Trusted Platform Module

Atmel AT97SC3204 LPC Interface

Summary

* See the full data sheet for detailed design information

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 200ms
- AVR® RISC Microprocessor
- Internal EEPROM Storage for RSA Keys
- 33MHz 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 Thin TSSOP, Wide TSSOP or 40-lead QFN Packages
- Offered in both Commercial (0 to 70°C) and Industrial (-40 to +85°C) Temperature Ranges

2. Description

The Atmel® AT97SC3204 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 200ms and a 1024-bit RSA signature in 40ms. Performance of the SHA-1 accelerator is 20µs per 64-byte block.

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.

5294BS–TPM–9/10

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

Table 1-1. Pin Configurations

Pin Name	Function
V_{CC}	3.3V Supply Voltage
SB3V	Standby 3.3V Supply Voltage
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
LCLK	33MHz PCI Clock Input
LFRAME#	LPC FRAME Input
CLKRUN#	PCI Clock Run Input/Output
LPCPD#	LPC Power Down Input
SERIQ	Serialized Interrupt Request Input/Output
GPIO6	General Purpose Input/Output
TestI	Test Input (disabled)
TestBI	Test Input (disabled)
ATest	Atmel Test Pin
NC	No Connect
NBO	Not Bounded out

Figure 2-1. Pinout Diagrams

28-pin Thin TSSOP
4.4 mm x 9.7 mm Body
0.65 mm Pitch

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

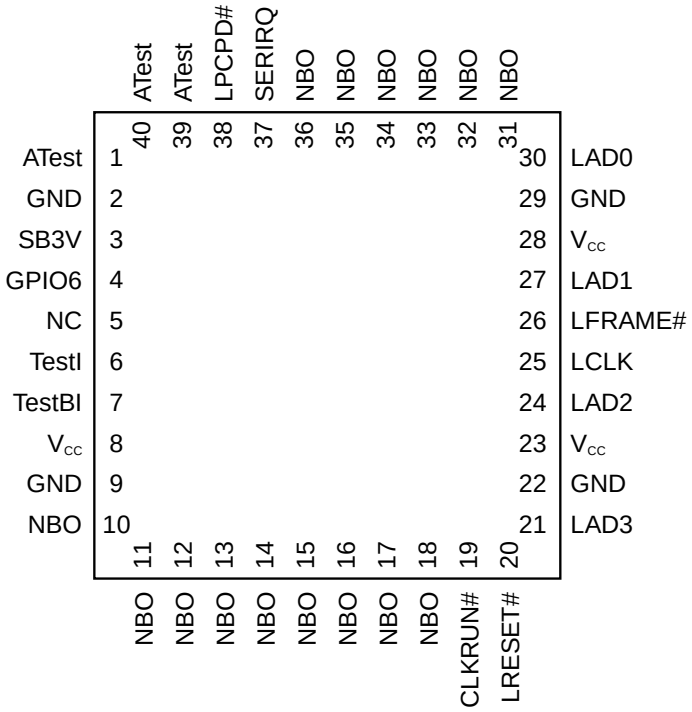
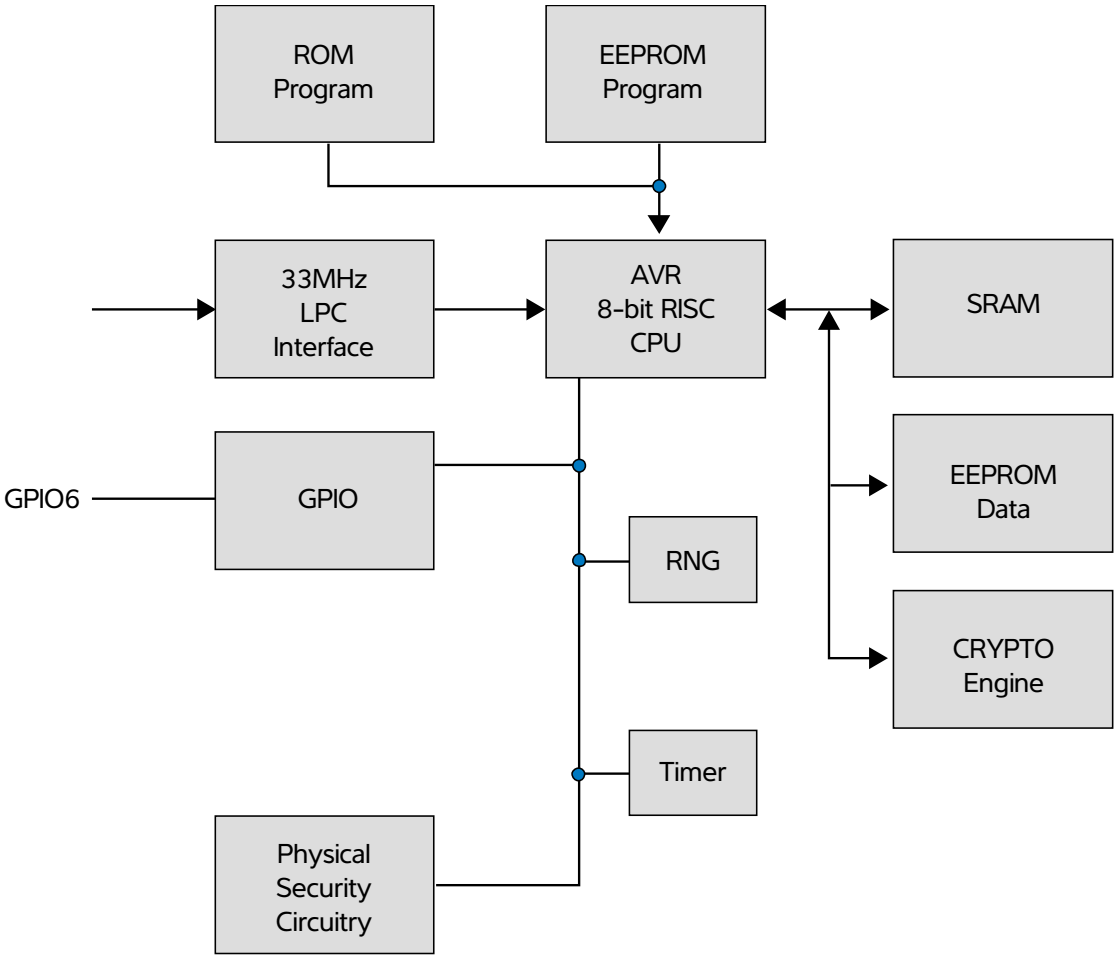


Figure 2-2. Atmel AT97SC3204 Block Diagram



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 to 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

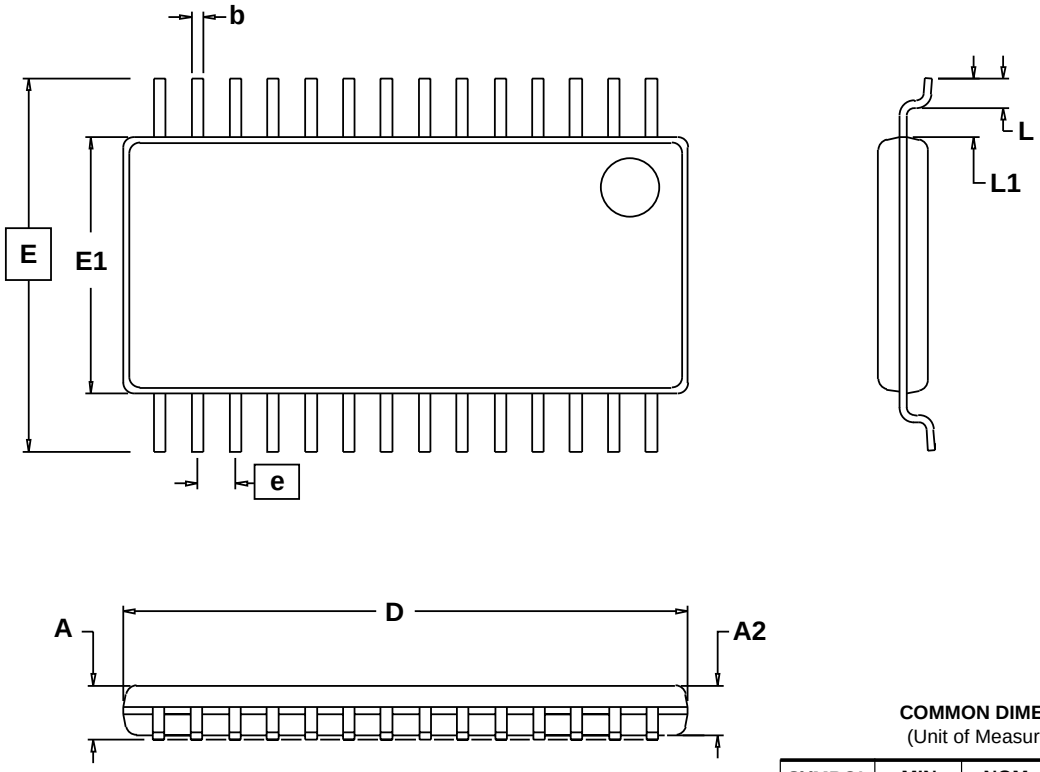
Table 1-2. Atmel AT24C256C Ordering Information

Atmel Ordering Code	Package		Operating Range
AT97SC3204[1]	28A2 (28-pin Thin TSSOP)	Lead-free, RoHS	Commercial (0°C to 70°C) Industrial (-40°C to 85°C)
AT97SC3204[1]	28A3 (28-pin TSSOP)	Lead-free, RoHS	Commercial (0°C to 70°C) Industrial (-40°C to 85°C)
AT97SC3204[1]	40ML1 (40-pin QFN) [2]	Lead-free, RoHS	Commercial (0°C to 70°C) Industrial (-40°C to 85°C)

Notes: 1. Please see the Atmel AT97SC3204 datasheet addendum for the complete catalog number ordering code

4. Package Drawing

28A2 – Thin TSSOP



1. Dimension "D" does not include mold flash, protrusions or gate burrs. Mold flash, protrusions and gate burrs shall not exceed .15mm (.006 in) per side.
2. Dimension "E1" does not include inter-lead flash or protrusions. Inter-lead flash and protrusions shall not exceed .25mm (.010 in) per side.
3. 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.
4. Dimension 'D' and 'E1' to be determined at Datum Plane H.

COMMON DIMENSIONS
(Unit of Measure = mm)

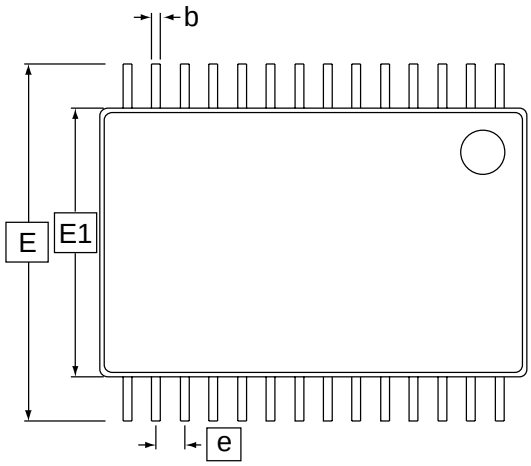
SYMBOL	MIN	NOM	MAX	NOTE
D	9.60	9.70	9.80	1,4
E		6.40 BSC		
E1	4.30	4.40	4.50	2,4
A			1.20	
A2	0.80	1.00	1.05	
b	0.19		0.30	3
e		0.65 BSC		
L	0.45	0.60	0.75	
L1		1.00 REF		

This drawing is for general information only. Please refer to JEDEC Drawing MO-153, Variation AE for additional information.

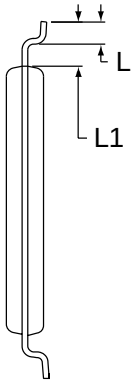
6/17/08

Package Drawing Contact: packagedrawings@atmel.com	TITLE	GPC	DRAWING NO.	REV.
	28A2, 28-lead, 4.4x9.7 mm Body, 0.65 pitch, Thin Shrink Small Outline Package (TSSOP)	TFL	28A2	B

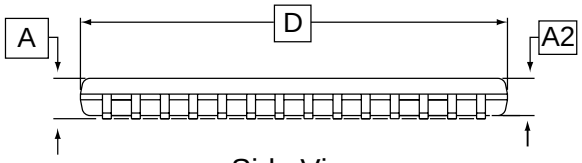
28A3 – TSSOP



Top View



End View



Side View

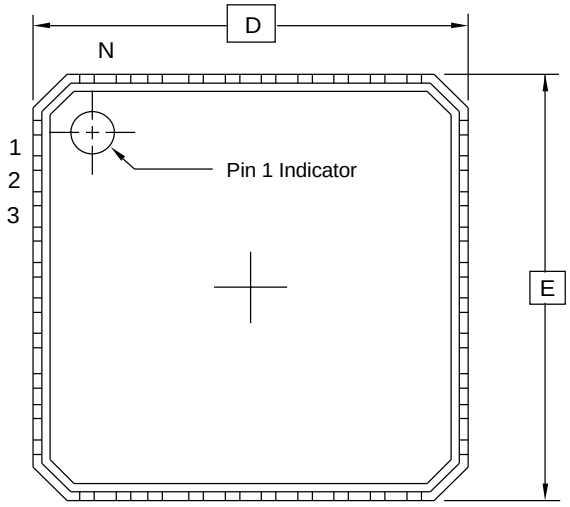
COMMON DIMENSIONS
(Unit of Measure = mm)

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		

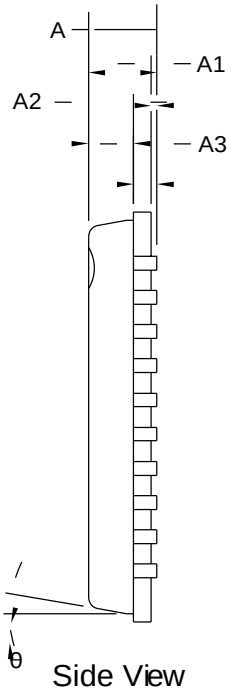
Note:
1. This drawing is for general information only. Please refer to JEDEC Drawing MO-153, Variation DB for additional information.
2. Dimension D does not include mold Flash, protrusions or gate burrs. Mold Flash, protrusions and gate burrs shall not exceed 0.15 mm (0.006 in) per side.
3. Dimension 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

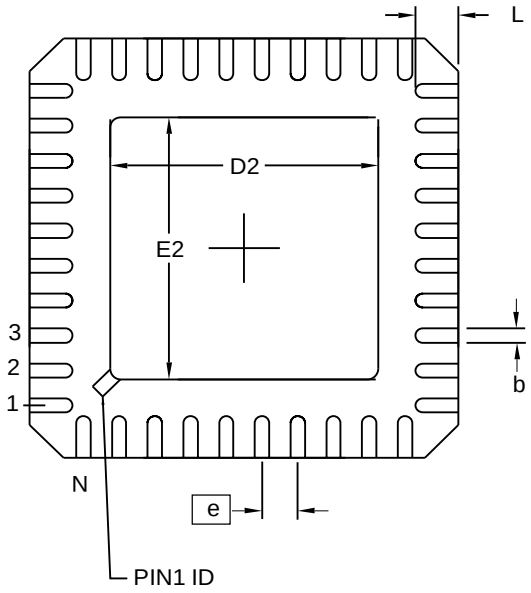
	TITLE	DRAWING NO.	REV.
2325 Orchard Parkway San Jose, CA 95131	28A3, 28-lead, 6.1 x 9.7 mm Body, 0.65 pitch, Thin Shrink Small Outline Package (TSSOP)	28A3	A



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

Note: 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

5. Revision History

Doc. Rev.	Date	Comments
5294BS	10/2010	Added Industrial Grade support detail
5294AS	01/2008	Initial document release

Product Contact

Product Line
pcsecurity@atmel.com

Sales Contact
www.atmel.com/contacts

Literature Requests
www.atmel.com/literature

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

Atmel Asia Limited
Unit 01-5 & 16, 19F
BEA Tower, Millennium City 5
418 Kwun Tong Road
Kwun Tong, Kowloon
HONG KONG
Tel: (+852) 2245-6100
Fax: (+852) 2722-1369

Atmel Munich GmbH
Business Campus
Parkring 4
D-85748 Garching b. Munich
GERMANY
Tel: (+49) 89-31970-0
Fax: (+49) 89-3194621

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

© 2010 Atmel Corporation. All rights reserved. / Rev.: **5294BS–TPM–10/10**

Atmel®, logo and combinations thereof, CryptoAuthentication™ and others are registered trademarks or trademarks of Atmel Corporation or its subsidiaries. Other terms and product names may be trademarks of others.

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 THE ATMEL TERMS AND CONDITIONS OF SALES LOCATED ON THE ATMEL WEBSITE, 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 AND 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 products 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 products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.