AT97SC3205T

Trusted Platform Module
I²C Interface

SUMMARY DATASHEET

Features

- Compliant to the Trusted Computing Group (TCG) Trusted Platform Module (TPM) Version 1.2 Specification
- Single-chip Turnkey Solution
- Hardware Asymmetric Crypto Engine
- Atmel AVR® RISC Microprocessor
- Internal EEPROM Storage for RSA Keys
- 400kHz Fast Mode/100kHz Standard Mode I²C Operation
- Secure Hardware and Firmware Design and Device Layout
- FIPS-140-2 Module Certified Including the High-quality Random Number Generator (RNG), HMAC, AES, SHA, and RSA Engines
- NV Storage Space for 2066 bytes of User Defined Data
- 3.3V Supply Voltage
- 28-lead Thin TSSOP or 32-pad QFN Packages
- Offered in Commercial (0°C to 70°C) and Industrial (-40 to +85°C) Temperature Range

Description

Atmel AT97SC3205T 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).

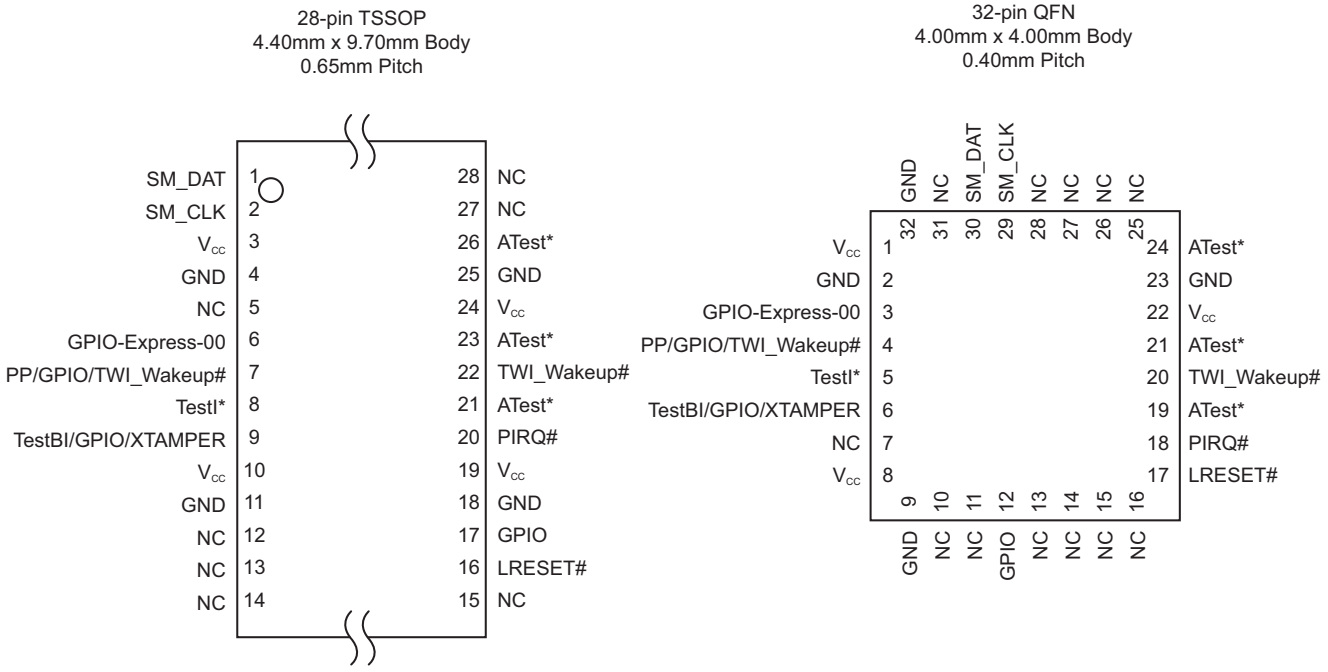
This is a summary document. The complete document is available under NDA. For more information, please contact your local Atmel sales office.

1. Pin Configuration and Pinouts

Table 1-1. Pin Configurations

Pin Name	Description
V_{CC}	3.3V Supply Voltage
GND	Ground
LRESET#	Reset Input Active Low
SM_DAT	Serial Data Input/Output
SM_CLK	Serial Clock Input
GPIO	General Purpose Input/Output
GPIO-Express-00	GPIO Assigned to TPM_NV_INDEX_GPIO_00
PP/GPIO	Hardware Physical Presence or GPIO Pin
TestI	Test Input (Disabled)
TestBI/GPIO/XTAMPER	Test Input (Disabled) / XTAMPER / GPIO Pin
TWI_Wakeup#	Low-Power Sleep Recovery (Active Low)
PIRQ#	SPI Interrupt Requests
ATest	Atmel Test Pin
NC	No Connect

Figure 1-1. Pinout Diagrams



Note: * Used for Atmel internal testing only. Tie to V_{CC} or GND directly or through a 4.7KΩ resistor.

Table 1-2. Pin Descriptions

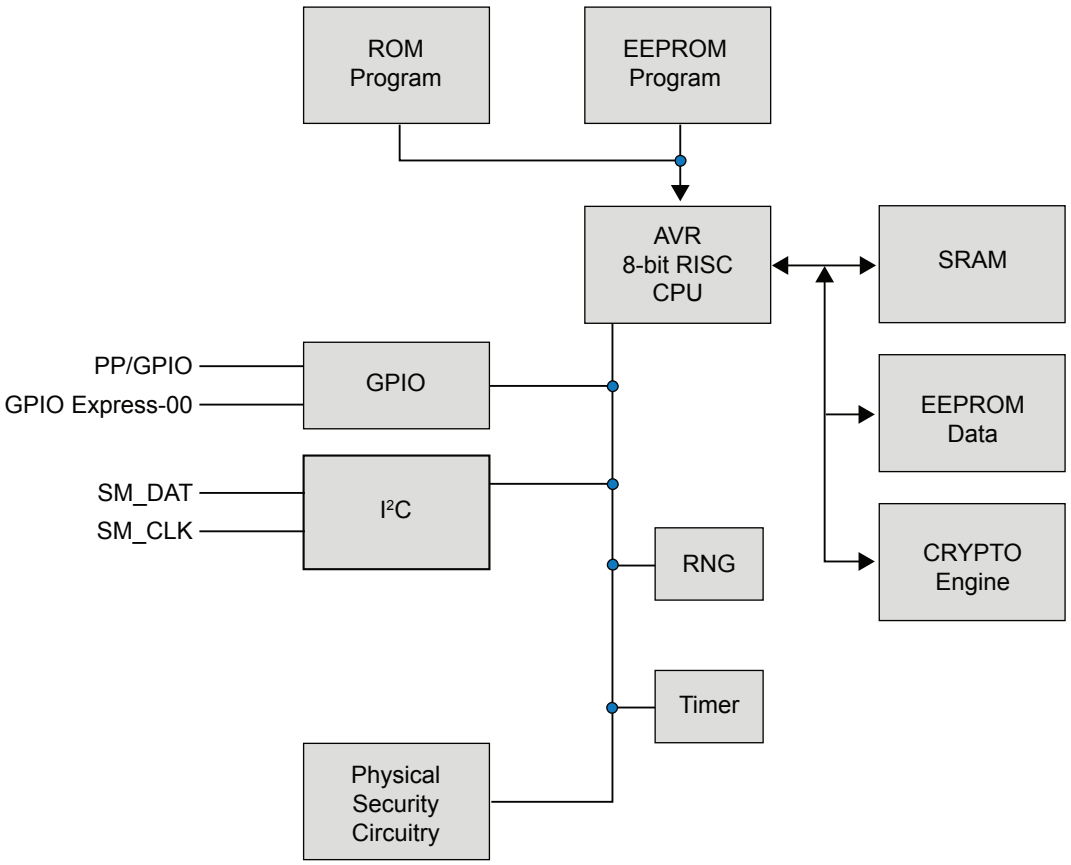
Pin	Description
V_{CC}	**Power Supply, 3.3V.** Care should be taken to prevent excessive noise. Effective decoupling of the V_{CC} inputs to the Atmel TPM is critical to assure consistently reliable operation over the lifetime of the system. The Atmel recommendation is for a decoupling bypass capacitor within the range of 2200pF to 4700pF to be placed as close as possible <5mm to each of the V_{CC} pins; located between each V_{CC} pin and the immediately adjacent GND pin. A 0.1µF decoupling bypass capacitor should be placed at the node in which these V_{CC} traces join as close as possible; <10mm to the TPM. In all cases, this bypass capacitor should be closer than the next closest component. All capacitors should be of high quality with dielectric ratings of X5R or X7R. A low-power state is automatically entered when the device is idle. No further action is required by the system to enter low-power mode.
GND	**System Ground.**
LRESET#	**Reset Active-Low.** Pulsing this signal low resets the internal state of the TPM and is equivalent to removal/restoration of power to the device. The required minimum reset pulse width is 2µs. On power-up, it is critical that Reset be kept active low until V_{CC} stabilizes.
SM_DAT	**I^2C Data Input/Output.** This pin serves as the Data Input/Output for the TPM. If one attempts to communicate over the interface at close to the rated speed of 400kHz, the size of the pull-ups on SM_DAT can be critical. A known value that functions properly at 400kHz is 800Ω on the SM_DAT line. One may experiment with different pull-up values and/or reduce the clock rate if desired.
SM_CLK	**I^2C Clock Input.** This pin serves as the Serial Clock Input to the TPM. If one attempts to communicate over the interface at close to the rated speed of 400kHz, the size of the pull-ups on SM_CLK can be critical. A known value that functions properly at 400kHz is 1.5KΩ on the SM_CLK line. One may experiment with different pull-up values and/or reduce the clock rate if desired. The TPM communication stability is increased the closer to a 50% duty cycle on the SM_CLK signal that can be provided. Although this becomes more critical at the rated speed of 400kHz, improvements from a 50% duty cycle can result at lower speeds as well.
GPIO	**General Purpose Input/Output.** If not used, tie high or low.
GPIO-Express-00	**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. GPIO-Express-00 also serves as the XOR chain Output during I/O test mode. Since GPIO-Express-00 has an internal pull-up it should be left floating if unused.
PP/GPIO	**General Purpose Input/Output.** Internal pull-down resistor. This pin is an indicator for hardware physical presence; active high. Default TPM configuration: GPIO input. Since PP/GPIO has an internal pull-down, it should be left floating if unused.
TestI	**Test Input.** TestI manufacturing test input disabled after manufacturing. Tie TestI to ground directly or through a 4.7KΩ resistor.
TestBI/GPIO/ XTAMPER	**Test Input.** The Atmel TPM does not support legacy addressing via the optional BADD implementation of this pin.The TestBI pin serves as the XTAMPER pin or an additional GPIO pin, active high. (See the application note, “Atmel Specific TPM Commands Reference Guide,” for details on XTAMPER implementation). If unused, this pin should be tied to ground directly or through a 4.7KΩ resistor.
TWI_Wakeup#	**Low-Power Sleep Recovery.** These two pins serve as the mechanism to allow the TPM to recover from its low-power sleep state after receiving the Atmel Specific command TPM_DeepSleep (See Atmel TPM Specific Commands document for further details). These pins must both be pulsed active low in order to recover from the low-power sleep state. If unused, pin 7 can be left floating or tied to GND either directly or through a 4.7KΩ resistor. Pin 22 should be tied to GND or V_{CC} either directly or through a 4.7KΩ resistor.

Table 1-2. Pin Descriptions (Continued)

Pin	Description
PIRQ#	**SPI Interrupt Requests.** If unused, this pin should be tied to ground directly or through a 4.7KΩ resistor.
ATest	**Atmel Test Pins.** Only utilized during manufacturing test. To optimize power savings and improve noise immunity, these ATest pins should be biased to V_{CC} or GND as follows: TSSOP Pin 21 / QFN Pin 19 TSSOP Pin 23 / QFN Pin 21 TSSOP Pin 26 / QFN Pin 24
NC	**No Connect Pins.** The AT97SC3205T TSSOP package has additional pins which are no connects and can be tied to GND, V_{CC}, or left floating at the customers discretion: NC – TSSOP Pin 5 NC – TSSOP Pin 12 NC – TSSOP Pin 13 NC – TSSOP Pin 14 NC – TSSOP Pin 15 NC – TSSOP Pin 27 NC – TSSOP Pin 28 The AT97SC3205T QFN package has additional pins which are no connects and can be tied to GND, V_{CC}, or left floating at the customers discretion: NC – QFN Pin 7 NC – QFN Pin 10 NC – QFN Pin 11 NC – QFN Pin 13 NC – QFN Pin 14 NC – QFN Pin 15 NC – QFN Pin 16 NC – QFN Pin 25 NC – QFN Pin 26 NC – QFN Pin 27 NC – QFN Pin 28 NC – QFN Pin 31

Note: 1. The substrate center pad for the 32-pin QFN is directly tied to GND internally; therefore, this pad can either be left floating or tied to GND.

2. Block Diagram



Communication to and from the TPM occurs through a 400kHz Fast mode/100kHz Standard mode. The TPM includes a hardware random number generator, including a FIPS certified Pseudo Random Number Generator which is used for key generation and TCG protocol functions. The RNG is also available to the system to generate random numbers which may be needed during normal operation.

The device 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 in the TCG TPM Main Specification, Parts 1 – 3, on the TCG Web site located at www.trustedcomputinggroup.org. This specification includes only mechanical, electrical and I^2C protocol information.

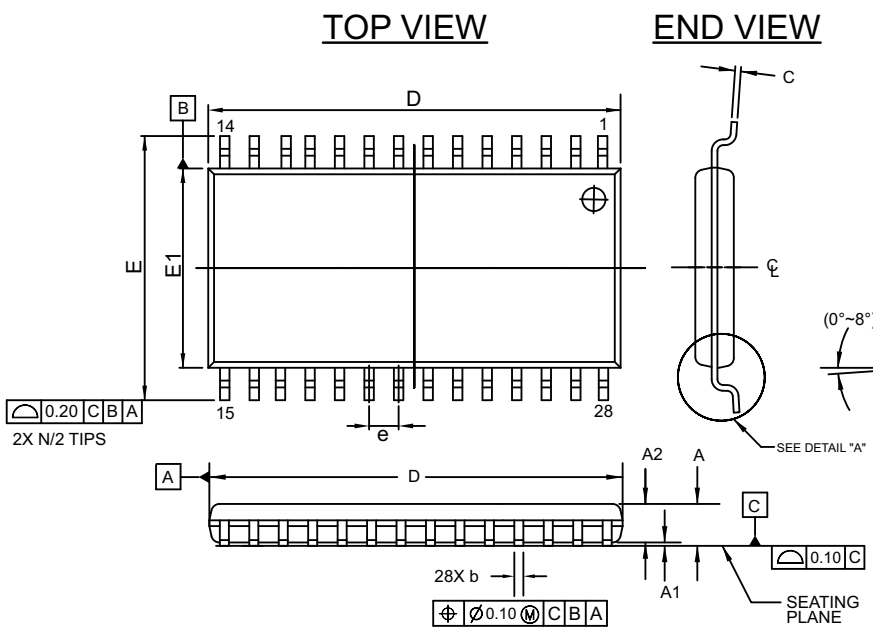
3. Ordering Information

Ordering Code	Package		Operational Range
AT97SC3205T[1]	28X1 (28-pin Thin TSSOP)	Lead-free, RoHS	Commercial (0°C to 70°C) Industrial (-40°C to 85°C)
AT97SC3205T[1]	32M3 (32-pin Very Thin QFN)		

Note: 1. Please see the AT97SC3205T datasheet addendum for the complete catalog number ordering code.

4. Package Drawings

4.1 28X1 — 28-lead Thin TSSOP



COMMON DIMENSIONS
(UNIT OF MEASURE=MM)

SYMBOL	MIN	NOM	MAX	NOTE
A	-	-	1.10	
A1	0.05	-	0.15	
A2	0.85	0.90	0.95	
b	0.19	-	0.30	2
c	0.09	-	0.20	
D	9.60	9.70	9.80	1
E	6.40BSC			
E1	4.30	4.40	4.50	1
e	0.65 BSC			
L	0.45	0.60	0.75	
R	0.09	-	-	
R1	0.09	-	-	
S	0.20	-	-	

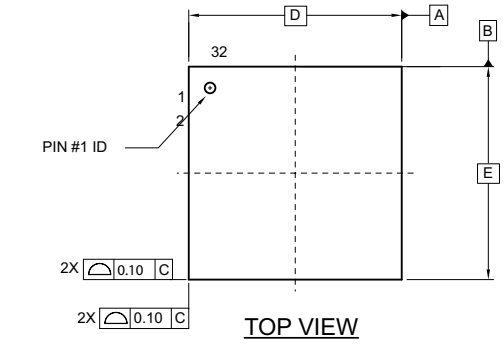
Note:

1. Refer to JEDEC drawing MO-153,variation AE
2. Dimension D does not include mold flash, protrusions or gate burrs. Mold flash,protrusions or gate burrs shall not exceed 0.15mm per end. Dimension E1 does not include interlead flash or protrusion. Interlead flash or protrusion shall not exceed 0.25mm per side.
3. Dimension "b" does not include dambar protrusion. Allowable dambar protrusion shall be 0.08mm total in excess of the "b" dimension at maximum material condition. Minimum space between protrusion and adjacent lead is 0.07mm.

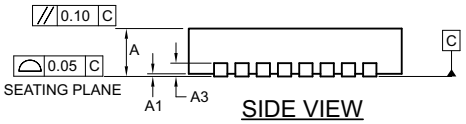
7/8/2011

Atmel Package Drawing Contact: packagedrawings@atmel.com	TITLE 28X1, 28-lead, 4.4mm Body Width, Plastic Thin Shrink Small Outline Package (TSSOP)	GPC TFL	DRAWING NO. 28X1	REV. A

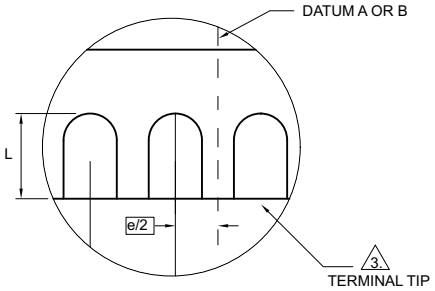
4.2 32M3 — 32-pad QFN



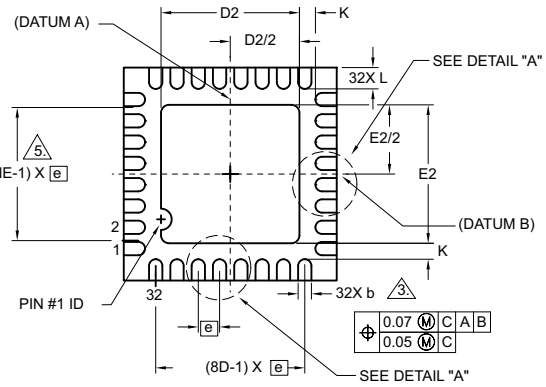
TOP VIEW



SIDE VIEW



DETAIL "A"



BOTTOM VIEW

COMMON DIMENSIONS
(Unit of Measure = mm)

SYMBOL	MIN	NOM	MAX	NOTE
A	0.80	0.85	0.90	
A1	0.00	0.02	0.05	
A3		0.20 REF		
D		4.0 BSC		
D2	2.50	2.60	2.70	
E		4.0 BSC		
E2	2.50	2.60	2.70	
b	0.15	0.20	0.25	
L	0.35	0.40	0.45	
K	0.20	–	-	
e		0.40 BSC		

NOTES :

1. DIMENSIONING AND TOLERANCING CONFORME TO ASME Y14.5M - 1994.
2. ALL DIMENSIONS ARE IN MILLIMETERS, 0 IS IN DEGREES.
3. DIMENSION b APPLIES TO METALLIZED TERMINAL AND IS MEASURED BETWEEN 0.15 AND 0.30mm FROM TERMINAL TIP. IF THE TERMINAL HAS THE OPTIONAL RADIUS ON THE OTHER END OF THE TERMINAL, THE DIMENSION b SHOULD NOT BE MEASURED IN THAT RADIUS AREA.
4. MAX. PACKAGE WARPAGE IS 0.05 mm.
5. MAXIMUM ALLOWABLE BURRS IS 0.076 mm IN ALL DIRECTIONS.
6. THIS DRAWING CONFORMES TO JEDEC REGISTERED OUTLINE MO-220

05/15/13

Atmel Package Drawing Contact: packagedrawings@atmel.com	TITLE 32M3, 32-pad 4.0 x 4.0 x 0.90mm Body, 0.40mm Lead Pitch, Very Thin Quad Flat No-Lead Package (VQFN)	GPC ZAK	DRAWING NO. 32M3	REV. A

5. Revision History

Doc. Rev.	Date	Comments
8883AS	02/2014	Initial summary document release.

Atmel Corporation 1600 Technology Drive, San Jose, CA 95110 USA **T:** (+1)(408) 441.0311 **F:** (+1)(408) 436.4200 | **www.atmel.com**

Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

Microchip:

AT97SC3205T-U3A16-20 AT97SC3205T-X3A14-20 AT97SC3205T-U3A16-10 AT97SC3205T-X3M43-00 AT97SC3205T-X3A16-10 AT97SC3205T-X3A16-20 AT97SC3205T-U3A14-10 AT97SC3205T-X3A14-10 AT97SC3205T-U3A14-20 AT97SC3205T-H3M44-20 AT97SC3205T-H3M46-20 AT97SC3205T-G3M44-10 AT97SC3205T-H3M4620B AT97SC3205T-G3M4600B AT97SC3205T-G3M46-10 AT97SC3205T-H3M4600B AT97SC3205T-H3M46-00 AT97SC3205T-G3M4610B AT97SC3205T-G3M4620B AT97SC3205T-H3M4610B AT97SC3205T-H3M44-00 AT97SC3205T-G3M4410B AT97SC3205T-G3M44-00 AT97SC3205T-G3M46-00 AT97SC3205T-H3M44-10 AT97SC3205T-G3M46-20 AT97SC3205T-H3M4420B AT97SC3205T-G3M4420B AT97SC3205T-G3M44-20 AT97SC3205T-H3M4400B AT97SC3205T-H3M46-10 AT97SC3205T-G3M4400B AT97SC3205T-H3M4410B AT97SC3205T-G3M4B20B AT97SC3205T-H3M4B-00 AT97SC3205T-H3M4B-20 AT97SC3205T-H3M4B10B AT97SC3205T-H3M4B-10 AT97SC3205T-G3M4C-10 AT97SC3205T-G3M4C-20 AT97SC3205T-H3M4C-20 AT97SC3205T-H3M4C-10 AT97SC3205T-U3A1C-20 AT97SC3205T-G3M4B-00 AT97SC3205T-U3A1C20B AT97SC3205T-H3M4B20B AT97SC3205T-G3M4C00B AT97SC3205T-X3A1C-10 AT97SC3205T-U3A1C-10 AT97SC3205T-G3M4B00B AT97SC3205T-H3M4C-00 AT97SC3205T-H3M4B00B AT97SC3205T-X3A1C20B AT97SC3205T-H3M4C20B AT97SC3205T-H3M4C10B AT97SC3205T-G3M4C20B AT97SC3205T-U3A1C10B AT97SC3205T-G3M4B10B AT97SC3205T-X3A1C-20 AT97SC3205T-X3A1C10B AT97SC3205T-H3M4C00B AT97SC3205T-G3M4C-00 AT97SC3205T-G3M4B-20 AT97SC3205T-G3M4B-10 AT97SC3205T-G3M4C10B