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 ± 10% or 5.0V ± 10%
- Meets GSM 11.11 & 11.12 Specifications and EMV 96 v3.1.1 Specification
- 5.0 MHz Maximum Internal Bus Frequency at 3.0V and 5.0V
- ESD Protection to ± 4000V
- Bond Pad Layout Conforming to ISO Standard ISO 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 or Unsawn 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
- 1 ms Program Time, 1 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

RAM and ROM

- 24576 Bytes of ROM, including 16 Bytes Reserved for Vectors
- 512 Bytes of RAM with Security Wipe on Selected Areas

Peripherals

- Single Bidirectional I/O Line (1-bit ISO 7816/3 Standard I/O Port) with Sample Bit
- Time Base Circuitry (with Preset and Maskable Interrupt Capabilities)
- Watchdog Capability
- CRC Module (allowing generation of Checksums (ISO/IEC 3309))
- Random Number Generator

Security

- Dedicated Hardware to Resist Power Analysis Attacks
- Low and High Voltage Monitors
- Low and High Temperature Monitors
- Low Frequency Monitor
- High Frequency Filter/Monitor
- 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

Development Tools

- Hardware Emulation Module (for the Motorola MMDS05® Development System)
  - Emulation Module (AT05SCEM3R)
- Software Simulator based on HIWARE's HI-WAVE® Product
  - Simulator Software (AT05SCRSIM)
  - Simulator I/O Peripheral Board (AT05SCSPBR)

8-bit Secure Microcontroller with 8K EEPROM and Advanced Security Features

AT05SC2408R

Preliminary

Rev. 1545AS–11/00

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

Description

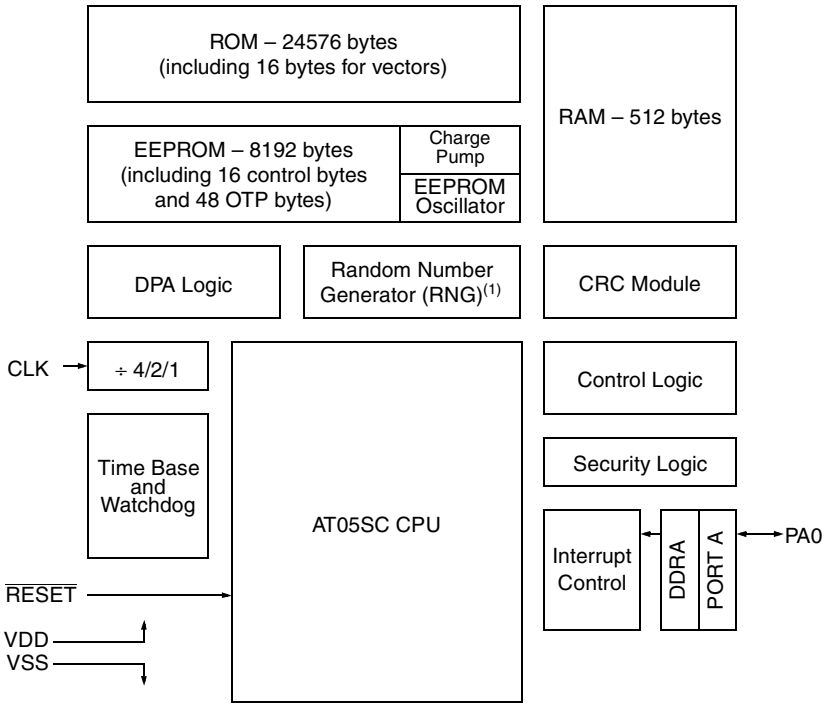
The AT05SC2408R is a member of Atmel's AT05SC family of single chip microcontrollers. Designed specifically for embedded conditional access systems and other security conscious systems, these devices are based on the industry-standard M68HC05 low-power core and its instruction set.

The AT05SC2408R 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 24K bytes of ROM, 512 bytes of RAM and 8K bytes of EEPROM. The EEPROM features 64-byte write, 1 ms program time, 1 ms erase time, typically more than 1,000,000 write/erase cycles, and greater than 10 years data retention.

Application areas for the AT05SC2408R include GSM Mobile Phones, Finance and Set-top boxes.

Block Diagram



Note: 1. A sampling/smoothing algorithm MUST be used in conjunction with the RNG to obtain statistically random results across all operating conditions.

Atmel 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 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) 1355-803-000, FAX (44) 1355-242-743
Atmel Grenoble, Avenue de Rochepleine, BP 123, 38521 Saint-Egreve Cedex, France, TEL (33) 4-7658-3000, FAX (33) 4-7658-3480

1545AS–11/00