Features

General

- High-performance, Low-power AVR® (AVR3 Core) Enhanced RISC Architecture
  - 133 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:
  - ISO Mode: 2.7V to 5.5V; PC Industry Compliant
  - USB Mode: 3.6V to 5.5V; Compliant with USB Specification V1.1
- Available in Wafers, Modules and Industry-standard Packages

Memory

- 64K Bytes of EEPROM, Including 64-byte OTP Area and 64-byte Bit-addressable Area
  - 1 to 128-byte Program/Erase
  - 2 ms Program, 2 ms Erase
  - Typically More than 500,000 Write/Erase Cycles
  - 10 Years Data Retention
- 64K Bytes of Flash Program Memory
  - 128-byte Page Programming
  - Minimum 10,000 Write/Erase Cycles
  - 10 Years Data Retention
- 3K Bytes of RAM

Peripherals

- Two I/O Ports (Configurable to Support Communication Protocols Including ISO 7816-3 and 2-wire Interfaces)
- USB Interface (4 Endpoints)
  - USB V1.1 Full-speed (12 Mbps) Certified, Suspend/Resume Modes Supported
  - 3 Configurable Endpoints in Addition to Endpoint EP0
  - 2 Endpoints with Double-buffering Capability (Ping-pong Mode)
  - Dynamic Pull-up Attachment
- DMA Controller
- Automatic USB/ISO Interface Detection Circuitry
- Two 16-bit Timers
- Random Number Generator (FIPS 140-1)
- 2-level, 8-vector Interrupt Controller
- Hardware DES and Triple DES DPA Resistant
- Checksum Accelerator
- Crypto-coprocessor
  - Pre-programmed Functions for Cryptography and Authentication Including RSA, DSA, Key Generation, ECC

Security

- Dedicated Hardware for Protection Against SPA/DPA Attacks
- Advanced Protection Against Physical Attack
- Environmental Protection Systems
- Voltage and Frequency Monitors
- Secure Memory Management/Access Protection (Supervisor Mode)

Development Tools

- Hardware Development Support on Voyager Emulation Platform (ATV1)

Secure Microcontroller

AT90SC6464C-USB

Summary

Rev. 1559BS–8/02

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 AT90SC6464C-USB is a low-power, high-performance, 8-bit microcontroller, based on the new AVR3 enhanced RISC architecture, featuring Flash program memory, EEPROM data memory and a 16-bit crypto-coprocessor dedicated to performing fast encryption and authentication functions.

The new AVR3 core allows linear addressing of up to 8M bytes of code and up to 16M bytes of data, and provides a number of new functional and security features. This new core executes powerful instructions in a single clock cycle, and allows the AT90SC6464C-USB to achieve throughputs close to 1 MIPS per MHz. The 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 AT90SC6464C-USB includes 128K bytes of Atmel's high density, nonvolatile memory. The on-chip downloadable Flash allows the program memory to be reprogrammed in-system. This technology combined with the versatile 8-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.

Pin Configuration

The AT90SC6464C-USB pinout conforms to the ISO 7816-2 and USB Full-speed V1.1 Interface specifications (the USB interface requires the addition of an external 4 MHz clock signal or 4 MHz crystal). A second I/O port is also provided,.

	ISO 7816-2 Interface	USB Interface with External Clock	USB Interface with Crystal
GND	Ground (reference voltage)	Ground (reference voltage)	Ground (reference voltage)
VCC (VBUS)	Power supply input	Power supply input (bus-powered device)	Power supply input (bus-powered device)
IN/OUT0 ($\overline{\text{CLKEN}}$)	I/O for serial data	Active low signal to disable/enable the clock signal source	I/O for serial data
IN/OUT1	Second I/O for serial data	Second I/O for serial data	Second I/O for serial data
CLK	Clock signal input to internal clock operating circuit	Clock signal input to internal clock operating circuit (4 MHz)	–
$\overline{\text{RST}}$	Reset signal input (a low state stops the *AVR* core)	Reset signal input (a low state stops the *AVR* core)	Reset signal input (a low state stops the *AVR* core)
USBDM	–	USB D- differential data	USB D- differential data
USBDP	–	USB D+ differential data	USB D+ differential data
XIN	–	–	Crystal signal input to drive internal clock operating circuit
XOUT	–	–	Crystal signal output to drive internal clock operating circuit

Note: By convention $\overline{\text{RST}}$ corresponds to RST in the ISO Interface protocol. $\overline{\text{RST}}$ in all cases, however, remains active low.

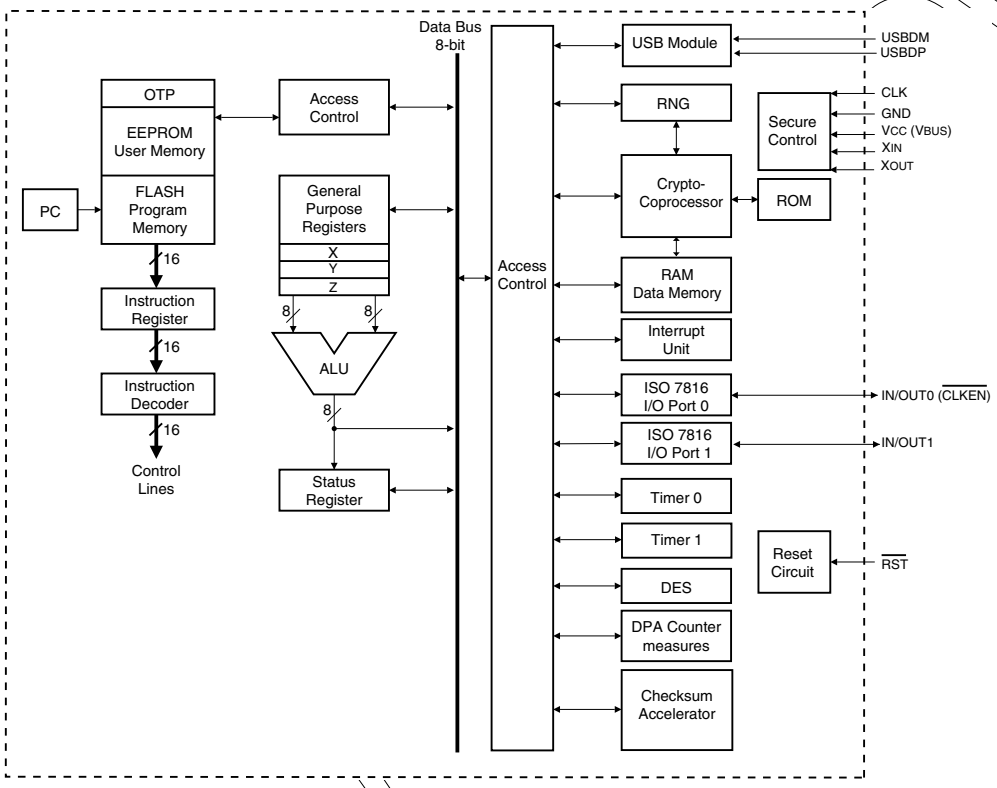
Architectural Overview

The AT90SC6464C-USB is based on the AVR (core #3) enhanced RISC architecture (see Figure 1).

The fast-access register file contains 32 x 8-bit general-purpose working registers, each of which can be accessed in a single clock cycle. Furthermore, the high-performance ALU (Arithmetic Logic Unit) operates directly on the 32 general-purpose working registers. This allows the processor to execute a complete ALU operation in a single clock cycle—two operands are output from the register file, the operation is executed, and the result is stored back in the register file, all in the same clock cycle. The ALU operations are divided into three main categories: arithmetic, logical and bit-functions.

Six of the 32 general-purpose registers can be used as three 16-bit indirect address register pointers X, Y, and Z, for addressing data space and allowing efficient address calculations. As the AT90SC6464C-USB has more than 64K bytes of data space to address, registers RAMPX, RAMPY and RAMPZ are concatenated with the X, Y and Z registers respectively for indirect addressing. RAMPD is concatenated with a part of the instruction word to enable direct addressing of 16M bytes of data (using LDS or STS). EIND is concatenated with register Z to enable extended indirect jumps and calls on 4M words of code (using EIJMP or EICALL).

Figure 1. The AT90SC6464C-USB AVR Enhanced RISC Architecture



The ALU performs arithmetic and logical operations on the contents of single registers, pairs of registers and between registers and constant values.

Conventional memory addressing modes can be used to access the register file, as these registers are assigned to the 32 lowermost data space addresses.

The I/O memory space contains 64 addresses for CPU peripheral functions such as control registers, timer/counters, internal and external interrupts, serial pins, and other I/O functions. The I/O memory space can be accessed directly, or as data space locations. One hundred and sixty additional peripherals registers are available.

The AVR3 core uses a Harvard architecture, with separate address spaces for program memory and data memory. Different addresses are used by the same memory block if used for program or data.

The FLASH program memory is accessed with single level pipelining; while one instruction is being executed, the next instruction is pre-fetched from the program memory. This mechanism allows each instruction to be executed in a single clock cycle.

The EEPROM includes 64 bytes of bit-addressable memory and 64 bytes of OTP (One Time Programmable) memory.

The 22-bit Program Counter (PC) on AT90SC6464C-USB can address 4M words (8M bytes) of program memory.

Most AVR instructions have a single 16-bit word format. Every program memory address contains a 16-bit or 32-bit instruction. The 3K bytes of data RAM can be accessed easily through the five different addressing modes supported in the AVR architecture.

A flexible interrupt controller has its control registers in the I/O space with an additional global interrupt enable bit in the status register. Each of the interrupts has a separate interrupt vector in the interrupt vector table at the beginning of the program memory. The different interrupts are prioritized according to their programmed priority level. When two interrupts with the same priority are detected at the same time, the interrupt with the lower source number is serviced first.

USB Module Functional Description

USB Hardware Block

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 four 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 below indicates the size of each endpoint.

Endpoint number	Size (in bytes)	Recommended data transfer type
EP0	8	CONTROL (mandatory)
EP1 (Ping-pong)	64	BULK IN
EP2 (Ping-pong)	64	BULK OUT
EP3	64	BULK, INTERRUPT, CONTROL, ISOCHRONOUS

Note: Ping-pong (double-buffering) mode is a special proprietary feature, transparent to the user, that allows software to read data from one bank while the hardware fills another bank, thereby saving processing and transaction time.

The bus controller manages the device addresses, monitors the status of the transaction, manages the DPRAMs and communicates with the AVR through a set of status and control registers, the UFI registers.

USB Software Block

The function controller must be implemented in the firmware of the microcontroller. This software must comply with Chapter 9 of the USB specifications V1.1.

Enumerating and executing functions should be done using USB interrupts (polling is possible but is more complicated to manage).

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

1559BS–8/02