High security 16-bit smart card microcontroller

AE44C

Features

18KB S-MONOS EEPROM, 128kB ROM
4kB RAM

Integrated Security Concept (ISC)
The AE44C designed under Renesas Electronics ISC is ideally suited for high security applications. The ISC means that security has been built in right from the start forming an integral part of the whole Smart Card design concept and is not just an add-on feature to standard modules or cores. 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.

All devices of the AE-series will be evaluated and certified by independent evaluation authorities.

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 Electronics Smart Card devices are fabricated using Metal Oxide Nitride Oxide Silicon (MONOS) 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 highly integrated memory of the AE44C enables it to support multiapplication cards based on sophisticated Operating Systems (OS), including Multos, JavaCard™ and Windows for Smart Card. It also allows for enhanced functionality of Mobile Communication cards and the implementation of advanced Value Added Services (VAS) to end users. These could include services such as stock exchange information, weather forecasts, online gaming, reservations for travel or theatre and e-commerce applications, which enable an operator to differentiate its product range as well as complex and secured M-commerce and Digital Signature applications.

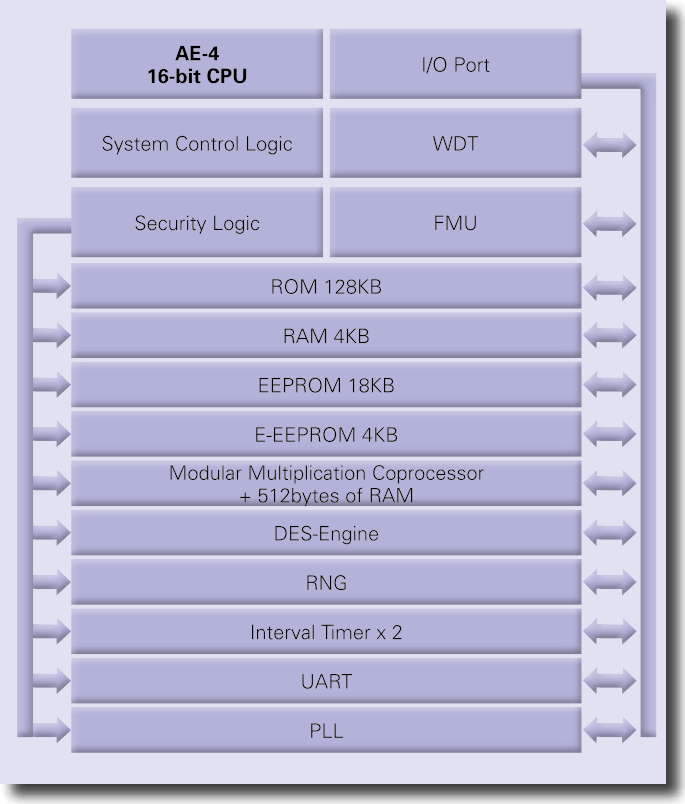
The large EEPROM memory is particularly useful for USIM cards, which have many more applications and items to store in the address book than typical GSM SIM cards. It will also allow the cards to support UMTS services such as financial services.

The coprocessor enables the implementation of e-commerce and WAP applications with enhanced security for end users. The high functional integration of the AE44C, including DES Engine, Phase Lock Loop (PLL), UART and interval timer, allows for easy migration from GSM SIM card to UMTS USIM card.

With these advanced high performance features the AE44C provides an ideal platform for both current and future financial and digital signature applications whilst easily supporting a true multi-application environment.

The AE44C is manufactured in specially controlled and ISO certified silicon factories located in Germany and Japan using a highly reliable 0.18µm CMOS process technology allowing much higher integration of memory into a smart card, which is particularly useful for USIM 3G cards with their stronger requirements for data and application storage.

The AE44C supports all the voltage classes A, B and C (1.8V to 5V) of the 3rd generation specification for mobile communication TS102.221.



Specification

Item	Specification
Process	0.18µm CMOS process
CPU	AE-4 High performance 16-bit CPU 16 Mbytes Linear Address Space
Minimum Instruction timing	0.25µs for 32-bit addition 1.75µs for 16 x 16-bit multiplication
EEPROM	MONOS EEPROM Process 18KB (including 4KB Extra EEPROM) Easy EEPMOV write by single instruction Read, write and erase of EEPROM byte by byte 1 to 128bytes programming with one instruction Protected against accidental writing and erasing Data retention minimum 10 years guaranteed over full operating temperature range EEPROM programming voltage generated on-chip Endurance: greater than 500,000 times Erase time: 2ms max Write time: 4ms max Overwrite time: 2ms max
ROM	128KB
RAM	4KB + 512bytes (coprocessor RAM)
Peripherals	Security sensors DES-Engine, Mminimum execution time is 18 clock cycle WDT (Watchdog Timer) RNG (Random Number Generator) FMU (Firewall Management Unit) UART PLL
Coprocessor	1024-bit key length 512bytes RAM RSA/ECC cryptography
Power	Single voltage power supply 4.5V to 5.5V 2.7V to 3.3V 1.62V to 1.98V
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) fclk = 1MHz to 5MHz (Vcc = 1.62V to 1.98V) Internal clock application can select external clock frequency or half external clock frequency as internal operation frequency.
Operating temperature	Standard -25 to + 85°C

Renesas Electronics Europe
www.renesas.eu
April 2010 Printed in UK **20-515A**