Features

General

- High-performance, Low-power secureAVRTM Enhanced RISC Architecture
  - 135 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 Range: 1.62V to 5.5V
- Compliant with GSM, 3GPP and EMV 2000 Specifications; PC Industry Compatible
- Available in Wafers, Modules and Industry-standard Packages

Memory

- 256K Bytes of ROM User Program Memory
- 32K Bytes of ROM Dedicated to Atmel's Crypto-library
- 72K Bytes of EEPROM, Including 128 OTP Bytes and 384-byte Bit-addressable Area
  - 1 to 128-byte Program/Erase
  - 1.25 ms Program / 1.25 ms Erase
  - 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
- 8K Bytes of RAM

Peripherals

- ISO 7816 Controller
  - Up to 625 kbps at 5 MHz
  - Compliant with T = 0 and T = 1 Protocols
- One I/O Port
- Optional USB 2.0 Full Speed interface with 5 endpoints and DMA controller
- Programmable Internal Oscillator (Up to 40 MHz for CPU and Crypto Accelerator)
- Two 16-bit Timers
- Random Number Generator (RNG)
- 2-level, 9-vector Interrupt Controller
- Hardware DES and Triple DES DPA/DEMA Resistant
- Checksum Accelerator
- CRC 16 & 32 Engine (Compliant with ISO/IEC 3309)
- 32-bit AdvX™ Cryptographic Accelerator for Public Key Operations with GF(2n)
- Multiplier and Firmware (RSA, ECC, Key Generation)

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)

Development Tools

- Voyager Emulation Platform (ATV4 Advanced) to Support Software Development
- IAR Systems EWAVR® V3.10 Debugger or Atmel's AVR Studio® Version 4.07 or Above
- Software Libraries and Application Notes

Secure Microcontroller for Smart Cards

AT90SC 25672RCT (-USB)

Preliminary Summary

6522AS–SMIC–05 Sep 05

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

Description

The AT90SC25672RCT(-USB) is a low-power, high-performance, 8/16-bit microcontroller with ROM program memory, EEPROM data memory, cryptographic accelerator based on the secureAVR enhanced RISC architecture. By executing powerful instructions in a single clock cycle, the AT90SC25672RCT(-USB) achieves throughputs close to 1 MIPS per MHz. Its Harvard architecture includes 32 generalpurpose working registers directly connected to the ALU, allowing two independent registers to be accessed in one single instruction executed in one clock cycle.

The AT90SC25672RCT(-USB) uses a new AVR® architecture, the secureAVR 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 cryptographic accelerator featured in this product is the AdvX, a 32-bit accelerator dedicated to performing fast encryption and authentication functions. It is combined with a 32K byte-ROM for a high-performance and secure crypto firmware.

The ability to map the EEPROM in the code space allows parts of the program memory to be reprogrammed in-system. This technology combined with the versatile 8/16-bit CPU on a monolithic chip provides a highly flexible and cost-effective solution to many smart card applications.

Additional security features include power and frequency 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 AT90SC25672RCT(-USB) is shown in Figure 1 hereafter.

Optional USB Controller Description

The AT90SC25672RCT(-USB) optionally features an USB V2.0 Full Speed controller which requires a 48 MHz external crystal for the data transfer. The USB interface consists of a Serial Interface Engine (SIE) and a Universal Function Interface (UFI). The SIE performs clock/data separation, NRZI encoding and decoding, bit stuffing, CRC generation and checking and serial-parallel data conversion.

The UFI connects the USB interface to the AVR. It consists of a protocol engine and provides five configurable data transfer endpoints, each with it's own DPRAM in the memory area. The data transfer type for each endpoint is configured by software. The table below indicates the characteristics of each endpoint:

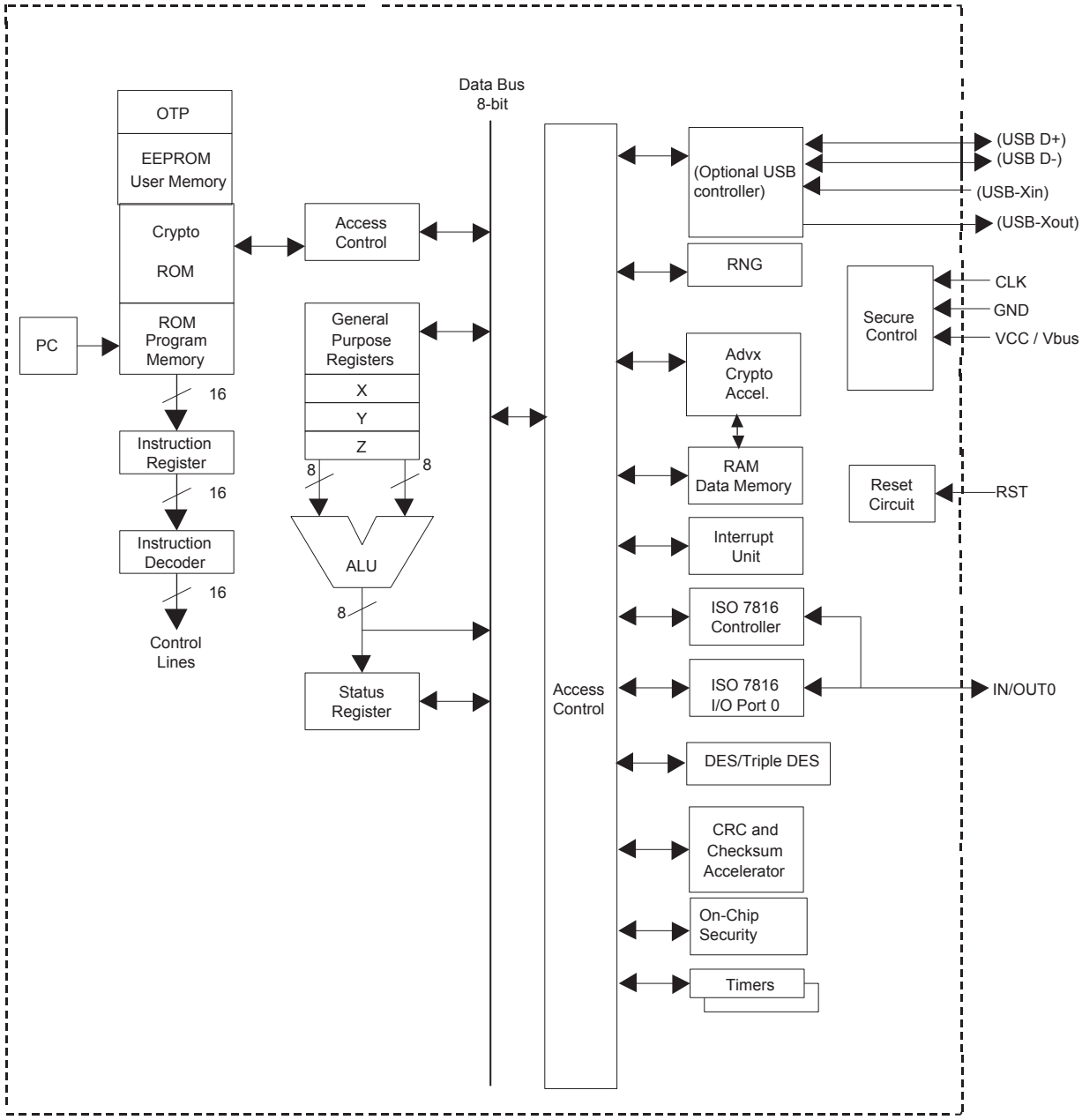
Table 1: Characteristics of each endpoint.

Endpoint number	Size (bytes)	Available data transfer modes
EP0	64	BULK, ISOCHRONOUS, INTERRUPT, CONTROL
EP1	2 * 64	BULK, ISOCHRONOUS, INTERRUPT
EP2	2 * 64	BULK, ISOCHRONOUS, INTERRUPT
EP3	64	BULK, ISOCHRONOUS, INTERRUPT, CONTROL
EP4	64	BULK, ISOCHRONOUS, INTERRUPT, CONTROL

A DMA controller allows a fast communication rate between the RAM of the CPU and the DPRAM.

The USB controller provides a dynamic pull-up attachment and detachment and a host detection mechanism. In addition, it offers an automatic interface detection between the USB 2.0 and the ISO7816 port.

Figure 1. AT90SC25672RCT(-USB) 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

Printed on recycled paper.

6522AS–SMIC–05 Sep 05