Features

- **Full Trusted Computing Group (TCG) Trusted Platform Module (TPM) Version 1.2 Compatibility**
- **Single-chip Turnkey Solution**
- **Hardware Asymmetric Crypto Engine**
- **2048-bit RSA Sign in 500 ms**
- **AVR® RISC Microprocessor**
- **Internal EEPROM Storage for RSA Keys**
- **100 kHz System Management Bus (SMBus™) Two-wire 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 ±10% Supply Voltage**
- **28-lead TSSOP Package or 40-lead QFN Package**
- **0–70°C Temperature Range**

Description

The AT97SC3203S is a fully integrated security module designed to be integrated into 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.

Table 1. Pin Configurations

Pin Name	Description
V_{CC}	3.3V (±10%) Supply Voltage
SB3V	Standby 3.3V (± 10%) Supply Voltage
V_{BAT}	2.5–4.0V Battery Input
GND	Ground
RESET#	Reset Input Active Low
SMBDAT	SMBus Data Input/Output
SMBCLK	SMBus Clock Input
AVRCLK	33-MHz AVR Clock Input
Xtall/32K in	32.768 kHz Crystal Input
XtalO	32.768 kHz Crystal Output
GPIO6	General Purpose Input/Output
TestI	Test Input (disabled)
TestBI	Test Input (disabled)
NC	No Connect
NBO	Not Bonded Out

Trusted Platform Module

AT97SC3203S

SMBus Two-Wire Interface

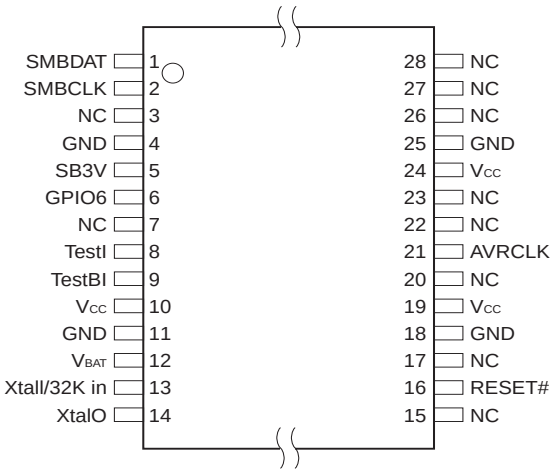
Summary

5132AS–TPM–1/07

Note: This is a summary document. A complete document is available through your local Atmel sales office.

Figure 1. Pin Configurations

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

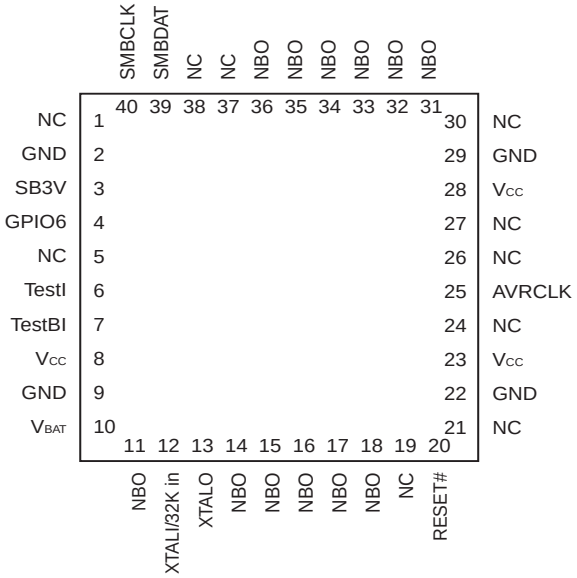
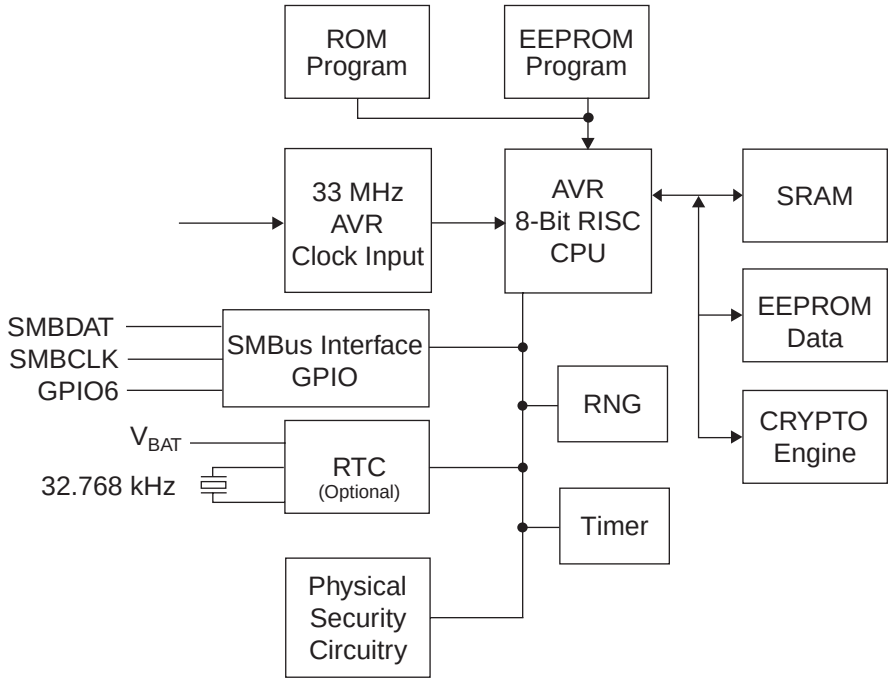


Figure 2. AT97SC3203S Block Diagram



Description (continued)

Communication to and from the TPM occurs through a modified 100-kHz SMBus two-wire interface. 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.

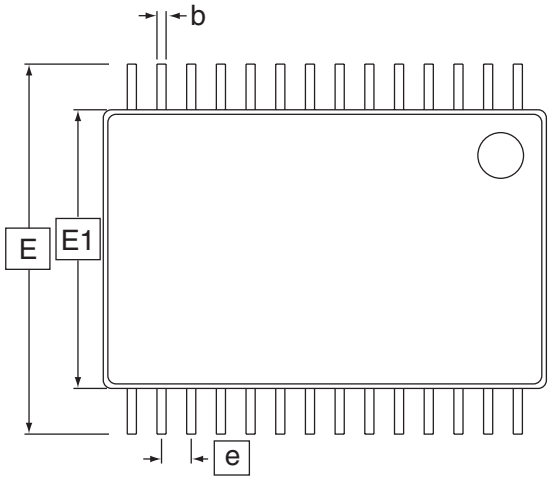
Full documentation for TCG primitives can be found on the TCG Web site located at www.trustedcomputinggroup.org. This specification includes only mechanical, electrical and SMBus protocol information

Table 2. Ordering Information

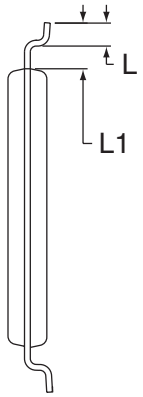
Ordering Code	Package		Operation Range
AT97SC3203S-X5A40	28A3 (28-pin TSSOP)	lead-free, RoHS	Commercial (0° to 70° C)
AT97SC3203S-X5M40	40ML1 (40-pin QFN)	lead-free, RoHS	Commercial (0° to 70° C)

Package Drawing

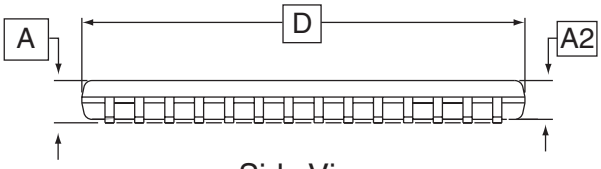
28A3 – TSSOP



Top View



End View



Side View

COMMON DIMENSIONS
(Unit of Measure = mm)

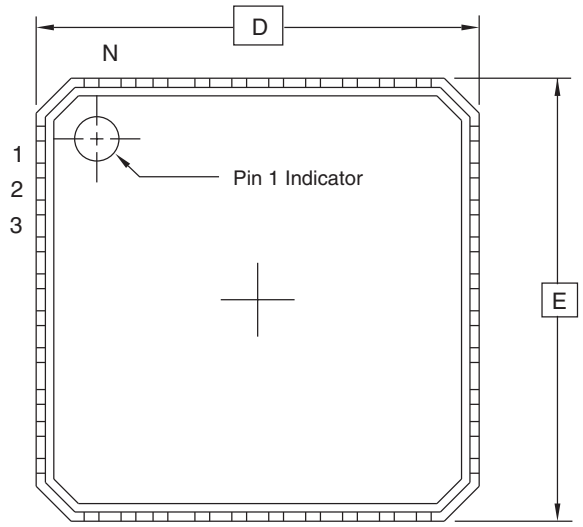
SYMBOL	MIN	NOM	MAX	NOTE
D	9.60	9.70	9.80	2, 5
E		8.10 BSC		
E1	6.00	6.10	6.20	3, 5
A	–	–	1.20	
A2	0.80	1.00	1.05	
b	0.19	–	0.30	4
e		0.65 BSC		
L	0.45	0.60	0.75	
L1		1.00 REF		

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.

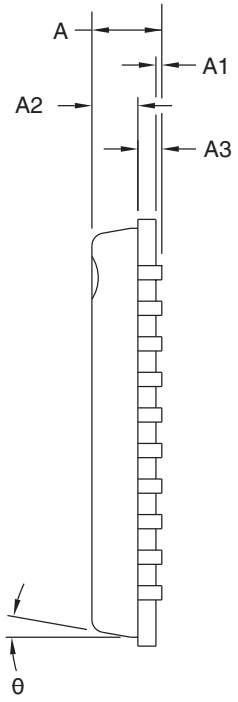
1/8/02

	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

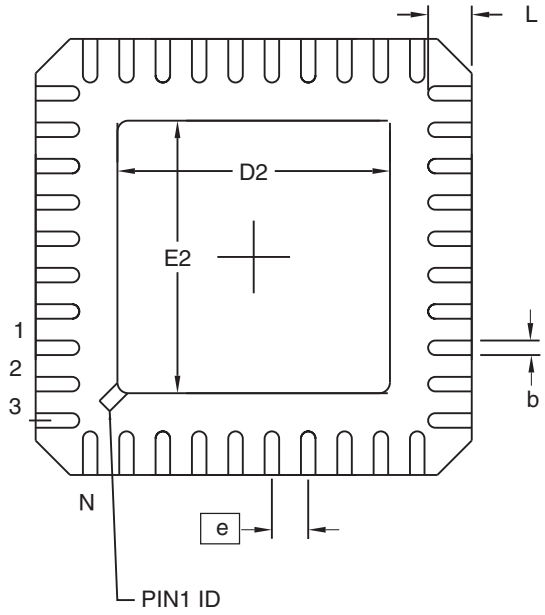
40ML1 - QFN



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.

3/9/04

	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 (MLF2)	40ML1	A

Revision History

Doc. Rev.	Date	Comments
5132AS	1/2007	Implemented revision history Added ‘Summary’ to page 1 Revised summary disclaimer text on page 1

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 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 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
Avenue de Rochepleine
BP 123
38521 Saint-Egreve Cedex, France
Tel: (33) 4-76-58-47-50
Fax: (33) 4-76-58-47-60

Literature Requests
www.atmel.com/literature

5132AS–TPM–1/07