

Features

General

- Strong Challenge-Response Authentication Using Digital Signature
- Digital Signature (RSA PKCS#1 V2.1, ECDSA)
- Message Authentication Code (3DES MAC, HMAC)
- Encryption (3DES, RSA PKCS#1 V2.1)
- Message Digest (SHA-1, SHA-256)
- Public Key Pair Generation (RSA including CRT, ECC)
- HOTP One-Time Password Generation
- High Speed Hardware Cryptographic Engines
 - Hardware 3DES Crypto Accelerator (112-bits keys)
 - Hardware 32-bit Public Key Crypto Accelerator (RSA 2048 bits, ECC 384 bits)
 - Hardware True Random Number Generator (RNG)
- SecureAVR™ 8-/16-bit RISC CPU
- Secure Architecture Based on ATMEL secureAVR Microcontroller
 - To meet Common Criteria EAL5+ requirements
- Internal 32K Bytes EEPROM (10 years data retention, 500K cycles) with password protected file system
- USB 2.0 Full Speed Certified
- USB-CCID Compliant (no specific driver required)
- Operating Range: 1.62V to 5.5V, -25°C to +85°C
- Low Power Consumption
- SOIC-8, 44-QFN or 44-LQFP package

Description

Based on ATMEL Smart Card chip design expertise and leadership. The AT98SC032CT-USB is a fully integrated secure solution (Hardware and Firmware) designed for computer security applications (e.g. Web portal login, PKCS#11 or MS-CAPI, Two-factor authentication, etc.).

This secure chip features a “crypto” application allowing strong authentication, one-time password generation, digital signature, data encryption, message digest, random number generation and public key generation. The administration application allows the management of contents and configuration of the chip.

Data is permanently stored in a 32 KByte file system which is fully customizable according to customer application requirements. Folders can be password protected, and file access rights can be defined to protect user sensitive data and restrict access to cryptographic features.

The AT98SC032CT-USB includes a hardware 3DES engine and a 32-bit crypto accelerator for public-key operations (RSA and Elliptic Curves algorithms). The chip also features a hardware Random Number Generator used to generate on-chip public keys and challenges during authentication process.

Communication with the chip occurs through a USB 2.0 interface running up to 12 Mbps. Compliance to the USB-CCID ensures an easy interaction with Linux and Windows applications (no specific driver is required).

State-of-the-art security features embedded in ATMEL Smart Cards (dedicated to Banking, ID and Pay-TV) are also included in the AT98SC032CT-USB: power and frequency protection logic, logical scrambling on data and address, power analysis countermeasures and EEPROM access control.



Secure ASSP

AT98SC032CT- USB Summary

6533AS-SMIC-13Oct06



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

The evaluation kit (P/N : AT98SC-EV2) includes sample board and/or USB dongles,, the ATMEL File System Creator software, a getting started guide and a sample PKCS#11 implementation.

The AT98SC032CT-USB 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.

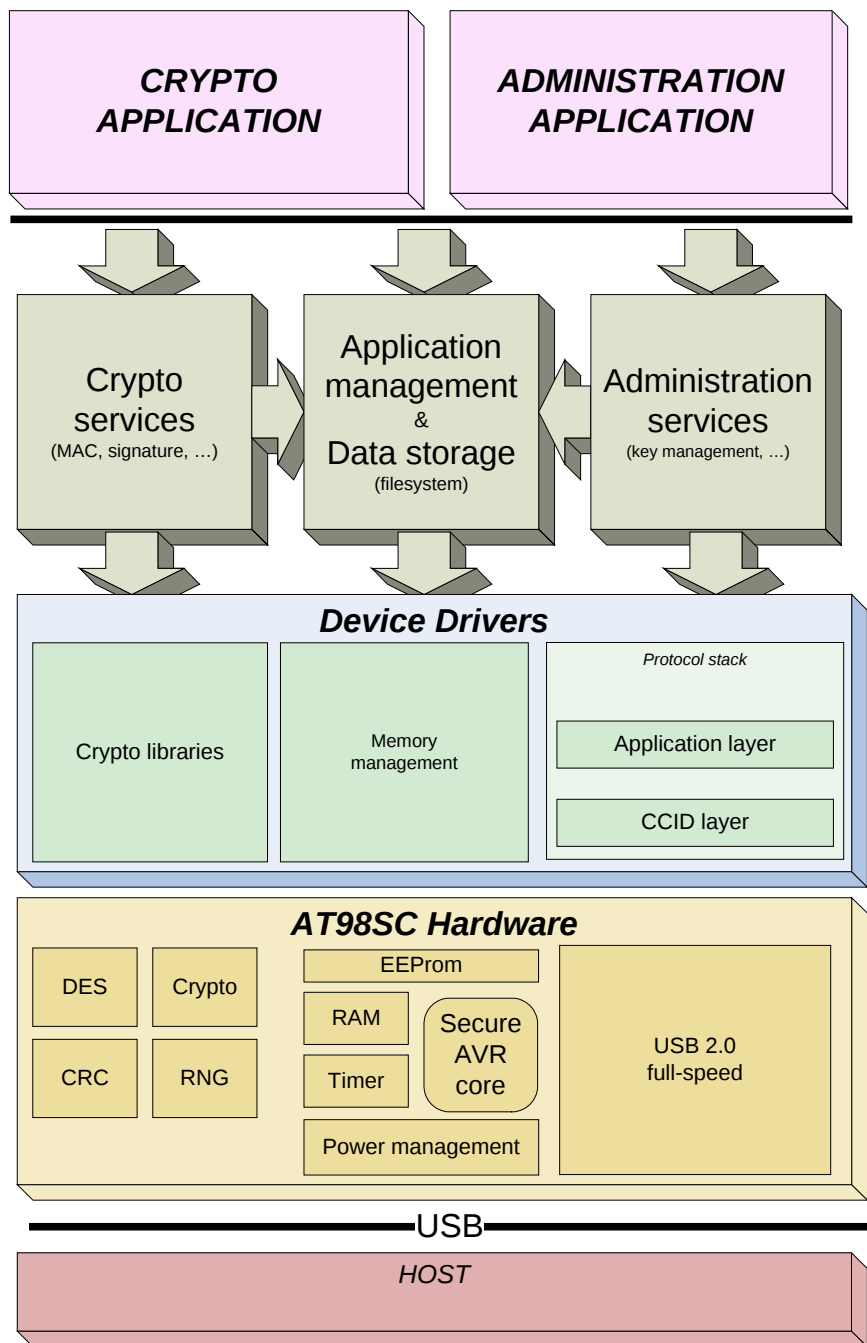
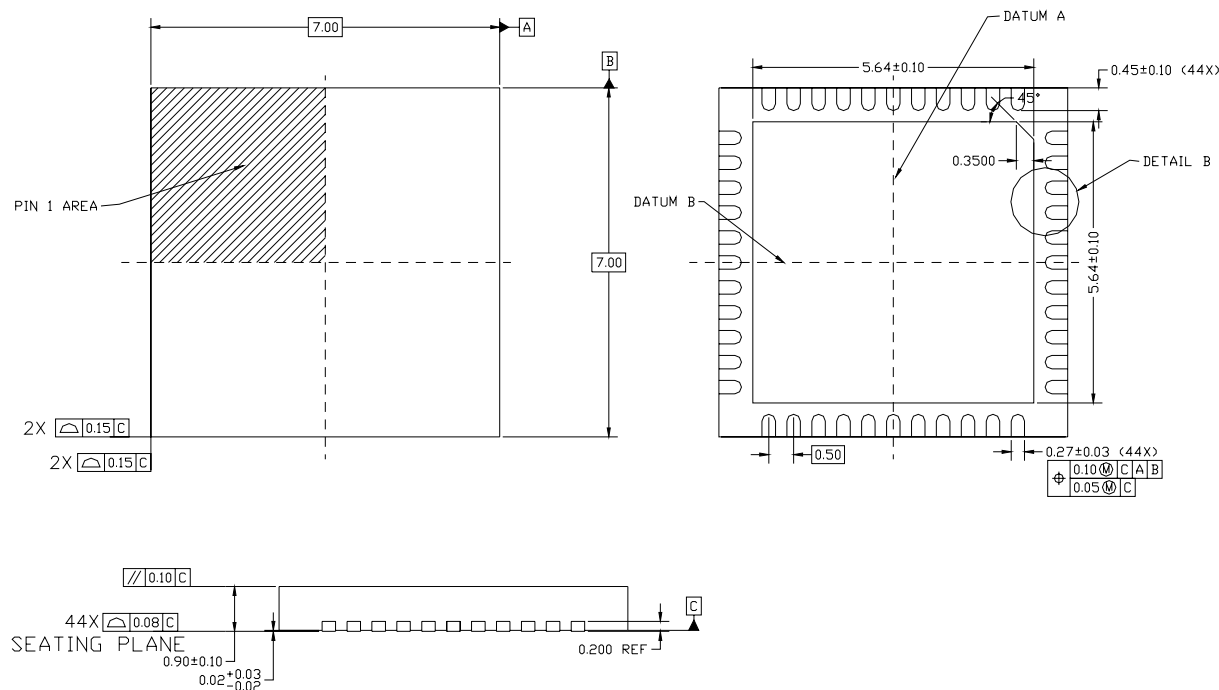
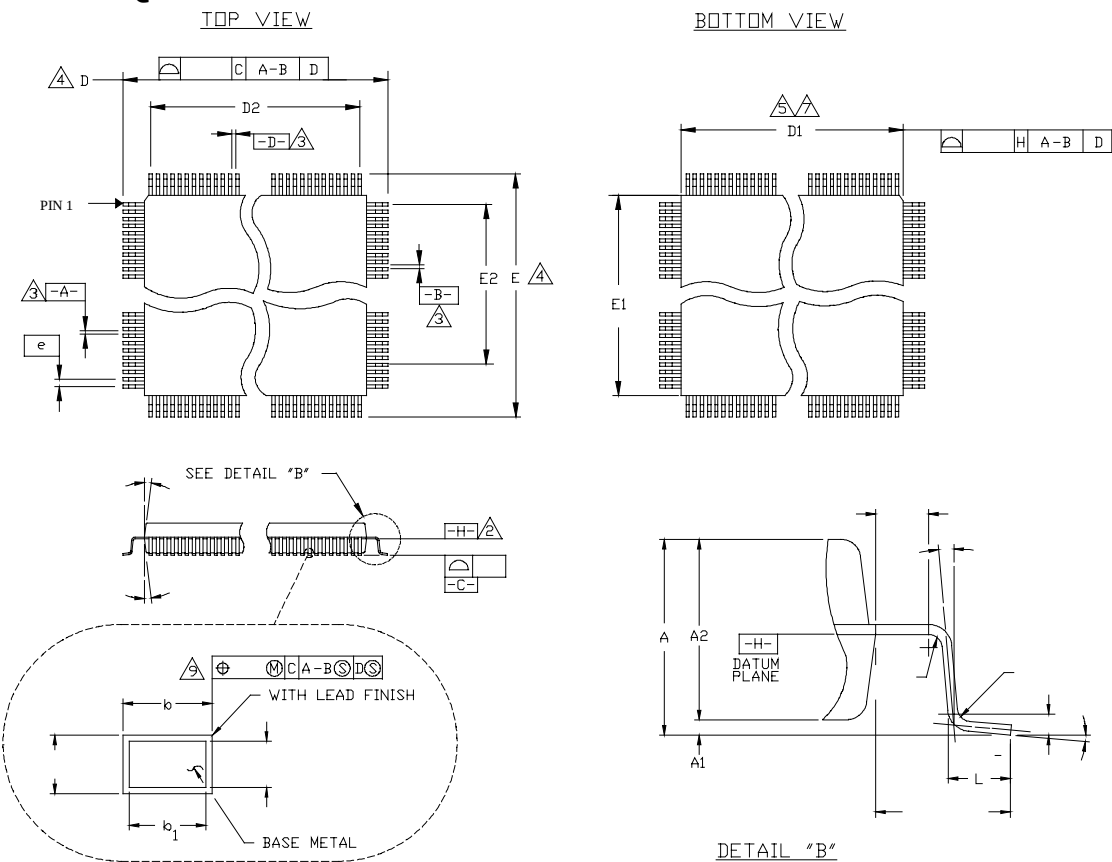


Figure 1. AT98SC032CT-USB Hardware and Firmware diagram

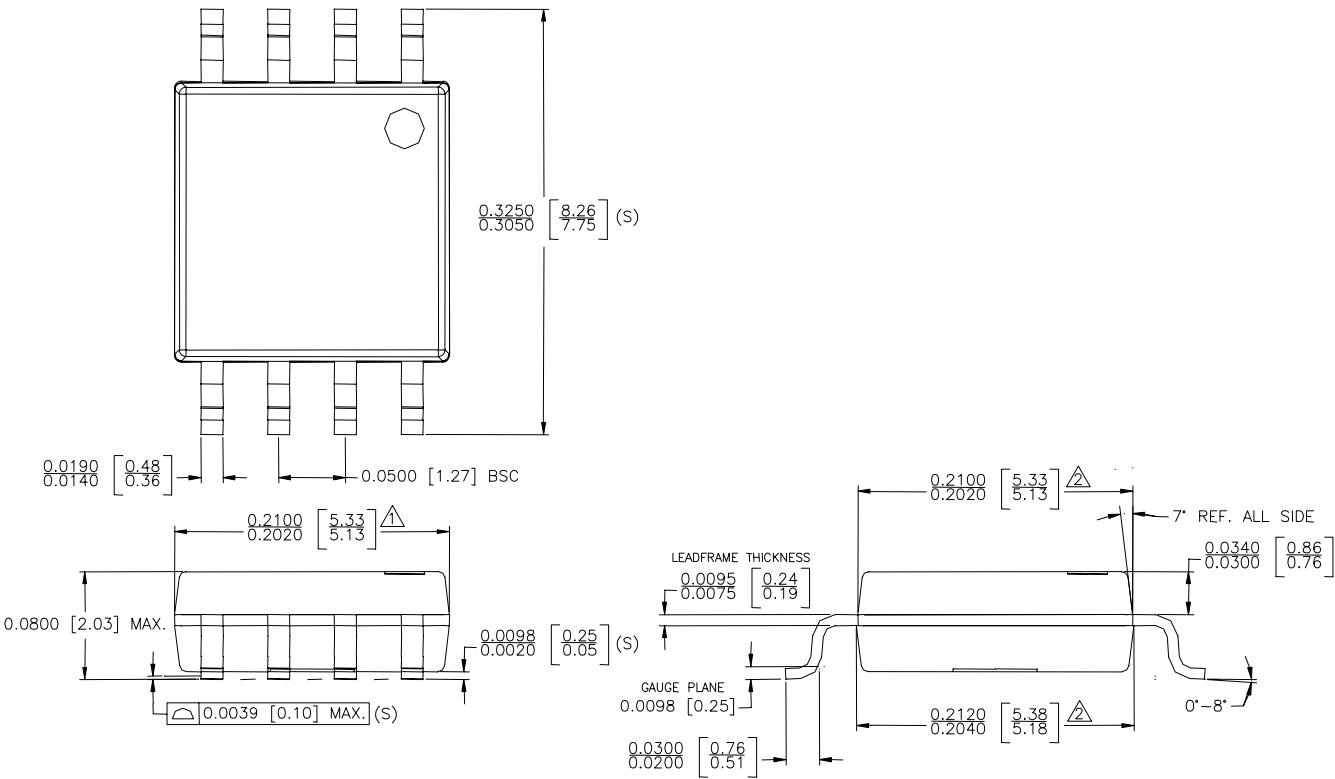
44-QFN



44-LQFP



SOIC-8





Atmel Corporation

2325 Orchard Parkway
San Jose, CA 95131
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 Tsimhatsui
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
Tel.: 1(408) 441-0311
Fax: 1(408) 436-4314

Microcontrollers

2325 Orchard Parkway
San Jose, CA 95131
Tel.: 1(408) 441-0311
Fax: 1(408) 436-4314

La Chantretrie

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
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
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

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 SALE 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 OF 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 product 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.

© 2006 Atmel Corporation. All rights reserved. Atmel®, logo and combinations thereof, Everywhere You Are® and others are registered trademarks or trademarks of Atmel Corporation or its subsidiaries. Other terms and product names may be trademarks of others.



Printed on recycled paper.

6533AS-SMIC-13Oct06