

High-security 16-bit dual-interface microcontroller



RS44C



RS44X / RS45X

The RS44X and RS45X are 16-bit secure dual-interface microcontrollers designed for high-performance and multifunction smart cards based on sophisticated Operating Systems (OS). They offer 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 device well suited for all different types of high security applications, such as those in the financial and identification fields. The RS44X and RS45X support both contact (ISO7816) and contactless (ISO14443) communication interfaces.

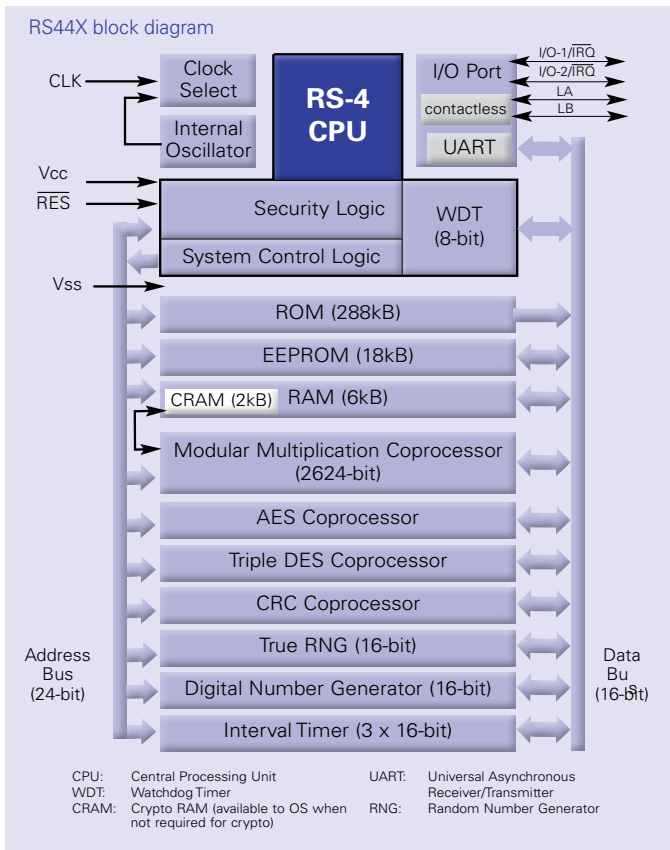
The contactless interface is designed for type A, B, FeliCa™ and MIFARE™ communication.

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.

RS44X / RS45X secure MCU specification

| CPU | Memory | Crypto Coprocessors | Peripherals | Security functions | Interface |
|---|--|--|---|--|---|
| <ul style="list-style-type: none"> • 16-bit RS-4 core • Up to 20MHz clock • 16 x 16-bit general purpose registers • 16MB linear address space • High performance, low-power • One clock cycle per instruction | <ul style="list-style-type: none"> • 18kB / 36kB EEPROM • 288kB ROM • 6+2kB RAM | <ul style="list-style-type: none"> • Modular multiplication <ul style="list-style-type: none"> – RSA 2624-bit, – Up to 40MHz clock • Triple DES • CRC • AES | <ul style="list-style-type: none"> • Internal oscillator • UART (supports 8 clk/etu) • Interval timers | <ul style="list-style-type: none"> • Detectors for voltage, frequency, others • True Random Number Generator (AIS31 class P2) • Watchdog timer • On-chip memory check • Fault-tolerant design | <ul style="list-style-type: none"> • Contact ISO/IEC 7816-3 • Contactless ISO/IEC14443 Type A, B and FeliCa™ • I/O-2 supported • MIFARE Plus™ |



RS44X/RS45X 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

AES coprocessor

- ECB/CBC and OFB supported
- 128-bit encryption in 113 clocks (173 clocks with key expansion included)

Triple DES coprocessor

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

EEPROM

High reliable 18kB (RS44X), 36kB (RS45X) 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

- 288kB user ROM

RAM

- 8kB: 6kB 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

Contactless interface

- ISO/IEC 14443 type A and B
- Supports FeliCa™ and MIFARE Plus™
- Rate up to 847 kbit/s

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
- Planned certifications: EMVCo/CC EAL5+

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
- Planned certification: EMVCo/CC EAL5+



RENESAS

Renesas Electronics Europe

www.renesas.eu

April 2010 Printed in UK 20-121B

© 2010 Renesas Electronics Europe.

All rights reserved. Printed in UK.