

## Features

### General

- Based on the ARM® SC100™ SecureCore™ 32-bit RISC Processor
- Two Instruction Sets
  - ARM High-performance 32-bit Instruction Set
  - Thumb® High-code-density 16-bit Instruction Set
- 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 50MHz
- Very Low Power Consumption
  - Industry Leader in MIPS/Watt
  - Low power Idle and Power down Modes
- Bond Pad Locations Confirming to ISO7816-2
- ESD Protection to  $\pm 6000V$
- Operating ranges: 1.62V to 5.5V, GSM/3G Compliant, PC Industry Compatible, EMV

### Memory

- 512K Bytes of ROM Program Memory
- 384K Bytes of EEPROM, Including 256 OTP Bytes
  - Typically More than 500,000 Write/Erase Cycles at a Temperature of 25°C
  - 10 Years Data Retention
- EEPROM Erase Only Mode
- Write EEPROM With or Without Autoerase
- 24K Bytes of RAM (2K Bytes shared with AdvX™ crypto processor)
- 32K Bytes of ROM dedicated to Atmel's crypto Library

### Peripherals

- One ISO 7816 Controller
  - Up to 625kbps at 5 MHz
- Serial Peripheral Interface (SPI) Controller (up to 20MHz)
- USB Interface (5 Endpoints)
  - USB V2.0 Full-speed (12Mbps), Suspend/Resume Modes Supported
  - 4 Configurable Endpoints in Addition to Endpoint EP0
  - Dynamic Pull-up Attachment
- USB\_IC (Inter Chip) 0.8e Interface
- Interface for External NAND Flash Memory
- Single Wire Interface (Digital Interface to RF front end chip)
- Two 16-bit Timers
- Random Number Generator (RNG)
- 2-level, 15-vector Interrupt Controller
- Hardware DES and Triple DES (DPA Resistant)
- Checksum Accelerator
- CRC 16/32 Engine
- 32-bit Cryptographic Accelerator for Public Key Operations
  - RSA, DSA, ECC, Diffie-Hellman
- High performance Hardware Java Card Accelerator

### Security

- Dedicated Hardware for Protection Against SPA/DPA Attacks
- Protection Against Physical Attack
- Environmental Protection Systems
- Voltage, Frequency, Light, and Temperature Protection Systems



## 32-bit Secure Microcontrollers

## AT91SC 512384RCT Summary

6525AS–SMIC–16Jan06



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



- Secure Memory Management/Access Protection

## Development Tools

- Hardware Development Support on the AT91SC Voyager Emulation Platform
- Software Libraries and Application Notes

## Description

The AT91SC512384RCT is a low power, high performance, 32-bit RISC microcontroller with ROM program memory, EEPROM data memory, and cryptographic accelerator, based on the ARM SC100 advanced secure processor. This general purpose 32-bit processor offers high performance, very low power consumption, and additional features to help combat fraud.

The AT91SC512384RCT features 384K bytes of high performance EEPROM (fast erase/write time, high endurance).

The AT91SC512384RCT also features a USB full speed 2.0 port to allow very high speed transactions with a USB host terminal. USB interface requires the addition of an external 48MHz resonator.

The AT91SC512384RCT features a SPI (Serial Peripheral Interface) port to provide either high speed interface with external terminal or to connect external NOR Flash memory. It also features an interface for NAND Flash memory.

On top of the SC100s MPU, a real hardware firewall can be used to increase the overall security level of the application without intense software development.

The cryptographic accelerator featured in the AT91SC series is the AdvX™, an N-bit multiplier-accumulator dedicated to performing fast encryption and authentication functions. AdvX is based on a custom 32-bit co-processor, thus enabling fast computation and low power operation. The AdvX in conjunction with controlling firmware running within the SC100 core, supports standard finite arithmetic functions (including RSA, DSA, DH and ECC) and GF(2N).

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 access controlled by a supervisor mode.

## Pin Configuration

The AT91SC512384RCT pinout configuration confirms to the ISO7816-2 interface.

Note: By convention, the  $\overline{\text{RST}}$  pin corresponds to the RST signal of the ISO7816-3 Protocol, both are active low.)

|                                               |                                                        |                                          |                                        |
|-----------------------------------------------|--------------------------------------------------------|------------------------------------------|----------------------------------------|
| <b>GND</b>                                    | Ground (reference voltage)                             | <b><math>\overline{\text{WE}}</math></b> | Flash Interface (Write Enable)         |
| <b>Vcc</b>                                    | Power Supply Input                                     | <b>ALE</b>                               | Flash Interface (Address Latch Enable) |
| <b>ISO I/O0</b>                               | Input or Output for serial data (ISO7816)              | <b>CLE</b>                               | Flash Interface (Command Latch Enable) |
| <b>ISO CLK</b>                                | Clock signal input to external clock operating circuit | <b><math>\overline{\text{CE}}</math></b> | Flash Interface (Chip Enable)          |
| <b>ISO <math>\overline{\text{RST}}</math></b> | Reset signal input, a low state stops the ARM core     | <b><math>\overline{\text{RE}}</math></b> | Flash Interface (Read Enable)          |
| <b>C6</b>                                     | SWP dedicated pin                                      | <b>IO0</b>                               | Flash Interface IO0                    |
| <b>USB D+</b>                                 | USB D+                                                 | <b>IO1</b>                               | Flash Interface IO1                    |
| <b>USB D-</b>                                 | USB D-                                                 | <b>IO2</b>                               | Flash Interface IO2                    |
| <b>USB XIN</b>                                | USB XIN                                                | <b>IO3</b>                               | Flash Interface IO3                    |

|                                   |                                 |                                       |                                                   |
|-----------------------------------|---------------------------------|---------------------------------------|---------------------------------------------------|
| <b>USB XOUT</b>                   | USB XOUT                        | <b><math>\overline{SS}/IO4</math></b> | SPI Slave Select/Flash Interface IO4              |
| <b><math>\overline{WP}</math></b> | Flash Interface (Write Protect) | <b>SCK/IO5</b>                        | SPI Clock/Flash Interface IO5                     |
|                                   |                                 | <b>MOSI/IO6</b>                       | SPI Master Output-Slave Input/Flash Interface IO6 |
|                                   |                                 | <b>MISO/IO7</b>                       | SPI Master Output-Slave Input/Flash Interface IO7 |

## Architectural Overview

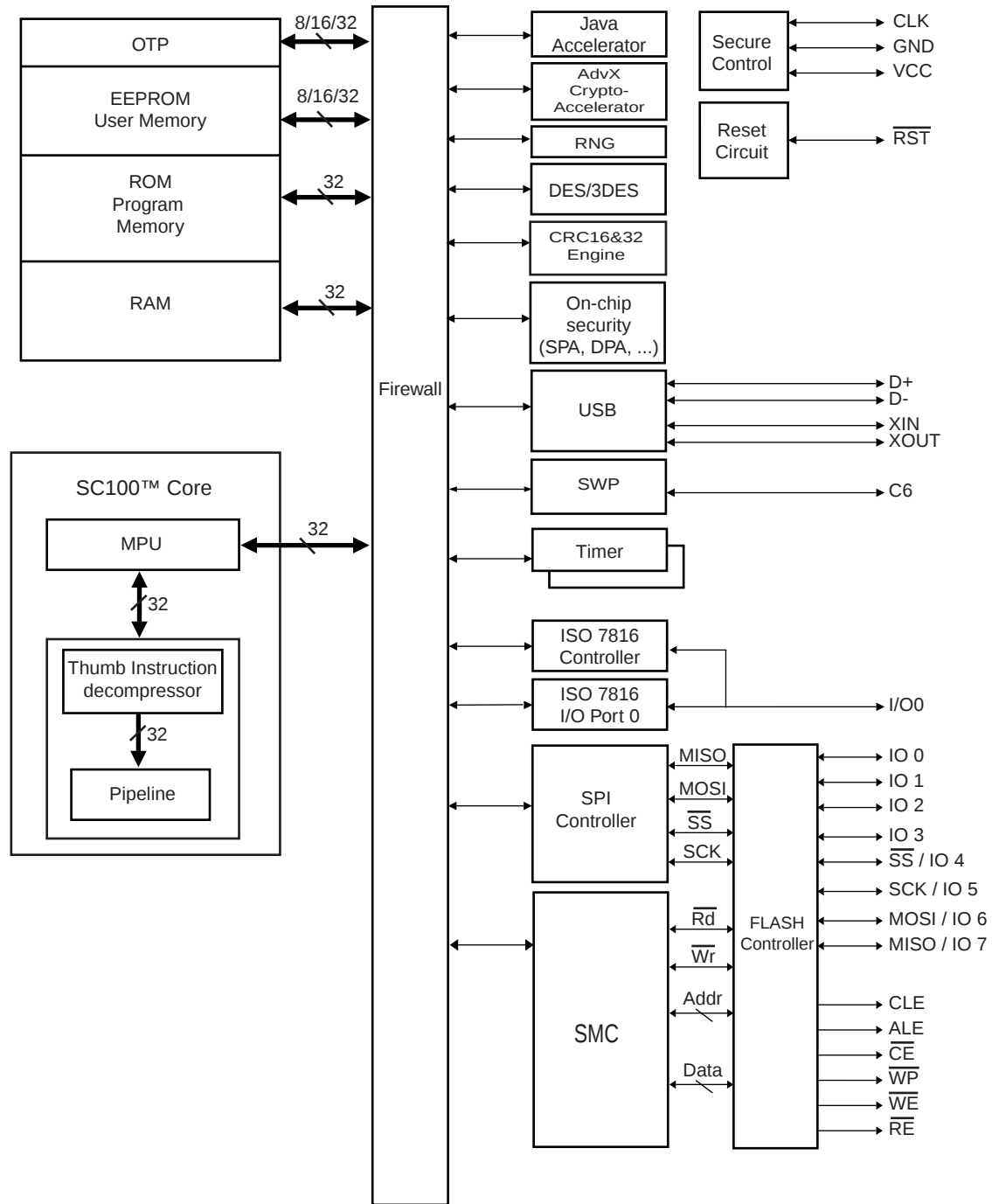
The SC100 is a 3 stage pipeline, 32-bit RISC processor. It uses a Von Neumann Load/store architecture, this architecture is characterized by a single data and address bus for instruction data. The SC100 processor employs a unique architectural strategy known as Thumb®, a super reduced instruction set 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 using 32-bit instructions and offering maximum performance
- The Thumb instruction set using 16-bit instructions and offering 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, whilst retaining most of the ARM 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 instruction set. Thumb code can be up to 35% smaller than the equivalent ARM code, whilst providing 160% of the performance of an equivalent ARM processor connected to a 16-bit memory system.

Figure 1 shows the block diagram of the AT91SC512384RCT device.



**Figure 1.** AT91SC512384RCT Block Diagram



## Atmel Corporation

2325 Orchard Parkway  
San Jose, CA 95131, USA  
Tel: 1(408) 441-0311  
Fax: 1(408) 487-2600

## Regional Headquarters

### Europe

Atmel Sarl  
Route des Arsenalux 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 Tsimshatsui  
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, USA  
Tel: 1(408) 441-0311  
Fax: 1(408) 436-4314

### Microcontrollers

2325 Orchard Parkway  
San Jose, CA 95131, USA  
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, USA  
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, USA  
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

---

## Literature Requests

[www.atmel.com/literature](http://www.atmel.com/literature)

**Disclaimer:** The information in this document is provided in connection with Atmel products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Atmel products. **EXCEPT AS SET FORTH IN ATMEL'S TERMS AND CONDITIONS OF SALE LOCATED ON ATMEL'S WEB SITE, ATMEL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ATMEL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ATMEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.** Atmel makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Unless specifically provided otherwise, Atmel products are not suitable for, and shall not be used in, automotive applications. Atmel's products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.

© Atmel Corporation 2006. All rights reserved. Atmel®, logo and combinations thereof, and others are registered trademarks. Everywhere You Are®, AdvX™ and others are the trademarks of Atmel Corporation or its subsidiaries.

ARM®, Thumb®, ARM powered®, SC100™, RealView™, and SecureCore™ are the trademarks of ARM Ltd.

Other terms and product names may be trademarks of others.



Printed on recycled paper.

6525AS-SMIC-16Jan06