Dual ISO15693 and ISO14443 Contact less Smart Card

Contactless interfaces

- Dual RF interface with auto detection between ISO/IEC 15693 and ISO14443 Type A mode
- ISO/IEC 15693 part is hardwired logic
- ISO/IEC 14443 part is CPU operated
- Field strength check allowing to start PICC mode
- 64-bit ISO/IEC15693 Unique Identifier (UID)
- 56- bit ISO/IEC14443 Unique Identifier (UID)
- Random ID support for Privacy mode

ISO14443 protocol (PICC mode)

- ISO 14443 Type A (106kpbs – 848 kbps)
- CPU
  - Software compatible CMOS 80X51 industry standard
  - Accelerated architecture with 16 bit CPU performance
  - Up to 30 MHz internal CPU clock
- Security
  - Hardware AES-128
  - Hardware DES/3DES
  - Hardware Random Number Generator FIPS140-2
- DMA
  - Fast data transfers independent on CPU
  - CRC, DES/3DES, AES, COMPARE, FILL, BER-TLV operations
- Peripherals
  - 2 x 16 bits Universal Timers/Counters
  - CRC16 Module ISO13239 compatible
- Memories
  - Code EEPROM 64kB
  - Data EEPROM 4kB shared with VICC
  - RAM 3328B (XRAM = 3072B, IRAM 256B)

ISO15693 protocol (VICC mode)

- Vicinity transponder mode
- ISO15693 standard compliant
- Support all mandatory and most of optional ISO 15693 commands and a set of custom commands
- Backward compliant with EM4233 family
- Data Storage Format Identifier (DSFID)
- Application Field Identifier (AFI) supported
- Security
  - New stream cipher Grain128a with 128-bit key
  - High secure proprietary crypto with 96 bit key
  - Hardware Random Number Generator
  - Three pass mutual authentication according to standard ISO 9798-2
  - Data authenticity protected with 32 bits MAC

EEPROM

- 4kB User Area shared for PICC and VICC
- Configurable VICC memory size up to 4kB
- PICC/VICC erase/write by 1/4/8/16 bytes
- 20 year data retention EEPROM
- EEPROM Endurance > 100 K cycles

Technical data

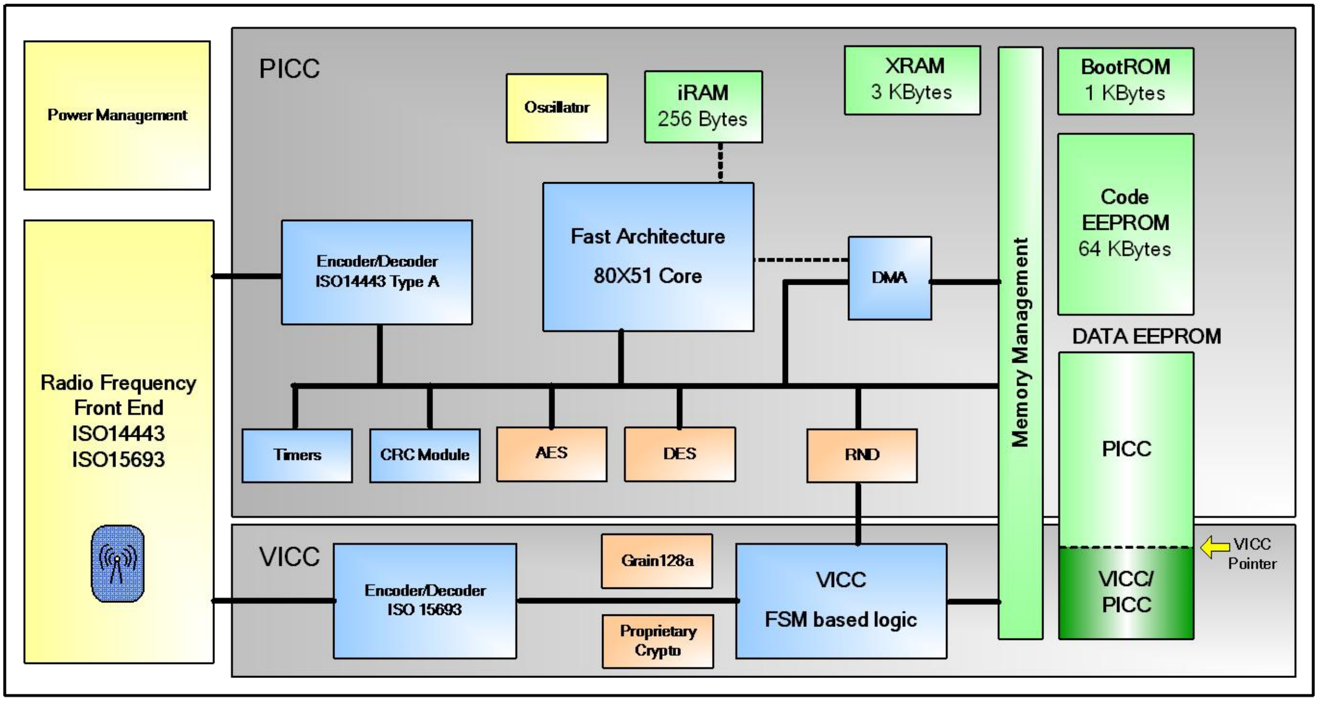
- On-chip resonant capacitor 16.6pF
- -40 to +85˚C temperature range

Typical Application:

- Access Control, Public Transportation
- High value data and Anti-counterfeit protection

Development support

- Development tools fully integrated within Keil uVision3/4 with examples, documentation samples (Emulator ordering reference EMX43)
- ISO14443 Low Level Library of code samples for OS developers



Introduction

The EM4333 is contact less Smart Card which integrates vicinity as well as proximity protocols in one chip using same antenna. It makes it usable in wide range of applications.

VICC part supports ISO15693 air interface with high level of security of data transfers. EM4333 brings a high security level offering a new open stream cipher Grain128a with key length of 128 bits. Grain cipher supports three pass mutual authentication and Message Authentication Code to ensure security of data transfers.

At the same time it supports also ISO14443 Type A protocol in PICC part which can communicate up to 848kbps in both directions suitable for proximity applications with high speed and high secure transfers. The PICC is operated by CPU 8051 allowing full flexibility given by customer software. The core offers AES-128, DES/3-DES and DMA coprocessors. DMA increases hardware performance for large memory operations.

The CPU is software compatible with the industry standard 8051 8 bits microprocessor, to guarantee the maximum reuse of tested software. The hardware implementation of the core is a modern design not relying on microcode, with an increase of up to 3 times on a standard 8051's clocks per instruction.

The chip includes a total 4kB of Data memory available for user in PICC and/or VICC with a maximum memory space sharing of 4kB between both modes.

Auto-detection

EM4333 is able to detect automatically if commands are sent in ISO15693 or ISO14443 protocol. In case of ISO15693 is received VICC part of device takes control of further communication. If ISO14443 command is received PICC part with CPU and customer software is in charge of further communication.

The unique feature of field strength detector ensures that PICC part is powered only in strong field thus ensuring the range of VICC is not affected by high speed and high secure PICC mode.

Configurable shared Data memory

The uniqueness of EM4333 is that Data EEPROM is shared between vicinity and proximity parts. Both protocols can have access to same data from different applications.

The Data memory is comprised of 4kB user memory and 1kB system area.

The PICC part controlled by customer software has always access to full memory since it is intended for more memory demanding and memory protected applications.

The ISO15693 access to memory can be controlled. The memory management allows set a maximum size of Data memory accessible for VICC thus separating memory spaces in PICC and VICC mode.

Data memory can be programmed in variety of granularities. It can be programmed at once as 1B, 4B, 8B or 16B offering high flexibility and compatibility to different systems and applications already in the field.

ISO15693 interface (VICC)

The vicinity interface VICC supports all modes according to ISO/IEC15693-2/3 standards including all mandatory, most of optional commands and in addition number of custom commands.

The EM4333 supports real vicinity mode which allows reaching minimum activation field down to 0.05A/m with ISO reference ID1 antenna and resonant frequency 14.2MHz.

In applications it allows to reach distance from reader antenna up to 60 cm.

VICC security

The VICC offers three modes of secure modes:

- ❑ Normal mode used by all users
- ❑ Safe Access mode granted to power users
- ❑ Administration mode for card personalization

The Safe Access and Administration mode can be protected by different level of security:

- ❑ Password protection
- ❑ Mutual authentication with proprietary crypto compliant with EM Microelectronic HF family
- ❑ Mutual authentication and MAC using new state-of-the-art stream cipher Grain128a

The Grain128a stream cipher uses key length of 128 bits and it allows not only mutual authentication but also message authentication code (MAC) of 32 bits to ensure security of all data transfers.

Every page in full 4kB memory can be protected against read or write access separately using protection bits. The protected pages can be then accessed or modified only in Safe Access or Administration mode.

VICC custom features

The vicinity part of EM4333 offers also transport mode, random ID, Debit and Get Debit commands for variety of applications.

To optimize range and communication speed it is possible to start to communicate in long range using VICC ISO15693 protocol and if tag is moved to stronger field to switch to high speed and secure PICC ISO14443 mode using command Switch to PICC.

ISO14443 Interface (PICC)

Proximity RF interface is configurable by software and it supports ISO/IEC 14443 Type A data encoding and decoding. This high speed interface sustains data transfer rates up to 848kbps. It offers the high level of flexibility in order to use symmetric or asymmetric data rates between reader and device. The data integrity in ISO/IEC 14443 Type A is handled by hardware using parity bits.

Low power contactless interface allows reaching minimum activation field down to 0.5 A/m with ISO reference ID1 antenna and resonant frequency 14.2MHz.

Code EEPROM Memory

The user application software for CPU 8051 is stored in on-chip Code EEPROM which size is 64kB. The cycling is limited to 1Kcycles.

The software in Code EEPROM can be even updated in the RF field.

DMA

The DMA block is essential for contactless applications. It permits to transfer data from and to RF interface in low power mode without CPU involvement.

The DMA block also significantly improves the performance for large memory operations. DMA is up to 8 times faster than CPU in memory transfers. It can also be used to transfer data from/to peripherals in parallel with CPU operation or in low power mode when CPU is in IDLE state.

The DMA supports several operations in parallel over transferred data to be even more efficient.

- ❑ CRC checksum
- ❑ AES/DES encryption/decryption
- ❑ Fill memory, compare memory places
- ❑ BER-TLV support

Crypto accelerators AES, DES/3DES

Symmetric encryption / decryption algorithm can be achieved using AES, DES and Triple DES on chip HW accelerators. The crypto modes can be used in different modes as EBC, CBC and CTR.

AES offers state-of-the-art security with 128 bit key length.

DES/3DES offers backward compatibility to previous products.

Random Number Generator

The on chip random number generator is tested according to FIPS140-2. This allows using random numbers beyond just randomizing transmissions or generating keys.

Development tools

Powerful development tools fully integrated into Keil uVision3/4 environment provide an efficient and user friendly development platform. An emulator EMX43 with RF extension allows fast and efficient development and debugging directly in the customer application

EM Microelectronic delivers with the device a Low Level Library of code samples which supports all transport layers of ISO14443-3/4 in Type A. The library functions allow easy and fast porting of customer software to the device.