Features

General

- Single Chip Turnkey Solution
- Strong Challenge-Response Authentication Using Digital Signature
- Digital Signature (3DES MAC, PKCS#1 RSASSA_PSS and RSASSA_PKCS1_v1_5, DSA, EC-DSA, HMAC)
- Encryption (3DES, PKCS#1 RSAES_OAEP and RSAES_PKCS1_v1_5)
- Message Digest (SHA-1, SHA-256)
- Public Key Pair Generation (RSA, RSA-CRT, DSA and EC-DSA)
- High Speed Hardware Cryptographic Engines
  - Hardware 3DES Crypto Accelerator (112-bits keys)
  - Hardware 32-bit Public Key Crypto Accelerator (RSA / DSA 2048 bits, ECC 384 bits)
- RSA 2048 signature in less than 360 ms, and verification in less than 60 ms
- 3DES encryption up to 50 KByte/s
- SecureAVR™ 8-/16-bit RISC CPU
- Internal 16K bytes EEPROM (10 years data retention, 500K cycles) with password protected file system
- Flexible communication interface (Serial Peripheral Interface (SPI), Two Wire Interface (TWI) or half-duplex ISO-7816 UART using T=0 or T=1 protocols)
- FIPS 140-2 Random Number Generator
- Secure Architecture Based on ATMEL secureAVR Microcontroller (AT90SC)
  - To meet FIPS140-2 requirements
  - To meet Common Criteria EAL4+ requirements
- Operating Range 1.62V to 5.5V
- Lower Power Consumption
- 20-QFN and 8-SOIC Packages

Description

Based on ATMEL Smart Card chip design expertise and leadership, the AT98SC016CU is a fully integrated secure solution (Hardware and Firmware) designed for embedded systems (Servers/Routers, Peripherals, Set Top Boxes, PDAs, Vending/gaming machines, 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 AT98SC016CU includes a hardware Triple DES supporting symmetric-key operations and a 32-bit crypto accelerator for public-key operations (RSA, DSA and Elliptic Curves signature algorithms).

The chip comprises also a FIPS 140-2 Random Number Generator used to generate on-chip public keys and challenges during authentication process.

Communication can occur through SPI or TWI using a proprietary block protocol, or through the ISO7816 UART interface using T=0 or T=1.

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 Card secure products dedicated for Banking, ID and Pay-TV are also included in the AT98SC016CU. This includes power and frequency protection logic, logical scrambling on data and address, power

Secure ASSP

AT98SC016CU Summary

6566AS–SMS–08Jun07

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

analysis countermeasures and EEPROM access control. The AT98SC016CU 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.

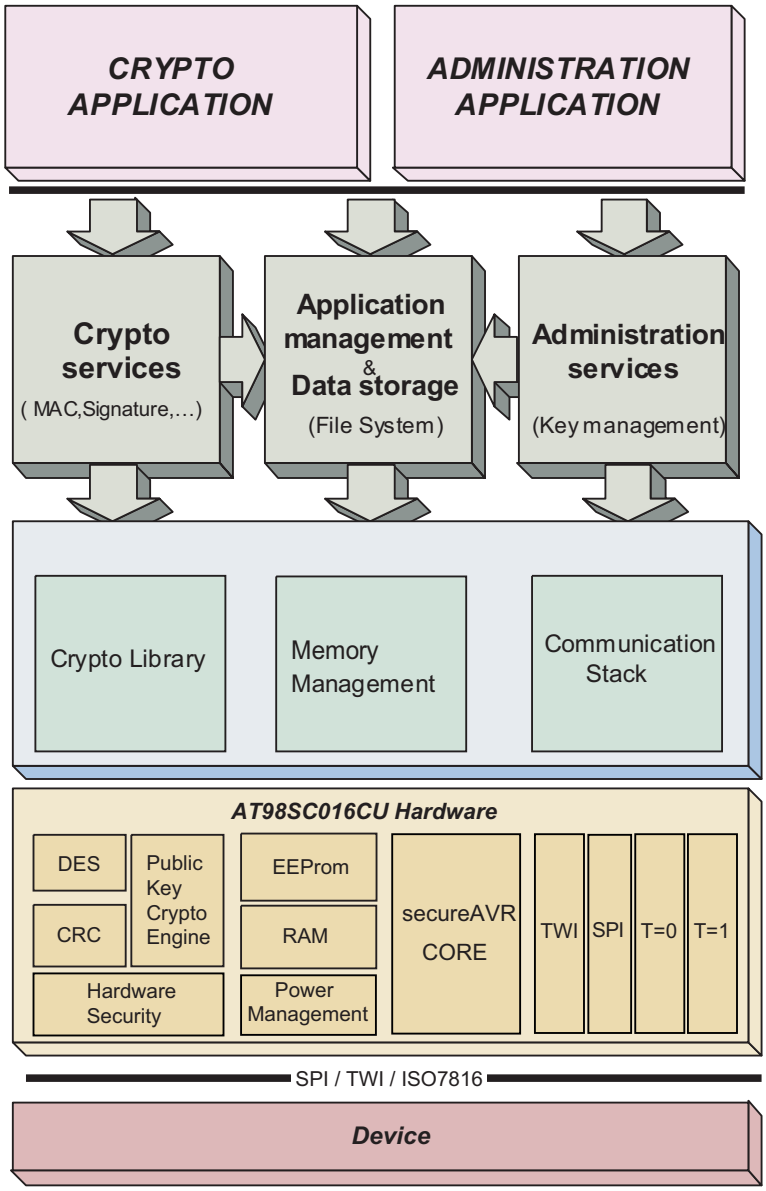
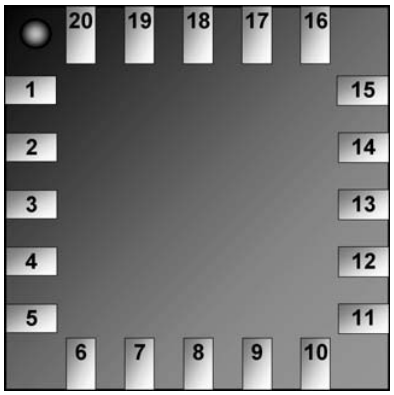


Figure 1. AT98SC016CU Hardware and Software Diagram

20-QFN (Quad Flat No Lead) - RoHS - All protocols



PIN#	Name	Description
1	**A0**	TWI Address selection line A0
2	**A1**	TWI Address selection line A1
3	**A2**	TWI Address selection line A2
4	**RST***	CPU Reset
5	**Vcc**	Power supply
6	**MISO**	SPI Master Input Slave Output
10	**MOSI**	SPI Master Output Slave Input
11	**GND**	Ground (reference voltage)
12	**SS* / SCL**	SPI Slave Select or TWI clock
13	**IO / SPISEL* / SDA**	ISO7816 I/O or SPI/TWI selection or TWI Data
14	**A3**	TWI Address selection line A3
15	**A4**	TWI Address selection line A4
16	**SCK**	SPI clock
20	**CLK / GND**	ISO 7816 Clock or Ground (reference voltage)
Other	**Not Connected**	(do not connect to GND)

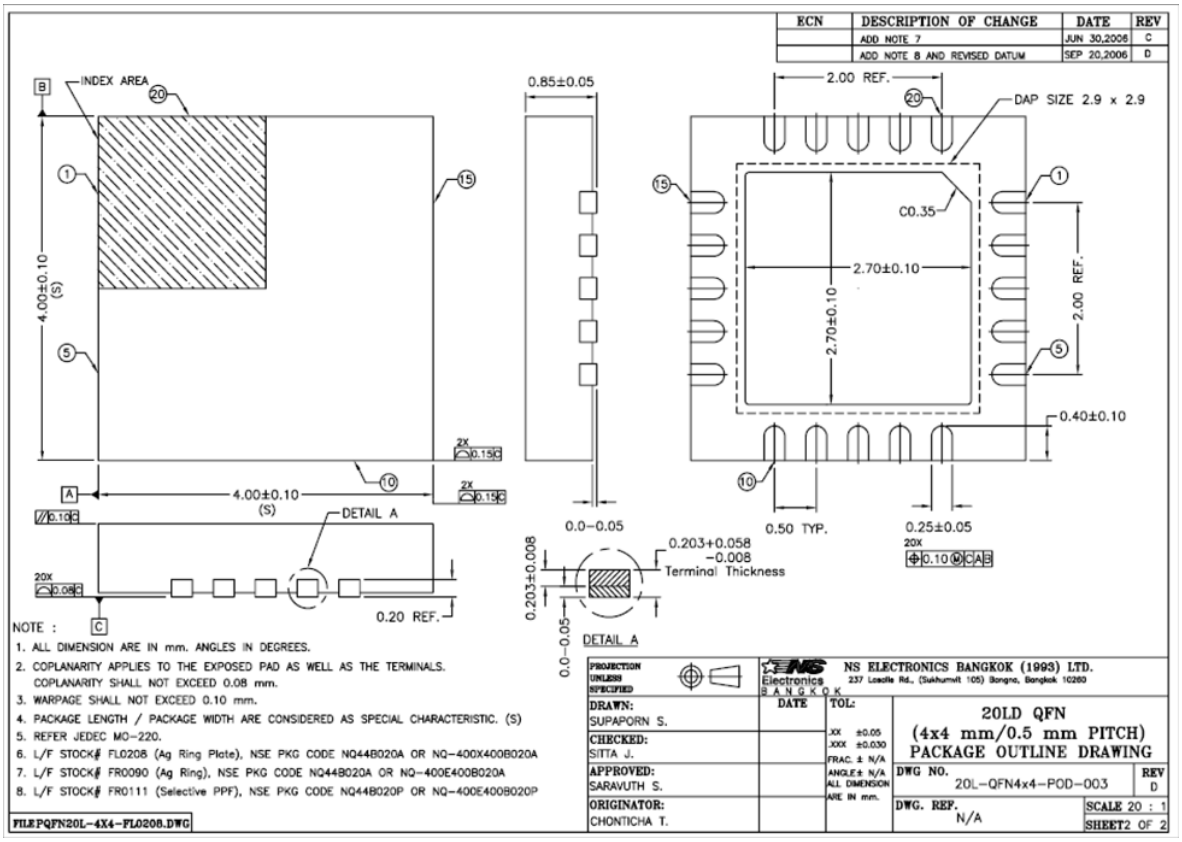
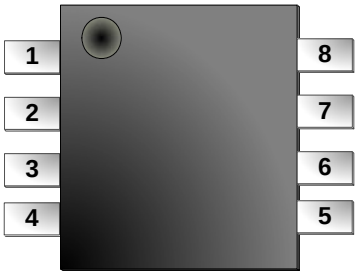


Figure 2. 20-QFN Package diagram, drawing and pinout.

8-SOIC (207 mils body) - RoHS - (SPI / TWI only)



PIN#	Name	Description
1	**MOSI**	SPI Master Output Slave Input
2	**GND**	Ground
3	**SS* / SCL**	SPI Slave Select / TWI clock
4	**SPISEL* / SDA**	SPI/TWI selection / TWI Data
5	**SCK**	SPI clock
6	**RST***	CPU Reset
7	**Vcc**	Power supply
8	**MISO**	SPI Master Input Slave Output

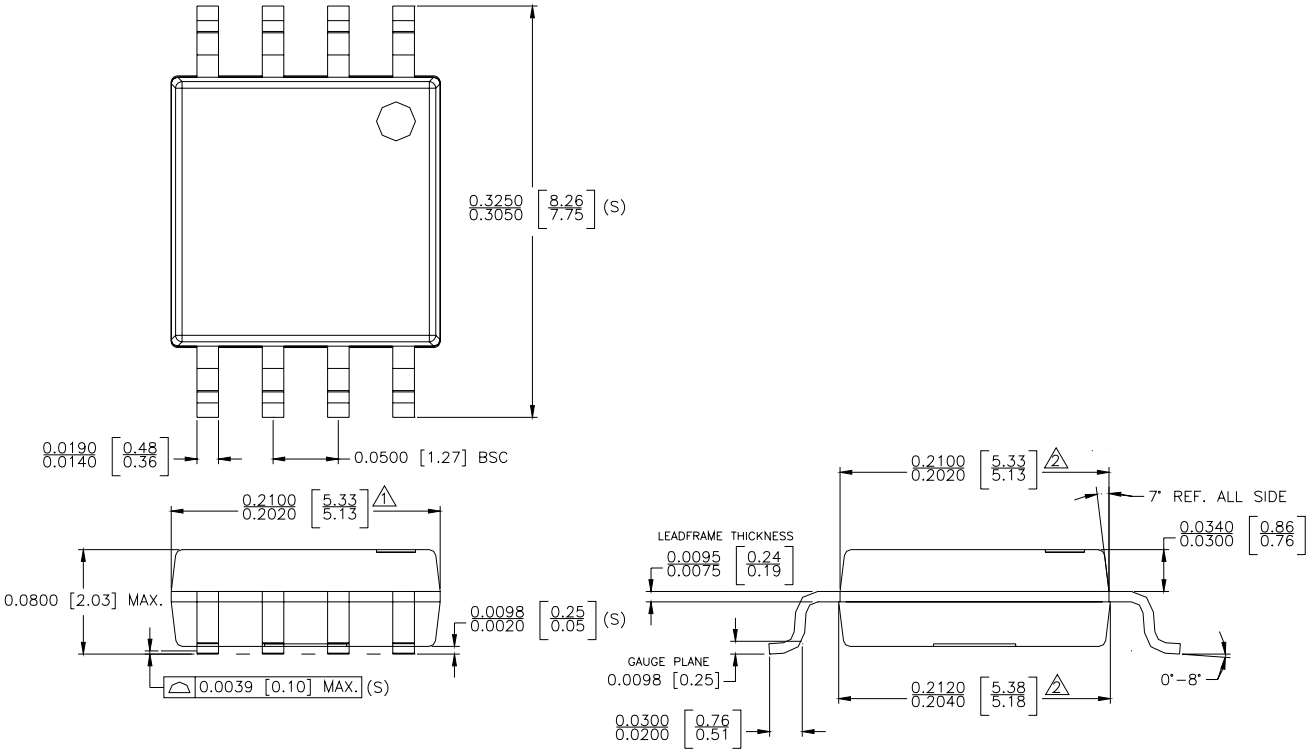


Figure 3. 8-SOIC Package diagram, drawing and pinout.

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

ASIC/ASSP/Secure Products
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

Tel: (33) 4-76-58-30-00
Fax: (33) 4-76-58-34-80

Literature Requests
www.atmel.com/literature