



# Secure Microcontroller AT90SC25672RCT-USB Summary

## Features

### General

- High-performance, Low-power 8/16-Bit 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  $\pm 6000V$
- Operating Ranges: 1.62 to 5.5V
- Compliant with GSM, 3GPP and EMV 2000 Specifications, PC Industry Compatible
- Available in Wafers, Modules, QFN44 and SOIC8 packages

### Memory

- 256K Bytes of ROM Program Memory
- 72K Bytes of EEPROM, Including 128 OTP Bytes and 384 Bit-addressable Bytes
  - 1 to 128-byte Program / Erase
  - 1.25ms Program / 1.25ms Erase
  - Typically 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 RAM Memory (6K bytes of CPU RAM, 2K bytes of Ad-X™ RAM, shared with the CPU core)
- 32K Bytes of ROM Dedicated to Inside's Crypto-library

### Peripherals

- One I/O Port
- One ISO 7816 Controller
  - Up to 625 Kbps at 5 MHz
  - Compliant with T=0 and T=1 Protocols
- USB 2.0 Full Speed interface with 5 endpoints and DMA controller
- Programmable Internal Oscillator (Up to 40 MHz for Ad-X and 40 Mhz for internal CPU Clock)
- Two 16-bit Timers
- Random Number Generator (RNG)
- 2-level Interrupt Controller
- Hardware DES and Triple DES DPA/DEMA Resistant
- Checksum Accelerator
- Code Signature Module
- CRC16 & 32 Engine (Compliant with ISO/IEC 3309)
- 32-Bit Cryptographic Accelerator (Ad-X for Public Key Operations)
  - RSA, DSA, ECC, Diffie-Hellman



## 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
- Temperature Monitor
- Light Protection
- Secure Memory Management/Access Protection (Supervisor Mode)

## Certification targeted

- CC EAL4+
- VISA
- CAST
- USB2.0

## Development Tools

- Voyager Emulation Platform (ATV4) to Support Software Development
- IAR Embedded Workbench® V4.21A Debugger or Atmel's AVR Studio® Version 4.07 or Above
- Software Libraries and Application Notes

# Description

The AT90SC25672RCT-USB is a low-power, high-performance, 8/16-bit microcontroller with ROM program memory, EPROM data memory, cryptographic accelerator based on the 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 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.

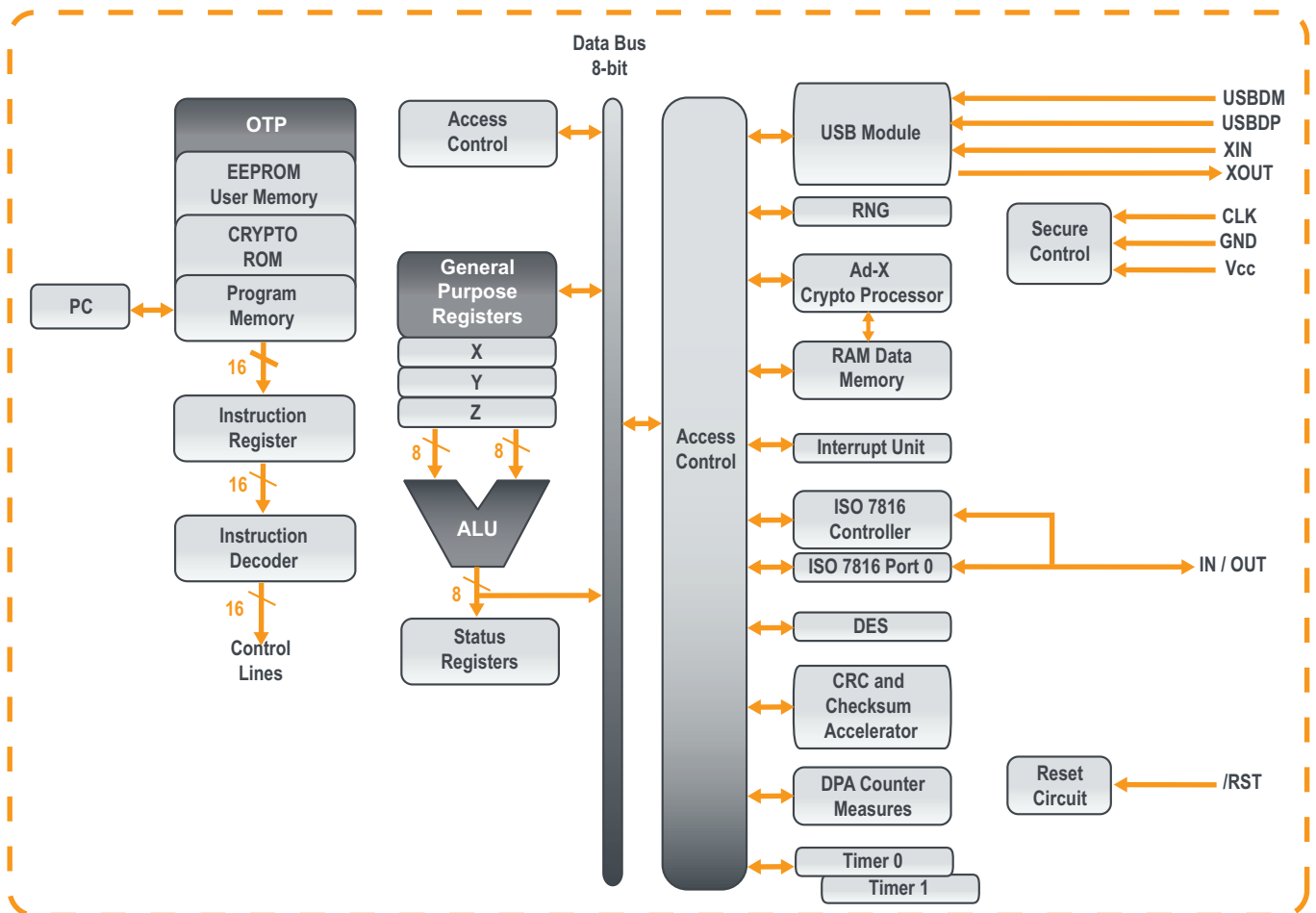
The AT90SC25672RCT-USB uses a new 8/16-bit RISC architecture, that allows the linear addressing of up to 8M bytes of code and up to 16M bytes of data as well as a number of new functional and security features.

The cryptographic accelerator featured in this product is the Ad-X, 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.

Figure 1: AT90SC25672RCT-USB Enhanced RISC Architecture



# USB Controller Description

The AT90SC25672RCT-USB 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 serialparallel data conversion.

The UFI connects the USB interface to the CPU. It consists of a protocol engine and provides five configurable data transfer endpoints, each with its own DPRAM in the memory area. The data transfer type for each endpoint is configured by software. The table 1 below indicates the characteristics of each endpoint.

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.

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



Figure 3: Pinout AT90SC25672RCT-USB - Package SOIC8 - ISO Mode

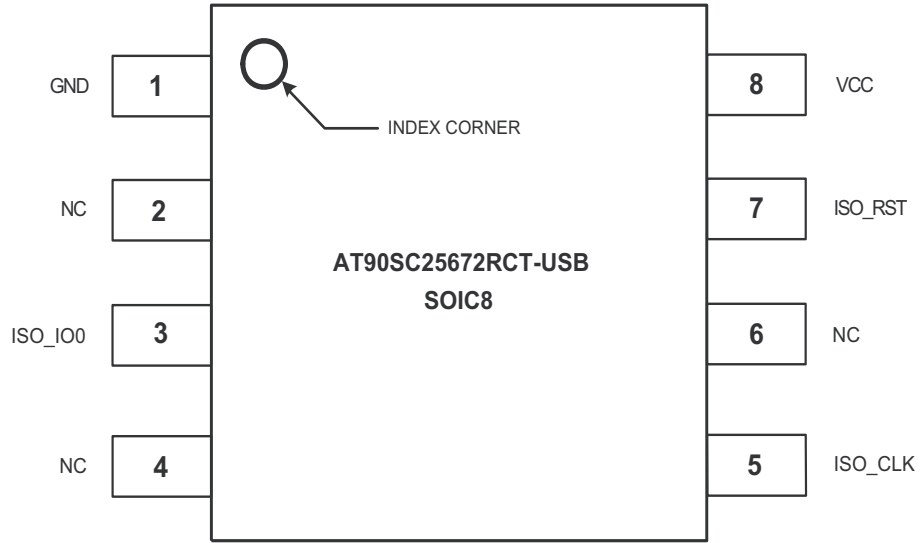


Figure 4: Pinout AT90SC25672RCT-USB - Package SOIC8 - USB Mode

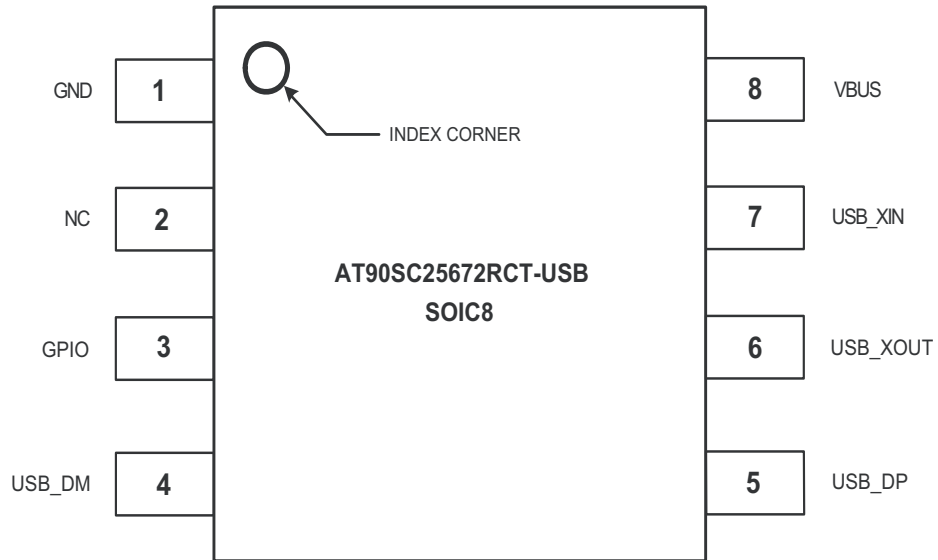
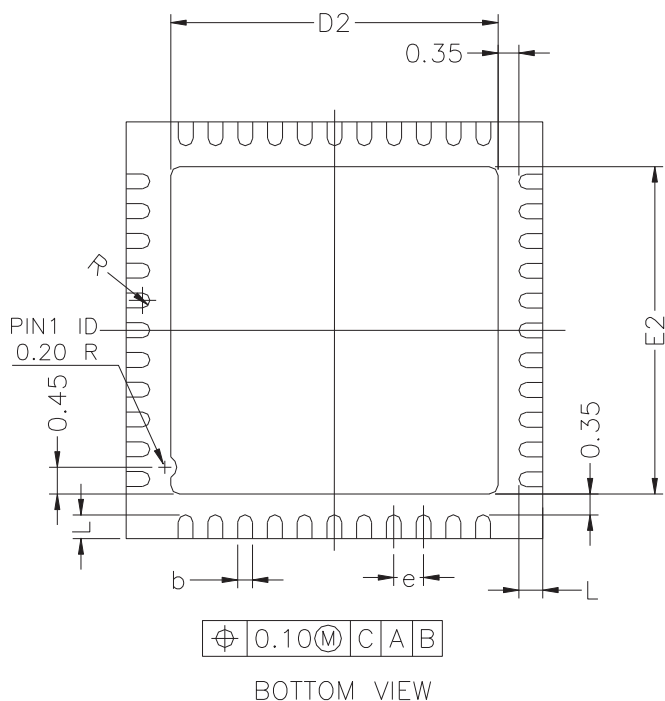
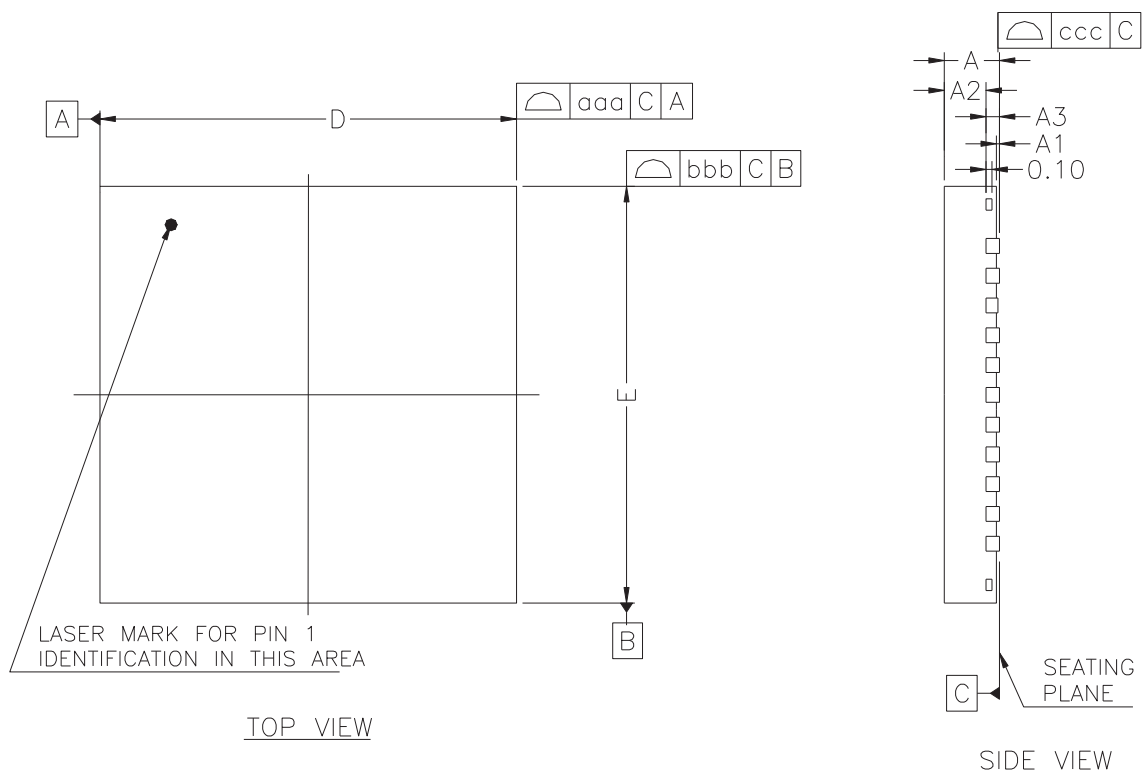


Figure 5: Quad Flat No Lead Package, 44 Leads

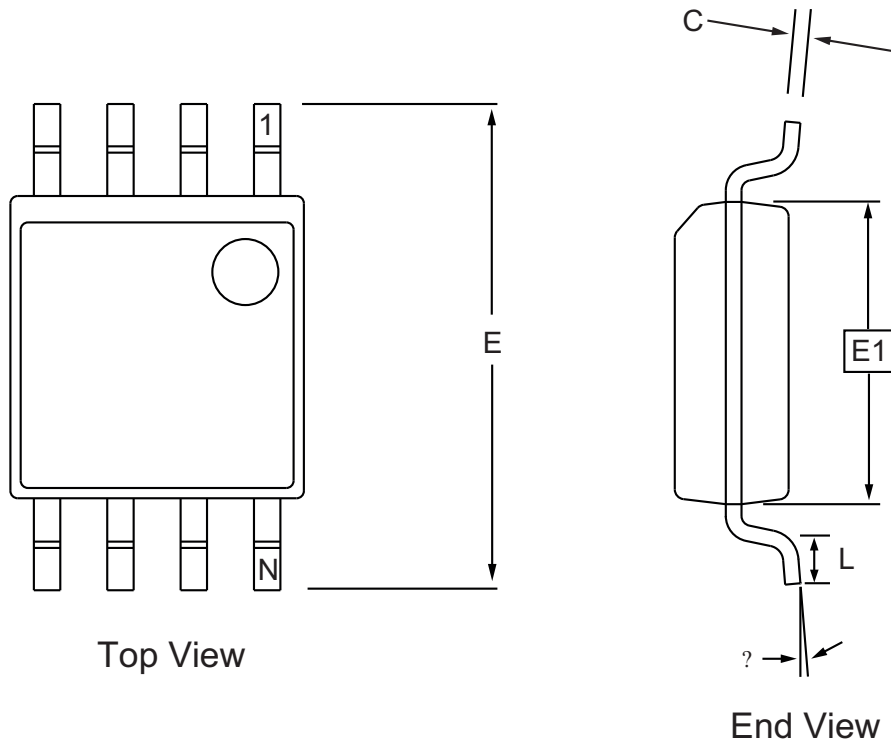


\* CONTROLLING DIMENSION : MM

SYMBOL	MILLIMETER			INCH		
	MIN.	NOM.	MAX.	MIN.	NOM.	MAX.
A	---	---	0.90	---	---	0.035
A1	---	---	0.05	---	---	0.002
A2	---	0.65	0.70	---	0.026	0.028
A3	0.20 REF.			0.008 REF.		
b	0.18	0.25	0.30	0.007	0.010	0.012
D	6.90	7.00	7.10	0.272	0.276	0.280
D2	5.40	5.50	5.60	0.213	0.217	0.220
E	6.90	7.00	7.10	0.272	0.276	0.280
E2	5.40	5.50	5.60	0.213	0.217	0.220
L	0.35	0.40	0.45	0.014	0.016	0.018
e	0.50 bsc			0.020 bsc		
R	0.090	---	---	0.004	---	---
TOLERANCES OF FORM AND POSITION						
aaa	0.10			0.004		
bbb	0.10			0.004		
ccc	0.05			0.002		

- NOTES :
1. ALL DIMENSIONS ARE IN MILLIMETERS.
  2. PACKAGE WARPAGE MAX 0.08 mm.

Figure 6: Plastic Small Outline Package - 8-lead - 0.209" Body



**COMMON DIMENSIONS**  
(Unit of Measure = mm)

SYMBOL	MIN	NOM	MAX	NOTE
A	1.70		2.16	
A1	0.05		0.25	
b	0.35		0.48	5
C	0.15		0.35	5
D	5.13		5.35	
E1	5.18		5.40	2, 3
E	7.70		8.26	
L	0.51		0.85	
?	0°		8°	
e	1.27 BSC			4

- Notes:
1. This drawing is for general information only; refer to EIAJ Drawing EDR-7320 for additional information.
  2. Mismatch of the upper and lower dies and resin burrs are not included.
  3. It is recommended that upper and lower cavities be equal. If they are different, the larger dimension shall be regarded.
  4. Determines the true geometric position.
  5. Values b and C apply to pb/Sn solder plated terminal.  
The standard thickness of the solder layer shall be 0.010 +0.010/-0.005 mm.