

---

## Features

### General

- Industry-standard M68HC05 Instruction Set, Including: 8 x 8 Bits Unsigned Multiply Instruction, True Bit Manipulation, Memory-mapped I/O
- Operating Voltage: 3.0V  $\pm$  10% or 5.0V  $\pm$  10%
- Meets GSM 11.11 & 11.12 Specifications and EMV 2000 Specification
- 5.0 MHz Maximum Internal Bus Frequency at 3.0V and 5.0V
- ESD Protection to  $\pm$  4000V
- Bond Pad Layout Conforming to ISO Standard ISO/IEC 7816-2
- External Maskable Interrupt on ISO Standard I/O Port (PA0)
- Power-saving Wait and Very Low-power Stop Modes
- Power-up Detection
- Available as Sawn Wafers, or in Industry-standard Packages and Modules

### EEPROM

- 8192 Bytes of EEPROM, Including 16 Control Bytes and 48 OTP Bytes
- 1- to 64-byte Write/Program/Erase
- 2 ms Program Time, 2 ms Erase Time
- 10 Years Data Retention
- Typically More than 1,000,000 Write/erase Cycles
- On-chip Charge Pump for EEPROM Programming, Driven by an Internal Oscillator

### ROM and RAM

- 32768 Bytes of ROM, Including 16 Bytes Reserved for Vectors
- 1024 Bytes of RAM with Security Wipe on Selected Areas

### Peripherals

- Single Bidirectional I/O Line (1-bit ISO/IEC 7816-3 Standard I/O Port)
- Time Base Circuitry (with Preset and Maskable Interrupt Capabilities)
- Watchdog Capability (Under Software Control)
- Hardware DES Module (Capable of Single Encryption or Decryption in 16 Clock Cycles)
- CRC Module (Allowing Generation of Checksums (ISO/IEC 3309))
- Random Number Generator (RNG)
- Serial Communications Interface (SCI)
  - Compliant with ISO/IEC 7816
  - Compliant with T = 0 and T = 1 Protocols
- 16-bit Timer with Prescaler and Autoload

### Security

- Dedicated Hardware to Resist Power Analysis Attacks
- Low and High Voltage Monitors with Narrow Voltage Window Mode
- Low and High Temperature Monitors
- Low Frequency Monitor
- High Frequency Filter/Monitor
- Advanced Physical Barrier to Enhance Tamper Resistance
- Illegal Access Reset
- Illegal Opcode Reset
- Memory Partitioning with Address Lockout Reset
- Scrambling Logic
- Tamper Monitor
- Physical Removal of Test Mode when Testing is Complete



---

## Secure Microcontroller for Smart Cards

---

**AT05SC3208R**

## Summary

Rev. 1554AS-11/01



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

## Current Development Tools

- Hardware Emulation Module (for the Motorola MMDS05 Development System)
  - Emulation Module (AT05SC3208R-EM3)

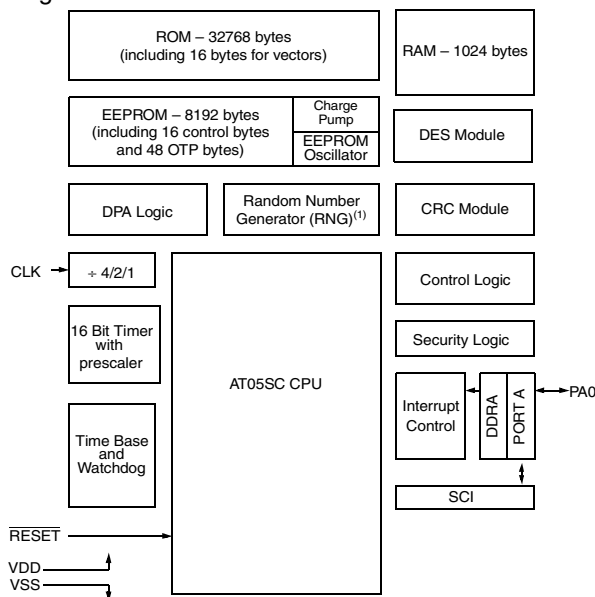
## Description

The AT05SC3208R is a member of Atmel's AT05SC family of single chip microcontrollers. Designed specifically for Smart-cards, embedded conditional access systems and other security conscious systems, these devices are based on the industry-standard M68HC05 low-power core and its instruction set.

The AT05SC3208R is designed to give a high level of protection against physical and power analysis attacks, and includes hardware features to assist in protecting against SPA and DPA attacks. On-board CRC and RNG modules are provided to assist in the design of high-security applications.

On-board memory comprises 32768 bytes of ROM, 1024 bytes of RAM and 8192 bytes of EEPROM. The EEPROM features 64-byte write, 2 ms program time, 2 ms erase time, typically more than 1,000,000 write/erase cycles, and greater than 10 years data retention. Application areas for the AT05SC3208R include GSM Mobile Phones, Finance and Set-top Boxes.

Figure 1. AT05SC3208R Block Diagram



© Atmel Corporation 2001.

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.

Corporate Headquarters, 2325 Orchard Parkway, San Jose, CA 95131, TEL (408) 441-0311, FAX (408) 487-2600  
Atmel Colorado Springs, 1150 E. Cheyenne Mtn. Blvd., Colorado Springs, CO 80906, TEL (719) 576-3300, FAX (719) 540-1759  
Atmel Grenoble, Avenue de Rochepleine, BP 123, 38521 Saint-Egreve Cedex, France, TEL (33) 4-7658-3000, FAX (33) 4-7658-3480  
Atmel Heilbronn, Theresienstrasse 2, POB 3535, D-74025 Heilbronn, Germany, TEL (49) 71 31 67 25 94, FAX (49) 71 31 67 24 23  
Atmel Nantes, La Chantrerie, BP 70602, 44306 Nantes Cedex 3, France, TEL (33) 0 2 40 18 18 18, FAX (33) 0 2 40 18 19 60  
Atmel Rousset, Zone Industrielle, 13106 Rousset Cedex, France, TEL (33) 4-4253-6000, FAX (33) 4-4253-6001  
Atmel Smart Card ICs, Scottish Enterprise Technology Park, East Kilbride, Scotland G75 0QR, TEL (44) 1355-357-000, FAX (44) 1355-242-743

ATMEL® is a registered trademark of Atmel.

Other terms and product names may be the trademarks of others.



Printed on recycled paper.

1554AS-15Nov01