

## Features

- TCG/TCPA V1.1b Compatible
- Single Chip Turnkey Solution
- Hardware Asymmetric Crypto Engine
- 2048 RSA Sign in 500 ms
- AVR 8-bit RISC Microprocessor
- Internal EEPROM Storage for RSA Keys
- 33 MHz LPC (Low Pin Count) Bus for Easy PC Interface
- Secure Hardware and Firmware Design
- True Random Number Generator (RNG)
- Secure Real-time Clock Option
- 3.3V  $\pm 10\%$  Supply Voltage
- 28-lead TSSOP Package or 40-lead QFN Package
- 0–70°C Temperature Range

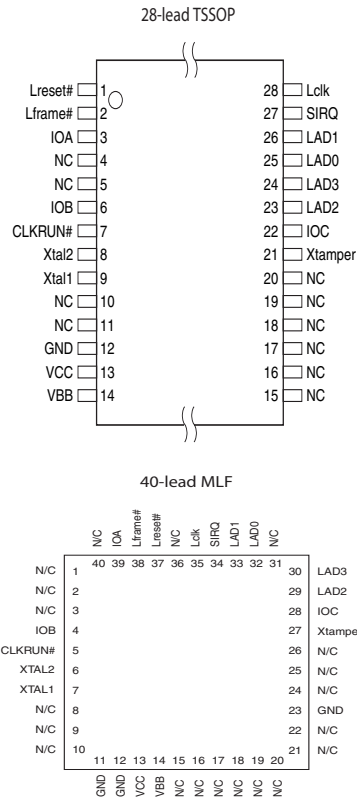
## Description

The AT97SC3201 is a fully integrated security module designed to be integrated into personal computers and other embedded systems. It implements version 1.1b of the Trusted Computing Platform Alliance (TCPA) specification for Trusted Platform Modules (TPM). This specification has been adopted by the Trusted Computing Group (TCG).

The TPM includes a crypto accelerator capable of computing a 2048-bit RSA signature in 500 ms and a 1024-bit RSA signature in 100 ms. Communication to and from the TPM occur through a 33-MHz LPC interface.

Figure 1. Pin Configurations

Pin Name	Description
Lreset#	System Reset, Active-low. Input
Lframe#	LPC Frame Indicator
Xtal1	32.768 kHz Crystal
Xtal2	32.768 kHz Crystal
LAD0–3	LPC Command, Address and Data
GND	Ground
V <sub>BB</sub>	2.5–4.0V Battery Input
V <sub>CC</sub>	3.3V ( $\pm 10\%$ ) Supply Voltage
CLKRUN#	Clock Control
SIRQ	Serial IRQ Line
Lclk	33-MHz PCI Clock
IOA	Input/Output A
IOB	Input/Output B
IOC	Input/Output C
Xtamper	External Tamper Detect



## Trusted Platform Module

## AT97SC3201

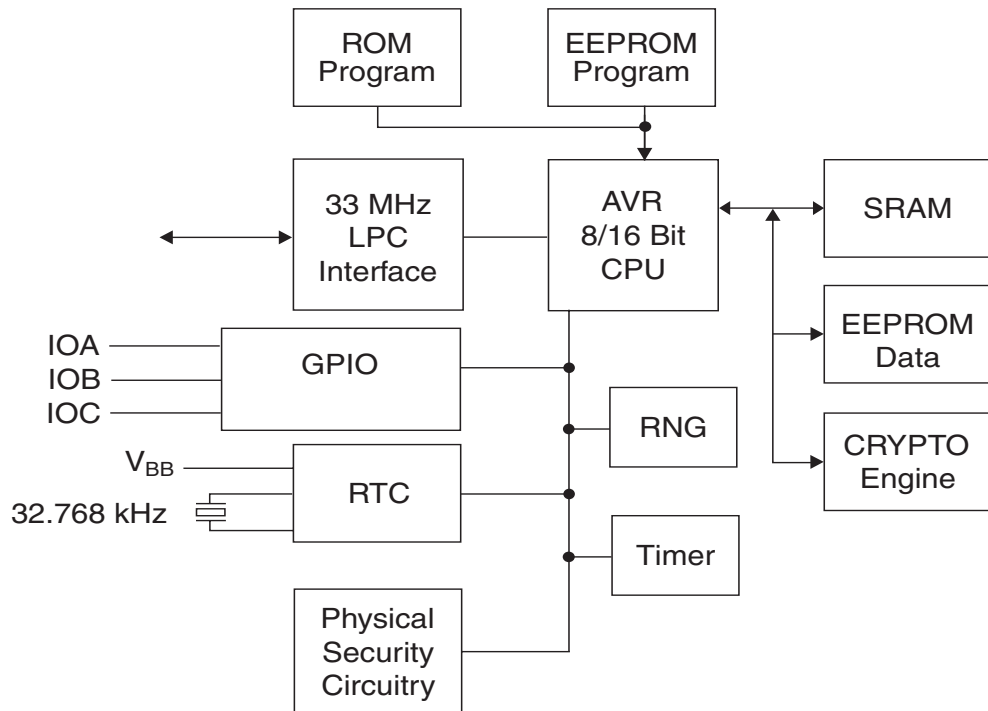
## Summary

Rev. 2015ES-TPM-06/05



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

**Figure 2.** AT97SC3201 Block Diagram



The chip includes a full hardware random number generator that is used for the TCG protocol and is also available to the system for any random numbers it may need during normal operation.

A real-time clock function is available using an external battery and crystal. The chip provides tamper detection if the battery or crystal are removed or tampered with, and the current time value can be signed by the appropriate internal keys to verify its accuracy. (Contact Atmel for current status of this option.)

The battery detector can be used without the crystal for lower cost. In this mode, the TPM can indicate to the system if it has been removed from the PC in any way and can also take actions internally.

The chip uses a dynamic internal memory management scheme to store from 10 to 20 keys. Other than the standard TCG commands (TPM\_Evictkey, TPM\_Loadkey), no system intervention is required to manage this internal key cache.

The TPM is offered to OEM manufacturers as a turnkey solution, including the firmware integrated on the chip. In addition, Atmel provides the necessary driver software for integration into certain operating systems, along with BIOS drivers. A TCG Software Stack (TSS), also supplied by Atmel and available under license, provides communication support to any application using MSCAPI or PKCS #11 Cryptographic APIs. (Contact Atmel for a complete list of operating systems supported.)

Full documentation for TCG primitives can be found on the TCG Web site, [www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org). This specification includes only mechanical and electrical information.

## Absolute Maximum Ratings

Operating Temperature.....	0°C to +70°C
Storage Temperature (without Bias).....	0°C to + 70°C
Voltage on I/O Pins.....	-0.1 to $V_{CC} + 0.3V$
Voltage on VCC with Respect to Ground.....	6.0V
Maximum ESD Voltage.....	2000V

**\*NOTICE:** Stresses beyond those listed under “Absolute Maximum Ratings” may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of this specification may cause temporary or permanent failure. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

**Table 1. DC Parameters\***

Symbol	Parameter	Min	Nom	Max	Units	Notes
$V_{CC}$	Supply Voltage	3.0	3.3	3.6	V	
$I_{CC}$	Operating Current at fclk = 33 MHz		25	50	mA	
$I_{ST}$	Static Current		5	10	mA	$V_{CC} = 3.6V$ ; fxtal = 0 Hz, active inputs
$I_{SL}$	Sleep Current, Chip Idle		40	100	$\mu A$	$V_{CC} = 3.6V$ ; fxtal = 0 Hz
$I_{BB}$	Battery Current		2	4	$\mu A$	$V_{CC} = 0V$ ; fxtal = 0 Hz
$I_{LIO}$	Input Leakage		0.1	3	$\mu A$	$V_{in} = V_{CC}$ or GND
$V_{IH}$	Input High Threshold	$0.5 * V_{CC}$		$V_{CC} + 0.5$	V	
$V_{IL}$	Input Low Threshold	-0.5		$0.3 * V_{CC}$	V	
$V_{OH}$	Output High Voltage	$0.9 * V_{CC}$	$0.98 * V_{CC}$		V	At $I_{OUT} = -500 \mu A$
$V_{OL}$	Output Low Voltage			$0.1 * V_{CC}$	V	At $I_{OUT} = 1.5mA$
$I_{OLCR}$	Output Low Current, CLKRUN#	7			mA	At $V_{OUT} = .615 * V_{CC}$
$C_I$	Input Pin Capacitance		6		pF	Note 1

\*  $V_{CC} = 3.0$  to  $3.6V$ ; Temperature =  $0$  to  $70^\circ C$

Note: 1. These parameters guaranteed by design.

**Table 2. AC Parameters\***

Symbol	Parameter	Min	Nom	Max	Units	Notes
T <sub>VAL</sub>	CLK to Signal Valid Delay – LAD0-3	2	5	11	ns	Measured at V <sub>rise</sub> = 0.285 * V <sub>CC</sub> and V <sub>fall</sub> = 0.615 * V <sub>CC</sub> . Measured from clk at V <sub>test</sub> = 0.4 * V <sub>CC</sub> ; Load = 200Ω
T <sub>ON</sub>	Float to Active Delay	2	4		ns	
T <sub>OFF</sub>	Active to Float Delay			28	ns	
T <sub>SU</sub>	Input Setup Time to CLK	7	2		ns	
T <sub>H</sub>	Input Hold Time from CLK	0	-500		ns	
T <sub>RST</sub>	Reset Active Time after Power Stable	1			ms	Note 2
T <sub>RST-CLK</sub>	Reset Active after CLK Stable	100			m	Note 2
T <sub>RST-OFF</sub>	Reset Active to Output Float Delay			40	ns	Note 2
T <sub>CLKIN</sub>	CLK Period	29.5	30	31	ns	Note 3
T <sub>CLKLO</sub>	CLK Low Duration	13.4		18	ns	Note 1, Note 3
T <sub>CLKHI</sub>	CLK High Duration	13.4		18	ns	Note 1, Note 3

\* CI = 10pf. V<sub>CC</sub> = 3.0 to 3.7V; Temperature = 0 to 70°C

- Note:
1. All parameters measured with respect to signal crossing V<sub>test</sub> = 0.4 \* V<sub>CC</sub> unless otherwise noted.
  2. These parameters guaranteed by design.
  3. The minimum parameter must never be violated under any circumstances unless I<sub>reset#</sub> is asserted. If proper CLKRUN# signaling is observed, the maximum specification can be violated.

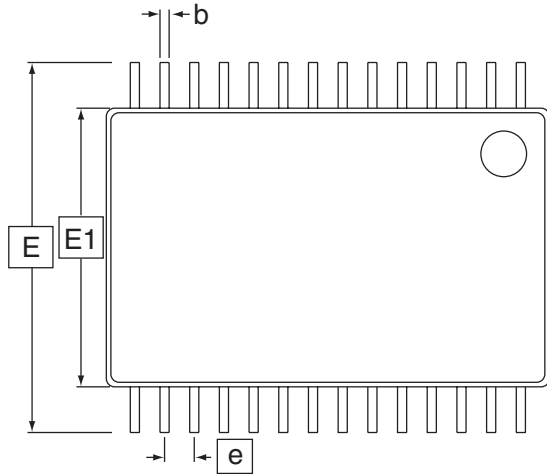
**Table 3. Ordering Information**

Ordering Code <sup>(1)</sup>	Package		Operation Range
AT97SC3201-09AC	28A3 (TSSOP)		Commercial (0° to 70° C)
AT97SC3201-X9AC	28A3 (TSSOP)	lead-free <sup>(2)</sup>	Commercial (0° to 70° C)
AT97SC3201-09MC	40ML1 (QFN)		Commercial (0° to 70° C)
AT97SC3201-X9MC	40ML1 (QFN)	lead-free <sup>(2)</sup>	Commercial (0° to 70° C)

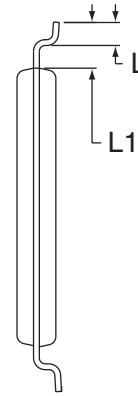
- Note:
1. Current as of time of publication. Contact Atmel Marketing for possible updated options.
  2. Also RoHS

## Package Drawing

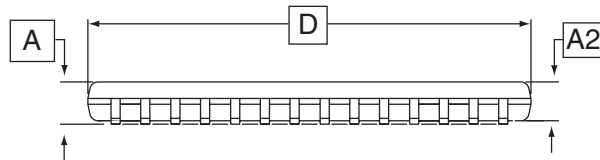
### 28A3 – TSSOP



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



2325 Orchard Parkway  
San Jose, CA 95131

#### TITLE

**28A3**, 28-lead, 6.1 x 9.7 mm Body, 0.65 pitch,  
Thin Shrink Small Outline Package (TSSOP)

#### DRAWING NO.

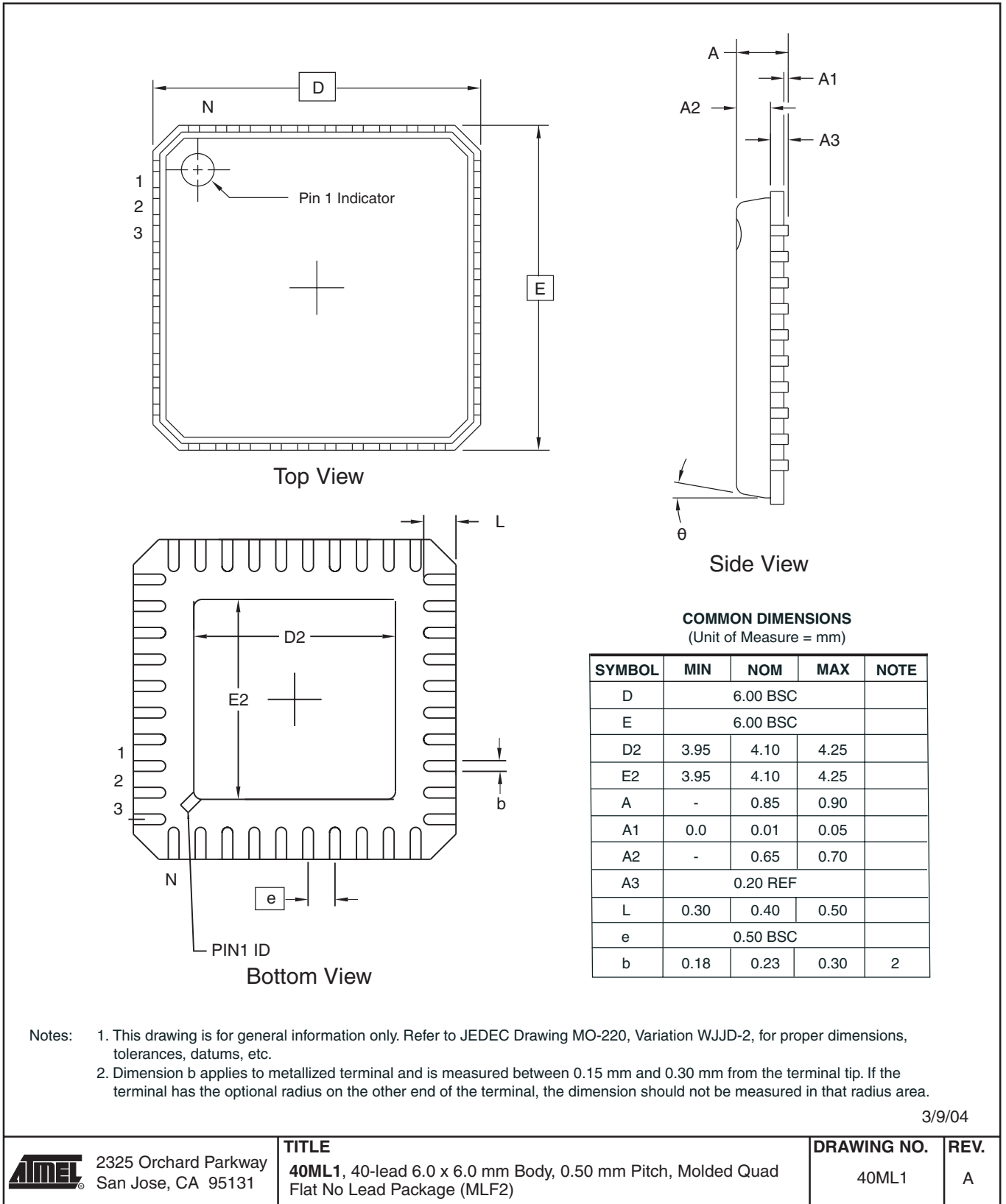
28A3

#### REV.

A



# 40ML1 - QFN





## 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 Arsenalux 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/Imaging/Hi-Rel MPU/ High Speed Converters/RF Datacom

Avenue de Rochepleine  
BP 123  
38521 Saint-Egreve Cedex, France  
Tel: (33) 4-76-58-30-00  
Fax: (33) 4-76-58-34-80

---

## Literature Requests

[www.atmel.com/literature](http://www.atmel.com/literature)

**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 ATMEL'S TERMS AND CONDITIONS OF SALE LOCATED ON ATMEL'S WEB SITE, 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 OF 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 product descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Atmel's products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.

© Atmel Corporation 2005. **All rights reserved.** Atmel®, logo and combinations thereof, Everywhere You Are® and others, are registered trademarks or trademarks of Atmel Corporation or its subsidiaries. Other terms and product names may be trademarks of others.



Printed on recycled paper.

2015ES-TPM-06/05