1. Features

- **Full Trusted Computing Group (TCG) Trusted Platform Module (TPM) Version 1.2 Compatibility**
- **Compliant with TCG PC Client Specific TPM Interface Specification Version 1.2**
- **Single-chip Turnkey Solution**
- **Hardware Asymmetric Crypto Engine**
- **2048-bit RSA® Sign in 500 ms**
- **AVR® RISC Microprocessor**
- **Internal EEPROM Storage for RSA Keys**
- **33 MHz LPC (Low Pin Count) Bus for Easy PC Interface**
- **Secure Hardware and Firmware Design and Chip Layout**
- **True Random Number Generator (RNG) – FIPS 140-2 Compliant**
- **NV Storage space for 1280 bytes of user defined data**
- **3.3V Supply Voltage**
- **28-lead TSSOP Package or 40-lead QFN Package**
- **0–70°C Temperature Range**

2. Description

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 (TCG) specification for Trusted Platform Modules(TPM).

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 50 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.

Figure 2-1. Pin Configurations

Pin Name	Description
V_{CC}	3.3V Supply Voltage
SB3V	Standby 3.3V Supply Voltage
V_{BAT}	2.5V - 4.0V Battery Input
GND	Ground
LRESET#	PCI Reset Input Active Low
LAD0	LPC Command, Address, Data Line Input/Output
LAD1	LPC Command, Address, Data Line Input/Output
LAD2	LPC Command, Address, Data Line Input/Output
LAD3	LPC Command, Address, Data Line Input/Output

Trusted Platform Module

AT97SC3203

LPC Interface

Summary

Note: See the full datasheet for detailed design information.

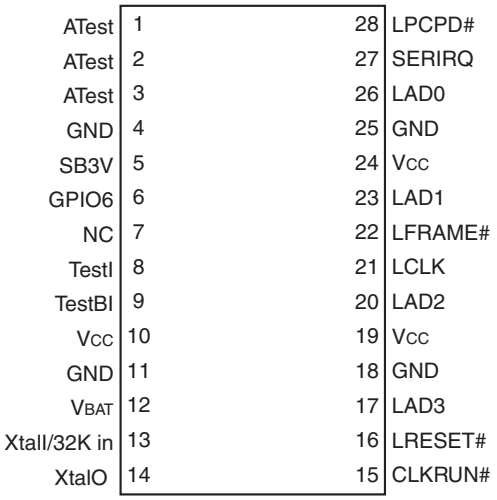
5116DS–TPM–1/08

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

Figure 2-1. Pin Configurations

Pin Name	Description
LCLK	33 MHz PCI Clock Input
LFRAME#	LPC Frame Input
CLKRUN#	PCI Clock Run Input/Output
LPCPD#	LPC Power Down Input
SERIQ	Serialized Interrupt Request Input/Output
Xtall/32K in	32.768 kHz Crystal Input
Xtal0	32.768 kHz Crystal Output
GPIO6	General Purpose Input/Output
TestI	Test Input (disabled)
TestBI	Test Input (disabled)
ATest	Atmel Test Pin
NC	No Connect
NBO	Not Bonded Out

28-pin TSSOP
6.1 mm x 9.7 mm Body
0.65 mm Pitch



40-pin QFN
6.0 mm x 6.0 mm Body
0.50 mm Pitch

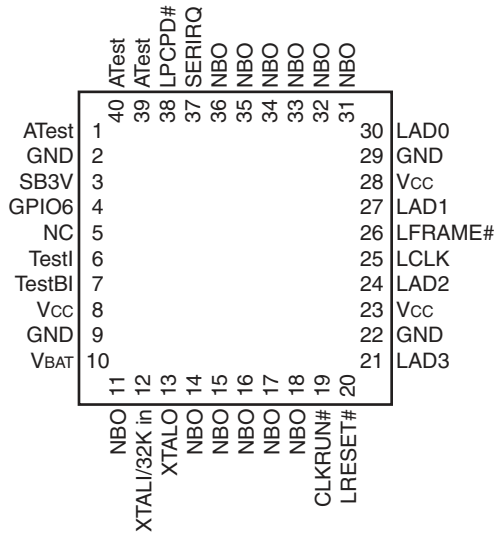
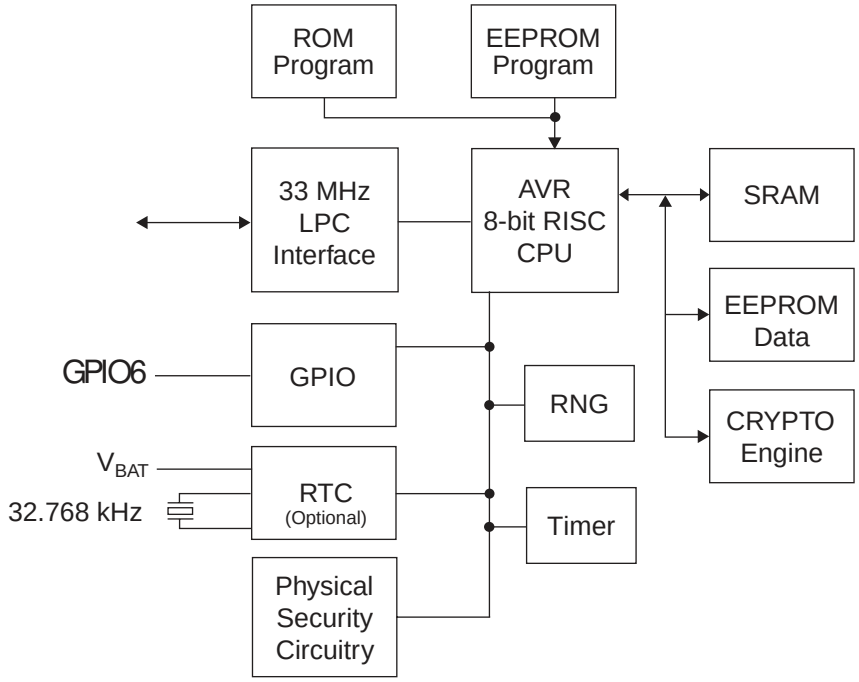


Figure 2-2. AT97SC3203 Block Diagram



2. Description (continued)

The TPM includes a hardware random number generator, including a FIPS-approved Pseudo Random Number Generator, that is used for key generation and TCG protocol functions. The RNG is also available to the system to generate random numbers that may be needed during normal operation.

The chip uses a dynamic internal memory management scheme to store multiple RSA keys. Other than the standard TCG commands (TPM_FlushSpecific, TPM_Loadkey2), no system intervention is required to manage this internal key cache.

The TPM is offered to OEM and ODM manufacturers as a turnkey solution, including the firmware integrated on the chip. In addition, Atmel provides the necessary device driver software for integration into certain operating systems, along with BIOS drivers. Atmel will also provide manufacturing support software for use by OEMs and ODMs during initialization and verification of the TPM during board assembly.

Full documentation for TCG primitives can be found in the TCG TPM Main Specification, Parts 1 – 3, on the TCG Web site located at https://www.trustedcomputinggroup.org/. TPM features specific to PC Client platforms are specified in the “TCG PC Client Specific TPM Interface Specification, Version 1.2”, also available on the TCG web site. Implementation guidance for 32-bit PC platforms is outlined in the “TCG PC Client Specific Implementation Specification for Conventional BIOS for TCG Version 1.2”, also available on the TCG web site.

3. Ordering Information

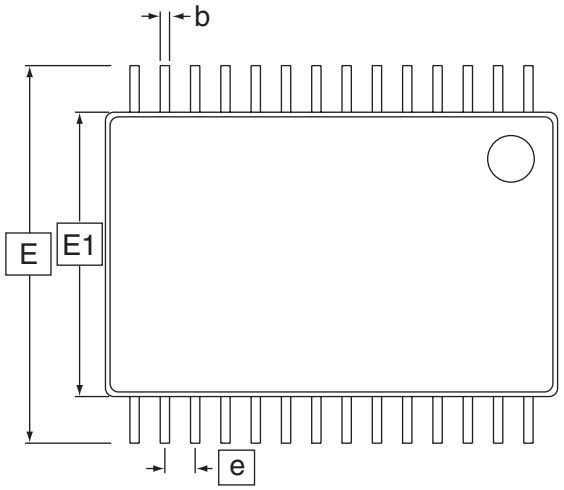
Table 3-1. Ordering Information

Ordering Code	Package		Operation Range
AT97SC3203[1]	28A3 (28-pin TSSOP)	Lead-free, RoHS	Commercial (0°C to 70°C)
AT97SC3203[1]	40ML1 (40-pin QFN)	Lead-free, RoHS	Commercial (0°C to 70°C)

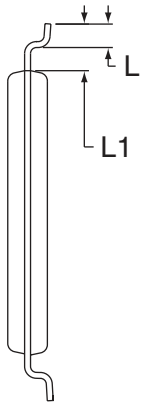
Note: 1. Please see the AT97SC3203 datasheet addendum for the complete catalog number ordering code.

4. Package Drawing

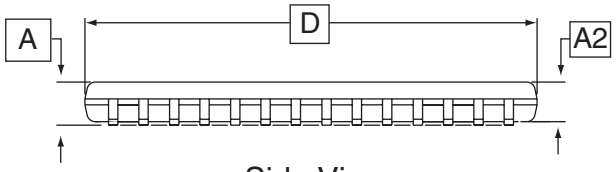
28A3 - TSSOP



Top View



End View



Side View

COMMON DIMENSIONS
(Unit of Measure = mm)

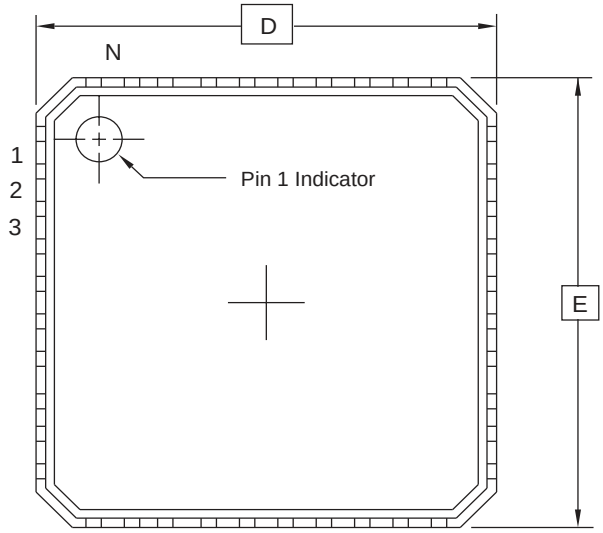
SYMBOL	MIN	NOM	MAX	NOTE
D	9.60	9.70	9.80	2, 5
E		8.10 BSC		
E1	6.00	6.10	6.20	3, 5
A	–	–	1.20	
A2	0.80	1.00	1.05	
b	0.19	–	0.30	4
e		0.65 BSC		
L	0.45	0.60	0.75	
L1		1.00 REF		

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.

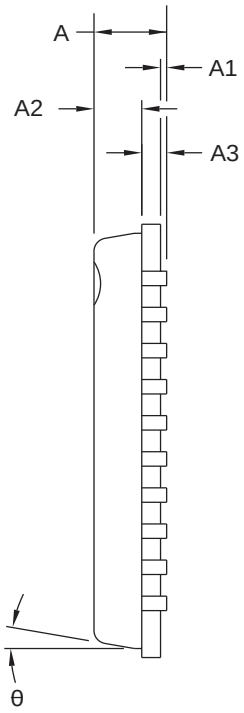
1/8/02

	TITLE	DRAWING NO.	REV.
2325 Orchard Parkway San Jose, CA 95131	**28A3**, 28-lead, 6.1 x 9.7 mm Body, 0.65 pitch, Thin Shrink Small Outline Package (TSSOP)	28A3	A

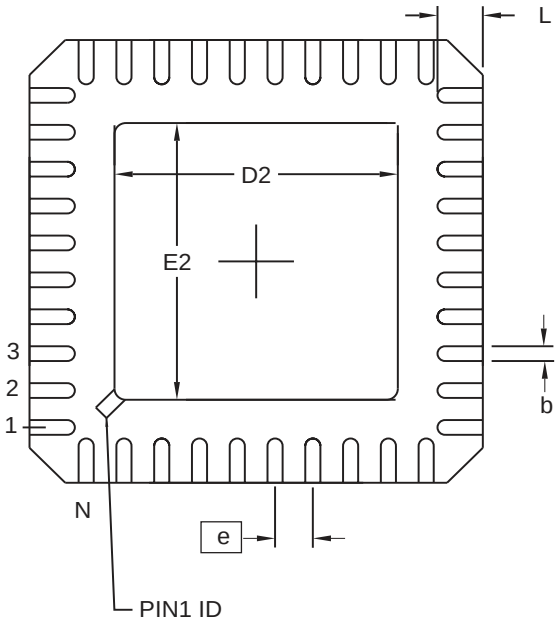
40ML1 - QFN



Top View



Side View



Bottom View

COMMON DIMENSIONS
(Unit of Measure = mm)

SYMBOL	MIN	NOM	MAX	NOTE
D		6.00 BSC		
E		6.00 BSC		
D2	3.95	4.10	4.25	
E2	3.95	4.10	4.25	
A	-	0.85	0.90	
A1	0.0	0.01	0.05	
A2	-	0.65	0.70	
A3		0.20 REF		
L	0.30	0.40	0.50	
e		0.50 BSC		
b	0.18	0.23	0.30	2

Notes:
1. This drawing is for general information only. Refer to JEDEC Drawing MO-220, Variation WJJD-2, for proper dimensions, tolerances, datums, etc.
2. Dimension b applies to metallized terminal and is measured between 0.15 mm and 0.30 mm from the terminal tip. If the terminal has the optional radius on the other end of the terminal, the dimension should not be measured in that radius area.

9/27/07

	TITLE	DRAWING NO.	REV.
2325 Orchard Parkway San Jose, CA 95131	**40ML1**, 40-lead 6.0 x 6.0 mm Body, 0.50 mm Pitch, Molded Quad Flat No Lead Package (QFN) Punched	40ML1	C

Revision History

Doc. Rev.	Date	Comments
5116DS	1/2008	Implemented revision history.

Headquarters

Atmel Corporation
2325 Orchard Parkway
San Jose, CA 95131
USA
Tel: 1(408) 441-0311
Fax: 1(408) 487-2600

International

Atmel Asia
Room 1219
Chinachem Golden Plaza
77 Mody Road Tsimshatsui
East Kowloon
Hong Kong
Tel: (852) 2721-9778
Fax: (852) 2722-1369

Atmel Europe
Le Krebs
8, Rue Jean-Pierre Timbaud
BP 309
78054 Saint-Quentin-en-
Yvelines Cedex
France
Tel: (33) 1-30-60-70-00
Fax: (33) 1-30-60-71-11

Atmel 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

Product Contact

Web Site
www.atmel.com

Technical Support
pcsecurity@atmel.com

Sales Contact
www.atmel.com/contacts

Literature Requests
www.atmel.com/literature