

## Features

### General

- High-performance, Low-power secureAVR™ Core Enhanced RISC Architecture
  - 135 Powerful Instructions (Most Executed in a Single Clock Cycle)
- Bond Pad Locations Conforming to ISO 7816-2
- ESD Protection to  $\pm 6000V$
- Operating Ranges: from 2.7V to 5.5V
- Compliant with ICAO specifications; EMV 2000 Specifications; PC Industry Compatible
- Power-saving Wait and Very Low-power Stop Modes
- Power-up Detection
- Available in Wafers, Modules, Dual Interface Module, Contactless Module or Inlay and Industry-standard Packages

### Contactless Mode

- Contactless Interface Controller (CIC) 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
- 3.4 MHz Internal Bus Maximum Frequency with a Clock Extracted From the External Clock and 20 (AVR®) or 40 MHz (AdvX™) if the Clock is Internally Generated
- 13.56 MHz Clock Extraction
- 3.4 MHz Internal Bus Frequency
- 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 424 kbps
- RF Frame: Up to 256 Bytes

### Memory

- 128K Bytes of ROM Program Memory
- 36K 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 Temperatures of 25°C
  - Minimum 10 Years Data Retention
- 5K Bytes of RAM + 256 Bytes of DMA Dedicated RAM
- 32K Bytes of ROM Dedicated to Atmel's Crypto Library

### Peripherals

- One ISO 7816 Controller
  - Up to 625 kbps at 5 MHz
  - Compliant with T= 0 and T= 1 Protocols
- Two I/O Ports (Configurable to Support ISO7816-3, 2-wire protocols...)
- 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)



## Secure Microcontroller for Smart Cards

## AT90SC 12836RCFT Summary

6515-SMIC-28Jun05



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



- Checksum Accelerator
- CRC 16 & 32 Engine (Compliant with ISO/IEC 3309)
- 32-Bit AdvX Cryptographic Accelerator for Public Key Operations
  - RSA, DSA, ECC, Diffie-Hellman
- DMA Controller (Used to Speed-Up Data Transfers when Communicating via the Contactless Interface)

## Security

- Dedicated Hardware for Protection Against SPA/DPA/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)
- Designed to meet Common Criteria EAL4+

## Development Tools

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

## Description

The AT90SC12836RCFT 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 AT90SC12836RCFT 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 AT90SC12836RCFT 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 AT90SC12836RCFT features 36K bytes of high-performance EEPROM (fast erase/write time, high endurance). This allows system developers to offer their customers a true 32K bytes EEPROM, while still being able to use the remaining 4K 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.

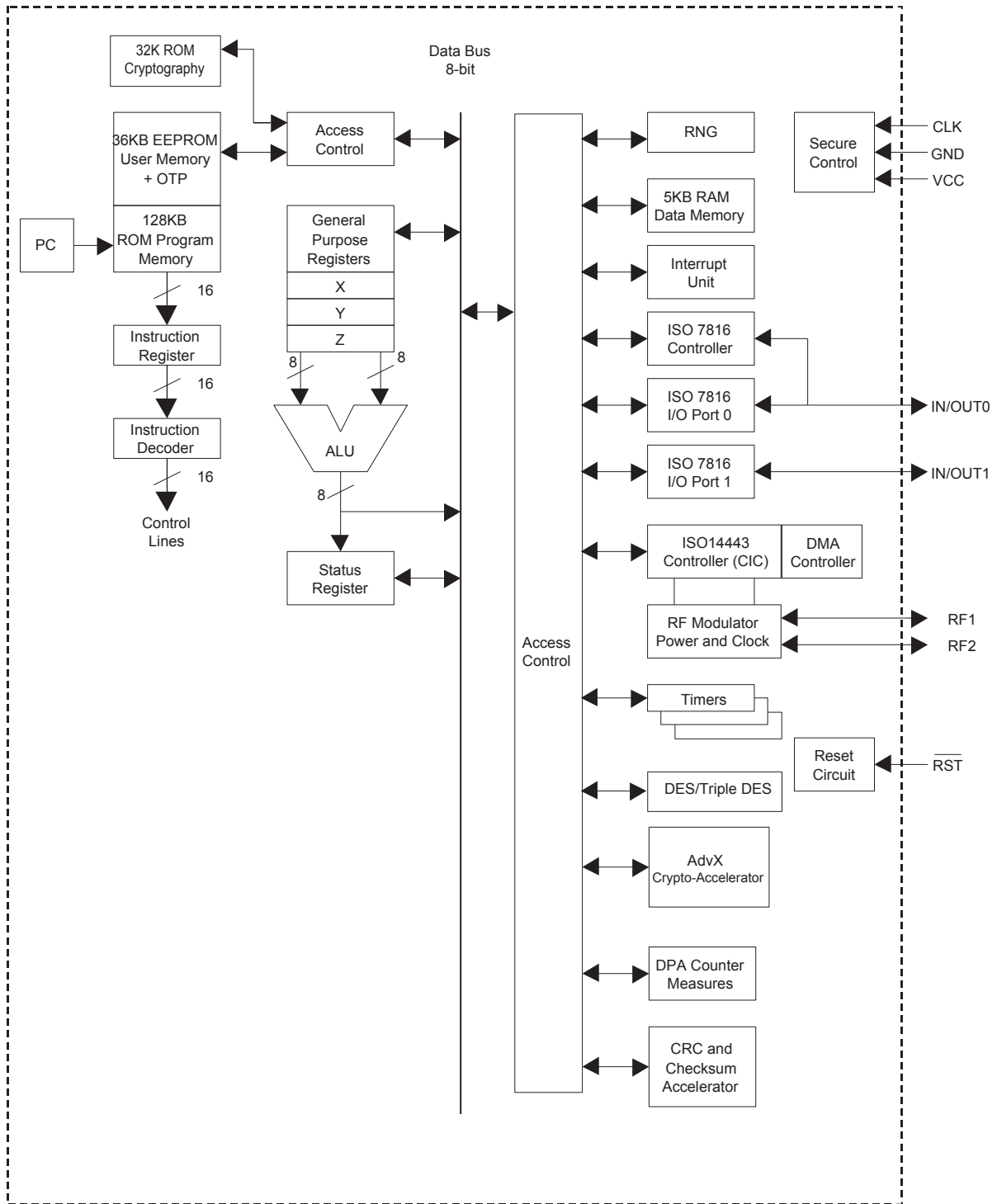
The cryptographic accelerator featured in the AT90SC12836RCFT is the new AdvX, a N-bit multiplier-accumulator dedicated to performing fast encryption and authentication functions. All cryptographic routines are executed on the secureAVR core which uses the AdvX accelerator during encryption/decryption. 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, DH and ECC) and GF(2<sup>N</sup>) arithmetic functions (including ECC).

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 AT90SC12836RCFT is shown in Figure 1.

Figure 1. AT90SC12836RCFT Contact/Contactless secureAVR Enhanced 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 Arsenalux 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](http://www.atmel.com/literature)

**Disclaimer:** The information in this document is provided in connection with Atmel products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Atmel products. **EXCEPT AS SET FORTH IN ATMEL'S TERMS AND CONDITIONS OF SALE LOCATED ON ATMEL'S WEB SITE, ATMEL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ATMEL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ATMEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.** Atmel makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Unless specifically provided otherwise, Atmel products are not suitable for, and shall not be used in, automotive applications. Atmel's products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.

© Atmel Corporation 2005. All rights reserved. Atmel®, logo and combinations thereof, Everywhere You Are® and others, are registered trademarks or trademarks of Atmel Corporation or its subsidiaries. Other terms and product names may be trademarks of others.



Printed on recycled paper.

6515-SMIC-28Jun05