

High Security 32-bit Smart Card Microcontroller

AE58C

digital signature

m-commerce

public key

WAP



Features

288kbytes EEPROM, 480kbytes ROM, 18kbytes RAM
2112bytes Coprocessor

Applications:-

The highly integrated memory of the AE58C enables it to support multi-application cards based on sophisticated Operating Systems (OS), including Multos and JavaCard™. 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 new Renesas Technology AE-5 family boasts impressive credentials. The AE58C offers ultimate performance through the enhancement of the CPU architecture that includes a 5-level pipeline and a byte code decoder and dispatcher. Renesas Technology's unique upward compatibility of AE58C with the existing AE-3 (8-bit) and AE-4 (16-bit) devices saves your investments while providing your applications with better performance and state-of-the-art security.

The AE58C 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 AE58C relies on the new Single Transistor Metal Oxide Nitride Oxide Silicon (S-MONOS) EEPROM Structure. S-MONOS combines higher density with the traditional MONOS advantages vs. other EEPROM structures e.g. high resistance to radiation disturbance, high reliability and endurance

The AE58C supports all the voltage classes A, B and C (1.8V to 5V) of the 3rd generation specification for mobile communication TS102.221.

The high functional integration of the AE58C, including DES and AES Engines, PLL (Phase-Lock-Loop), UART, DMA and interval timer, facilitates the implementation of the latest requirements for OS and applications. As an example new requirements defined in ETSI TS 102.221 release 6 specification such as Fi/Di=512/64 and selectable push-pull buffer are supported by the integrated UART and DMA.

Integrated Security Concept (ISC):-

The AE58C 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 cores, security has been built in from the start forming an integral part of the whole Smart Card design concept. The whole ISC process e.g. secure chip design environment, secured production facilities and secure handling during shipment to the customer are constantly reviewed in order to maximise the overall security package. Consequently selected devices in the AE-5 family will be independently evaluated and certified as required.

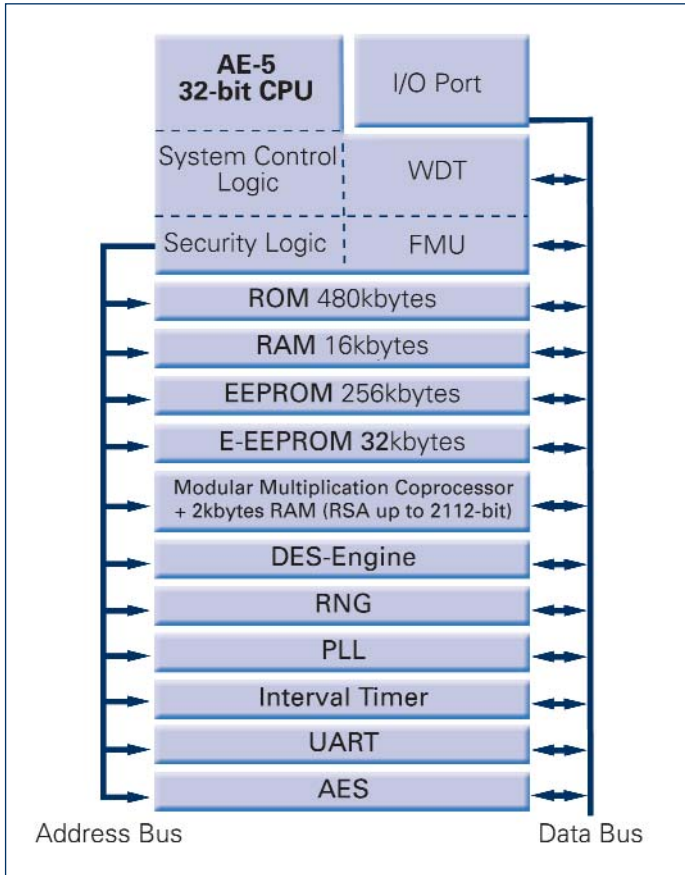
Many security features such as integrated sensors, distributed layout, on-chip data encryption, DES engine and power analysis attack protection are all included providing a strong on-chip hardware security structure.

Other important security features on the controller include a Firewall Management Unit (FMU), a Random Number Generator (RNG) and a Watchdog Timer (WDT).

Uniquely, Renesas Technology 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 cryptographic coprocessor is complementary to the

design concept ensuring final operating system efficiency, application integrity and performance meet tomorrows needs today. This coprocessor is equipped with its own 2kbyte RAM and supports asymmetric cryptography algorithms (RSA, Elliptic Curves) with key sizes of up to 2112-bit. A multifunctional Advanced Cryptographic Library (ACL) is available containing secure RSA calculations, various hash functions and key generation with highest protection against all currently known attacks such as SPA (Simple Power Analysis), DPA (Differential Power Analysis), DFA (Differential Fault Analysis), timing attacks and other possible hardware or software attacks. In addition a new hardware module for the next generation symmetric algorithm the AES (Advanced Encryption Standard) is implemented as well as a more traditional hardware DES engine, making the AE58C best prepared for the future .



For more information please contact your Renesas representative or visit our website.

Specification

| Item | Specification |
|---|---|
| CPU | <ul style="list-style-type: none"> Two-way general register configuration Sixteen 8-bit registers + eight 16-bit registers, or eight 32-bit registers High Speed Operation Max clock rate: internal clock 16MHz (at 3V) AddSubtract: 62.5ns MultiplyDivide: 62.5/100ns Streamlined, concise instruction set Instruction length: 2 or 10bytes Register/mem-register/mem arithmetic and logic operations MOV instruction for data transfer between registers/mem and memory Instruction set features Multiply instruction (8-bits x 8-bits and 16-bits x 16-bits) Divide instruction (16-bits / 8-bits and 32-bits / 16-bits) Bit accumulator instructions Register indirect specification of bit positions EEPROM write instruction (EEPMOV.B and EEPMOV.P/W) High-speed block transfer instruction |
| Coprocessor | <ul style="list-style-type: none"> 2112bit key length 2kbytes RAM RSA/ECC cryptography (RSA, Key generation, hash available as secure crypto library) |
| EEPROM | <ul style="list-style-type: none"> S-MONOS EEPROM Process 256kbytes EEPROM 32kbytes 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 EEPROM programming voltage generated on-chip Endurance: greater than 500,000 times Erase time: 1.5ms max Write time: 3ms max Overwrite time: 1.5ms max |
| ROM | 480kbytes User ROM |
| RAM | 16kbytes + 2kbytes for coprocessor |
| DES Engine | Yes |
| AES Engine | Yes |
| 16-bit Timers | 2ch External Clock |
| Peripherals | <ul style="list-style-type: none"> WDT (Watchdog Timer) RNG (Random Number Generator) FMU (Firewall Management Unit) Integrated Security Sensors DMAC (direct memory access to the RAM) 2 x UART, ISO7816-3 T=0, T=1 and Full Duplex capable I/O Port: I/O-1, I/O-2 |
| Power | <ul style="list-style-type: none"> Single voltage power supply 4.5V to 5.5V 2.7V to 3.3V 1.62V to 1.98V |
| Clock Frequency Range | <ul style="list-style-type: none"> External Clock Input: fclk = 1MHz to 10MHz (Vcc = 4.5V to 5.5V) fclk = 1MHz to 10MHz (Vcc = 2.7V to 3.3V) fclk = 1MHz to 10MHz (Vcc = 1.62V to 1.98V) Internal Clock: application can select multiple of external clock frequency (x1, x1.5, x2, x3, x4,) or external clock frequency divide by 2 as internal operation frequency. |
| Operating temperature | <ul style="list-style-type: none"> Standard -25 to + 85°C |
| Shipping Form | Wafer and COT (Chip On Tape-Module) |
| Compliant with standards/specifications | <ul style="list-style-type: none"> ISO/IEC 7816-3 ETSI TS102.221 (Release 6) |

