

ICs FOR SECURITY APPLICATIONS

1 0 **F** 1 1 0 **E** 1 1 0 1 1 1 0 0 1
 0 1 **L** 0 **E** 1 **E** 1 0 1 0 1 1 0 1 0
 1 0 **A** 1 **N** 0 **P** 1 1 0 1 1 0 1 1 1
 0 1 **S** **E** **C** **U** **R** **E** 1 1 0 0 1 1 0 1
 0 0 **H** 1 **R** 1 **O** 0 1 0 1 1 0 1 1 0
 1 1 0 1 **Y** 0 **M** 1 0 1 1 0 1 0 0 1
 1 0 1 0 **P** 1 1 0 1 0 1 1 0 1 1 0
 1 1 1 0 **T** 0 1 1 0 1 1 0 1 0 1 1
 0 1 0 1 **I** 1 0 **S** 1 0 1 1 0 1 0 1
 1 **A** **L** **G** **O** **R** **I** **T** **H** **M** 1 0 1 0 1 0
 1 1 0 1 **N** 0 0 **A** 1 0 1 1 0 **M** 0 0
 1 1 0 1 1 0 **I** **N** **T** **E** **R** **F** **A** **C** **E** 1
 1 0 1 1 0 1 0 **D** 1 1 0 1 1 **U** 1 1
 0 1 0 1 0 1 1 **A** 0 1 1 0 1 1 0 1
 1 1 0 1 1 **S** **E** **R** **I** **A** **L** 1 0 1 1 0
 1 0 1 0 0 1 1 **D** 0 1 1 0 1 0 1 0

- Solutions for all security applications:
 - Physical access control
 - Asset protection
 - Sensitive content protection
 - Transaction privacy
 - Remote user authentication
 - Web commerce
- Full customer support for rapid application implementation:
 - Software development tools
 - System emulation
- Security ICs based on:
 - Secure Flash/EEPROM
 - Encryption algorithms
 - 8, 16 and 32-bit RISC microcontrollers
 - Standard serial interfaces
- Standard product solutions based on Atmel's proven expertise in system level integration:
 - Rapid time-to-market
 - Low risk

SECURITY APPLICATIONS

- Authentication/ Access Control
- Data Security
- Personnel and Asset Management
- Financial Transactions

Applications

Security applications have a number of common requirements. These include the need for a fair, clearly understood means of authentication, and the right balance between the cost and inconvenience of the security measures and the level of security imposed. Atmel's security ICs provide the **highest** levels of security at **reasonable** prices, and offer the flexibility and ease of implementation to minimize the inconvenience. Some of the most common application areas for these products are as follows:

Authentication/Access Control

Atmel has ICs that can ensure that equipment and replacement parts are **authentic** or only the proper people are granted access to a facility. These devices can be used, for example, in campus cards that give students access to college resources, or in loyalty cards that build up consumer profiles and offer discounts. When used for component **identification** they ensure that the elements of a system are correctly matched, and give configuration details. Many applications in **transport** are great time-savers: smart tickets for rapid access to public transport, RF tags in vehicles for collecting road tolls without stopping, and baggage ID tags to ensure the bags stay with passengers on air flights.

Ideal for these applications are Atmel's **AT88SC** family of secure serial EEPROMs and the **AT88RF** series of contactless RFID transponders.

Data Security

Most electronic data is **valuable**, and needs to be protected during transmission or when stored in an accessible medium. Secure ICs can beneficially be used in digital TV set-top boxes, postal meters, driver licenses, health/insurance cards, or for Web encryption. In all of these, the data is **encrypted** for storage or transmission and only decrypted at the final point of use. The encryption algorithms are chosen to give a level of security appropriate for the application, and are extremely difficult to crack.

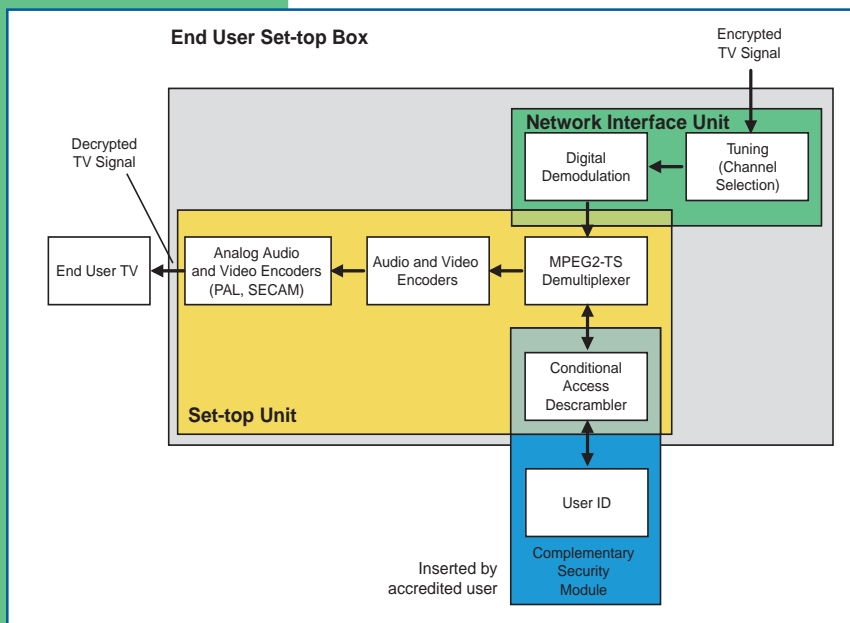
Atmel's three families of secure microcontrollers are targeted at these applications: the industry-standard MCS-51®-based **AT89SC** family and M68HC05®-based **MSC** family, or the proprietary RISC AVR®-based **AT90SC** family.

Personnel and Asset Management

High-value mobile devices such as PCs or test/measurement equipment need to be protected. They should be confined to certain localities or to the charge of accredited people only. Atmel's contactless **AT24RF08** IC is ideal for this application. Mounted inside the device being protected, it can be programmed with the unique identity and configuration of the device, and associated with the ID codes of people authorized to take the device out of its confined area. Doorway detectors monitor the movement of the device and can **disable** it if it is removed by an unauthorized person.

Financial Transactions

When electronic data represents **money**, the highest levels of security are required. Atmel can respond to this challenge with its families of secure cryptocontrollers (the **AT90SCC** and **MSC05** families). Emerging applications for these devices include multi-purpose bank cards, electronic purse (the CEPS European standard for example), and the most rapidly growing application of all **Web commerce**.



Encrypted Digital TV Reception/Decryption

Architecture

The architecture shown in the block diagram underlies all Atmel's secure ICs. The key features are as follows:

An **embedded microcontroller** is used for overall system control and to interpret the encryption algorithm. Atmel offers the choice between the industry-standard MCS-51 or M68HC05, or the proprietary RISC AVR – one of the most powerful 8-bit MCUs on the market. For simple security measures such as PIN number authentication, or challenge/response, **dedicated logic** is used in certain products.

Atmel's technological leadership in **EEPROM** is used to the full in the provision of data memory. High-speed, low-power, millions of write cycles, and almost impossible to penetrate.

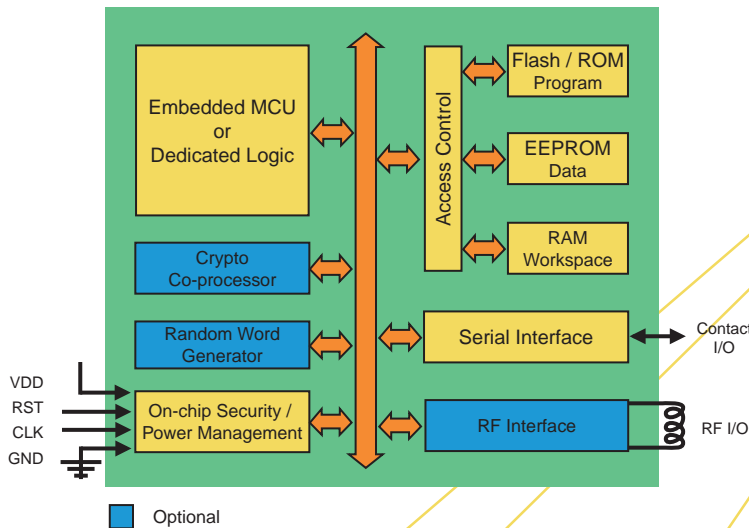
Highly-efficient **SRAM** provides the workspace for both the MCU and the crypto co-processor.

High-security products incorporate a custom-designed **crypto co-processor** (modular exponentiation unit) to implement the encryption algorithm. Running independently of the MCU, this

minimizes the delay in encrypting or decrypting data that would take a hacker years to crack using a supercomputer.

The **random word generator** makes it almost impossible to replicate the behavior of the IC, and thereby obtain an encryption key previously used.

SECURE IC ARCHITECTURE



Secure IC Architecture

Protecting the on-chip memory blocks is a sophisticated **access control unit**, that provides address and data bus scrambling and detects any non-standard attempt at memory access. The latter can trigger a memory erase.

Secure software storage on-chip is provided by Atmel's proprietary **Flash** memory. This has the advantages of loading application code at the last stage of IC fabrication or even at the customer site. Software upgrades can be carried out with no delay by programming stocks of blank devices. Space-saving **ROM** can also be used for program storage.

In addition to these features, Atmel's secure ICs incorporate precautions against physical attack: scrambled bus routing, phantom metal layers, data obfuscation and other Atmel proprietary techniques.

The embedded microcontrollers are fully supported with application development and emulation tools. The aim is to reduce the time-to-market of the end-user application.

The serial interface offers a choice between the industry standards: I²C, SPI, USB, ISO7816. This allows the IC to be seamlessly connected to almost any consumer or industrial device.

Contactless products contain an ISO 14443-compliant **RF interface**.

The **on-chip security and power management** unit protects the device against over- and under-power, over- and under-frequency and other attempts to tamper with it, and masks its power consumption profile. Each device can have a unique ID and transport code.

Atmel Corporation is a leading manufacturer of nonvolatile memory, microcontrollers, logic programmable ICs and application-specific circuits. Our strategy is to develop products – which leverage our patented position in nonvolatile memory – that can provide customers a competitive edge.

Headquartered in San José, California, Atmel operates fabs in Colorado Springs, USA, Nantes and Rousset, France and Heilbronn, Germany.

Security Products Marketing

USA

Tel : (+1)(719) 540-1834

Fax : (+1)(719) 540-1759

France

Tel : (+33)(0)4 42 53 61 29

Fax : (+33)(0)4 42 53 60 01

United Kingdom

Tel : (+44)(0) 1355 355000

Fax : (+44)(0) 1355 242743

Corporate Headquarters

2325 Orchard Parkway

San Jose, CA 95131

USA

Tel : (+1)(408) 441 0311

Fax : (+1)(408) 436 4300

Europe

Atmel U.K. Ltd

Coliseum Business Centre

Riverside Way, Camberley

Surrey GU15 3YL, England

Tel : (+44)(0)(1276) 68 66 77

Fax : (+44)(0)(1276) 68 66 97

Asia

Atmel Asia Ltd

Room 1219

Chinachem Golden Plaza

77 Mody Road

Tsimshatsui East, Kowloon

Hong Kong

Tel : (+852) 272 19 778

Fax : (+852) 272 21 369

Japan

Atmel Japan KK

Tonetsu Shinkawa Bldg, 9F

1-24-8 Shinkawa

Chuo-Ku, Tokyo 104-0033

Japan

Tel : (+81) 3 3523 3551

Fax : (+81) 3 3523 7581

E-mail

literature@atmel.com

Web Site

http://www.atmel.com

Atmel offers a full line of silicon chips for every requirement, including those specifically designed for high-security applications:

Atmel Security Products

| Secure Serial EEPROMs with PIN | | | | | |
|---|--------------|--|------------|--------------|--------------|
| AT88SC101 | 1024 x 1 | 1 Zone | | | |
| AT88SC102 | 2 (512 x 1) | 2 Zones | | | |
| AT88SC1601 | 16K x 1 | 1 Zone | | | |
| AT88SC1604 | 4 (4K x 1) | 4 Zones | | | |
| Secure Serial EEPROMs with PIN and Authentication | | | | | |
| AT88SC153 | 3 (64 x 8) | Up to 3 Zones | | | |
| AT88SC1608 | 8 (256 x 8) | Up to 8 Zones | | | |
| Contactless (RFID) ICs | | | | | |
| AT88RF256 | 256 x 1 | Read/Write RFID Transponder with Passwords and Locking | | | |
| AT88RF8714 | 2K x 8 | Contactless Card IC with AVR Microprocessor, 8K byte ROM, 256 byte RAM | | | |
| AT24RF08 | 1K x 8 | Combination Serial EEPROM with RFID Interface | | | |
| MCS-51-based Secure Microcontrollers | | | | | |
| Name | Flash Memory | EEPROM | RAM | T=0 Hardware | Power Supply |
| AT89SC168 | 16K bytes | 8K bytes | 256 bytes | Yes | 5V |
| AT89SC168A | 16K bytes | 8K bytes | 512 bytes | No | 2.7 - 5.5V |
| AT89SC1616A | 16K bytes | 16K bytes | 512 bytes | No | 2.7 - 5.5V |
| AT89SC248A | 24K bytes | 8K bytes | 512 bytes | No | 2.7 - 5.5V |
| AVR-based Secure Microcontrollers | | | | | |
| Name | Flash Memory | EEPROM | RAM | Crypto Proc. | Power Supply |
| AT90SC1616C | 16K bytes | 16K bytes | 1K bytes | Yes | 3 - 5V |
| AT90SC3232 | 32K bytes | 32K bytes | 1.5K bytes | No | 3 - 5V |
| AT90SC3232C | 32K bytes | 32K bytes | 1K bytes | Yes | 3 - 5V |
| AT90SC3220 | 32K bytes | 20K bytes | 1.5K bytes | No | 3 - 5V |
| AT90SC248C | 24K bytes | 8K bytes | 1K bytes | Yes | 3 - 5V |
| AT90SC4848C | 48K bytes | 48K bytes | 2.5K bytes | Yes | 3 - 5V |
| M68HC05-based Secure Microcontrollers | | | | | |
| Name | ROM | EEPROM | RAM | Power Supply | |
| MSC0406 / AT05SC0901 | 9K bytes | 1K bytes | 240 bytes | 3V or 5V | |
| MSC0407 / AT05SC2304 | 23K bytes | 4K bytes | 384 bytes | 3V or 5V | |
| MSC0501 / AT05SC2004C | 20K bytes | 4K bytes | 384 bytes | 3V or 5V | |
| MSC0801 / AT05SC2004RF | 20K bytes | 4K bytes | 896 bytes | 3V or 5V | |
| MSC0402 / AT05SC2308 | 23K bytes | 8K bytes | 256 bytes | 3V or 5V | |
| MSC1114 / AT05SC3232C | 32K bytes | 32K bytes | 1.6K bytes | 3V or 5V | |

Security Solutions

Atmel's experts can easily custom design a chip to meet almost any specification. From simple secure memories to sophisticated MCU capabilities; let us be your partner. Together we'll find tomorrow's silicon solution for you today.

© Atmel Corporation 1999

Photo: Studio Cadrage

Atmel, the Atmel logo and AVR are registered trademarks of Atmel Corporation. Terms and product names may be trademarks of others. All figures in this brochure are for illustrative purposes only. See Atmel data books for definitive figures and for applicable limitations and warranties.

1305A-6/99/11M

