



Secure Solution AT98SC016CU Summary

General Features

Cryptographic Services

- Public Key Pair Generation
- Digital Signature Generation / Verification
- Encryption / Decryption
- Message Digest
- Random Number Generation

Cryptographic Algorithms

- DES / 3DES
- RSA up to 2048 bits
- DSA up to 2048 bits
- ECC up to 384 bits

Software Features

- Strong Challenge-Response Authentication using Digital Signature
- Secure Channel using AKEP-1 Authentication Protocol
- Command Set to perform Cryptographic Operations
- Command Set to personalize and customize the AT98SC016CU
- Password-protected File System

Memory

- File System 16 Kbytes
- Write Endurance 500 Kcycles/Data Retention 10 Years
- 2ms Program + 2ms Erase

Communication

- Slave SPI Serial Interface, INSIDE's Proprietary Protocol
- I²C (Two Wire Interface), INSIDE's Proprietary Protocol
- ISO7816 UART using T=0 or T=1 Protocols

Packages

- 20-QFN (RoHS compliant) 4mm x 4mm
- 8-SOIC (RoHS compliant) 5mm x 5mm

Hardware Platform

- 8-/16-bit RISC CPU
- Hardware Random Number Generator
- Hardware 3DES Crypto Accelerator (112-bits keys)
- Hardware 32-bit Public Key Crypto Accelerator
- Operating Range 1.62V to 5.5V
- Low Power consumption

Certifications / Standards

- EAL4+ Ready
- Protocols and Algorithms based on FIPS Standards

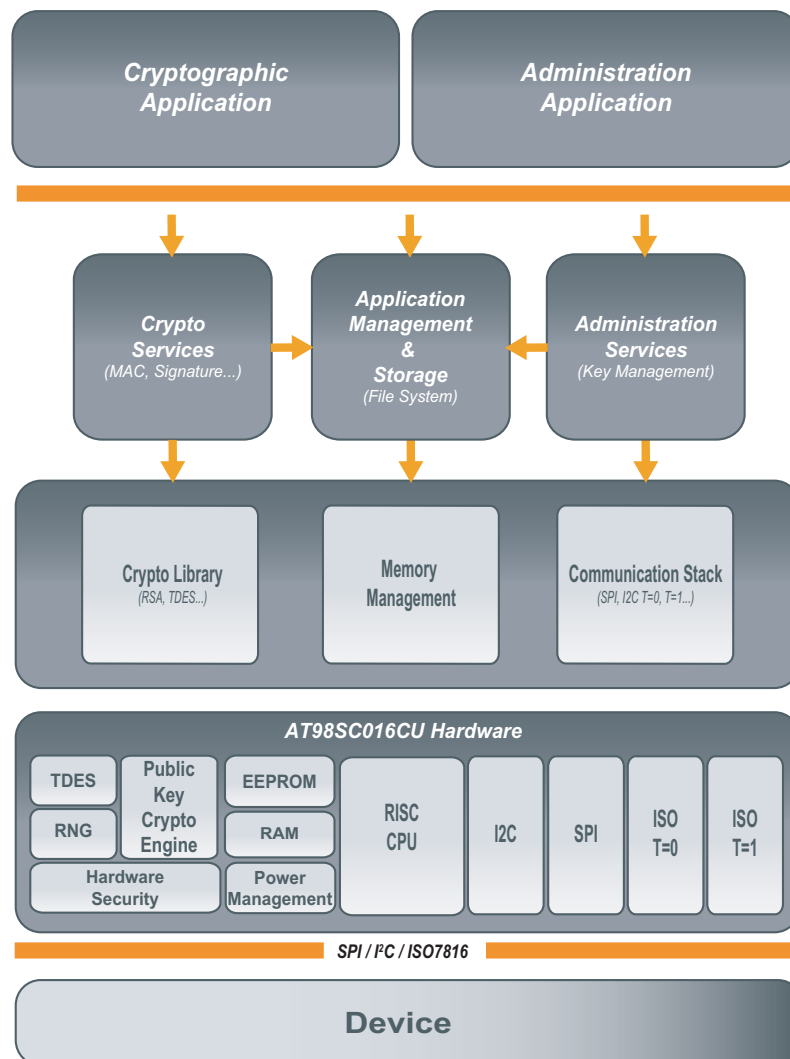
Description

The AT98SC016CU is an ASSP designed to secure various systems against counterfeiting, cloning or identity theft. It is a hardware security module that can be used in many applications such as IP protection, access control or hardware protection.

The proven technology used in AT98SC016CU security modules is already widespread and used in national ID/health cards, e-passports, bank cards (storing user Personal Identification Number, account numbers and authentication keys among others), pay-TV access control and cell phone SIM cards (allowing the storage of subscribers' unique ID, PIN code, and authentication to the network), where cloning must definitely be prevented.

Designed to keep contents secure and avoid leaking information during code execution, the AT98SC016CU include voltage, frequency and temperature detectors, illegal code execution prevention, tampering monitors and protection against side channel attacks and probing. The chips can detect tampering attempts and destroy sensitive data on such events, thus avoiding data confidentiality being compromised. Strong Authentication capability, secure storage and flexibility thanks to its various interfaces (SPI, I2C, ISO7816), low pin count and low power consumption are main features of the AT98SC016CU. Its embedded firmware provided advanced functions such as Strong Challenge-Response authentication, large Cryptographic command set, various Public domain cryptographic algorithms, Cryptographic protocols, Secure Channel Protocols, Robust communication protocol.

Figure 1 Software and Hardware Architecture



Ordering Information

- **Legal**
 - A **Non-Disclosure Agreement** must be signed with Inside Secure.
 - An **Export License** for cryptographic hardware/software must be granted.
- **Quotation and Volume**
 - For the minimum order of quantity and the annual volume, please contact your local INSIDE Secure sales office.
- **Part Number**
 - See below.

Starter Kit

The AT98SC Starter Kit provides an easy path to master the cryptographic and secure data storage features of the AT98SC security modules. The content is :

- AT98SC016CU samples with 1 dedicated test socket
- 1 generic USB to SPI / I²C adapter
- 1 CD-ROM containing a support documentation set (getting started, application notes, reference design), some demo applications to get an insight into the AT98SC features, the "AT98SC Manager" tool to design the file system and to personalize samples, a hardware independent cryptographic API with source code.

Reference		Description
AT98xx016CU-P		P = Z : QFN20 Package R : SOIC8 Package
Reference	Application	Description
AT98SC-STK01-016R	Embedded Security	Starter Kit for AT98SC016CU in SOIC8 package - SPI/I2C configuration
AT98SC-STK11-016R	Embedded Security	Starter Kit for AT98SC016CU in SOIC8 package - SPI/I2C configuration (no SPI/I2C adapter inside)
AT98SC-STK01-016R	SmartCard	Starter Kit for AT98SC016CU in SOIC8 package - ISO7816 configuration
AT98SC-STK01-016Z	Embedded Security	Starter Kit for AT98SC016CU in QFN20 package - SPI/I2C configuration
AT98SC-STK11-016Z	Embedded Security	Starter Kit for AT98SC016CU in QFN20 package - SPI/I2C configuration (no SPI/I2C adapter inside)
AT98SC-STK01-016Z	SmartCard	Starter Kit for AT98SC016CU in QFN20 package - ISO7816 configuration

The photographs and information contained in this document are not contractual and may be changed without notice. Brand and product names may be registered trademarks or trademarks of their respective holders.

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