# Atmel AT97SC3204

## Trusted Platform Module LPC Interface

### SUMMARY DATASHEET

## Features

- Fully 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 1.2
- Single-chip, turnkey solution
- Hardware asymmetric crypto engine
- Atmel® AVR® RISC microprocessor
- Internal EEPROM storage for RSA keys
- 33MHz Low Pin Count (LPC) bus for easy PC interface
- Secure hardware and firmware design and chip layout
- Internal, high-quality Random Number Generator (RNG) – FIPS 140-2 compliant
- NV storage space for 1756 bytes of user defined data
- 3.3V supply voltage
- 28-lead thin TSSOP, 28-lead wide TSSOP, or 40-pad QFN packages
- Offered in both commercial (0 to 70°C) and industrial (-40 to +85°C) temperature ranges

## 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.

**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

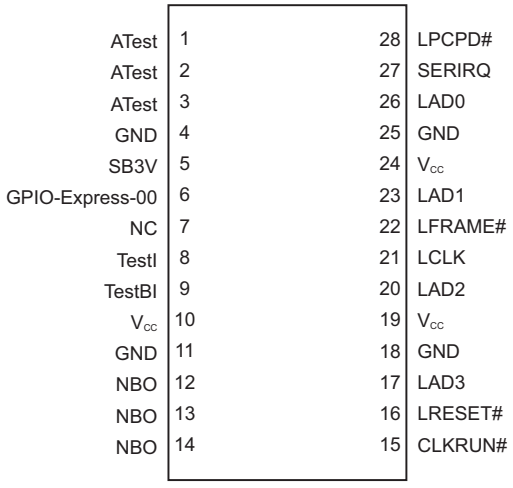
**Table 1-1. Pin Configurations**

| Pin name | Function |
|---|---|
| $V_{CC}$ | 3.3V Supply Voltage |
| 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 |
| SERIRQ | Serialized Interrupt Request Input/Output |
| GPIO-Express-00 | GPIO assigned to TPM_NV_INDEX_GPIO_00 |
| TestI | Test Input (Disabled) |
| TestBI | Test Input (Disabled) |
| ATest | Atmel Test Pin |
| NC | No Connect |
| NBO | Not Bounded Out |

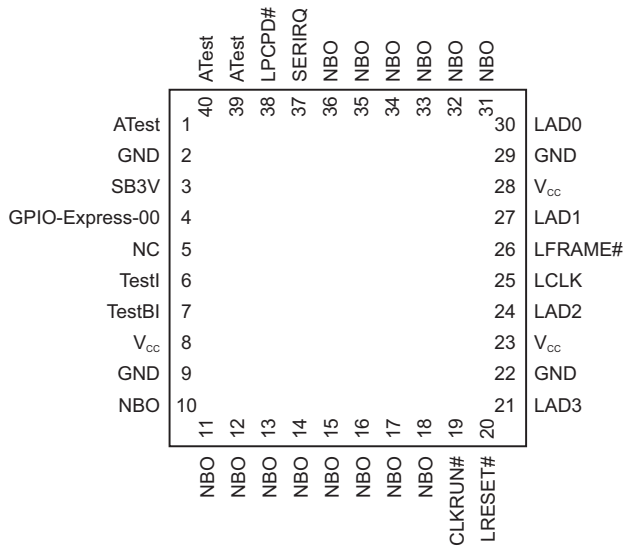
**Table 1-2. Pinouts**

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

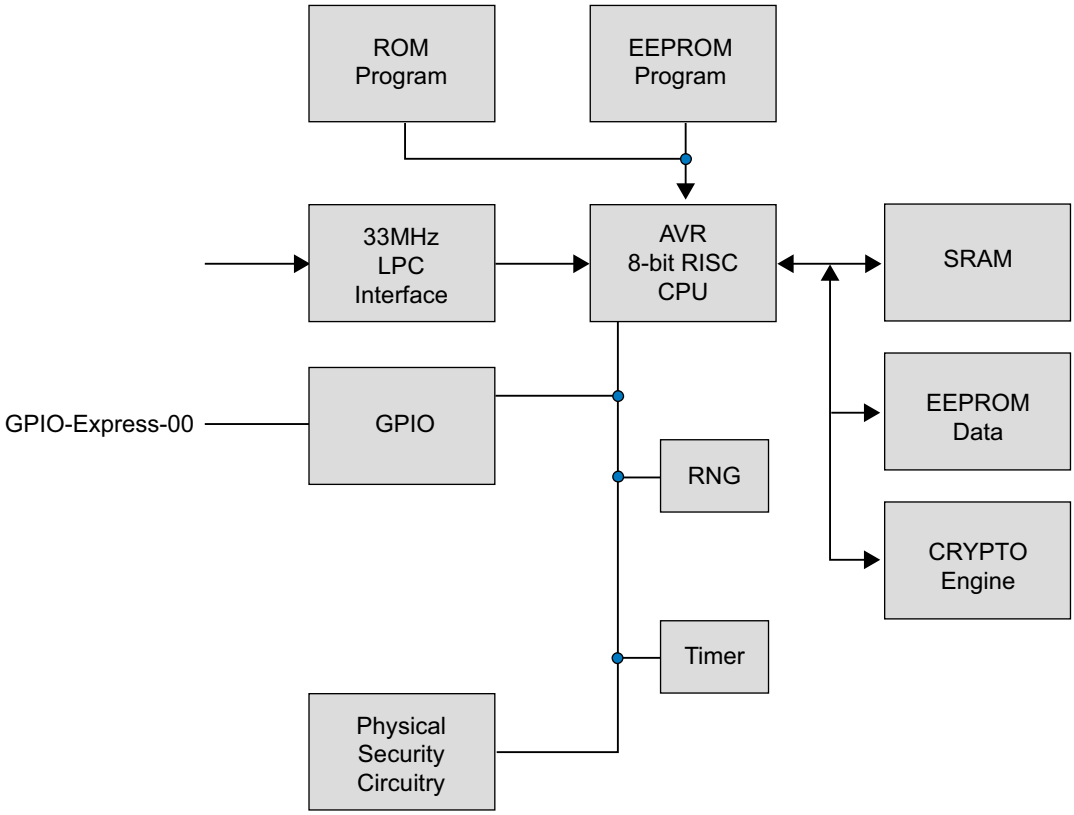
28-pin TSSOP
6.1mm x 9.7mm Body
0.65mm Pitch




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



## 2. 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 website.

# 3. Ordering Information

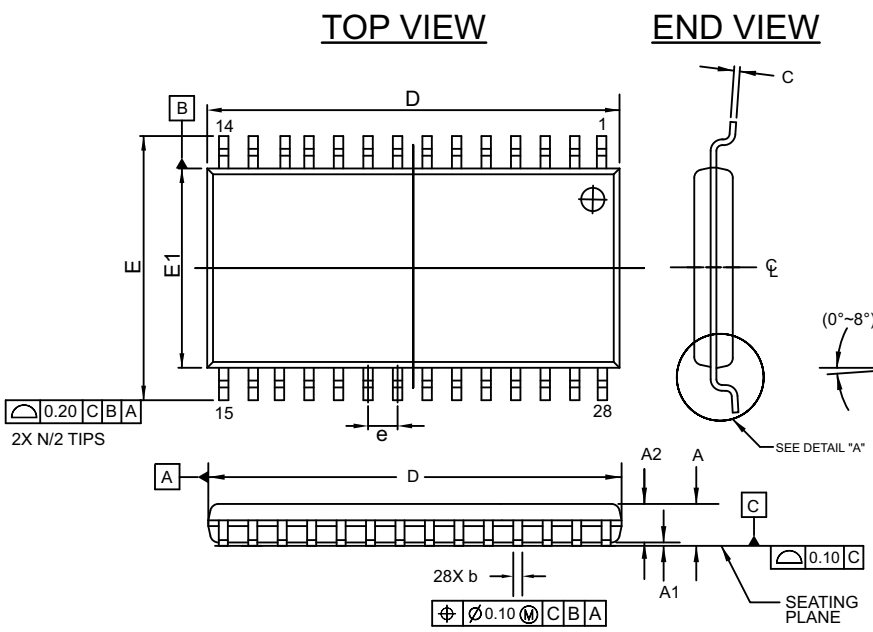
| Atmel Ordering Code | Package | | Operating Range |
|---|---|---|---|
| AT97SC3204[1] | 28X1 (28-pin thin TSSOP) | Lead-free, RoHS | Commercial (0°C to 70°C)<br>Industrial (-40°C to 85°C) |
| AT97SC3204[1] | 40ML1 (40-pin QFN) | | |

Note: 1. Please see the AT97SC3204 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) |
| **40ML1** | 40-pad 6.0 x 6.0x0.9mm body, 0.50mm pitch, Very-thin Quad Flat No Lead (VQFN) |

# 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 | - | - | |

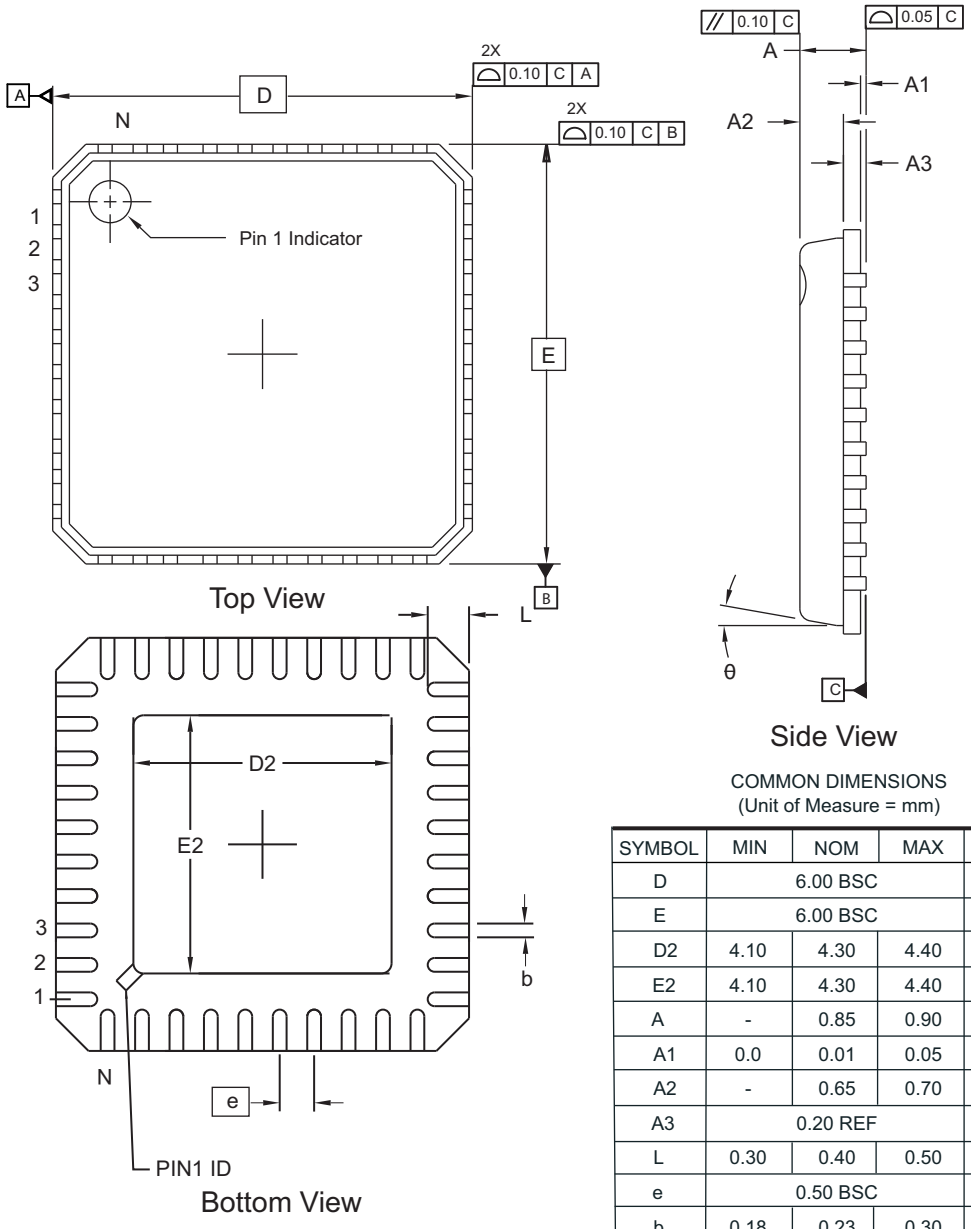
Note:

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

## 4.2 40ML1 — 40-pad VQFN




COMMON DIMENSIONS
(Unit of Measure = mm)

| SYMBOL | MIN | NOM | MAX | NOTE |
|---|---|---|---|---|
| D | | 6.00 BSC | | |
| E | | 6.00 BSC | | |
| D2 | 4.10 | 4.30 | 4.40 | |
| E2 | 4.10 | 4.30 | 4.40 | |
| 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.

09/23/11

| Atmel<br>Package Drawing Contact:<br>packagedrawings@atmel.com | **TITLE**<br>40ML1, 40-pad 6.0 x 6.0x0.9 mm Body, 0.50 mm pitch, Very-Thin Quad Flat No Lead Package (VQFN) Punched | **GPC**<br>ZJI | **DRAWING NO.**<br>40ML1 | **REV.**<br>D |
|---|---|---|---|---|

# 5. Revision History

| Doc. Rev. | Date | Comments |
|---|---|---|
| 5295ES | 03/2013 | Removed bullet from features: 2048-bit RSA® sign in 200ms.<br>Updated footers and disclaimer page. |
| 5295DS | 12/2012 | Changed GPIO6 to GPIO-Express-00.<br>Updated package drawings 28A3 and 40ML1.<br>Updated package drawing 28A1 to 28X1.<br>Updated template and Atmel logos. |
| 5295CS | 03/2011 | Corrected header and footers. |
| 5295BS | 10/2010 | Added Industrial Grade support detail. |
| 5295AS | 01/2008 | Initial document release. |

Enabling Unlimited Possibilities®

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

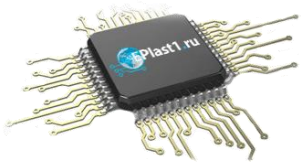
Компания «ЭлектроПласт» предлагает заключение долгосрочных отношений при поставках импортных электронных компонентов на взаимовыгодных условиях!

Наши преимущества:

- Оперативные поставки широкого спектра электронных компонентов отечественного и импортного производства напрямую от производителей и с крупнейших мировых складов;
- Поставка более 17-ти миллионов наименований электронных компонентов;
- Поставка сложных, дефицитных, либо снятых с производства позиций;
- Оперативные сроки поставки под заказ (от 5 рабочих дней);
- Экспресс доставка в любую точку России;
- Техническая поддержка проекта, помощь в подборе аналогов, поставка прототипов;
- Система менеджмента качества сертифицирована по Международному стандарту ISO 9001;
- Лицензия ФСБ на осуществление работ с использованием сведений, составляющих государственную тайну;
- Поставка специализированных компонентов (Xilinx, Altera, Analog Devices, Intersil, Interpoint, Microsemi, Aeroflex, Peregrine, Syfer, Eurofarad, Texas Instrument, Miteq, Cobham, E2V, MA-COM, Hittite, Mini-Circuits,General Dynamics и др.);

Помимо этого, одним из направлений компании «ЭлектроПласт» является направление «Источники питания». Мы предлагаем Вам помощь Конструкторского отдела:

- Подбор оптимального решения, техническое обоснование при выборе компонента;
- Подбор аналогов;
- Консультации по применению компонента;
- Поставка образцов и прототипов;
- Техническая поддержка проекта;
- Защита от снятия компонента с производства.




**Как с нами связаться**

**Телефон:** 8 (812) 309 58 32 (многоканальный)
**Факс:** 8 (812) 320-02-42
**Электронная почта:** org@eplast1.ru
**Адрес:** 198099, г. Санкт-Петербург, ул. Калинина, дом 2, корпус 4, литера А.