

High security 32-bit smart card microcontroller



AE55C1



Features

40kB EEPROM, 240kB ROM, 8kB RAM 2112bytes coprocessor

Applications

The highly integrated memory and outstanding 32-bit CPU performance of the AE55C1 enables it to support multi-application cards based on sophisticated Operating Systems (OS), including JavaCard™, and MULTOS as well as SECCOS (Secure Chip Card Operating System) used for high security banking applications. Therefore the AE55C1 is best suitable for DDA payment, PayTV, ID applications and electronic purse used for payments in parking garages, public transport (ticketing), or as protection of minors (authentication at cigarette machines).

It also allows for enhanced functionality of Mobile Communication (SIM) 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, as well as complex and secured M-commerce and Digital Signature applications.

The new Renesas Electronics AE-5 family boasts impressive credentials. The AE55C1 offers ultimate performance through the enhancement of the CPU architecture that includes a 5-level pipeline and a byte code decoder and dispatcher. Renesas Electronics unique upward compatibility of AE55C1 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 AE55C1 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 (EEPROM, RAM, ROM) into a smart card, which is particularly useful for new innovative applications with their stronger requirements for complex OS, data and application storage.

The high functional integration of the AE55C1, including DES, PLL (Phase-Lock-Loop), UART, DMA and interval timer, facilitates the implementation of the latest requirements for OS and applications. As an example the integrated UART and DMA achieve the future 512/64 Fi/Di requirement.

With these advanced high performance features the AE55C1 provides an ideal platform for both current and future financial and digital signature applications whilst easily supporting a true multi-application environment.

Integrated Security Concept (ISC)

The AE55C1 designed under Renesas Electronics 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.

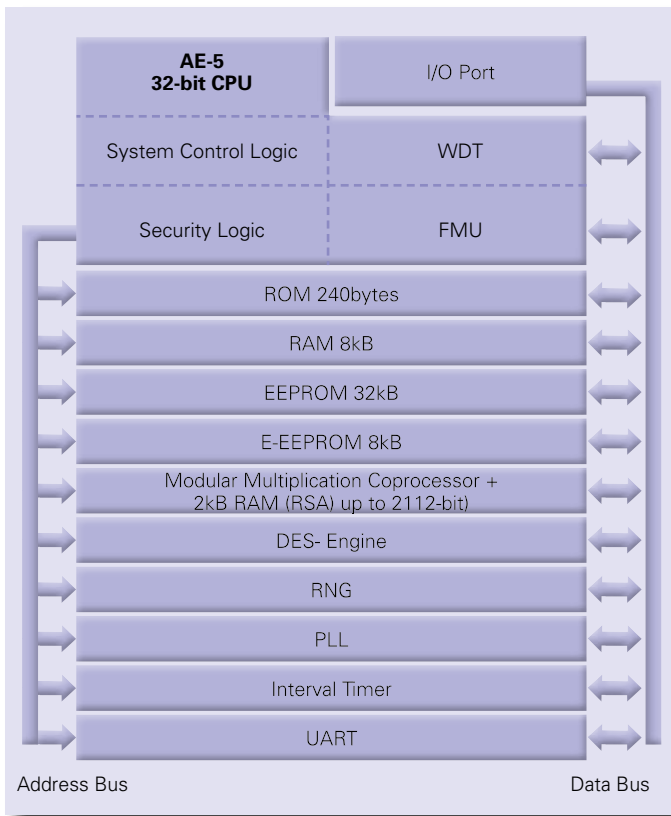
Many security features such as integrated sensors, distributed layout, on-chip data encryption, DES engine and power analysis attack protection are all included providing a strong on-chip hardware security structure.

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 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.

A high performance cryptographic coprocessor is complementary to the design concept ensuring final operating system efficiency, application integrity and an outstanding performance that meet tomorrows needs today. This coprocessor is equipped with its own 2kB 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.

The AE55C1 will be independently evaluated and certified conform to CC (Common Criteria) and ZKA (banking with digital signature) confirming the high security features of the AE55C1 making it best prepared for the future.



Specification

Item	Specification
CPU	<p>Two-way general register configuration</p> <ul style="list-style-type: none"> • Sixteen 8-bit registers + eight 16-bit registers, or eight 32-bit registers <p>High Speed Operation</p> <ul style="list-style-type: none"> • Max clock rate: internal clock 12MHz (at 3V) • AddSubtract: 83 ns • MultiplyDivide: 83 / 1000 ns <p>Streamlined, concise instruction set</p> <ul style="list-style-type: none"> • 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 (EEPROM.B and EEPROM.P/W)
 - High-speed block transfer instruction

Coprocessor

2112-bit key length
2kbytes RAM
RSA/ECC cryptography (RSA, Key generation, hash available as secure crypto library)

EEPROM

MONOS EEPROM Process
32kB EEPROM
8kB EXTRA EEPROM
Easy EEPROM write by single instruction
Read, write and erase of EEPROM byte by byte
1 to 64b 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

240kB User ROM

RAM

6kB + 2kB for coprocessor

DES

Engine Yes

16-bit Timers

2ch external clock

Peripherals

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

Single voltage power supply
4.5V to 5.5V
2.7V to 3.3V
1.62V to 1.98V

Clock

External clock input:

Frequency

fclk = 1MHz to 10MHz (Vcc = 4.5V to 5.5V)

Range

fclk = 1MHz to 10MHz (Vcc = 2.7V to 3.3V)

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

Standard -25 to + 85°C

Shipping Form

Wafer and COT (Chip On Tape-Module)



Renesas Electronics Europe

www.renesas.eu

April 2010 Printed in UK 20-100C

© 2010 Renesas Electronics Europe.

All rights reserved. Printed in UK.