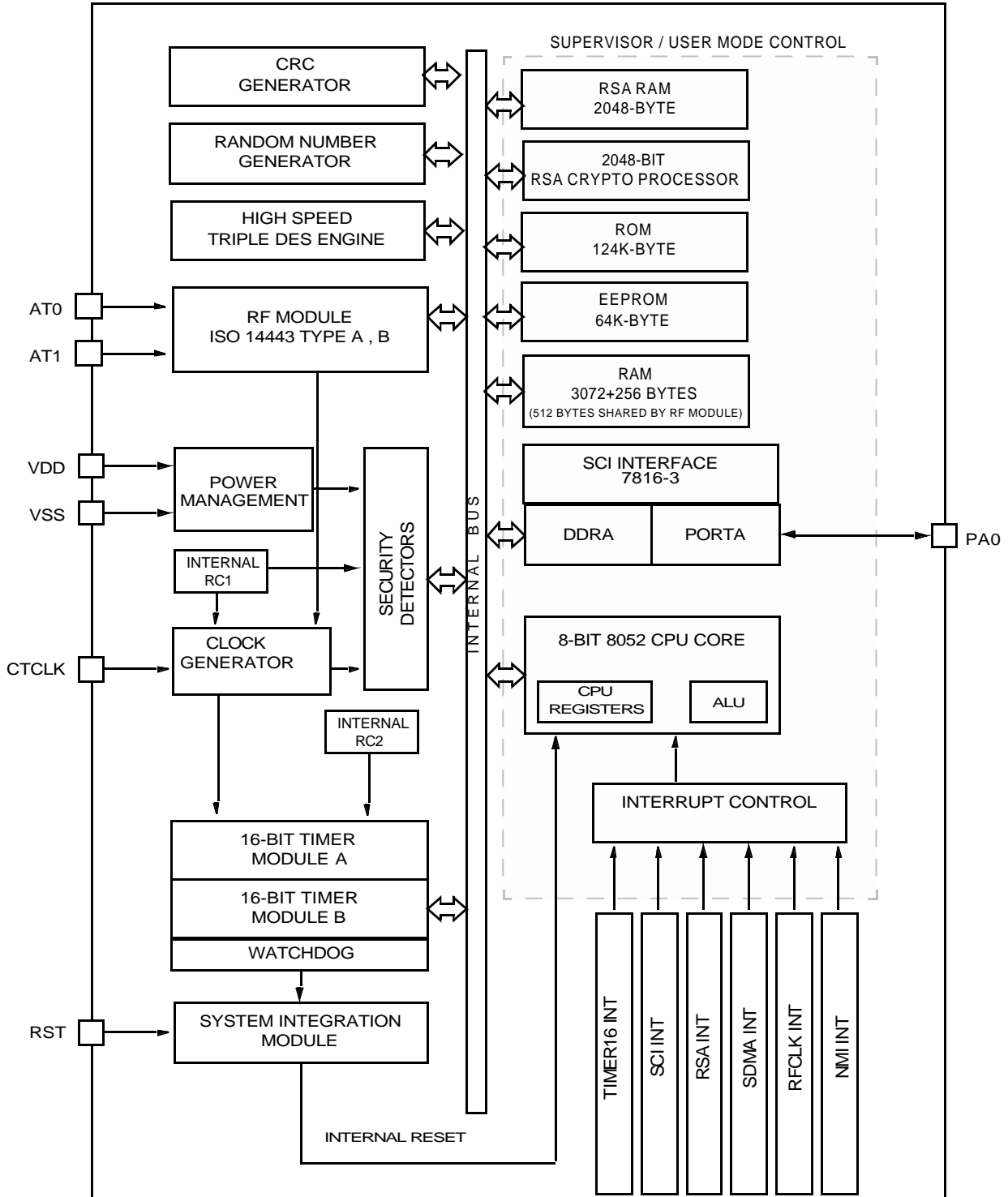

Figure 1. µT83RFC12864 MCU Block Diagram