AE45C

High Security 16-bit Smart Card Microcontroller

Features

- 32.5Kbytes EEPROM
- 96Kbytes ROM
- 4.5Kbytes RAM
- 1024-bit Coprocessor

Integrated Security Concept (ISC)

The AE45C designed under Renesas Technology ' s ISC is ideally suited for high security applications. The ISC means that security is not an add-on feature to standard modules or coressecurity has been built in from the start forming an integral part of the whole Smart Card design concept. The whole ISC process (secure chip design environment, secured production facilities and secure handling during shipment to the customer) is constantly reviewed in order to maximise the overall security package.

The AE45C has been certified under the Common Criteria to EAL4+ using Protection Profile BSI-PP-0002-2001.

Many security features such as integrated sensors, distributed layout, Random Number Generation (RNG), Watch Dog Timer (WDT), DES-Engine and power analysis attack protection are all included providing a strong on- chip hardware security structure.

Uniquely, Renesas Smart Card devices are fabricated using a MONOS (Metal Oxide Nitride Oxide Silicon) EEPROM structure. MONOS advantages compared to standard EEPROM structures are: high resistance to radiation disturbance; high reliability; and endurance.

A high performance Coprocessor is complementary to the design concept ensuring final operating system efficiency, application integrity and performance that meet tomorrow's needs today.

Applications

The AE45C fulfils the requirements of Smart Card applications requiring large memory, high security and high speed secure authentication, data encryption or electronic signature. Examples include: Public Key Infrastructure (PKI), Wireless Application Protocol (WAP), m-commerce, digital signature, and USIM/UMTS.

Where PKI is a core requirement, a high speed Coprocessor is needed that can process arithmetical data in a time frame that ensures a fast and free flowing application environment. The AE45C Coprocessor ensures the high performance required by today's high security applications.

Applications such as WAP and m-commerce are continually expanding in scope and consequently the need for greater memory storage for both data and program code is constantly increasing. The AE45C provides a significant increase in ROM for program storage over previous devices whilst ensuring a balance of EEPROM for data storage.

The move from single to multi-application on a single component is also rising due in part to new systems such as WAP and m-commerce. This requires not only additional memory for application data storage but also features such as Firewall Management Units (FMU) in order to provide data integrity between applications.

Specifications

Process
- 0.35µm CMOS process

CPU
- AE-4 High performance 16-bit CPU
- 16Mbytes Linear Address Space

Minimum Instruction Timing
- 0.25µs for 32-bit addition
- 1.75µs for 16 x 16-bit multiplication

EEPROM
- MONOS (Metal Oxide Nitride Oxide Silicon) EEPROM Process
- 32 Kbytes
- 512 Bytes EXTRA
- Easy EEPMOV write by single instruction
- Read, write and erase of EEPROM Byte by Byte
- 1 to 64 Bytes programming with one instruction
- Protected against accidental writing and erasing
- Data retention minimum 10 years
- EEPROM programming voltage generated onchip
- Endurance: greater than 100,000 times
- Erase time: 2ms max
- Write time: 4ms max
- Overwrite time: 2ms max

ROM
- 96 Kbytes

RAM
- 4 Kbytes

Peripherals
- Security sensors
- DES-Engine, Minimum execution time is 18 clock cycle
- Watchdog Timer supports real time OS & applications with exact time measurements
- Random Number Generator
- Firewall Management Unit
- PLL

Coprocessor
- 1024-bit Key length
- 512 Bytes RAM
- RSA/ECC Cryptography

Power
- Single voltage power supply
- 4.5V to 5.5V
- 2.7V to 3.3V

Clock Frequency Range
- External Clock Input

fCLK = 1MHz to 10MHz (Vcc = 4.5V to 5.5V)

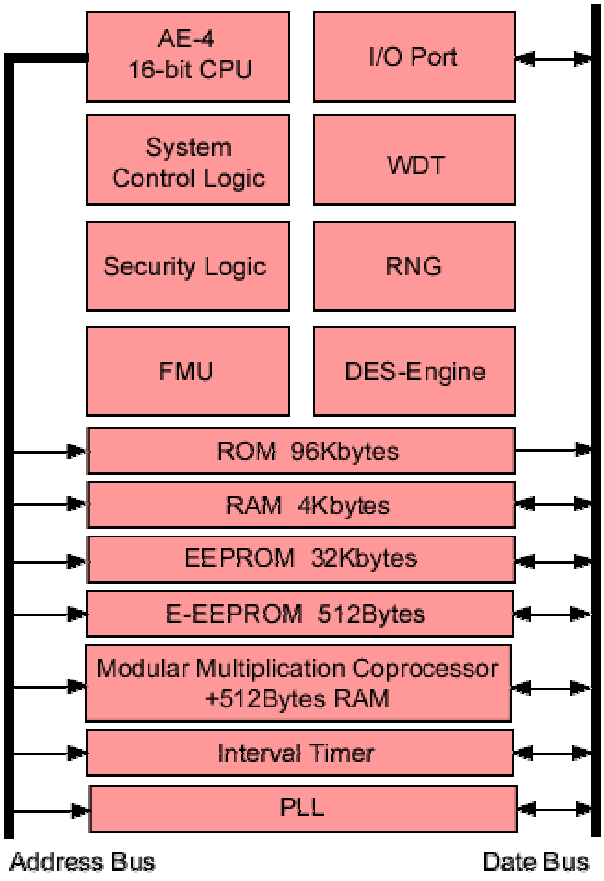
fCLK = 1MHz to 5MHz (Vcc = 2.7V to 3.3V)

- Internal Clock application can select external clock frequency or half external clock frequency as internal operation frequency.

Operating Temperature Range
- standard -25 to + 85°C

Shipping Form 8 inch wafer
- Sawn wafer, unsawn wafer and Chip on Tape (COT) Module

Block Diagram



For further information on Renesas Technology's Smart Card products and services including details of sales offices in your region, please visit:

www.renesas.com/smartcard

June 2003