Features

General

- Based on the ARM® SC100™ SecurCore™ 32-bit RISC Processor
- Two Instruction Sets
  - ARM High-performance 32-bit Instruction Set
  - Thumb® High-code-density 16-bit Instruction Set
- 4-Gbyte Linear Address Space
- Von Neumann Load/Store Architecture
  - Single 32-bit Data Bus for Instructions and Data
- 3-stage Pipeline Architecture
  - Fetch, Decode and Execute Stages
- 8-bit, 16-bit, and 32-bit Data Types
- On-chip Programmable System Clock up to 50 MHz
- Very Low Power Consumption:
  - Industry Leader in MIPS/Watt
  - Low-power Idle and Power-down Modes
- Bond Pad Locations Conforming to ISO 7816-2
- ESD Protection to ± 6000V
- Operating Ranges: 2.7V to 5.5V, GSM/3G Compliant, PC Industry Compatible, EMV

Memory

- 256K Bytes of ROM Program Memory
- 72K Bytes of EEPROM User Memory, Including 256 OTP Bytes
  - Typically More than 500,000 Write/Erase Cycles
- 10K Bytes of RAM

Peripherals

- Two I/O Ports
  - Configurable to Support Communication Protocols, Including ISO 7816-3 and 2-wire Protocols
- ISO 7816 Controller
  - Up to 625 kbps at 5 MHz
- Serial Peripheral Interface (SPI) Controller (up to 12 MHz)
- Two 16-bit Timers
- Random Number Generator (RNG)
- 2-level, 12-vector Interrupt Controller
- Hardware DES and Triple DES
- Checksum Accelerator
- CRC 16 / 32 Engine
- 32-bit Cryptographic Accelerator for Public Key Operations Including GF(2^N)
  - RSA, DSA, ECC, Diffie-Hellman
- Advanced MPU
- High-performance Hardware Java Card Accelerator

Security

- Dedicated Hardware for Protection Against SPA/DPA Attacks
- Advanced Protection Against Physical Attack
- Environmental Protection Systems
- Voltage and Frequency Monitors
- Secure Memory Management/Access Protection

Development Tools

- Hardware Development Support on the ATV3-91SC Voyager Emulation Platform. See the ATV3-91SC Emulator Product Preview for Further Details.

32-bit Secure Microcontroller for Smart Cards

AT91SC25672RC

Summary

Rev. 1575CS–SMIC–09/03

Note: This is a summary document. A complete document is available under NDA. For more information, please contact your local Atmel sales office.

Description

The AT91SC25672RC is a low-power, high-performance, 32-bit RISC microcontroller with ROM program memory, EEPROM data memory, and cryptographic accelerator, based on the new ARM SC100 advanced secure processor. The SC100 embedded core is the first member of the ARM SecurCore family. This general-purpose 32-bit processor offers high performance, very low power consumption, and additional features to help combat fraud.

The AT91SC25672RC features 72K bytes of high-performance EEPROM (fast erase/write time, high endurance). This allows system developers to offer their customers a true 64K bytes EEPROM, while still being able to use the remaining 8K bytes for their own purposes (e.g. customization and patches).

The cryptographic accelerator featured in the AT91SC series is the new AdvX™. It is based on a 32-bit multiplier-accumulator architecture which is designed to perform fast encryption and authentication functions. This enables fast computation and low-power operation. The AdvX, in conjunction with controlling firmware running within the SC100 core, supports standard finite fields arithmetic functions (including RSA, DSA, DH, ECC) and GF(2^N).

On top of the SC100´s MPU, a real hardware firewall can be used to increase the overall security level of the application without intense software development.

Unique hardware features significantly accelerate the execution of Java Card Byte Code by removing the common software bottlenecks encountered during the implementation of a Java Virtual Machine.

Additional security features include power and frequency protection logic, logical scrambling on program data and addresses, power analysis countermeasures and memory accesses controlled by a supervisor mode.

Pin Configuration

The AT91SC25672RC pinout conforms to the ISO 7816-2 interface. It also provides a second I/O port.

GND	Ground (reference voltage)
V_{CC}	Power supply input
I/O0	Input or output for serial data
I/O1	Second input or output for serial data Also used as Slave Select line for the SPI controller
MOSI	SPI Master output – Slave input
MISO	SPI Master input – Slave output
SCK	SPI Clock
CLK	Clock signal input to internal clock operating circuit
$\overline{\text{RST}}$	Reset signal input, a low state stops the ARM core

Note: By convention, the $\overline{\text{RST}}$ pin corresponds to the RST signal of the ISO 7816-3 Protocol. Both are active low.

Architectural Overview

The SC100 is a 3-stage pipeline, 32-bit RISC processor. It uses a Von Neumann load/store architecture, which is characterized by a single data and address bus for instructions and data.

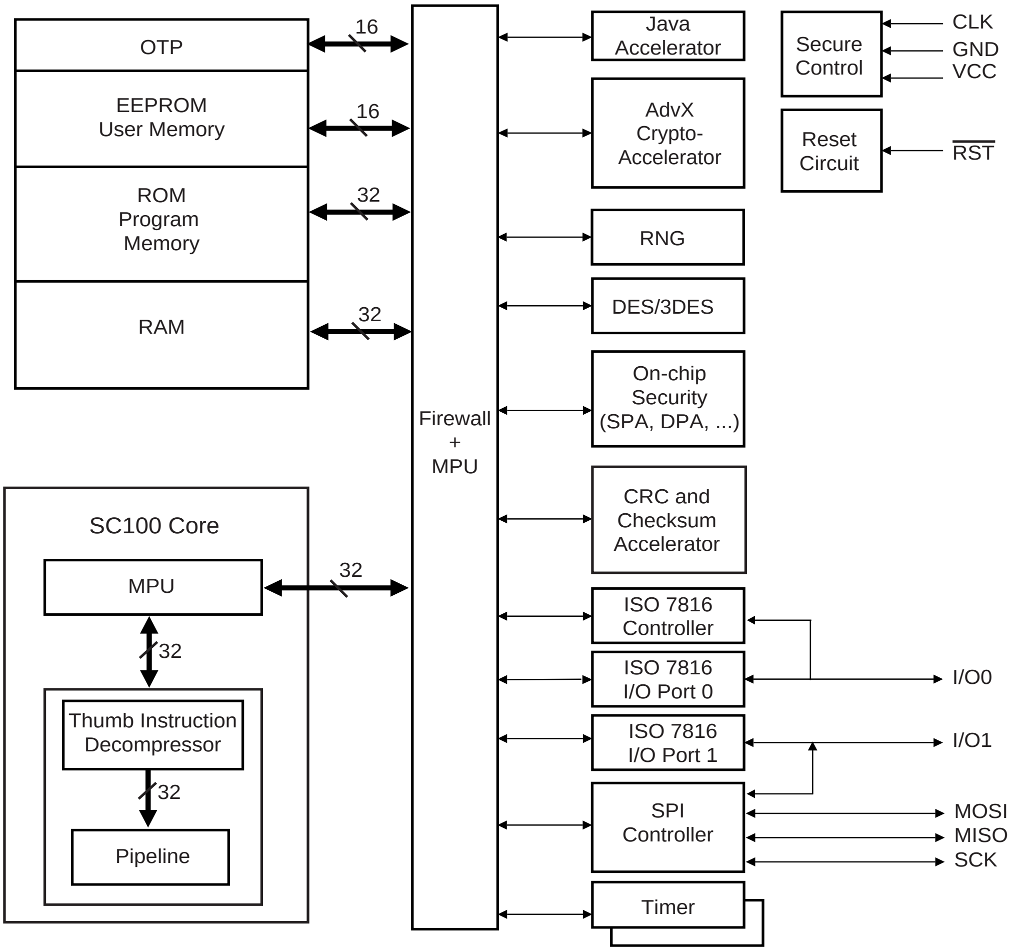
The SC100 processor employs a unique architectural strategy known as Thumb®, a super-reduced instruction set that is ideally suited for high-volume applications with memory restrictions, and applications where code density is an important factor. Essentially, the SC100 processor has two instruction sets:

- The standard ARM instruction set uses 32-bit instructions and offers maximum performance.
- The Thumb instruction set uses 16-bit instructions and offers maximum code density.

Both instruction sets operate on 8-bit, 16-bit, and 32-bit data types.

The Thumb´s 16-bit instruction length allows it to achieve almost twice the density of standard ARM code, while retaining most of the ARM´s performance advantage over a traditional 16-bit processor using 16-bit registers. This is possible because the 16-bit Thumb instructions operate on the same 32-bit register set as the 32-bit ARM instructions. Thumb code can be up to 35% smaller than the equivalent ARM code, while providing 160% of the performance of an equivalent ARM processor connected to a 16-bit memory system.

Figure 1. Block Diagram



Atmel Headquarters

Corporate Headquarters
2325 Orchard Parkway
San Jose, CA 95131
TEL 1(408) 441-0311
FAX 1(408) 487-2600

Europe
Atmel Sarl
Route des Arsenaux 41
Case Postale 80
CH-1705 Fribourg
Switzerland
TEL (41) 26-426-5555
FAX (41) 26-426-5500

Asia
Room 1219
Chinachem Golden Plaza
77 Mody Road Tsimhatsui
East Kowloon
Hong Kong
TEL (852) 2721-9778
FAX (852) 2722-1369

Japan
9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
Japan
TEL (81) 3-3523-3551
FAX (81) 3-3523-7581

Atmel Operations

Memory
2325 Orchard Parkway
San Jose, CA 95131
TEL 1(408) 441-0311
FAX 1(408) 436-4314

Microcontrollers
2325 Orchard Parkway
San Jose, CA 95131
TEL 1(408) 441-0311
FAX 1(408) 436-4314

La Chantrerie
BP 70602
44306 Nantes Cedex 3, France
TEL (33) 2-40-18-18-18
FAX (33) 2-40-18-19-60

ASIC/ASSP/Smart Cards
Zone Industrielle
13106 Rousset Cedex, France
TEL (33) 4-42-53-60-00
FAX (33) 4-42-53-60-01

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906
TEL 1(719) 576-3300
FAX 1(719) 540-1759

Scottish Enterprise Technology Park
Maxwell Building
East Kilbride G75 0QR, Scotland
TEL (44) 1355-803-000
FAX (44) 1355-242-743

RF/Automotive
Theresienstrasse 2
Postfach 3535
74025 Heilbronn, Germany
TEL (49) 71-31-67-0
FAX (49) 71-31-67-2340

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906
TEL 1(719) 576-3300
FAX 1(719) 540-1759

***Biometrics/Imaging/Hi-Rel MPU/
High Speed Converters/RF Datacom***
Avenue de Rochepleine
BP 123
38521 Saint-Egreve Cedex, France
TEL (33) 4-76-58-30-00
FAX (33) 4-76-58-34-80

e-mail
literature@atmel.com

Web Site
http://www.atmel.com

Atmel Corporation makes no warranty for the use of its products, other than those expressly contained in the Company's standard warranty which is detailed in Atmel's Terms and Conditions located on the Company's web site. The Company assumes no responsibility for any errors which may appear in this document, reserves the right to change devices or specifications detailed herein at any time without notice, and does not make any commitment to update the information contained herein. No licenses to patents or other intellectual property of Atmel are granted by the Company in connection with the sale of Atmel products, expressly or by implication. Atmel's products are not authorized for use as critical components in life support devices or systems.

Printed on recycled paper.