

## High-security 16-bit microcontroller



### RS44C



#### RS44C

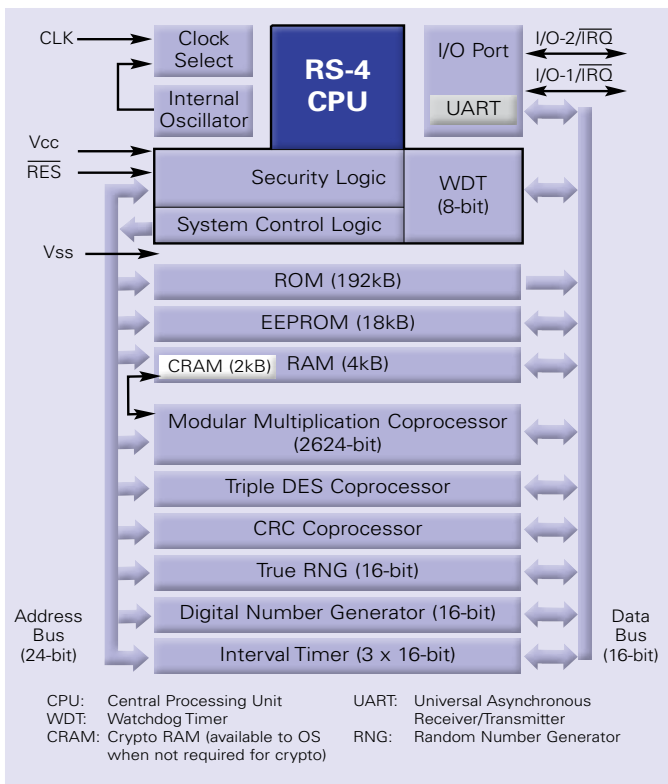
The RS44C is a 16-bit secure microcontroller designed for high-performance and multifunction smart cards based on sophisticated Operating Systems (OS). It offers enhanced performance comparable to conventional 32-bit secure microcontrollers and five times faster than Renesas' conventional 16-bit secure microcontrollers. This high performance, together with the integrated encryption processing functions, makes the RS44C well suited for all different types of high security applications, such as those in the financial and identification fields.

Special features, like internal frequency adjustment, together with low-power design methodologies, ensure optimised functionality for portable devices.

The RS-4 family is upwardly compatible with our existing AE-4 secure microcontrollers and its features and support tools are designed to make the implementation of a secure system easier for the software developer.

#### RS44C secure MCU specification

CPU	Memory	Crypto Coprocessors	Peripherals	Security functions	Interface
<ul style="list-style-type: none"> <li>• 16-bit RS-4 core</li> <li>• Up to 20MHz clock</li> <li>• 16 x 16-bit general purpose registers</li> <li>• 16MB linear address space</li> <li>• High performance, low-power</li> <li>• One clock cycle per instruction</li> </ul>	<ul style="list-style-type: none"> <li>• 18kB EEPROM</li> <li>• 192kB ROM</li> <li>• 4+2kB RAM</li> </ul>	<ul style="list-style-type: none"> <li>• Modular multiplication                             <ul style="list-style-type: none"> <li>– RSA 2624-bit,</li> <li>– Up to 40MHz clock</li> </ul> </li> <li>• Triple DES</li> <li>• CRC</li> </ul>	<ul style="list-style-type: none"> <li>• Internal oscillator</li> <li>• UART (supports 8 clk/etu)</li> <li>• Interval timers</li> </ul>	<ul style="list-style-type: none"> <li>• Detectors for voltage, frequency, others</li> <li>• True Random Number Generator (AIS31 class P2)</li> <li>• Watchdog Timer</li> <li>• On-chip memory check</li> <li>• Fault-tolerant design</li> </ul>	<ul style="list-style-type: none"> <li>• Contact</li> <li>• ISO/IEC 7816-3</li> <li>• I/O-2 supported</li> </ul>



## RS44C features

### CPU

- High-performance 16-bit RS-4 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: 20MHz
- Add or Subtract: 1 clock cycle
- Multiply 16 x 16-bit: 4 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 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 EEPMOV/P.W)
- High-speed block transfer instruction

### Modular multiplication coprocessor

- Max clock rate: 40MHz
- 2624-bit (max) modular multiplication
- Suitable for RSA and ECC

### Triple DES coprocessor

- 2key/3key triple DES calculation in 54 clocks
- Single DES in 18 clock cycles

## EEPROM

### High reliability 18kB EEPROM (F-SMONOS)

- E/W time: 2.0ms (typ)
- E/W cycle: 500k (typ)
- Data retention: 10 years
- High-speed smart overwrite
- 256B OTP area (ROM option)
- Unique chip ID writing option
- EEPROM write by single instruction
- 1 to 64 bytes programming with one instruction
- EEPROM programming voltage and timing generated on-chip

### ROM

- 192kB User ROM

### RAM

- 6kB: 4kB RAM + 2kB coprocessor RAM

### Internal oscillator

- Asynchronous clock from external clock
- Supports maximum performance mode
- Low-power clock stop and sleep mode

### UART

- ISO/IEC 7816-3 T=0/T=1
- High-speed 8clock/etu communication

### I/O Port: 2 channels

- Supports external interrupt

### 16-bit Interval Timer: 3 channels

- Input Clock selectable: external/internal

### RNG

- AIS31/P2 compliant 16-bit True Random Generator (TRNG)

### CRC Coprocessor

- CRC-16-CCITT polynomial
- 1 cycle calculation from data input

### Security

- Watchdog timer (ROM option)
- Detectors for voltage/frequency/temperature/light etc.
- Protection of memory and bus data
- Memory data check function
- Certifications: EMVCo/CC EAL5+ (planned)

### Operating voltage

- 3V, 5V

### Operating frequency

- External input frequency: 1 to 8MHz

### Operating temperature

- -25 to +85°C

### Shipping form

- Wafer, COT (Chip On Tape), etc.

### Development tool

- Integrated development environment (High-performance embedded workshop)
- Full spec emulator: E100
- 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 Renesas Cryptographic Library (RCL)
- RSA, CRT, Key Generation, Hash
- Certification: EMVCo/CC EAL5+ (planned)

