Features

General

- Based on the ARM® SC100™ SecurCore™ 32-bit RISC Processor
- Two Instructions 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 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: 1.62V to 5.5V, GSM/3G Compliant, PC Industry Compatible, EMV

Memory

- 128M Bytes of external Flash memory
  - Typically 100,000 Write/Erase Cycles
- 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 accelerator)
- 32K Bytes of ROM dedicated to ATMEL's crypto-library

Peripherals

- ISO 7816 Controller
  - Up to 625 kbps 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
- Checksum Accelerator
- CRC 16 / 32 Engine
- Hardware DES and Triple DES
- 32-bit Cryptographic Accelerator for Public Key Operations
- 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, Frequency, Light and Temperature Protection Systems

Development Tools

- Hardware Development Support on the ATV4-91SC Voyager Emulation Platform
- Software Libraries and Application Notes

32-bit Secure Microcontrollers

AT91SC512384-128M

Summary

6553A-SPD-03May07

Note: This a summary and draft document. For more information, please contact your local Atmel sales office.

Description

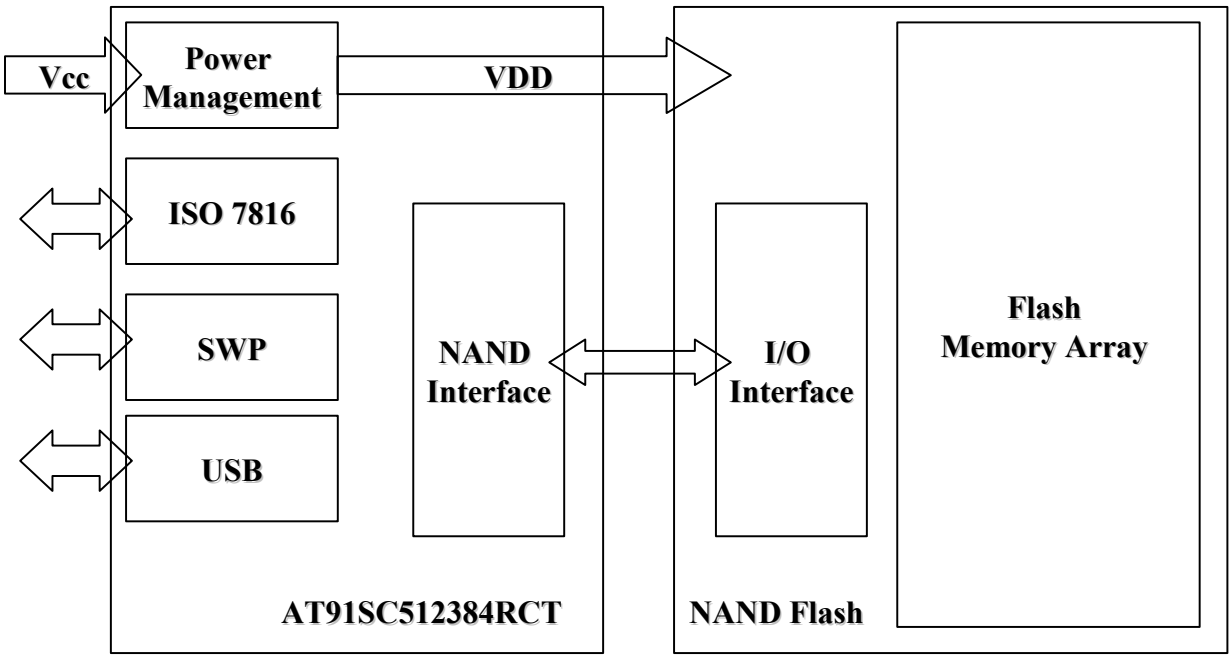
The AT91SC512384-128M is a dual chip solution, binding the AT91SC512384RCT device to a NAND Flash memory.

The AT91SC512384RCT is a Secure Microcontroller, low-power, high-performance, 32-bit RISC microcontroller with ROM program memory, internal 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 NAND Flash features are industry standard, High density, Low power, and lowest semiconductor cost-per-megabyte Flash solution. It provides 128M Bytes of Flash memory, organized in a 128M x 8 bits configuration.

The AT91SC512384-128M is delivered in an Plug-In SIM package with necessary drivers to manage all its peripherals.

Figure 1. AT91SC512384-128M Architecture



Architectural Overview

The AT91SC512384RCT secure microprocessor is attached to the NAND Flash device thru an interface providing:

- Power supply to the Flash memory, whatever external Vcc delivered
- Data transfer between the two devices and control on Flash memory

Atmel Corporation

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

Regional Headquarters

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/Secure Products
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

Literature Requests
www.atmel.com/literature

6553A-SPD-03May07