

## High-security 16-bit microcontroller



### AE470

#### Features

144kB EEPROM; 288kB ROM; 8kB RAM; enhanced environmental specifications.

#### Applications

The AE470G is a secure microcontroller based on Renesas' AE4 CPU, already featured in hundreds of millions of SIM and USIM applications. This device has been further enhanced to meet the technical requirements specific to the wireless cellular machine to machine (M2M) market. Its highly integrated memory of 288kB ROM and 144kB EEPROM enables it to support multi-application cards based on sophisticated Operating Systems (OS) such as JavaCard™.

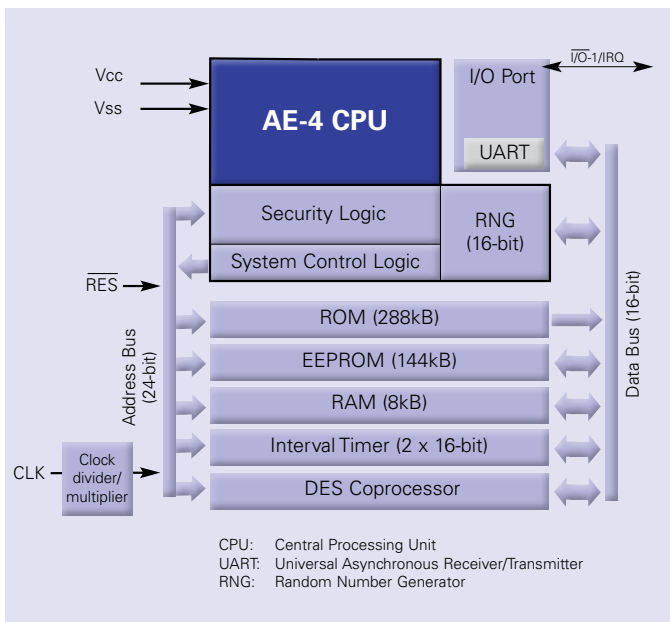
The AE470G is manufactured in specially controlled and ISO-certified silicon factories, using a highly reliable 150nm CMOS process technology. The device has been qualified against an extended temperature range (-40 to +105°C, with cyclic profile), which, combined with its superior EEPROM technology, featuring 500K write/erase cycles and 10 year data retention, makes it particularly suitable for the extreme environmental demands of M2M applications.

The AE470G supports the A,B and C voltage classes (1.8V to 5V) of the current release of specifications for mobile communication ETSI-SCP.

#### AE470G secure MCU specification

CPU	Memory	Operating temperature	Interface	Security functions	Package
<ul style="list-style-type: none"> <li>• 16-bit AE-4 Core</li> <li>• 16MB linear address space</li> <li>• Up to 10MHz clock frequency</li> </ul>	<ul style="list-style-type: none"> <li>• 288kB ROM</li> <li>• 8kB RAM</li> <li>• 144kB EEPROM</li> <li>• EEPROM features : 500K w/e cycles, 10 year data retention (cyclic temperature profile)</li> </ul>	<ul style="list-style-type: none"> <li>• -40 to +105°C M2M conditions (cyclic temperature profile).</li> </ul>	<ul style="list-style-type: none"> <li>• Contact ISO/IEC 7816-3</li> <li>• Interval timers</li> <li>• DES coprocessor</li> </ul>	<ul style="list-style-type: none"> <li>• Detectors for voltage, etc</li> <li>• Random Number Generator</li> <li>• On-chip memory encryption &amp; check etc.</li> <li>• DES coprocessor</li> </ul>	<ul style="list-style-type: none"> <li>• USON-8 (5 x 6 mm)</li> </ul>

JavaCard™ is a registered trademark of SUN Microsystems



### Integrated Security Concept (ISC)

The AE470G, designed under Renesas Technology's 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; it 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 included providing a strong on-chip hardware security structure. Uniquely, Renesas Technology smart card devices are fabricated using Metal Oxide Nitride Oxide Silicon (MONOS) EEPROM structure. The advantages of MONOS compared to standard EEPROM structures are high resistance to radiation disturbance, high reliability and endurance.

### Specification

#### CPU

- 16-bit AE-4 core in 0.15  $\mu\text{m}$  CMOS technology with 24-bit linear addressing
- High-speed CPU based on the H8/300H CPU
- 16 x 16-bit general purpose registers
- Up to 16MB linear address space
- Two-way general register configuration
- 16 x 8-bit registers + 16 x 16-bit registers, or 8 x 32-bit registers
- High-performance, low-power
- Up to 10MHz at 3V
- Add/subtract: 0.20  $\mu\text{s}$
- Multiply/divide: 1.40  $\mu\text{s}$

#### On-chip memory

- 288kB ROM
- 8kB RAM
- 128kB + 16kB F-SMONOS EEPROM
- Write/erase granularity: 128 Bytes
- Write/erase time: 2.4 ms max
- Page unit erase time: 1.3 ms max
- Page unit overwrite time: 1.1 ms max
- Data retention time: 10 years guaranteed
- Rewrite endurance: 500,000 times
- Protected against accidental writing and erasing
- High-speed block transfer instruction
- Additional features tailored for M2M applications
- Highly reliable EEPROM supporting continuous operation over extended periods of time, 500,000 rewrite cycles, and a data storage period after programming of 10 years.

#### Operating temperature range

- -40 to +105°C (cyclic temperature profile)

#### I/O Port

- 1 channel
- UART
- ISO/IEC 7816-3 T=0/T=1, Half Duplex capable
- High-speed 8 clock/etu communication

#### RNG

- 16-bit random generator

#### Internal timer

- 2 x 16-bit Interval Timers

#### DES Coprocessor

- Single DES in 18 clock cycles (ECB mode)
- Triple DES and CBC, OFB, CFB modes can be implemented by software

#### Security

- Detectors for voltage/frequency etc.
- Operating voltage 1.8/3/5V

#### Package

- 8-pin ultra-thin small-outline non-lead (USON) surface mount package measuring only 5.0 x 6.0 mm (0.65 mm thick)

#### Development tool

- Integrated development environment (High-performance Embedded Workshop)
- Full spec emulator: E6000 and device simulator
- C/C++ Compiler
- Documentation/support
- Hardware Manual
- User Guidance for security-conscious software design
- Application Notes
- Supported by dedicated application engineering team

