Features

General

- **Single Chip Turnkey Solution**
- **Strong Challenge-Response Authentication Using Digital Signature**
- **Digital Signature (3DES MAC, RSA PKCS#1, ECDSA)**
- **Encryption (3DES, RSA PKCS#1)**
- **Message Digest (SHA-1, SHA-256)**
- **Public Key Pair Generation (RSA including CRT or ECC)**
- **High Speed Hardware Cryptographic Engines**
  - **Hardware 3DES Crypto Accelerator (112-bits keys)**
  - **Hardware 32-bit Public Key Crypto Accelerator (RSA 2048 bits, ECC 239 bits)**
- **SecureAVR™ 8-/16-bit RISC CPU**
- **Internal 8K bytes EEPROM (10 years data retention, 500K cycles) with password protected file system**
- **Serial Peripheral Interface (SPI) or UART * Interface and 1 GPIO**
- **Hardware True Random Number Generator (RNG)**
- **Secure Architecture Based on ATMEL secureAVR Microcontroller (AT90SC)**
  - **To meet FIPS140-2 requirements**
  - **To meet Common Criteria EAL5+ requirements**
- **Operating Range 1.62V to 5.5V**
- **Lower Power Mode**
- **44-QFN and 8-SOIC* Packages**

Description

Based on ATMEL Smart Card chip design expertise and leadership. The AT98SC008CT is a fully integrated secure solution (Hardware and Firmware) designed for embedded systems (Servers/Routers, Peripherals, Set Top Boxes, PDAs, etc.).

This secure chip has been designed to serve anti-cloning, access control and hardware protection applications. It provides an embedded crypto application allowing a strong authentication, digital signature, encryption, message digest and secure storage of user data (keys, etc.).

The AT98SC008CT includes a hardware Triple DES supporting symmetric-key operations and a 32-bit crypto accelerator for public-key operations (RSA and Elliptic Curves signature algorithms).

The chip comprises also a hardware Random Number Generator used to generate on-chip public keys and challenges during authentication process.

Communication with the chip occurs through a SPI interface running up to 2 Mbps (UART interface will be implemented in the future).

In addition to the crypto application, the chip provides a robust communication protocol, a persistent data storage with secure memory management (access control, anti-tearing), and an administration application to manage contents and configuration of the chip.

State-of-the-art security features embedded in Smart Cards secure products dedicated for Banking, ID and Pay-TV are also included in the AT98SC008CT. Including power and frequency protection logic, logical scrambling on data and address, power analysis countermeasures and EEPROM access control.

Note: * Introduced in future product

Secure ASSP

AT98SC008CT Summary

The AT90SC008CT is offered to OEM manufacturers as a turnkey and easy-to-use solution, including the firmware integrated on the chip. ATMEL provides an evaluation kit, a full datasheet, and an application note for customer integration support.
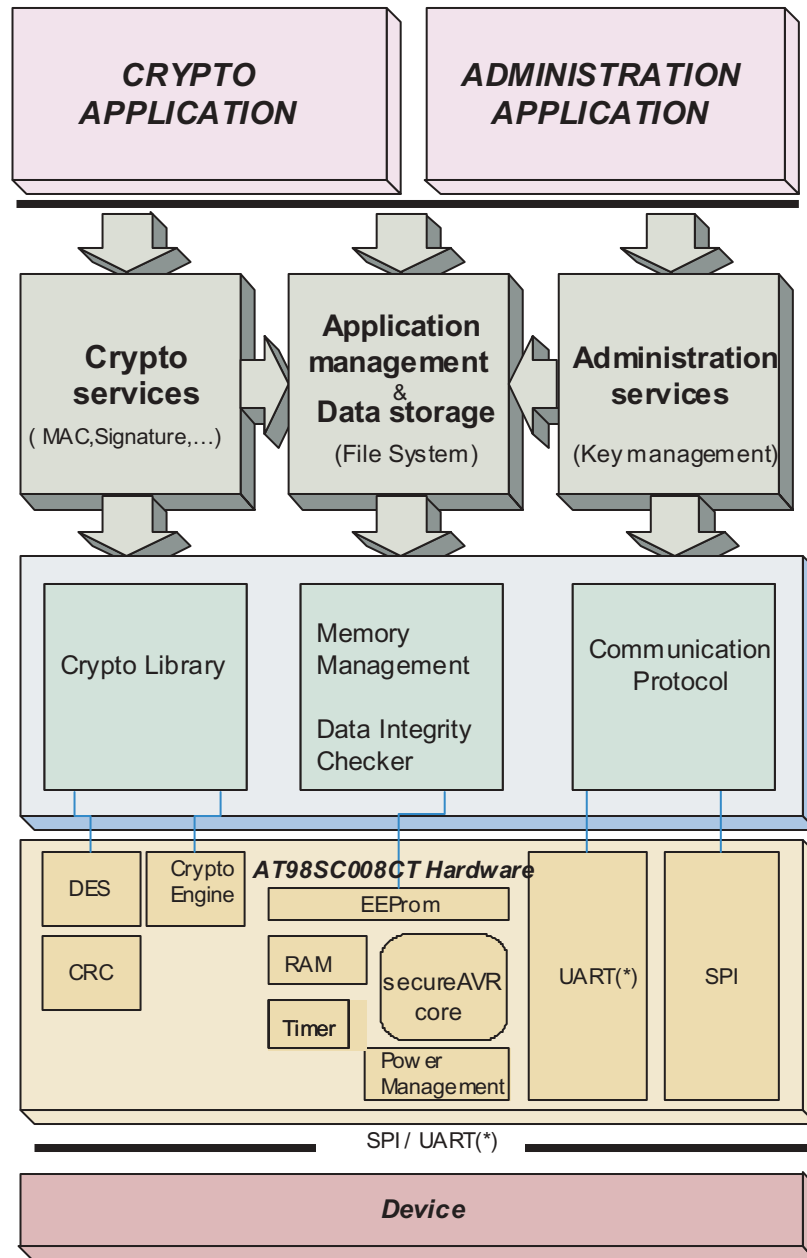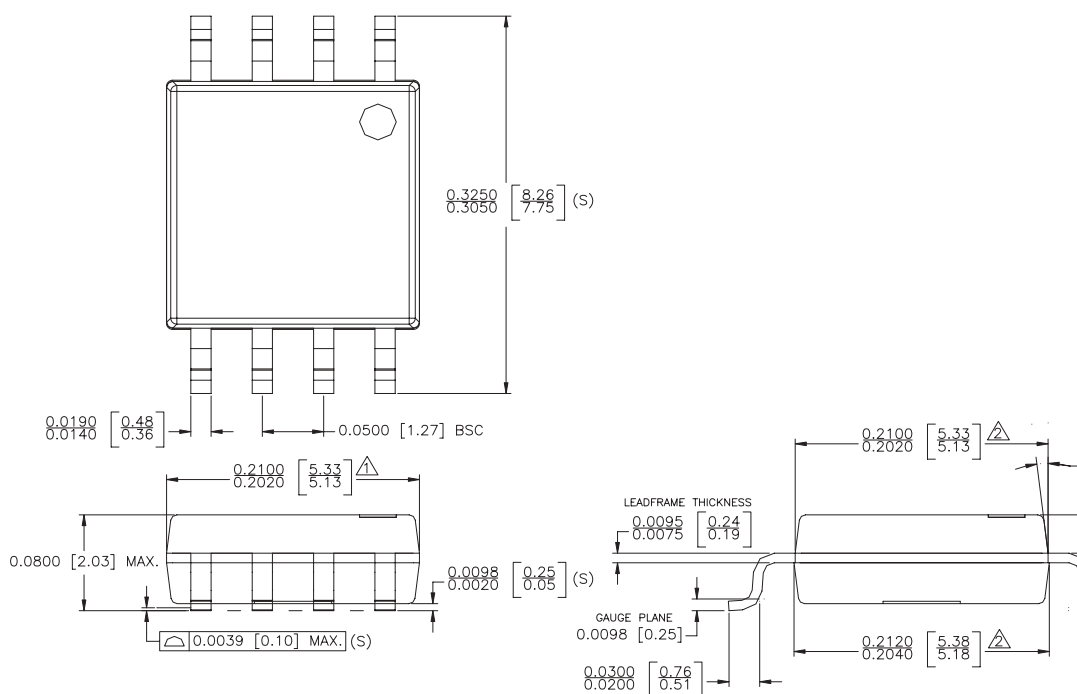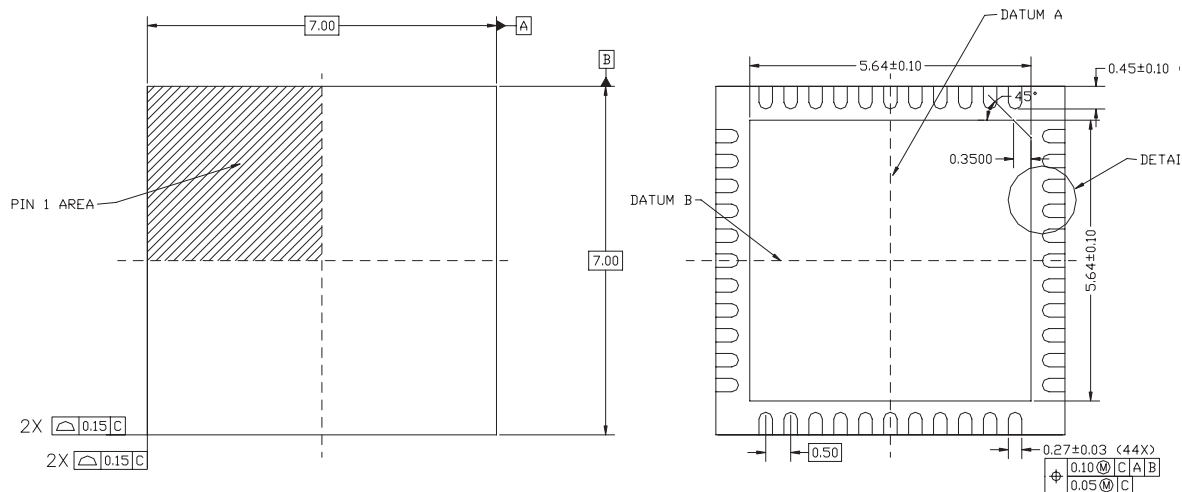

Figure 1. AT98SC008CT Hardware and Software Diagram

Note: * Introduced in future product

8 leads SOIC (207 mils body) *

$\frac{0.3250}{0.3050} \left[\frac{8.26}{7.75}\right]$ (S)

$\frac{0.0190}{0.0140} \left[\frac{0.48}{0.36}\right]$

0.0500 [1.27] BSC

$\frac{0.2100}{0.2020} \left[\frac{5.33}{5.13}\right]$

0.0800 [2.03] MAX.

$\frac{0.0098}{0.0020} \left[\frac{0.25}{0.05}\right]$ (S)

0.0039 [0.10] MAX. (S)

$\frac{0.2100}{0.2020} \left[\frac{5.33}{5.13}\right]$

LEADFRAME THICKNESS
$\frac{0.0095}{0.0075} \left[\frac{0.24}{0.19}\right]$

GAUGE PLANE
0.0098 [0.25]

$\frac{0.0300}{0.0200} \left[\frac{0.76}{0.51}\right]$

$\frac{0.2120}{0.2040} \left[\frac{5.38}{5.18}\right]$

44-QFN (Quad Flat No Lead)

7.00

A

B

7.00

PIN 1 AREA

2X 0.15 C

2X 0.15 C

DATUM A

5.64±0.10

0.45±0.10

45°

0.3500

DETAI

DATUM B

5.64±0.10

0.50

0.27±0.03 (44X)

0.10 (M) C A B
0.05 (M) C

Figure 2. Package Drawings

Note: * Introduced in future product

ATMEL®

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 Arsenaux 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

Printed on recycled paper.

6526AS–SMIC–25Jan06