Features

General

- High-performance, Low-power secureAVR™ Enhanced RISC Architecture
  - 137 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: 2.7V to 5.5V
- Compliant with ICAO and FIPS201 Specifications, GSM and EMV2000 Specifications
- Available in Wafers, Contact Modules, Dual Interface Modules, Full Contactless Modules or Inlays and Industry-standard Packages

Contactless Mode

- RF Contactless Interface with Full Support for ISO/IEC 14443 Type A and B Protocols
- Supply Voltage Clamp and Regulation
- Full-bridge Power Rectification
- On-chip Tuning Capacitance: 10 pF up to 120 pF
- 13.56 MHz Clock Extraction
- Internal Bus Maximum Frequency: 3.4 MHz (External clock) or 40MHz (Internal clock)
- Reader-to-card:
  - ISO/IEC Type A: 100% ASK Modulation and Modified Miller Bit Coding
  - ISO/IEC Type B: 10% ASK Modulation and NRZ Bit Coding
- Card-to-reader:
  - ISO/IEC Type A: Generation of 847.5Khz Subcarrier with OOK Modulation and Manchester Bit Coding
  - ISO/IEC Type B: Modulation of Incoming RF Carrier by Resistive Load Switching / Generation of 847.5Khz Subcarrier with BPSK Modulation / NRZ Data Encoding
- Baud Rates: Up to 848 kbps
- RF Frame: Up to 256 Bytes

Memory

- 256K Bytes of ROM Program Memory
- 32K Bytes of ROM Dedicated to ATMEL's Cryptographic Libraries
- 144K Bytes of EEPROM, Including 128 OTP Bytes and 384-byte Bit-addressable Bytes
  - 1 to 128-byte Program / Erase
  - 1ms Program / 1ms Erase
  - Typically 500,000 Write/Erase Cycles at a Temperature of 25°C
  - 10 Years Data Retention
- 8K Bytes of RAM + 256 Bytes of DMA Dedicated RAM

Peripherals

- Interrupt Driven ISO14443 Contactless Controller with Transmit / Receive
- One ISO 7816 Controller
  - Up to 625 kbps at 5 MHz
  - Compliant with T=0 and T=1 Protocols
- One I/O Port
- Programmable Internal Oscillator (Up to 40 MHz for AdvX™ and up to 20 MHz for Internal CPU Clock)
- Three 16-bit Timers (Watchdog capability)
- Random Number Generator (RNG)
- 2-level, 8-vector Interrupt Controller
- Hardware DES and Triple DES DPA/SPA/DEMA Resistant
- Checksum Accelerator
- CRC16 & 32 Engine (Compliant with ISO/IEC 3309)

Secure Microcontroller for Smart Cards

AT90SC 256144RCFT Summary

6534AS–SCIC–13Oct06

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

- **32-bit AdvX™ Cryptographic Accelerator for Public Key Operations with GF92n) Multiplier and Firmware (RSA, DSA, ECC, Key Generation, AES, MD5, SHA-1, SHA-256)**
- **DMA Controller to Speed-up Data Transfers when communicating via the Contactless Interface**
- **EAES 128 Engine (Optional)**

Security

- **Dedicated Hardware for Protection Against SPA/DPA/SEMA/DEMA Attacks**
- **Advanced Protection Against Physical Attack, Including Active Shield**
- **Environmental Protection Systems**
- **Voltage Monitor**
- **Frequency Monitor**
- **Light protection**
- **Temperature Monitor**
- **Secure Memory Management/Access Protection (Supervisor Mode)**
- **Designed to meet Common Criteria EAL5+**

Development Tools

- **Voyager Emulation Platform (ATV4 Advanced) to Support Software Development**
- **IAR Embedded Workbench AVR® V3.20c Debugger or Atmel's AVR Studio® Version 4.07 or Above**
- **Software Libraries and Application Notes**

Description

The AT90SC256144RCFT is a low-power, high-performance, 8-/16-bit microcontroller with ROM program memory, EEPROM data memory, based on the secureAVR enhanced RISC architecture and with a dual interface (contact+contactless).

By executing powerful instructions in a single clock cycle, the AT90SC256144RCFT 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 AT90SC256144RCFT uses the secureAVR architecture that allows the linear addressing of up to 8M bytes of code and up to 16M bytes of data as well as a number of new functional and security features.

The AT90SC256144RCFT features 144K bytes of high-performance EEPROM (fast erase/write time, high endurance).This allows system developers to offer their customers a true 128K bytes EEPROM, while still being able to use the remaining 16K bytes for their own purposes (customization and patches, for example). The ability to map the EEPROM in the code space allows parts of the program memory to be reprogrammed in-system.

The cryptographic accelerator featured in the AT90SC256144RCFT is the new AdvX, a N-bit multiplier-accumulator dedicated to performing fast encryption and authentication functions. All cryptographic routines are executed on the secureAVR core which uses the AdvX accelerator during encryption/decryption. AdvX is based on a 32-bit technology, thus enabling fast computation and low power operation. AdvX supports standard finite fields arithmetic functions (including RSA, DSA and DH) and GF(2N) arithmetic functions (including ECC).

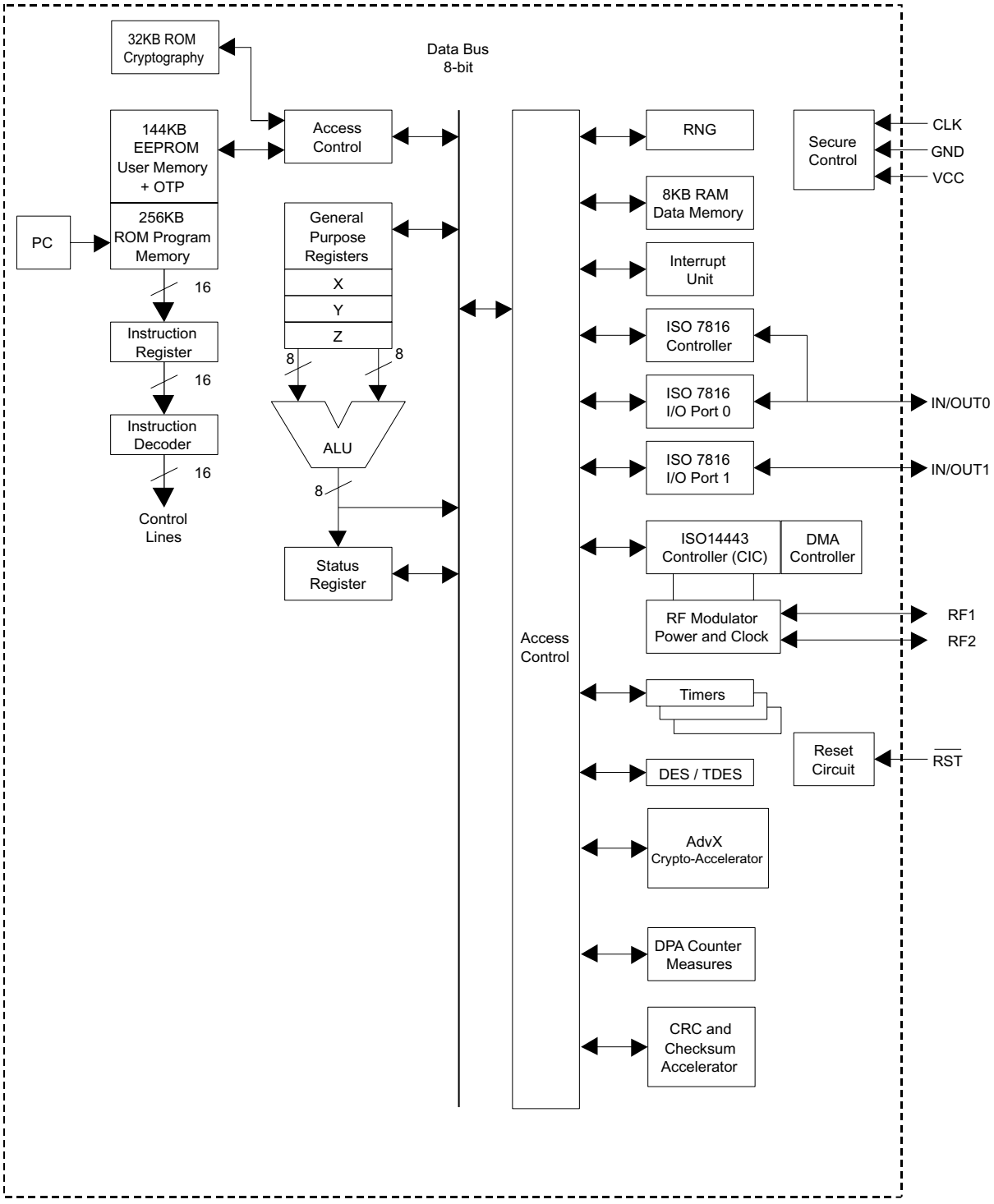
An AES 128 Engine is provided as an optional feature.

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

This product is specifically designed for Smart Cards and targets Access Control and ID applications.

A block diagram of the AT90SC256144RCF is shown in Figure 1

Figure 1. AT90SC256144RCFT Contact/Contactless secureAVR Enhanced RISC Architecture



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 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 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

.

6534AS–SCIC–13Oct06