### **Features**

#### General

- High-performance, Low-power secureAVR<sup>™</sup> RISC Architecture
  - 133 Powerful Instructions (Most Executed in a Single Clock Cycle)
- Low-power Idle and Power-down Modes
- Bond Pad Locations Conforming to ISO 7816-2
- ESD Protection to ± 6000V
- Operating Ranges: from 2.7V to 5.5V
- Compliant With EMV 2000 Specifications; PC Industry Compatible
- Available in Wafers, Modules and Industry-standard Packages

# Memory

- 48K Bytes of ROM Program Memory
- 2K Bytes of EEPROM, Including 64-byte OTP Area and 192-byte Bit-addressable Area
  - 1 to 64-byte Program/Erase
  - 2 ms Program, 2 ms Erase
  - Typically 1,000,000 Write/Erase Cycles
  - 10 Years Data Retention
- 1K Bytes of RAM

# **Peripherals**

- ISO 7816 Controller
  - Up to 625 kbs at 5 MHz
  - Compliant with T = 0 and T = 1 Protocols
- One I/O Port
- Programmable Internal Oscillator (Up to 16 MHz on ROM)
- One 16-bit Timer
- Random Number Generator (RNG)
- 2-level, 5-vector Interrupt Controller
- Checksum Accelerator
- CRC 16 Engine (Compliant with ISO/IEC 3309)
- Hardware DES and Triple DES Is DPA Resistant

# Security

- Dedicated Hardware for Protection Against SPA/DPA Attacks
- Advanced Protection Against Physical Attack, Including Active Shield
- Environmental Protection Systems
- Voltage Monitor
- Frequency Monitor
- Temperature Monitor
- Light Protection
- Secure Memory Management/Access

# **Development Tools**

- Hardware/Software Development Support on Voyager Emulation Platform (ATV2)
- IAR Systems C-Spy® Debugger or AVR Studio® Version 4.06 or later
- Software Libraries and Application Notes



# Secure Microcontroller for Smart Cards

# AT90SC4802R

# **Preliminary**



local Atmel sales office.

available under NDA. For more information, please contact your

Rev. 1579AS-SMIC-25Nov02





# **Description**

The AT90SC4802R is a low-power, high-performance, 8-/16-bit microcontroller, based on the secureAVR<sup>™</sup> RISC architecture, with ROM program memory and EEPROM data memory. By executing powerful instructions in a single clock cycle, the AT90SC4802R achieves throughputs close to 1 MIPS per MHz. Its Harvard architecture includes 32 general-purpose working registers directly connected to the ALU, allowing two independent registers to be accessed in one single instruction executed in one clock cycle.

The AT90SC4802R uses the secureAVR architecture that allows the linear addressing of up to 8M bytes of code and up to 16M bytes of data, and also provides a number of new functional and security features.

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

A block diagram of the AT90SC4802R is shown in Figure 1.

Data Bus 8-bit OTP Access **RNG** Secure - GND Control Control VCC **EEPROM** User Memory General ROM Program Purpose PC Memory Registers 16 Access RAM Control Z **Data Memory** Instruction 8 Register Interrupt 16 Unit ALU ISO 7816 Instruction Controller Decoder 8 **1**16 ISO 7816 IN/OUT0 I/O Port 0 Control Status Lines Timer Register Reset RST Circuit 3 DES DPA Counter measures CRC and Checksum Accelerator

Figure 1. AT90SC4802R Secure AVR RISC Architecture





# **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 2002.

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.

ATMEL<sup>®</sup> and AVR Studio<sup>®</sup> are the registered trademarks of Atmel. secureAVR<sup>™</sup> is a trademark of Atmel.

 $C\text{-Spy}^{\$}$  is a registered trademark of IAR Systems AB. Other terms and product names may be the trademark of others.

