AT97SC3205

Trusted Platform Module – SPI Interface

SUMMARY DATASHEET

Features

- Compliant to the Trusted Computing Group (TCG) Trusted Platform Module (TPM) Version 1.2 Specification
- Compliant with TCG PC Client-Specific TPM Interface Specification (TIS) Version 1.3
- Single-chip, Turnkey Solution
- Hardware Asymmetric Crypto Engine
- Atmel® AVR® RISC Microprocessor
- Internal EEPROM Storage for RSA Keys
- Serial Peripheral Interface (SPI) Protocol Up to 45MHz*
  (*Typical PC Operating Range is 24MHz to 33MHz)
- Secure Hardware and Firmware Design and Chip 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 and 32-pad QFN Package
- Offered in Both Commercial (0°C to 70°C) and Industrial (-40°C to +85°C) Temperature Ranges

Description

The Atmel AT97SC3205 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).

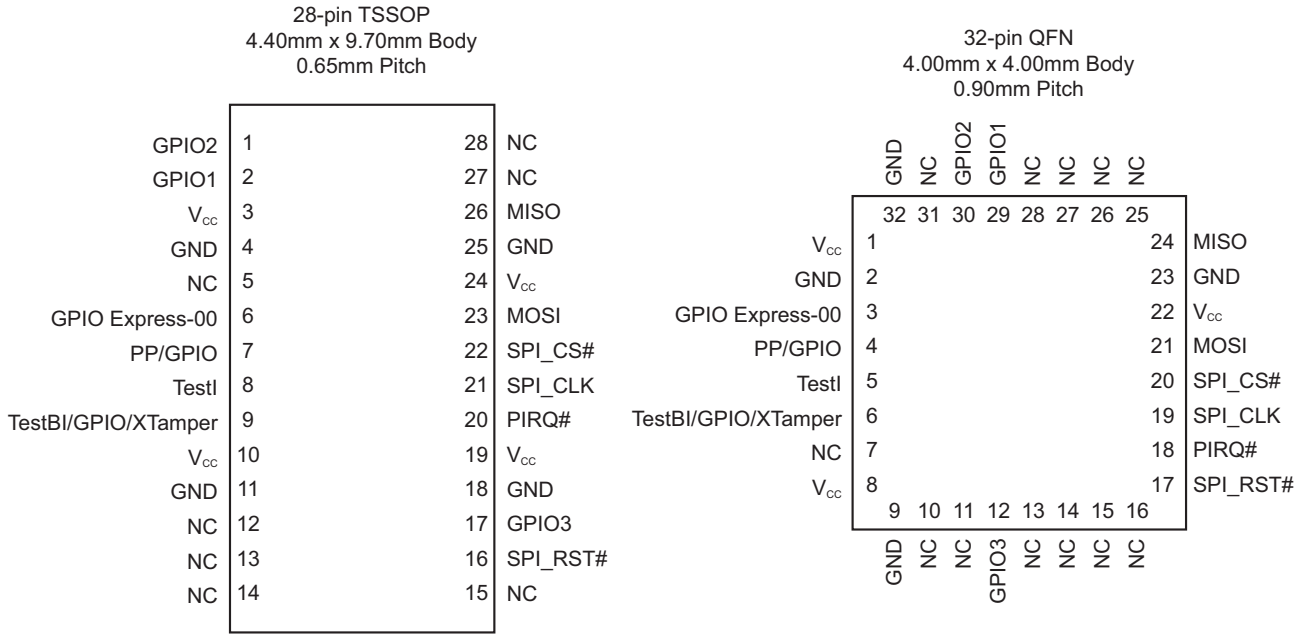
This is a summary document. The complete document is available under NDA. For more information, please contact your local Atmel sales office.

1. Pin Configurations and Pinouts

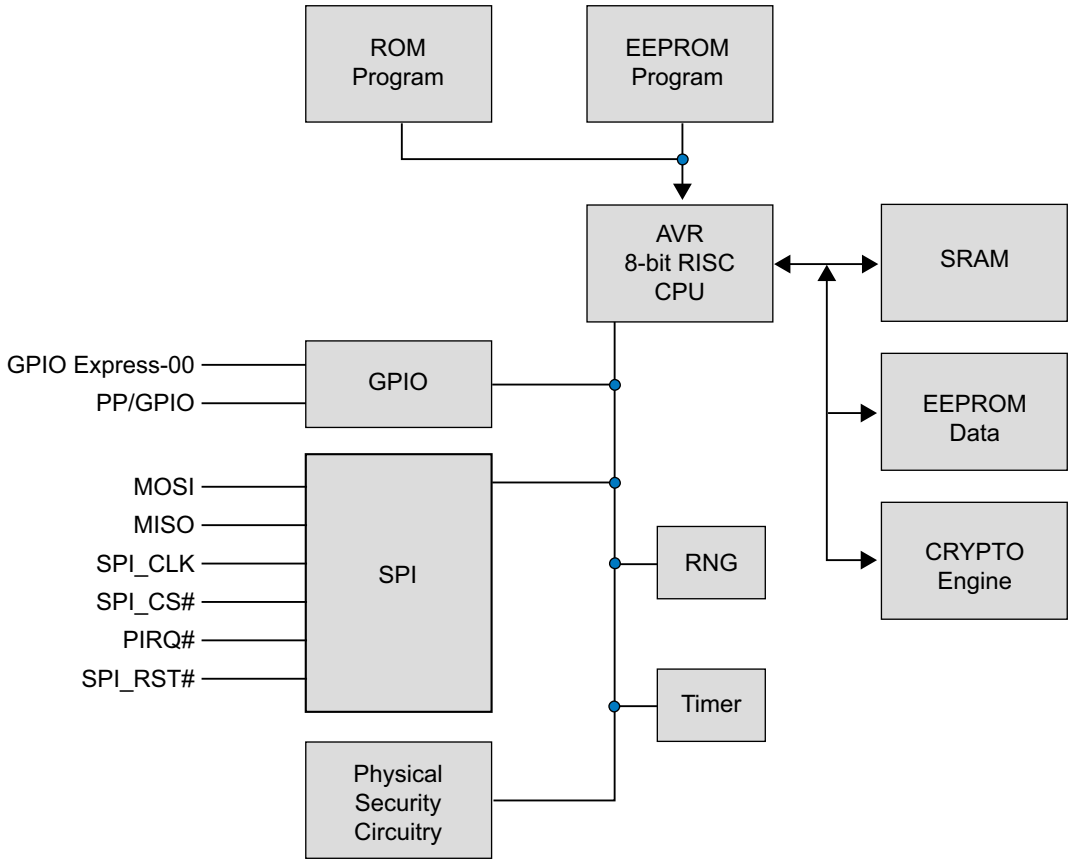
Table 1-1. Pin Configurations

Pin Name	Function
V_{CC}	3.3V Supply Voltage
GND	Ground
GPIO Express-00	GPIO assigned to TPM_NV_INDEX_GPIO_00
PP/GPIO	Hardware Physical Presence or GPIO pin.
GPIO	General Purpose Input/Output Pin
MISO	SPI Slave Data Output
MOSI	SPI Slave Data Input
PIRQ#	SPI Interrupt Requests
SPI_CLK	SPI Clock Input
SPI_CS#	SPI Chip Select
SPI_RST#	SPI Reset Pin
TestI	TestI Manufacturing Test Input (Disabled)
TestBI	TestBI Manufacturing Test Input (Disabled)
XTamper	Indicate External Tamper Event
NC	No Connect

Figure 1-1. Pinouts



2. Block Diagram



The TPM includes hardware Random Number Generator (RNG), including a FIPS certified 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 1.3, also available on the TCG web site. Implementation guidance for PC platforms is outlined in the TCG PC Client Specific Implementation Specification for Conventional Bios, version 1.2, also available on the TCG web site.

3. Pin Description

Table 3-1. 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, which should be 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 chip is idle. No further action is required by the system to enter low-power mode.
GND	**System Ground.**
GPIO Express-00	**General Purpose Input/Output. Internal pull-up resistor.** This pin is mapped to NV Index TPM_NV_INDEX_GPIO_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.
GPIO	**General Purpose Input/Output.** If unused, this pin can be tied to GND or V_{CC} at the customers discretion.
MISO	**Master In Slave Out. SPI Slave Data Output.** This pin serves as the SPI Data output from the TPM.
MOSI	**Master Out Slave In. SPI Slave Data Input.** This pin serves as the SPI Data Input to the TPM.
PIRQ#	**SPI Interrupt Pin, Active-low.** This pin is used by the TPM to assert interrupts. If unused, this pin should be tied to ground directly or through a 4.7KΩ resistor.
SPI_CLK	**Clock used to drive the SPI bus.** This pin should be asserted high for power savings when the TPM is not in use.
SPI_CS#	**SPI_CS# Chip Select, Active-low**. The TPM chip select.
SPI_RST#	**SPI Reset Pin, Active-low.** Pulsing this signal low resets the internal state of the TPM, and is equivalent to removal/restoration of power to the chip. The required minimum reset pulse width is 2µs. On power-up, it is critical that reset be kept active-low until V_{CC}, and SPI_CLK stabilize. To be compliant with TCG requirements, this pin needs to be tied to system reset. TPM_Init is indicated by asserting this pin.
TestI	**TestI Manufacturing Test Input.** Disabled after manufacturing. Tie TestI to ground directly or through a 4.7kΩ resistor.
TestBI/GPIO/ XTamper	**TestBI Manufacturing Test Input**. The Atmel TPM does not support legacy addressing via the optional BADD implementation of this pin.The TestBI pin also 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.
NC	**No Connect Pins (TSSOP).** The AT97SC3205 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

Table 3-1. Pin Descriptions (Continued)

Pin	Description
NC	**No Connect Pins (QFN).** The AT97SC3205 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.

4. Ordering Information

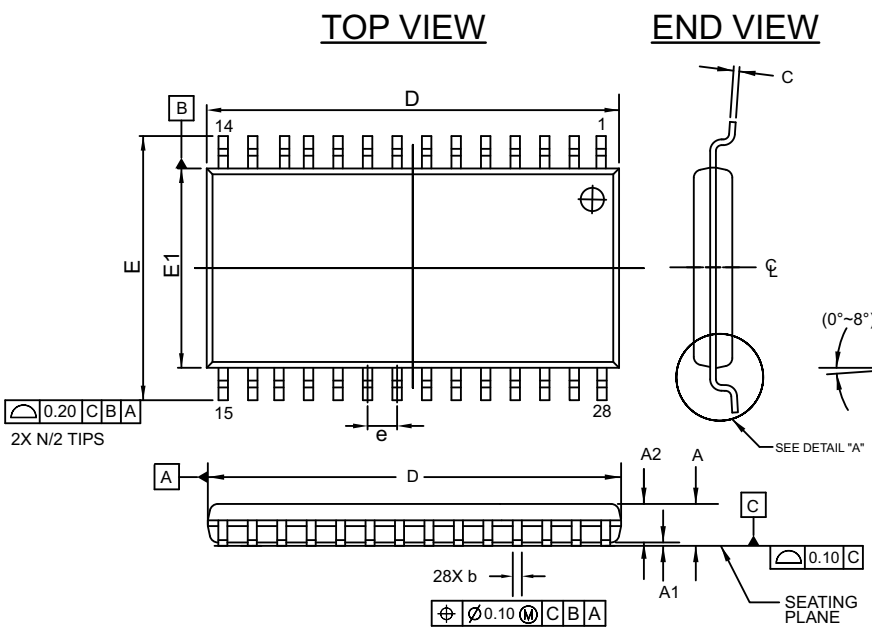
Atmel Ordering Code	Package		Operating Range
AT97SC3205[1]	28X1 (28-pin thin TSSOP)	Lead-free, RoHS	Commercial (0°C to 70°C) Industrial (-40°C to 85°C)
	32M3 (32-pin very thin QFN)		

Note: 1. Please see the AT97SC3205 datasheet addendum for the complete catalog number ordering code.

Package Type	
28X1	28-lead, 4.4mm body width, Plastic Thin Shrink Small Outline (thin TSSOP)
32M3	32-pad, 4.0 x 4.0 x 0.9mm body, 0.4mm lead pitch, Very Thin Quad Flat No-Lead (QFN)

5. Package Drawings

5.1 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	-	-	

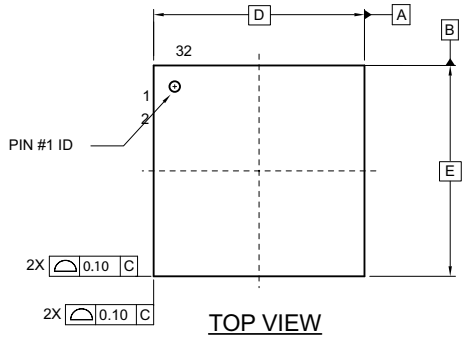
Note:

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.

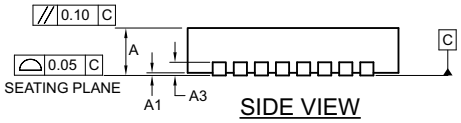
7/8/2011

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

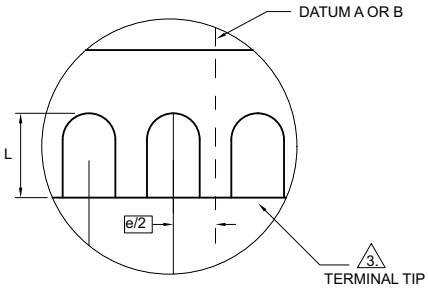
5.2 32M3 — 32-pad QFN



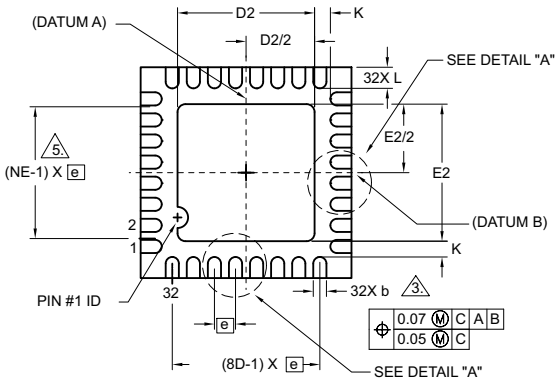
TOP VIEW



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

6. Revision History

Doc. Rev.	Date	Comments
8884AS	02/2014	Initial summary document release