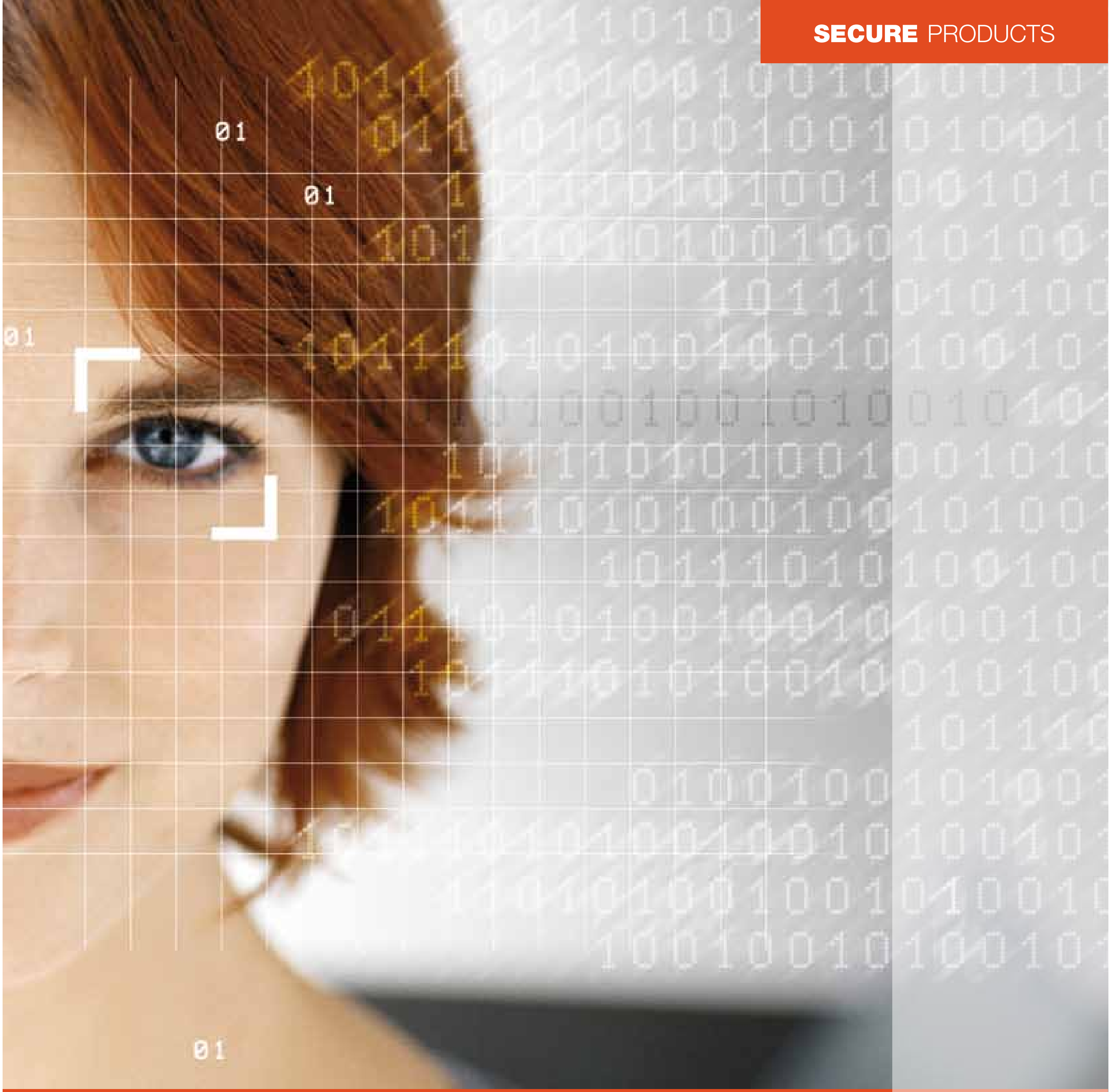
# **SECURE** PRODUCTS



- ↗ Microcontrollers
- ↗ Security Modules
- ↗ Secure System on Chip
- ↗ Reader chips
- ↗ CryptoAuthentication
- ↗ Secure Memories
- ↗ CryptoController

ATMEL®

## Worldwide Leadership

For over 25 years, Atmel® has been a leading designer and manufacturer of advanced integrated circuits (ICs) for smart cards and embedded security applications. With a broad portfolio of secure solutions and its long-term commitment to security, Atmel is able to address markets which demand high-level of confidentiality and security.

## Product Offering

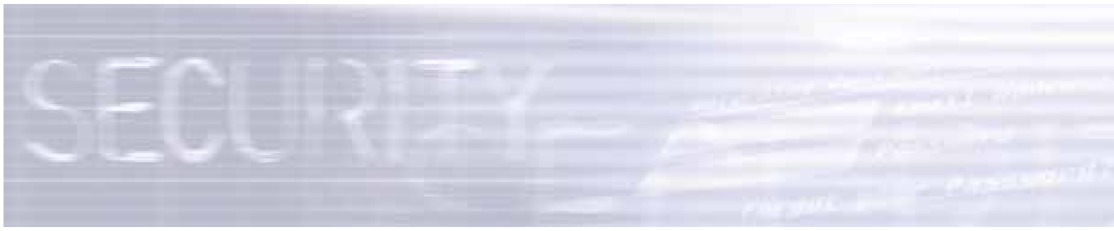
- Secure Microcontrollers
- Security Modules
- Secure System on Chip
- Smart Card reader ICs
- CryptoAuthentication
- Secure Memories
- CryptoController

## Applications

- Banking
- Mobile Phones
- Machine-to-Machine
- ePayment
- Pay-TV
- PC Security
- ePassport
- Government ID
- Access Control
- Electronic Transactions Security
- Anti-Cloning Devices
- Transportation

## Security

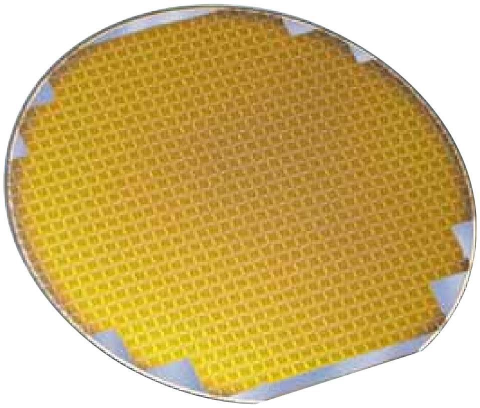
Atmel's products meet the stringent needs of the security market with the highest security certifications for ICs in the industry including Common Criteria EAL4+/EAL5+, FIPS 140-2, ZKA and EMVCo approvals.



## Process Technology

Atmel has leading-edge technologies, global manufacturing capacity and world-class design expertise, using the most advanced processes including:

- CMOS with embedded EEPROM and Flash non volatile memories for secure ICs
- Silicon Germanium (SiGe) Bipolar and BiCMOS for high-frequency RF interfaces



## R&D Investment

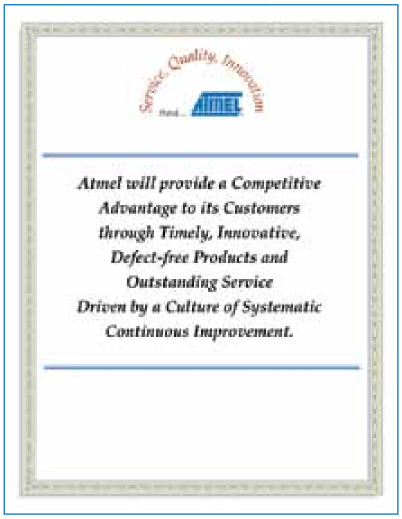
Atmel maintains its competitive edge in process technology evolution and product innovation by means of an on-going program of research and development, undertaken in collaboration with leading industries and key clients.

## Facilities

Headquartered in San Jose, California, Atmel operates two fabrication plants in the United States and Europe: Colorado Springs (USA) and Rousset (France). Atmel has opted for fablight strategy with external foundries.

## Quality Commitment

Atmel has a corporate-wide commitment to quality that extends to every level of its activities. The objective is continuous improvement and total customer satisfaction. All manufacturing facilities meet international quality standards recognition ISO 9001 and are QML-Q certified. Through its network of R&D, design, manufacturing, sales and distribution facilities in over 60 countries, Atmel is committed to a customer-oriented approach.



Service, Quality, Innovation

And... ATMEL

*Atmel will provide a Competitive*
*Advantage to its Customers*
*through Timely, Innovative,*
*Defect-free Products and*
*Outstanding Service*
*Driven by a Culture of Systematic*
*Continuous Improvement.*

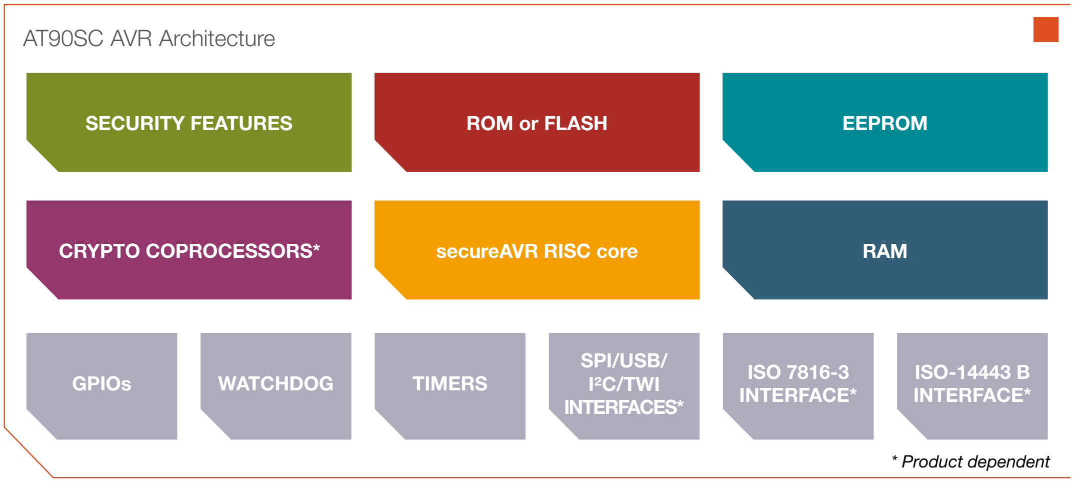
## 8-/16-bit RISC CPU

Give your applications the competitive edge with our high-performance secure microcontrollers using Atmel enhanced 8-/16-bit RISC architecture.

secureAVR®

- High-performance 8-/16-bit RISC Core
- Low-power Consumption
- Cost-effective Architecture
- Hardware Optimized for C, Javacard™
- Enhanced Addressing
- Advanced Security
- Internal Clock (up to 40 MHz)
- ISO 7816, USB, SPI, $I^2C$/TWI, ISO14443B
- GPIOs

AT90SC offers a complete range of fully compatible products.



AT90SC AVR Architecture

SECURITY FEATURES

ROM or FLASH

EEPROM

CRYPTO COPROCESSORS*

secureAVR RISC core

RAM

GPIOs

WATCHDOG

TIMERS

SPI/USB/ $I^2C$/TWI INTERFACES*

ISO 7816-3 INTERFACE*

ISO-14443 B INTERFACE*

* *Product dependent*

## secureAVR® based CPUs

Suited to mass-volume market, secureAVR products offer advanced security features, higher performance (advanced EEPROM, clock speed, access time…) and larger memories for high-end mobile solutions, running on open platforms OS e.g JavaCard™. The enhanced secureAVR platform offers additional security for the most stringent application needs.

## Enhanced secureAVR based CPUs with PKI

Secure your banking, pay-TV and e-ID applications with Atmel's fast cryptocontrollers. Our AdvX™ crypto-accelerator offers the performance and security level you need for all your DDA (Dynamic Data Authentication) and PKI requirements. Software developers can either select ciphering functions from our complete and certified library, or alternatively build their own implementation.

### Encryption/Decryption, Digital signature, Data integrity verification, Key generation, Secure key storage

- Advanced multiplier architecture supports Zp and GF ($2^n$) arithmetics
- High performance, low power
- Up to 4096-bit key length RSA®,
- ECC over Zp (all P-xxx FIPS 186-2 curves)
- High-performance certified crypto-library (toolbox)
- Side channel resistant
- Fault Injection Resistant
- Optional customer crypto development capability
- Compliant with contactless applications
- Hash Algorithms support (FIPS 180-2 compliant)

## secureAVR based CPUs with Contactless Interface

Want to go contactless? With a portofolio of products from 8 Kbytes up to 144 Kbytes of EEPROM, Atmel's contactless and dual interface secure microcontrollers are specifically tailored to serve e-Government, Transportation and Banking applications.

Atmel's products bring significant value to the e-ID market by improving the speed during the control of personal identity and protecting the privacy of e-ID holders. They are designed to meet the Common Criteria EAL5+ security level.

## Applications

- ID
- e-Passport
- Driving-License
- e-Ticketing
- e-Purse
- Access Control

## Security through Experience

Atmel has more than 25 years expertise in secure microcontroller designs for smart cards with some of the highest certifications for ICs in the industry including:

- Common Criteria EAL4+/EAL5+
- EMVCo
- FIPS 140-2, level 3 and 4
- ZKA
- JCB

Common Criteria EAL4+ Certified

Common Criteria EAL5+ Certified

## AT90SC Product Guide

### Part Number Identification

**AT90SC XXX YYY R C F T U**

**AT:** Atmel
**90:** AVR core
**SC:** Smart Cards

**XXX:** ROM or Flash
**YYY:** EEPROM

**R:** ROM program memory
**C:** Crypto-engine

**F:** RF interface
**T:** 0.18 µm
**U:** 0.15 µm

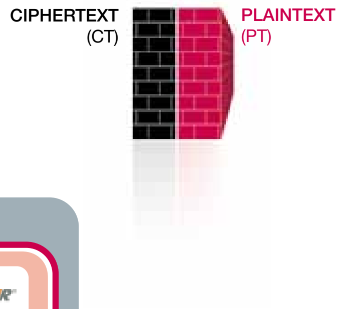
| Part Number | EEPROM | ROM | Flash | RAM | Voltage | T-DES |
|---|---|---|---|---|---|---|
| *secureAVR-based* | | | | | | |
| AT90SC9604RU | 4K | 96K | N/A | 2K | 2.7 - 5.5V | Yes |
| AT90SC16018RU | 18K | 160K | N/A | 4K | 2.7 - 5.5V | Yes |
| AT90SC19236RU | 36K | 192K | N/A | 4K | 1.62 - 5.5V | Yes |
| AT90SC3636U | 36K | N/A | 36K | 6K | 1.62 - 5.5V | Yes |
| AT90SC25672RU | 72K | 256K | N/A | 6K | 1.62 - 5.5V | Yes |
| AT90SC128112RU | 112K | 128K | N/A | 4K | 1.62 - 5.5V | No |
| AT90SC288144RU | 144K | 288K | N/A | 6K | 1.62 - 5.5V | Yes |
| *secureAVR-based with PKI* | | | | | | |
| AT90SC13612RCU | 12K | 136K | N/A | 4.5K | 2.7 - 5.5V | Yes |
| AT90SC1818CT | 18K | N/A | 18K | 5K | 2.7 - 5.5V | Yes |
| AT90SC20818RCU | 18K | 208K | N/A | 4.5K | 2.7 - 5.5V | Yes |
| AT90SC3636CT-USB | 36K | N/A | 36K | 8K | 1.62 - 5.5V | Yes |
| AT90SC12836RCT | 36K | 128K | N/A | 5K | 2.7 - 5.5V | Yes |
| AT90SC24036RCU | 36K | 240K | N/A | 6K | 2.7 - 5.5V | Yes |
| AT90SC25672RCT | 72K | 256K | N/A | 8K | 1.62 - 5.5V | Yes |
| AT90SC25672RCT-USB | 72K | 256K | N/A | 8K | 1.62 - 5.5V | Yes |
| AT90SC28848RCU | 48K | 288K | N/A | 8K | 2.7 - 5.5V | Yes |
| AT90SC28872RCU | 72K | 288K | N/A | 8K | 2.7 - 5.5V | Yes |
| AT90SC144144CT | 144K | N/A | 144K | 8K | 1.62 - 5.5V | Yes |
| AT90SC320288RCT | 288K | 320K | N/A | 8K | 1.62 - 5.5V | Yes |
| *secureAVR-based, contactless* | | | | | | |
| AT90SC6408RFT | 8K | 64K | N/A | 1.2K | 2.7 -5.5V | Yes |
| AT90SC12872RCFT | 72K | 128K | N/A | 5.2K | 2.7 -5.5V | Yes |
| AT90SC256144RCFT | 144K | 256K | N/A | 8.2K | 2.7 -5.5V | Yes |

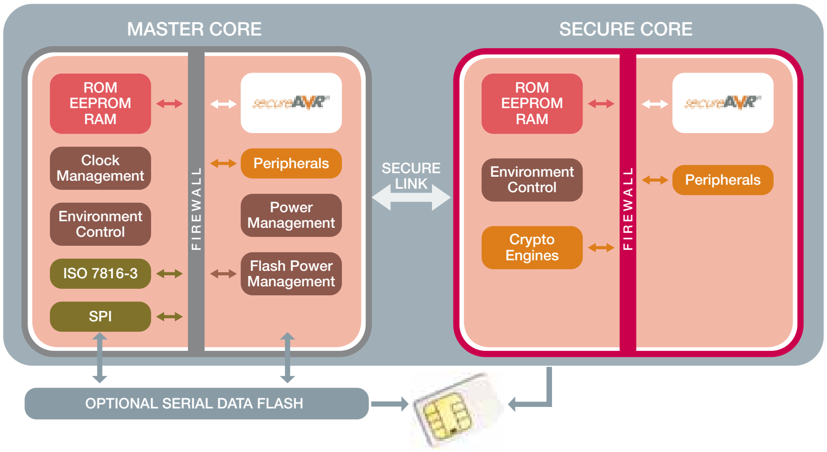
# TwinAVR™ Secure Dual Core Microcontroller

The TwinAVR is the industry first dual core secure microcontroller. It offers two independent cores, fully featured with CPU, memories and peripherals on a single chip to address the most security demanding Smart Card applications such as PayTV Conditional Access as well as Embedded Systems applications. The TwinAVR also features a built-in Flash interface for large data storage solutions where a Flash die and the TwinAVR are fitted in a standard Smart Card Module.

## Innovative Architecture

The innovative dual core architecture simplifies the implementation of the RED/BLACK concept of segregation between highly sensitive plaintext data (RED) and encrypted data (BLACK). The TwinAVR offers the Master Core to implement the BLACK domain and the Secure Core to implement the RED domain.





## Key Features

- **Master Core**
  8-/16–bit RISC secureAVR® Core
  128K ROM, 36K EEPROM, 6K RAM
  30MHz Internal Clock

- ISO 7816-3 Smart Card Interface
- DataFlash® Interface
- Optional 4Mbit DataFlash
- Common Criteria EAL5+

- **Secure Core**
  8-/16–bit RISC secureAVR® Core
  64K ROM, 18K EEPROM, 6K RAM
  30MHz Internal Clock
  AdvX™ Crypto Processor
  Hardware TDES
  Hardware AES
  AIS31 TRNG

| Part Number | Master Core | | | Secure Core | | | Flash | Voltage | Available |
|---|---|---|---|---|---|---|---|---|---|
| | ROM | EEPROM | RAM | ROM | EEPROM | RAM | | | |
| AT90SDC100 | 128K | 36K | 6K | 64K | 18K | 6K | N/A | 2.7V-5.5V | Now |
| AT90SDC104 | 128K | 36K | 6K | 64K | 18K | 6K | 4Mbit | 2.7V-5.5V | Q1 2010 |

# (U)SIM Solutions for M2M

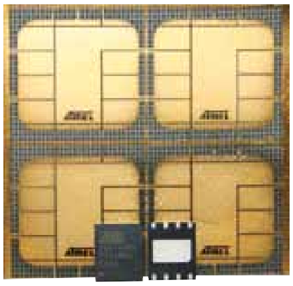
Atmel has developed new secure microcontrollers for cellular Machine-to-Machine communication modules. By using GSM and UMTS networks, these modules provide wireless connectivity to a range of equipments that communicate without human intervention. Network communication can be granted by the (U)SIM tailored to withstand extreme environmental conditions. Extended guarantees and new packaging are the key benefits of using Atmel secureAVR® 8-/16-bit microcontroller solutions.

## Applications

- Tracking and Inventory Management
- Telemetry
- Payment and Transaction
- Monitoring and Alerting
- Home Security
- Fixed Wireless Terminals
- Remote Control

## Key Features

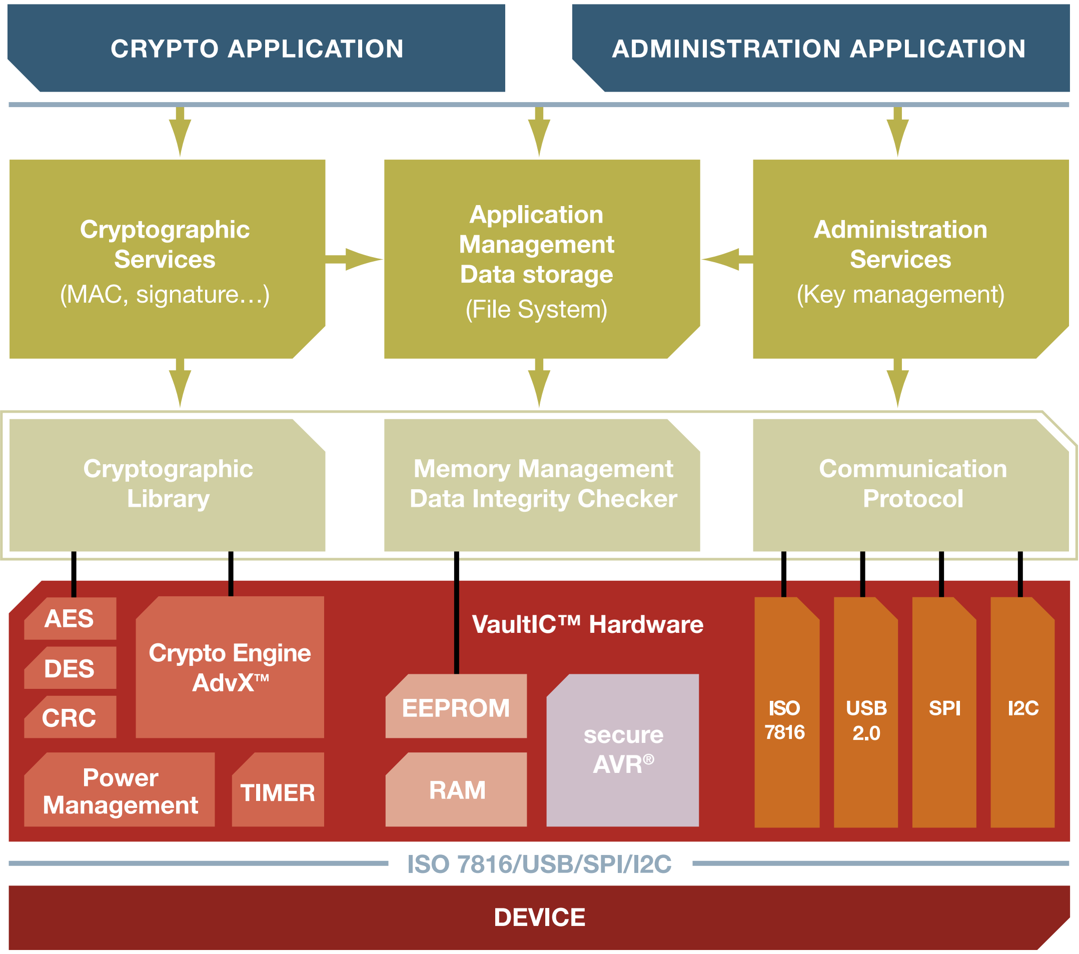
- 8-/16-bit RISC secureAVR core
- Extended Temperature Range [-40°C ;105°C]
- 10 years data retention over full temperature range
- Tiny DFN8 package solution



| Part Number | EEPROM | ROM | RAM | Voltage | Package |
|---|---|---|---|---|---|
| AT90M25672RU | 72K | 256K | 6K | 1.62-5.5V | DFN8, QFN44 |

## Turnkey Security Modules

Protect your applications against high-tech goods counterfeiting, multimedia contents copying and identity theft with our VaultIC™ family of security modules. Based on Atmel smart card chip design expertise, the VaultIC is a complete turnkey and easy to use solution (hardware and firmware) designed to secure Embedded Systems.


CRYPTO APPLICATION
ADMINISTRATION APPLICATION
Cryptographic Services (MAC, signature…)
Application Management Data storage (File System)
Administration Services (Key management)
Cryptographic Library
Memory Management Data Integrity Checker
Communication Protocol
AES
DES
CRC
Crypto Engine AdvX™
Power Management
TIMER
VaultIC™ Hardware
EEPROM
RAM
secure AVR®
ISO 7816
USB 2.0
SPI
I2C
ISO 7816/USB/SPI/I2C
DEVICE

## Hardware Platform

- SecureAVR Architecture
- High Level Cryptographic Services Based on Hardware Accelerators
- USB 2.0 Full Speed Interface, USB CCID Compliant
- SPI, ISO 7816, I2C Interfaces
- Designed to meet C.C. EAL4+ and FIPS 140-2 certifications
- Reference Design USB Token (VaultIC420 / VautIC440 / VaultIC460)
- Reference Design IP Protection (VaultIC200 / VaultIC400)

## Advanced Cryptographic Features

- Strong challenge-response authentication
- Digital signature (RSA PKCS#1 v2.1, DSA, ECDSA)
- Data encryption (AES, 3DES, RSA PKCS#1 v2.1)
- Message digest (SHA1, SHA256)
- Public Key generation (RSA 4096, DSA, ECC)
- HOTP one time password
- MAC (AES, 3DES, HMAC)

The VaultIC family is ideally suited to secure and protect applications such as smart meters, femtocells, telehealth, USB drives and gaming platforms.

| Part Number | EEPROM | I/O Interface | Voltage | Package |
|---|---|---|---|---|
| VaultIC200 | 4K | SPI, I2C, ISO 7816 | 2.7-5.5V | SOIC-8, DFN-8 |
| AT98SC016CU | 16K | SPI, I2C, ISO 7816 | 1.62-5.5V | QFN20, SOIC-8 |
| VaultIC400 | 16K | SPI, I2C, ISO 7816 | 1.62-5.5V | QFN20, SOIC-8 |
| AT98SC032CT-USB | 32K | USB 2.0, ISO 7816 | 2.7-5.5V | QFN44, SOIC-8 |
| VaultIC420 | 32K | USB 2.0, SPI, I$^2$C, ISO 7816 | 2.7-5.5V | QFN44, SOIC-8 |
| VaultIC440 | 64K | USB 2.0, SPI, I$^2$C, ISO 7816 | 2.7-5.5V | QFN44, SOIC-8 |
| VaultIC460 | 128K | USB 2.0, SPI, I$^2$C, ISO 7816 | 2.7-5.5V | QFN44, SOIC-8 |

## Development Kit

The VaultIC evaluation kit provides a user-friendly hardware and software package that allows the evaluation of the product.

### Hardware

- A Set of product samples
- An Evaluation board
- USB to SPI / I2C / ISO 7816 adapter
- A USB dongle

### Software

- A getting started document
- VaultIC Manager to personalize the VaultIC File System
- The official demonstration application to get an insight of VaultIC features
- Many advanced tutorial scripts to ease the understanding of VaultIC
- High Level Cryptographic Libraries for easy System Integration

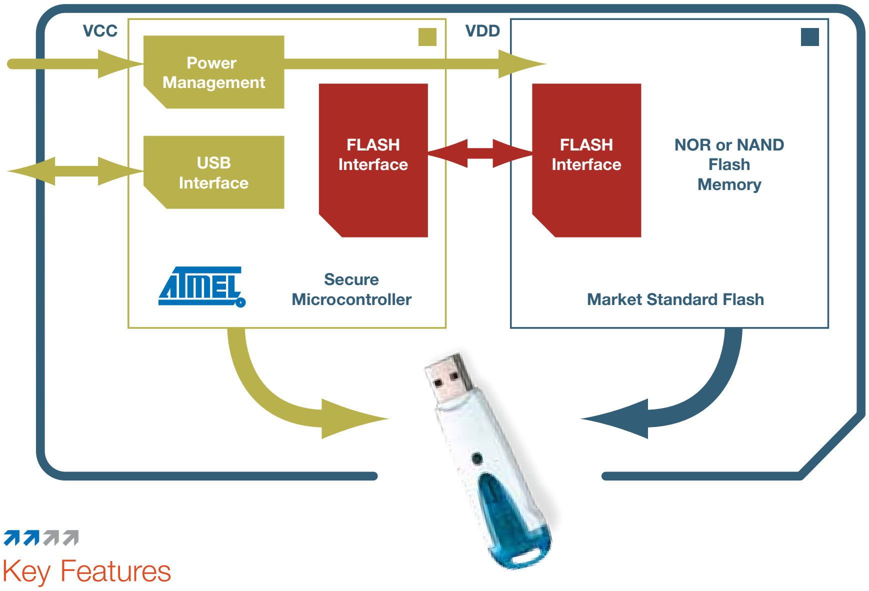
# Secure System-On-Chip

Atmel offers two Secure System-On-Chip families based on different dedicated architectures:

- 8-/16-bit secureAVR® for compact devices with low power consumption and fast computation
- ARM 32-bit SecureCore™ SC100 for very demanding applications

Both architectures offer fast and robust cryptography engines (DES, TDES, AES, RSA, ECC…), security features, together with a choice of memory profiles, various interfaces (SPI, USB, I²C, MMC, ISO7816…) and different packages for an easy integration on Printed Circuits Boards.

## Example of USB Secure Data Storage Solution



## Key Features

- secureAVR® or ARM® SC100
- USB 2.0 Full Speed and Inter-Chip USB Interface
- Memory extension interfaces: external NAND Flash memory, SPI (NOR Flash memory)
- Communication interfaces: I2C, SPI, ISO7816, GPIOs
- Real Time Clock
- Hardware Co-Processors for 3DES, RSA, AES Cryptography
- FIPS 140-2 Level 3 and 4 and C.C EAL4+/EAL5+
- NFC support with Single Wire Protocol

| Part Number | EEPROM | ROM | RAM | Flash | Interface | Voltage | PKI | RTC |
|---|---|---|---|---|---|---|---|---|
| AT90SO4 | 4K | 96K | 2K | - | I2C, SPI, ISO 7816, GPIOs | 2.7-5.5V | No | No |
| AT90SO64 | 64K | - | 12K | 64K | USB, I²C, SPI, ISO 7816, GPIOs | 2.7-5.5V | Yes | Yes |
| AT90SO128 | 128K | 288K | 12K | - | USB, I²C, SPI, ISO 7816, GPIOs | 2.7-5.5V | Yes | Yes |
| AT90SC12818RCU | 18K | 128K | 6K | - | SPI, I²C, ISO7816, GPIOs | 1.62-5.5V | Yes | No |
| AT90SC25672RCT-USB | 72K | 256K | 8K | - | USB, ISO 7816 | 1.62-5.5V | Yes | No |
| AT90SC144144CT | 144K | - | 8K | 144K | SPI, ISO 7816 | 1.62-5.5V | Yes | No |
| AT90SC320288RCT | 288K | 320K | 8K | - | SPI, ISO 7816 | 1.62-5.5V | Yes | No |
| AT91SC512384RCT | 384K | 512K | 24K | - | USB, NAND, SPI, ISO 7816 | 1.62-5.5V | Yes | No |
| AT91SC192192CT-USB | 192K | - | 24K | 192K | USB, NAND, SPI, ISO 7816 | 1.62-5.5V | Yes | No |
| AT91SC464384RCU | 384K | 464K | 18K | - | SWP, ISO 7816 | 1.62-5.5V | Yes | No |

# Development Tools for AT90SC, AT90SO and AT91SC

The Atmel smart card development kit is a user-friendly hardware and software package that allows easy development, simulation and code emulation of AT90SC, AT90SO and AT91SC family products. The kit includes a complete set of tools for tuning and speeding-up your application development.

secureAVR®

POWERED ARM®

## Key Hardware Tools

- Voyager™ emulation platform ATV™4 including contactless features and ATV4P
- Eagle 3-in-1 board: reader / spy / simulator
- USB development board
- AT91SC Evaluation Board

## Key Software Tools

- IAR systems Embedded Workbench® development environment (compiler, assembler, linker, debugger)
- ARM developer suite™
- RealView® MDK-ARM
- Smart access command script editor
- Embedded libraries
  - Easy start hardware abstract libraries (HAL)
  - Advanced first software layers (FSL)
  - Crypto toolbox

IAR SYSTEMS

## Reader Chips

Working with industry leaders such as Gemalto® and Omnikey®, Atmel provides a large portfolio of products to address various security applications: PC link readers, smartcard keyboards, e-health card readers, point of sales terminals and set top boxes.

| | AT89C5121 | AT83C5121 | AT83C21GC | AT83R5122 | AT89C5122 | AT83C22OK | AT83C5123 | AT83C23OK | AT83C5127 | AT90SCR050 | AT90SCR100 | AT83C26 | AT83C24 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Serial Interface | | | USB Interface | | | | | | Serial & USB Interface | | Level Shifter | |
| *Microcontroller* | | | | | | | | | | | | | |
| Flash (KB) | 16 | | | | 32 | 32 | | | | | 64 | | |
| ROM (KB) | | 16 | | 32 | | | 30 | | 16 | 16 | | | |
| Core | C51 | C51 | C51 | C51 | C51 | C51 | C51 | C51 | C51 | AVR | AVR | | |
| Firmware | | | Gemalto | | | Omnikey | | Omnikey | | | | | |
| Performance | 16MHz | 16MHz | 16MHz | 48MHz | 48MHz | 48MHz | 48MHz | 48MHz | 48MHz | 48MHz | 48MHz | | |
| *Serial Interface* | | | | | | | | | | | | | |
| USB Device Endpoints | | | | 7 | 7 | 7 | 5 | 5 | 5 | 8 | 8 | | |
| USB Host Endpoints | | | | | | | | | | | 4 | | |
| UART | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | |
| SPI | | | | 1 | 1 | 1 | | | | | 1 | | |
| High Speed SPI | | | | | | | | | | | 1 | | |
| Analog Interface | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2+3SAM | 1 |
| *Card Interface* | | | | | | | | | | | | | |
| Digital Interface | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | | | |
| Alternate Card | ✓ | ✓ | | ✓ | ✓ | | ✓ | | ✓ | | | | |
| Synchronous Card | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| USB Card | | | | | | | | | | | ✓ | | |
| ESD Protection | 4kV | 4kV | 4kV | 4kV | 4kV | 4kV | 4kV | 4kV | 4kV | 4kV | 4kV | | |
| *DC/DC Converter* | | | | | | | | | | | | | |
| 3V & 5V Modes | 60mA | 60mA | 60mA | 60mA | 60mA | 60mA | 60mA | 60mA | 60mA | 60mA | 60mA | 60mA | 60mA |
| 1,8V Mode | 35mA | 35mA | 35mA | 35mA | 35mA | 35mA | 35mA | 35mA | 35mA | 35mA | 35mA | 35mA | 35mA |
| Voltage Supervisor | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| *Other Features* | | | | | | | | | | | | | |
| I/O Ports (LED) | 14(2) | 14(2) | 14(2) | 46(7) | 46(7) | (2) | 13/17(4) | (2) | 13/17(4) | (1) | 38(4) | | |
| Power Supply (V) | 2.85-5.5 | 2.85-5.5 | 2.85-5.5 | 3.0-5.5 | 3.0-5.5 | 3.0-5.5 | 3.0-5.5 | 3.0-5.5 | 3.0-5.5 | 2.7-5.5 | | | |
| Crypto Engine | | | | | | | | | | | AES/RNG | | |
| Packages | SSOP24 | SSOP24 | SSOP24 | QFP64<br>QFN64 | QFP64<br>QFN64 | QFP64<br>QFN64 | QFP32<br>QFN32 | QFP32<br>QFN32 | QFP32<br>QFN32 | QFN28<br>QFN24** | QFN64*<br>QFP64**<br>QFN32 | QFP48<br>QFN48 | QFN28<br>SO28 |

* available on 64 pin package
** on request

## ISO 7816 Interface

- Card Clock up to 8 MHz
- Easy and Fast Data Transfer
- Up to 420 Kbps

## Integrated DC/DC

- High Efficiency: 80 to 98%
- Drives 5V, 3V, 1.8V Cards
- Card Power Supervisor

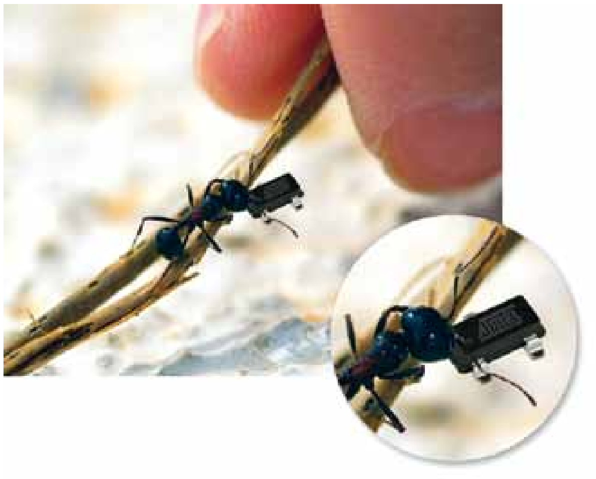
## Reference Designs and Tools

On top of our standard development tools, two reference design kits developed in partnership with Omnikey and Gemalto are available to enable the easy implementation of pre-certified and ready-to-use solutions: AT89RFD-02 (USB interface) AT89RFD-05 (Serial interface), and AT89RFD-06 (PCMCIA).

## CryptoAuthentication™

CryptoAuthentication is Atmel's first family of secure authentication ICs using the SHA-256 hash algorithm with a 256 bit key length, providing robust hardware authentication at a very cost effective price. With CryptoAuthentication developers can easily implement secure authentication and validation of physical or logical elements in virtually all microprocessor based systems using the straightforward 256 bit challenge / response protocol and it is ideal for handheld electronic systems or any embedded system where space is a premium with features such as, a tiny 3-pin SOT23 package and a single pin interface.

CryptoAuthentication's host side IC a full authentication solutions. The host chip off-loads key storage and the execution algorithms and significantly reduces both system cost and complexity by removing the need for system designer to design or test the cryptographic algorithms.



## Development Kits

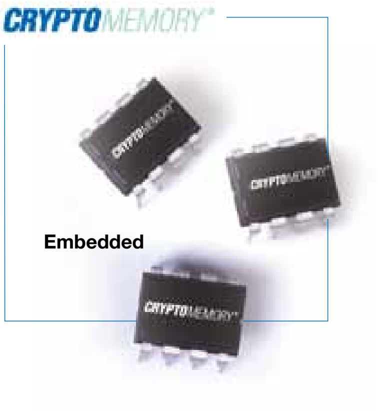
- AT88CK109STK – Javan Start Kit. Includes microbase, socket board, and IC samples.
- AT88CK109BK3 – Javan socket board with 2 SOT23-3 sockets for Host and Client development. Comes with CryptoAuthentication samples.
- AT88CK101BK3 – Javan Jr. socket board with 1 SOT23-3 socket for Client only development. Comes with CryptoAuthentication samples.
- AT88CK301ADP – Adaptor board for solution on any system besides AVR
- AT88SA-ADK1 – Rhino+ Evaluation Kit, Includes a small USB PCB with an on-board AT88SA102S

## Applications

- Authentication of Replaceable Items
- Software and Media Anti-piracy
- Network and Computer Access Control
- Portable Media Player and GPS System
- Key Exchange for Encrypted Downloads
- Prevention of Clones for Demo and Evaluation Boards
- Authenticated Communications for Control Networks
- Anti-Clone Authentication for Daughter Cards
- Physical Access Control (Electronic Lock & Key)

| Part Number | Org | Voltage | Description | I/O | RoHS | Temp |
|---|---|---|---|---|---|---|
| AT88SA102S | N/A | 2.5-5.5V | SHA-256 authentication with high speed single wire interface and less than 100nA sleep current | 1 | Yes | -40°C to 85°C |
| AT88SA10HS | N/A | 2.5-5.5V | Host side security IC for CryptoAuthentication AT88SA102S and AT88SA100S | 1 | Yes | -40°C to 85°C |
| AT88SA100S | N/A | 2.5-5.5V | SHA-256 battery authentication with high speed single wire interface and less than 100nA sleep current | 1 | Yes | -40°C to 85°C |

# CryptoMemory®



### The Worlds Only Secure Serial EEPROM

This embedded family of devices in the plastic package option provides secure serial EEPROM storage for sensitive information within an embedded system. CryptoMemory cryptographic security IC's offer a low cost, high security solution for any embedded application requiring data protection and using only synchronous protocol.

A cryptographic algorithm encrypts data and passwords as well as generate Message Authentication Codes (MAC) thereby providing a secure place where information remains safe even under attack. CryptoMemory is the only secure memory family of devices in the industry with mutual authentication between device and host, plus data encryption. Both synchronous and asynchronous protocols are available.

## CryptoMemory Advantages

- No Operating System Needed; Easy to Program
- Cost Savings up to 50% Compared to Microprocessor Implementation
- Fast Time to Market
- Can be used in both embedded and smart card applications

## Development Kits

- Javan Starter Kit, AT88CK109STK
- Aris+ Development Kit, AT88SC-ADK2
- Tuema Development Kit, AT88SC-SDK1

| Device | User Memory | Memory Zones | Passwords | Authentication | Encryption | Interface Type | VCC |
|---|---|---|---|---|---|---|---|
| AT88SC0104CA | 1Kbit | 4 | Yes | Yes | Yes | ISO7816 + 2-wire | 2.7-3.3 |
| AT88SC0204CA | 2Kbit | 4 | Yes | Yes | Yes | ISO7816 + 2-wire | 2.7-3.3 |
| AT88SC0404CA | 4Kbit | 4 | Yes | Yes | Yes | ISO7816 + 2-wire | 2.7-3.3 |
| AT88SC0808CA | 8Kbit | 8 | Yes | Yes | Yes | ISO7816 + 2-Wire | 2.7-3.3 |
| AT88SC0104C | 1 Kbit | 4 | Yes | Yes | Yes | ISO7816 + 2-wire | 2.7-5.5 |
| AT88SC0204C | 2 Kbit | 4 | Yes | Yes | Yes | ISO7816 + 2-wire | 2.7-5.5 |
| AT88SC0404C | 4 Kbit | 4 | Yes | Yes | Yes | ISO7816 + 2-wire | 2.7-5.5 |
| AT88SC0808C | 8 Kbit | 8 | Yes | Yes | Yes | ISO7816 + 2-wire | 2.7-5.5 |
| AT88SC1616C | 16 Kbit | 16 | Yes | Yes | Yes | ISO7816 + 2-wire | 2.7-5.5 |
| AT88SC3216C | 32 Kbit | 16 | Yes | Yes | Yes | ISO7816 + 2-wire | 2.7-5.5 |
| AT88SC6416C | 64 Kbit | 16 | Yes | Yes | Yes | ISO7816 + 2-wire | 2.7-5.5 |
| AT88SC12816C | 128 Kbit | 16 | Yes | Yes | Yes | ISO7816 + 2-wire | 2.7-5.5 |
| AT88SC25616C | 256 Kbit | 16 | Yes | Yes | Yes | ISO7816 + 2-wire | 2.7-5.5 |

# CryptoRF®

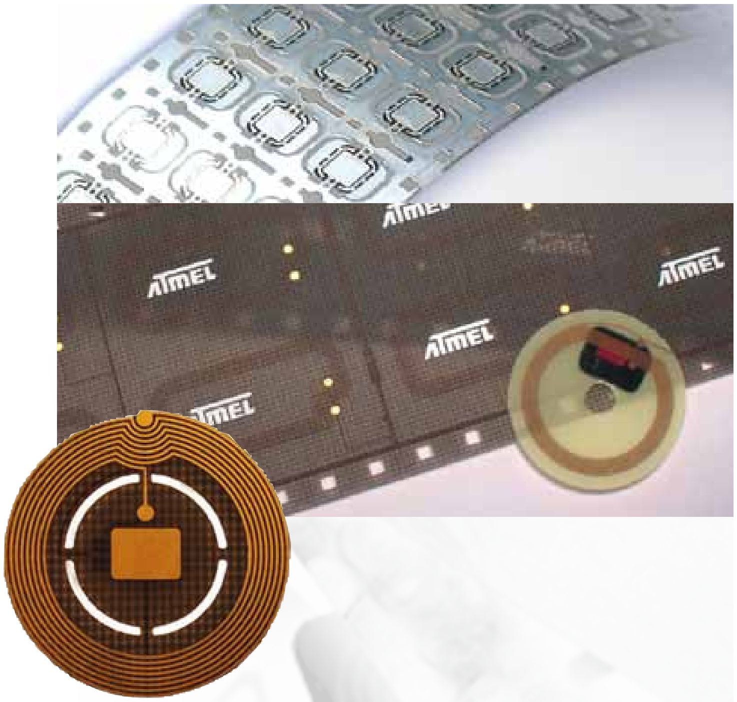
CryptoRF supports the most stringent security standards used for anti-cloning and anti-counterfeiting, identification, and e-purse.
The CryptoRF® family of devices for contactless tags, smart cards, and label applications are available with memory densities from 4 Kbits to 64 Kbits.

Atmel offers the industry's largest range of devices based on our proven secure technology.

### World's Largest Family of Secure RF Memories

- 64-bit Mutual Authentication Protocol
- Stream Encryption Ensuring Data Privacy
- Multiple Key Sets for Authentication and Encryption
- Cryptographic Message Authentication Codes (MAC)
- Encrypted Passwords with Attempt Counters
- Selectable Access Rights by Zone
- Tamper Sensors
- Compliant with Industry Standards

CRYPTORF®



| Device | User Memory | Memory Zones | Passwords | Authentication | Encryption | Interface Type |
|---|---|---|---|---|---|---|
| AT88RF04C | 4 kbit | 4 | Yes | Yes | Yes | ISO14443 Type B |
| AT88SC0808CRF | 8 kbit | 8 | Yes | Yes | Yes | ISO14443 Type B |
| AT88SC1616CRF | 16 kbit | 16 | Yes | Yes | Yes | ISO14443 Type B |
| AT88SC3216CRF | 32 kbit | 16 | Yes | Yes | Yes | ISO14443 Type B |
| AT88SC6416CRF | 64 kbit | 16 | Yes | Yes | Yes | ISO14443 Type B |

## Applications

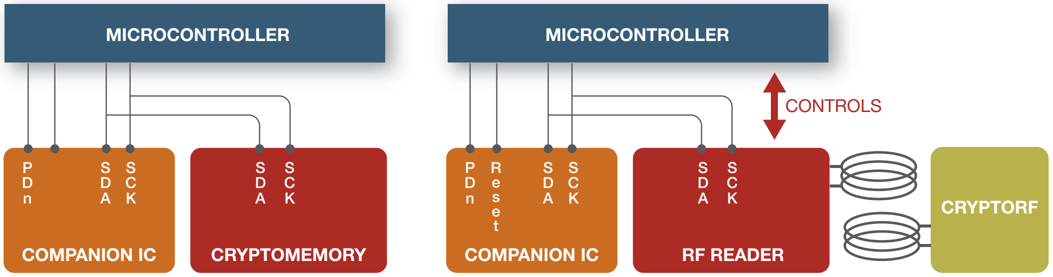
- Anti-Counterfeiting
- Tags
- Industrial RFID
- Identification Cards
- E-Purse
- Labels

## Development Kits

- Bamboo Starter Kit, AT88CK201STK
- Keen+ Development Kit, AT88SCRF-ADK2
- CryptoRF/Skytek Development Kit, AT88SCRF-S7DK2p

## CryptoCompanion™

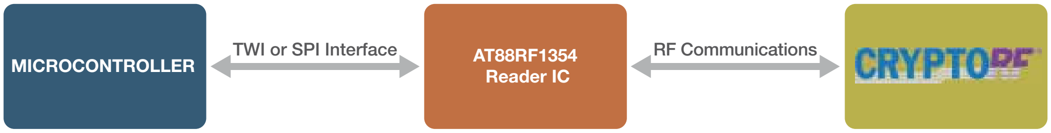
CryptoCompanion eliminates the need to implement the CryptoMemory or CryptoRF host side algorithm in software. Using the standard SHA-1 algorithm, the device provides secure key storage and management of up to 16 keys. CryptoCompanion simplifies and secures deployment of CryptoMemory or CryptoRF by avoiding algorithm and key disclosure from reverse-compilation of system operating code. In addition, CryptoCompanion incorporates a robust random number generator usable for the entire system security.



| Device | Memory | Authentication | Encryption | Interface Type | VCC | Package |
|---|---|---|---|---|---|---|
| AT88SC018 | 4 Kbit | Yes | Yes | 2-wire | 2.7-5.5 | 8-SOIC |

## 13.56 MHz Reader IC

Atmel's AT88RF1354 reader IC communicates with RFID transponders using the ISO 14443-B communication interface standard. The device is compatible with 3.3V and 5V host microcontrollers with two-wire or SPI serial interfaces. The AT88RF1354 performs all of the RF encoding, timing, and protocol functions, greatly reducing the burden on the host microcontroller.



| Device | Interface Type | VCC | Package |
|---|---|---|---|
| AT88RF1354 | SPI + 2-wire | 2.7-5.5 | 36-pin QFN |

## CryptoController

For the ultimate in hardware-based data security, count on Atmel's Trusted Platform Module (TPM), a complete turnkey solution providing ultra-strong security for computing systems. Primary TPM capabilities:

- IP protection
- System integrity
- Authentication
- Secure communication

The core building blocks for the Atmel TPM are our popular AVR microcontroller and our expertise in silicon security technologies. Additional security measures include active shielding and a variety of tamper-evident circuits. Available in a 28-lead TSSOP and a space-saving 40-lead QFN package, Atmel's TPM provides a cost-effective solution for all computing devices.

## Based on Atmel's 8-bit AVR RISC CPU

- Full Trusted Computing Group (TCG) v1.2 rev 103 Specification Compatibility
- 2048-bit Hardware RSA Crypto Accelerator
- Hardware SHA-1 Accelerator, 50 µs / 64-byte Block
- On-chip Storage of up to 21 User Keys
- Reliable EEPROM for Nonvolatile Storage, No Batteries Required
- True Hardware Random Number Generator
- 3.3V Operation +/- 10% Supply Voltage
- 28-lead TSSOP and 40-lead QFN Package Options

The Atmel TPM implements the full specification developed by the Trusted Computing Group that is increasingly being adopted as the industry standard for secure remote communication between all types of electronic devices. Because Atmel provides embedded firmware, no customer-developed firmware is required. A TCG Software Stack (TSS), BIOS (both MAD & MPD), WHQL certified drivers for Microsoft® Windows® operating systems, Linux® drivers, and applications all ensure effortless integration of the most advanced and affordable security technology available today.

## Embedded Development Kit

The kit includes:

- TPM TWI module
- Mounted on AT90USBKey board
- Standard A to mini B USB device cable
- Mini A to receptacle A USB host adapter
- USB flash drive
- Alternate 9V battery supply cable
- Flash drive with sample code and all necessary documentation

| Part Number | Description | I/O Interface |
|---|---|---|
| AT97SC3204 | Fully V1.2 TCG-compliant Security Processor, Microsoft® Windows Vista™ Logo Compliant, Secure Key Generation and Storage of up to 21 RSA Keys, RNG, SHA-1, 2048/RSA Sign-in < 200ms | LPC |
| AT97SC3204T | Fully V1.2 TCG-compliant Security Processor, Optimized for Embedded Systems, Secure Key Generation and Storage of up to 21 RSA Keys, RNG, SHA-1, 2048/RSA Sign-in < 200ms | TWI |

## Headquarters

**Atmel Corporation**
2325 Orchard Parkway
San Jose, CA 95131
*USA*
Tel: (1) 408 441-0311
Fax: (1) 408 487-2600

## International

**Atmel Asia**
Unit 01-05 & 16, 19/F
BEA Tower, Millennium City 5
418 Kwun Tong Road
Kwun Tong, Kowloon
*Hong Kong*
Tel: (852) 2245-6100
Fax: (852) 2722-1369

**Atmel Europe**
Le Krebs
8 Rue Jean-Pierre Timbaud
BP 309
78054 St-Quentin-en-Yvelines Cedex
*France*
Tel: (33) 1-30-60-70-00
Fax: (33) 1-30-60-71-11

**Atmel 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

## Product Contact

**Product Line**

secureproducts@atmel.com

**Literature Requests**

www.atmel.com/literature

**Web Site**

www.atmel.com

Rev.: 6523E-SMS-10/09 2K

**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 SALES 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 AND 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 products 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.