

High-security 16-bit microcontroller



AE56U

Applications

Modern personal computing is a target area for attackers using highly sophisticated methods, and there is an increasing demand for security. The smart USB token is a convenient form factor widely adopted in this environment to enable secure internet, secure login, remote access, digital signature and secure e-mail. The AE56U is a single-chip microcomputer unit (MCU) built around the high speed AE-5 CPU core especially designed as a secure device for smart USB token platforms. One UART ISO/IEC7816-3 compliant, 16 configurable General Purpose I/O, USB Full Speed 2.0, EEPROM, ROM, RAM, random number generator (RNG), watchdog timers, a firewall management unit, interval timers, and coprocessors are integrated on the chip. The AE-5 CPU is a 32-bit-core that provides compatibility with the earlier AE-3 and AE-4 CPUs at the object level. Operating at a maximum internal clock rate of 12MHz, it rapidly executes bit manipulation instructions, arithmetic and logic instructions, and data transfer instructions.

Integrated Security Concept (ISC)

The AE56U 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.

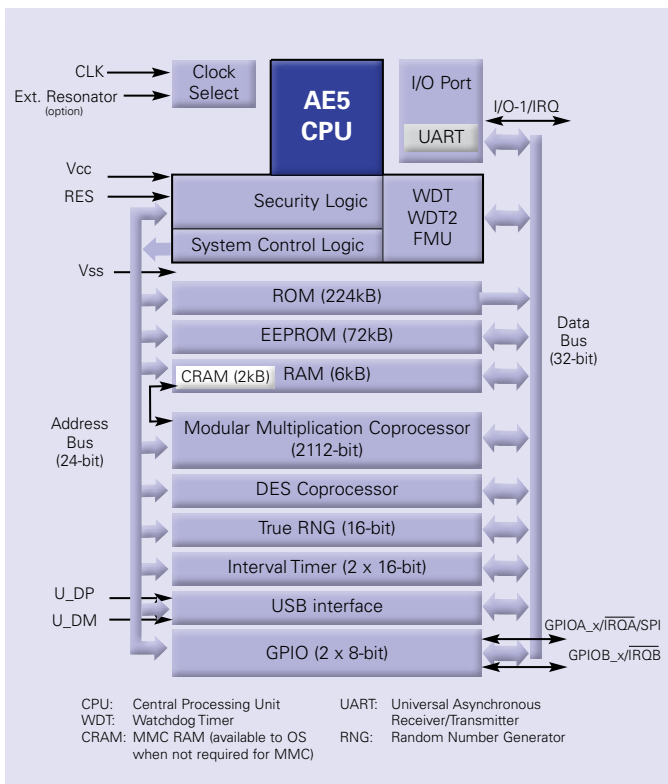
The whole ISC process (secure chip design environment, secured production facilities and secure handling during shipment to the customer) is constantly reviewed in order to maximise the overall security package.

Many security features such as integrated sensors, distributed layout, Random Number Generator (RNG), 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.

AE56U secure MCU specification

CPU	Memory	Crypto Coprocessors	Interface	Security functions	Peripherals
<ul style="list-style-type: none"> • 32-bit AE-5 core • Up to 12MHz internal clock • 8 x 32-bit general purpose registers (configurable in 16-bit registers) • 16MB linear address space • High performance, low-power • One clock cycle per instruction 	<ul style="list-style-type: none"> • 72kB EEPROM • 224kB ROM • 6+2kB RAM 	<ul style="list-style-type: none"> • Modular multiplication RSA 2112-bit, Up to 24MHz clock • DES 	<ul style="list-style-type: none"> • Contact ISO/IEC 7816-3 • USB 2.0 full speed (standard commands supported by hardware) • 2 ports of 8-bit GPIOs with SPI support and 2 high-current output lines 	<ul style="list-style-type: none"> • Detectors for voltage, light, etc • True random number generator • 2 Watchdog timer • Firewall management unit 	<ul style="list-style-type: none"> • DMAC • 2 Interval timers



EEPROM

High-reliability 72kB EEPROM

- E/W time: 2.0ms (typ)
- E/W cycle: 100k (Max)
- Data retention: 10 years
- Easy EEPROM write by single instruction
- EEPROM write by single instruction
- 128 Bytes programming with one instruction
- EEPROM programming voltage and timing generated on-chip

ROM

- 224kB user ROM

RAM

- 8kB: 6kB RAM + 2kB coprocessor RAM

Internal oscillator

- Asynchronous clock from external clock
- External resonator (option) for USB clock and system clock
- Low-power clock stop and sleep mode

USB

- USB 2.0 full speed mode (12MB/s)
- Standard commands processed by hardware
- Support for control and bulk transfer
- 5 endpoints can be specified
- 18 kinds of interrupts

UART

- IIS0/IEC 7816-3 T=0/T=1, full duplex capable
- High-speed 8clock/etu communication
- Support for DMA (Direct Memory Access)

I/O Port: 16 channels

- Support external interrupt (falling/rising edge)
- High-speed SPI support (two 32-bit shift register)
- 2 channels high-current capable
- Open-drain/push-pull mode selectable

16-bit interval timer: 2 channels

- Input clock selectable: divider 32, 64, 128, 256

RNG

- AIS31compliant 16-bit True Random Number Generator (TRNG)

Security

- Detectors for voltage/frequency/temperature/light etc.
- Firewall Management Unit

Operating voltage

- 3V, 5V

Operating frequency

- External input frequency: 1 to 5MHz

Operating temperature

- -25 to +85°C

Shipping form

- Wafer, etc...

Development tool

- Integrated development environment (High-performance Embedded Workshop)
- Full spec. emulator: E6000H
- C/C++ compiler

Documentation/support

- Hardware manual
- User guidance for security-conscious software design
- Application notes
- Supported by dedicated application engineering team

Optional software library

- Tamper-resistant Advanced Cryptographic Library (ACL)
- USB CCID/HID class firmware



AE56U features

CPU

- High-performance 32-bit AE-5 Core
- Upwardly compatible with AE-4
- Instruction execution: 1 clock (min)
- 16MB linear address space
- High performance, low-power

High-speed operation

- Max clock rate: 12MHz
- Add or subtract: 1 clock cycle
- Multiply 16 x 16-bit: 1 clock cycles
- Divide 16 ÷ 8-bit: 12 clock cycles

Two-way general register configuration

- 16 x 8-bit registers + 16 x 16-bit registers, or 8 x 32-bit registers

Streamlined, concise instruction set

- Instruction length: 2 up to 10 bytes
- Register/memory arithmetic and logic operations
- MOV instruction for data transfer between register/memory

Instruction set features

- Multiply instruction (8 x 8-bit and 16 x 16-bit)
- Divide instruction (16 ÷ 8-bit and 32 ÷ 16-bit)
- Bit accumulator instructions
- Register indirect specification of bit positions
- EEPROM write instruction (EEPMOV.B and EEPROMOV/P.W)
- High-speed block transfer instruction

Modular multiplication coprocessor

- Max clock rate: 24MHz
- 2112-bit (Max) modular multiplication

DES coprocessor

- Single DES calculation in 18 clocks cycles
- Triple DES calculation in 75 clock cycles (implemented by software)



Renesas Electronics Europe

www.renesas.eu

April 2010 Printed in UK 20-122B

© 2010 Renesas Electronics Europe.

All rights reserved. Printed in UK.