
Features

- Compliant with Trusted Computing Group (TCG) Trusted Platform Module (TPM) Main Specification Version 1.2
- Compliant with TCG PC Client Specific TPM Interface Specification Version 1.2
- Single Chip Turnkey Solution
- Hardware Asymmetric Crypto Engine
- 2048 RSA Sign in 500 ms
- AVR[®] RISC Microprocessor
- 33 MHz LPC (Low Pin Count) Bus for Easy PC Interface
- Secure Hardware and Firmware Design
- True Random Number Generator (RNG) – FIPS 140.2 compliant
- Secure Real-time Clock Option
- 3.3V ±10% Supply Voltage
- 28-lead TSSOP Package or 40-lead QFN Package
- 0–70°C Temperature Range

Description

The AT97SC3203 Trusted Platform Module (TPM) is the latest offering from Atmel, the world's leading choice for TPMs. Atmel, supplier of the world's first production v1.1b TPM, the AT97SC3201, expands its success into v1.2 TPMs with the AT97SC3203. Atmel continues to pace the development of TPM technology and actively participates in the Trusted Computing Group (TCG) and contributes expertise in the development of the TPM specifications. By utilizing Atmel TPMs, you can be confident that you are implementing the most advanced TPMs available on the market today and in the future.

The AT97SC3203 is a fully integrated security module designed to be integrated into personal computers and other embedded systems. It implements version 1.2 of the Trusted Computing Group specification for Trusted Platform Modules.

The TPM includes a cryptographic accelerator capable of computing a 2048-bit RSA signature in 500 ms and a 1024-bit RSA signature in 100 ms. Performance of the SHA-1 accelerator is 150 µs per 64-byte block. In most cases, TCG key generation operations will be completed using a proprietary mechanism in less than 1 msec.

The chip communicates with the PC through the LPC interface. The TPM supports SIRQ (for interrupts) and CLKRUN to permit clock stopping for power savings in mobile computers.



Trusted Platform Module

AT97SC3203

Summary

Advance Information

Rev. 5116AS-TPM-7/05



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

Table 1. Pin Descriptions

| Name | TSSOP Pin # | QFN Pin # | Type | Description |
|-------------|----------------|----------------|-----------------|--|
| LAD[3:0] | 17, 20, 23, 26 | 30, 27, 24, 21 | Input or Output | LPC Multiplexed Command, Address, Data: Internal pull-ups are provided. |
| LFRAME# | 22 | 26 | Input | LPC frame: Indicates the start of an LPC cycle, or an abort. |
| LPCPD# | 28 | 32 | Input | Power Down: Indicates that the TPM should prepare for power to be shut off on the LPC interface. If this pin is unused, it should be tied to the 3V power supply pin through a resistor. |
| CLKRUN# | 15 | 19 | Input or Output | PCI Clock Run: Active low output enabling the system LPC clock. If this pin is unused, it should be tied to ground. |
| LCLK | 21 | 25 | Input | 33MHz PCI clock provides timing for all transactions on the PCI bus. |
| LRESET# | 16 | 20 | Input | PCI signal to reset all devices that reside on the PCI bus. |
| SERIRQ | 27 | 31 | Input or Output | Serialized Interrupt Request Signal. If the SERIRQ function is enabled, this pin should be connected to the CPU SERIRQ input, and the line pulled to the 3V power supply pin through a resistor. If this pin is unused, it should be tied to the 3V power supply pin through a resistor. |
| SB3V | 5 | 3 | Input | Standby 3.3V Supply. If no separate standby power supply is connected to this pin, the pin should be tied directly to the 3V power supply pin. |
| 3V | 10, 19, 24 | 8, 23, 28 | Input | Primary 3.3V DC power supply input rail supplied by the motherboard. May be referred to as Vcc. |
| GND | 4, 11, 18, 25 | 2, 9, 22, 29 | Input | System ground. |
| NC | 1 | 39 | Output | No connect. This pin may be floated. If the XOR chain I/O test mode is used, the pin should be tied to ground directly or through a resistor. Reserved for the SMBus Data I/O function. |
| NC | 2 | 40 | Output | No connect. This pin may be floated. If the XOR chain I/O test mode is used, the pin should be tied to ground directly or through a resistor. Reserved for the SMBus Clock Input function. |
| VNC | 3 | 1 | Output | Vendor No Connect, as designated in the PC Client TIS specification. This pin may be floated. If the XOR chain I/O test mode is used, the pin should be tied to ground directly or through a resistor. |
| GPIO6 | 6 | 4 | Input or Output | General Purpose Input/Output. Internal Pull-up Resistor. This pin is mapped to NV Index TPM_NV_INDEX_GPIO_00 and serves as the GPIO-Express-00. Default TPM configuration: GPIO Input. GPIO6 also serves as the XOR chain Output during I/O test mode. |
| NC | 7 | 5 | Input | No Connect. This input pin has an internal pull-down resistor and may be floated. If the XOR chain I/O test mode is used, the pin should be tied to the 3V power supply directly or through a resistor. |
| TestI | 8 | 6 | Output | TPM manufacturing test input disabled. This pin may be floated. If the XOR chain I/O test mode is used, the pin should be tied directly to ground. |
| TestBI/BADD | 9 | 7 | Input | TestBI and BADD functions disabled. This pin should be tied directly to ground. |



Table 1. Pin Descriptions (Continued)

| Name | TSSOP Pin # | QFN Pin # | Type | Description |
|--------------|-------------|-----------|--------|--|
| VBAT | 12 | 10 | Input | 3.3V Battery Input. If no external battery is connected to this pin, the pin should be tied directly to the 3V power supply pin. |
| Xtall/32K in | 13 | 12 | Input | 32 kHz Crystal Oscillator Input or 32 kHz Clock Input. This pin should be tied to ground if not used. |
| XtalO | 14 | 13 | Output | 32 kHz Crystal Oscillator Output. |

Absolute Maximum Ratings (Preliminary)

| | |
|--|-------------------------------|
| Operating Temperature..... | 0°C to +70°C |
| Storage Temperature (without Bias)..... | 0°C to + 70°C |
| Voltage on I/O Pins..... | -0.1 to V _{CC} +0.3V |
| Voltage on VCC with Respect to Ground..... | 6.0V |
| Maximum ESD Voltage..... | 2000V |

***NOTICE:** Stresses beyond those listed under “Absolute Maximum Ratings” may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of this specification may cause temporary or permanent failure. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

Table 2. DC Parameters (Preliminary)

VCC = 3.0 to 3.6V; Temperature = 0 to 70°C

| Symbol | Parameter | Min | Nom | Max | Units | Notes |
|--------|------------------------------------|-----------|------------|-----------|-------|--|
| Vcc | Supply Voltage | 3.0 | 3.3 | 3.6 | V | |
| Icc | Operating Current at fclk = 33 MHz | | 25 | 50 | mA | |
| IST | Static Current | | 5 | 10 | mA | Vcc =3.6V; fxtal = 0 Hz; active inputs |
| ISL | Sleep Current, Chip Idle | | 40 | 100 | µA | VCC = 3.6V; fxtal = 0 Hz |
| IBB | Battery Current | | 2 | 4 | µA | VCC = 0V; fxtal = 0 Hz |
| ILIO | Input Leakage | | 0.1 | 3 | µA | Vin = VCC or GND |
| VIH | Input High Threshold | 0.5 * Vcc | | 0.5 + Vcc | V | |
| VIL | Input Low Threshold | -0.5 | | 0.3 * Vcc | V | |
| VOH | Output High Voltage | 0.9 * Vcc | 0.98 * Vcc | | V | At IOU _T = -500 µA |
| VOL | Output Low Voltage | | | 0.1 * Vcc | V | V At IOU _T = 1.5 mA |
| IOLCR | Output Low Current, CLKRUN# | 7 | | | mA | At VOU _T = .615 * VCC |
| CI | Input Pin Capacitance | | 6 | | pF | Note 1 |

Notes: 1. These parameters guaranteed by design.

Table 3. AC Parameters

CI = 10pf.; VCC = 3.0 to 3.7V; Temperature = 0 to 70-C

| Symbol | Parameter | Min | Nom | Max | Units | Notes |
|----------|--------------------------------------|------|------|-----|-------|--|
| TVAL | CLK to Signal Valid Delay – LAD0-3 | 2 | 5 | 11 | nS | Measured at $V_{trise} = 0.285 * VCC$ and $V_{tfal} = 0.615 * VCC$. Measured from clk at $V_{test} = 0.4 * VCC$; Load = 200. |
| TON | Float to Active Delay | 2 | 4 | | nS | |
| TOFF | Active to Float Delay | | | 28 | nS | |
| TSU | Input Setup Time to CLK | 7 | 2 | | nS | |
| TH | Input Hold Time from CLK | 0 | -500 | | nS | |
| TRST | Reset Active Time After Power Stable | 1 | | | mS | Note 1 |
| TRST-CLK | Reset Active After CLK Stable | 100 | | | mS | Note 1 |
| TRST-OFF | Reset Active to Output Float Delay | | | 40 | nS | Note 1 |
| TCLKIN | CLK Period | 29.5 | 30 | 31 | nS | Note 3 |
| TCLKLO | CLK Low Duration | 13.4 | | 18 | nS | Note 2, Note 3 |
| TCLKHI | CLK High Duration | 13.4 | | 18 | nS | Note 2, Note 3 |

- Notes:
1. These parameters guaranteed by design.
 2. All parameters measured with respect to signal crossing $V_{test} = 0.4 * VCC$ unless otherwise noted.
 3. The minimum parameter must never be violated under any circumstances unless $L_{reset\#}$ is asserted. If proper $CLK_{RUN\#}$ signaling is observed, the maximum specification can be violated.

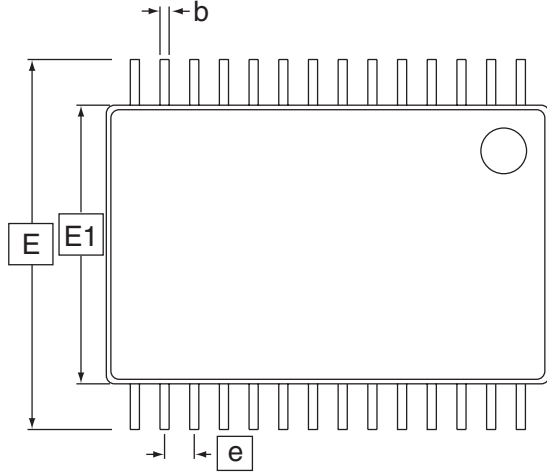
Table 4. Ordering Information

| Ordering Code ⁽¹⁾ | Package | | Operation Range |
|------------------------------|--------------|--------------------------|--------------------------|
| AT97SC3203-01AC | 28A3 (TSSOP) | | Commercial (0° to 70° C) |
| AT97SC3203-X1AC | 28A3 (TSSOP) | Lead-free ⁽²⁾ | Commercial (0° to 70° C) |
| AT97SC3203-01MC | 40ML1 (QFN) | | Commercial (0° to 70° C) |
| AT97SC3203-X1MC | 40ML1 (QFN) | Lead-free ⁽²⁾ | Commercial (0° to 70° C) |

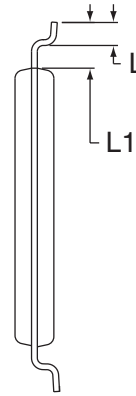
- Notes:
1. Current as of publication date. Contact Atmel marketing for status update.
 2. Also RoHS

Package Drawing

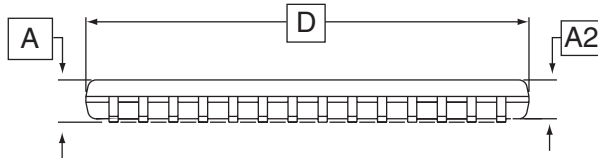
28A3 – TSSOP



Top View



End View



Side View

COMMON DIMENSIONS (Unit of Measure = mm)

| SYMBOL | MIN | NOM | MAX | NOTE |
|--------|----------|------|------|------|
| D | 9.60 | 9.70 | 9.80 | 2, 5 |
| E | 8.10 BSC | | | |
| E1 | 6.00 | 6.10 | 6.20 | 3, 5 |
| A | – | – | 1.20 | |
| A2 | 0.80 | 1.00 | 1.05 | |
| b | 0.19 | – | 0.30 | 4 |
| e | 0.65 BSC | | | |
| L | 0.45 | 0.60 | 0.75 | |
| L1 | 1.00 REF | | | |

- Notes:
1. This drawing is for general information only. Please refer to JEDEC Drawing MO-153, Variation DB for additional information.
 2. Dimension D does not include mold Flash, protrusions or gate burrs. Mold Flash, protrusions and gate burrs shall not exceed 0.15 mm (0.006 in) per side.
 3. Dimension E1 does not include inter-lead Flash or protrusions. Inter-lead Flash and protrusions shall not exceed 0.25 mm (0.010 in) per side.
 4. Dimension b does not include Dambar protrusion. Allowable Dambar protrusion shall be 0.08 mm total in excess of the b dimension at maximum material condition. Dambar cannot be located on the lower radius of the foot. Minimum space between protrusion and adjacent lead is 0.07 mm.
 5. Dimension D and E1 to be determined at Datum Plane H.

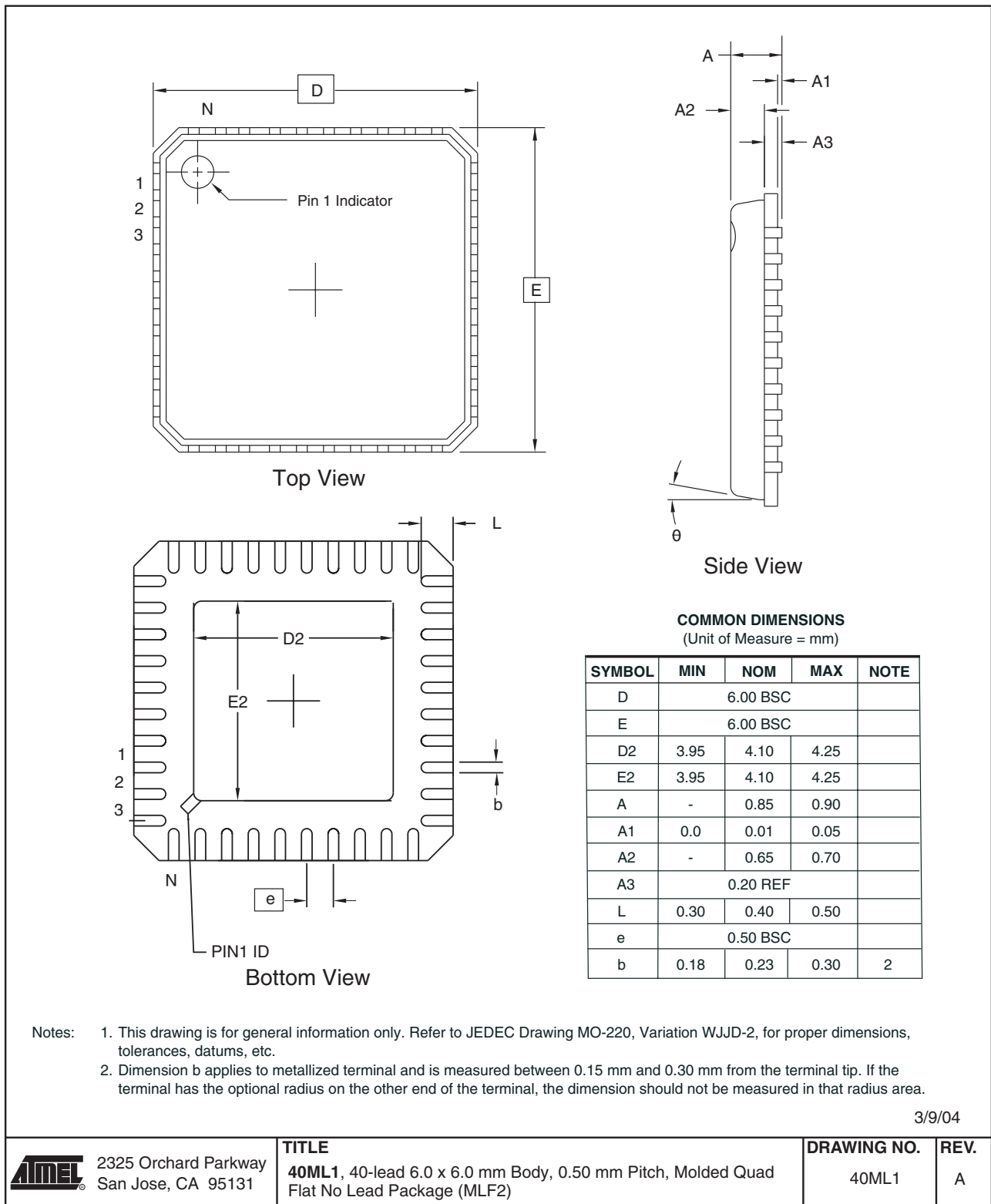
1/8/02

2325 Orchard Parkway
San Jose, CA 95131

TITLE
28A3, 28-lead, 6.1 x 9.7 mm Body, 0.65 pitch,
Thin Shrink Small Outline Package (TSSOP)

DRAWING NO. 28A3
REV. A

40ML1 – QFN





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 Arsenalux 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

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.

© Atmel Corporation 2005. **All rights reserved.** Atmel®, logo and combinations thereof, Everywhere You Are®, AVR®, 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.

5116AS-TPM-7/05