

1. Features

- Full trusted computing group (TCG) trusted platform module (TPM) version 1.2 compatibility
- Compliant with TCG PC client specific TPM interface specification version 1.2
- Single-chip turnkey solution
- Hardware asymmetric crypto engine
- 2048-bit RSA[®] sign in 200ms
- AVR[®] RISC microprocessor
- Internal EEPROM storage for RSA keys
- 33MHz LPC (Low pin count) bus for easy PC 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 supply voltage
- 28-lead Thin TSSOP, Wide TSSOP or 40-lead QFN packages
- Offered in both commercial (0 to 70°C) and industrial (-40 to +85°C) temperature ranges

2. 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.



Trusted Platform Module

Atmel AT97SC3204 LPC Interface

Summary

- * See the full data sheet for detailed design information

5295CS-TPM-3/11



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

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
SERIQ	Serialized interrupt request input/output
GPIO6	General purpose input/output
TestI	Test input (disabled)
TestBI	Test input (disabled)
ATest	Atmel test pin
NC	No connect
NBO	Not bounded out

Figure 2-1. Pinout diagrams

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

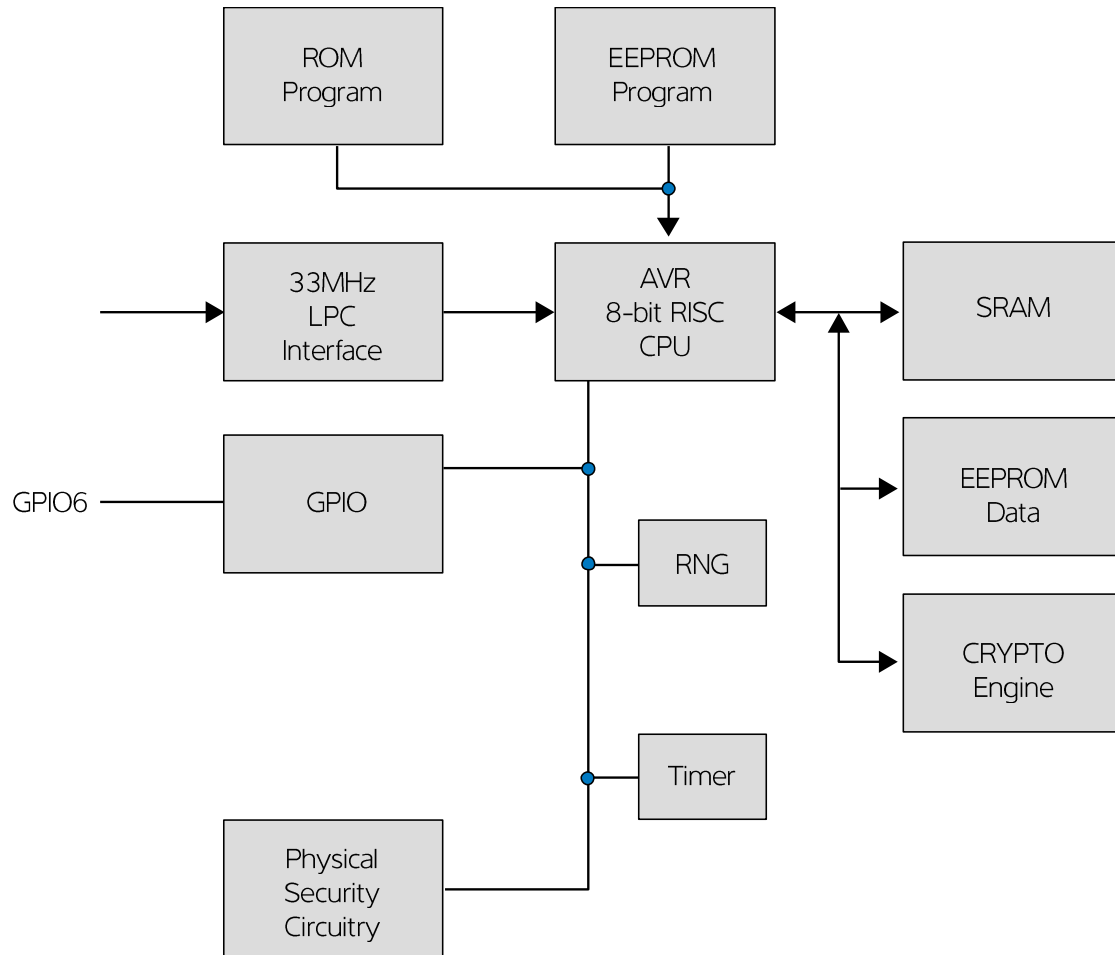
28-pin TSSOP
6.1 mm x 9.7 mm Body
0.65 mm Pitch

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

ATest	1	28	LPCPD#
ATest	2	27	SERIRQ
ATest	3	26	LAD0
GND	4	25	GND
SB3V	5	24	V _{CC}
GPIO6	6	23	LAD1
NC	7	22	LFRAME#
TestI	8	21	LCLK
TestBI	9	20	LAD2
V _{CC}	10	19	V _{CC}
GND	11	18	GND
NBO	12	17	LAD3
NBO	13	16	LRESET#
NBO	14	15	CLKRUN#

ATest	1	40	ATest	39	38	37	36	35	34	33	32	31	30	LAD0
GND	2		GND	2									29	GND
SB3V	3		SB3V	3									28	V _{CC}
GPIO6	4		GPIO6	4									27	LAD1
NC	5		NC	5									26	LFRAME#
TestI	6		TestI	6									25	LCLK
TestBI	7		TestBI	7									24	LAD2
V _{CC}	8		V _{CC}	8									23	V _{CC}
GND	9		GND	9									22	GND
NBO	10		NBO	10									21	LAD3
NBO	11		NBO	11										
NBO	12		NBO	12										
NBO	13		NBO	13										
NBO	14		NBO	14										
NBO	15		NBO	15										
NBO	16		NBO	16										
NBO	17		NBO	17										
NBO	18		NBO	18										
CLKRUN#	19		CLKRUN#	19										
LRESET#	20		LRESET#	20										

Figure 2-2. Atmel AT97SC3204 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 web site.

3. Ordering information

Table 1-2. Atmel AT24C256C ordering information

Atmel ordering code	Package		Operating range
AT97SC3204 ⁽¹⁾	28A2 (28-pin Thin TSSOP)	Lead-free, RoHS	Commercial (0°C to 70°C) Industrial (-40°C to 85°C)
AT97SC3204 ⁽¹⁾	28A3 (28-pin TSSOP)	Lead-free, RoHS	Commercial (0°C to 70°C) Industrial (-40°C to 85°C)
AT97SC3204 ⁽¹⁾	40ML1 (40-pin QFN) ⁽²⁾	Lead-free, RoHS	Commercial (0°C to 70°C) Industrial (-40°C to 85°C)

Notes: 1. Please see the Atmel AT97SC3204 datasheet addendum for the complete catalog number ordering code

4. Package drawing

28A2 – Thin TSSOP

COMMON DIMENSIONS
(Unit of Measure = mm)

SYMBOL	MIN	NOM	MAX	NOTE
D	9.60	9.70	9.80	1,4
E	6.40 BSC			
E1	4.30	4.40	4.50	2,4
A			1.20	
A2	0.80	1.00	1.05	
b	0.19		0.30	3
e	0.65 BSC			
L	0.45	0.60	0.75	
L1	1.00 REF			

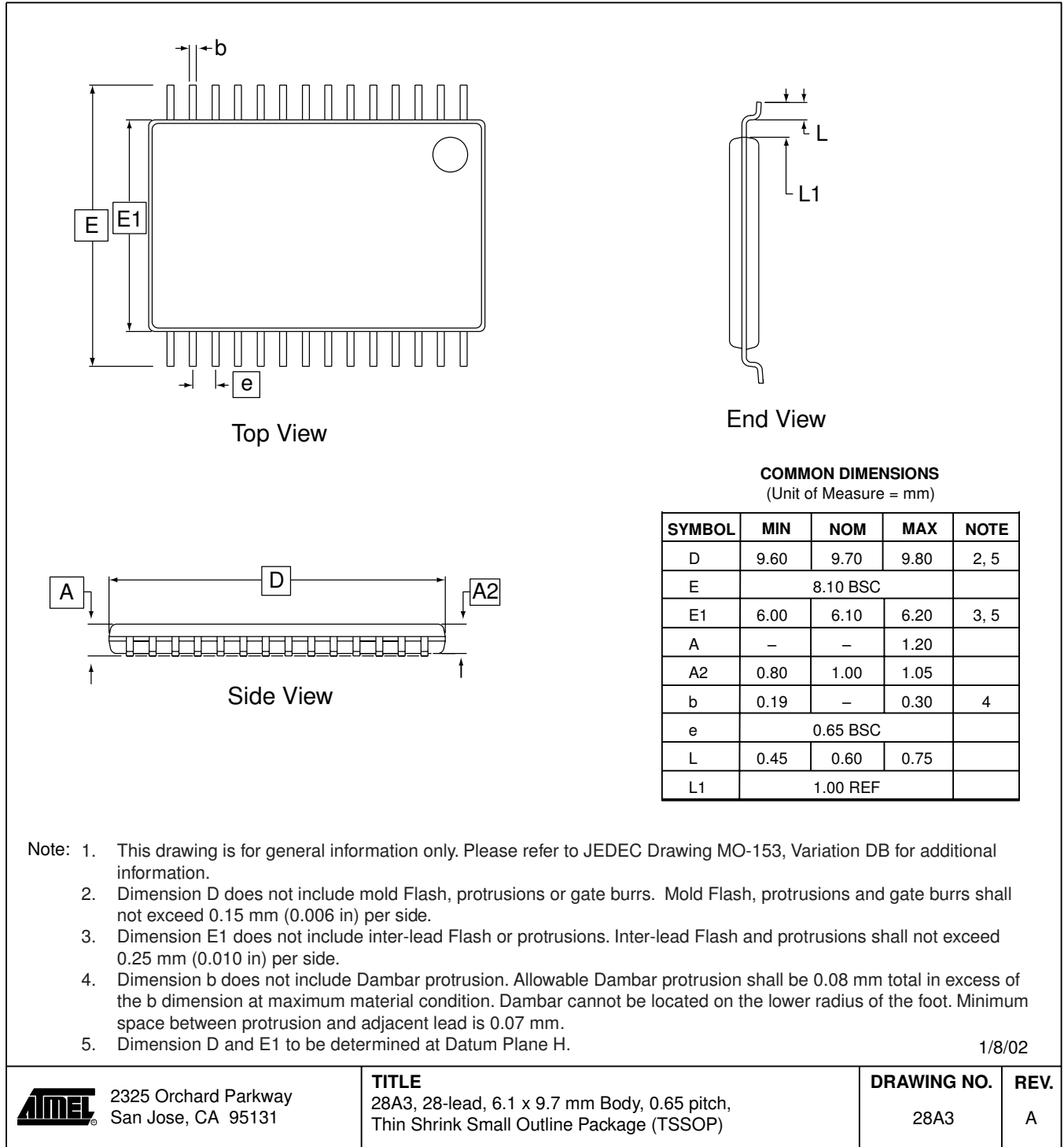
- Dimension "D" does not include mold flash, protrusions or gate burrs. Mold flash, protrusions and gate burrs shall not exceed .15mm (.006 in) per side.
- Dimension "E1" does not include inter-lead flash or protrusions. Inter-lead flash and protrusions shall not exceed .25mm (.010 in) per side.
- Dimension '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.
- Dimension 'D' and 'E1' to be determined at Datum Plane H.

This drawing is for general information only. Please refer to JEDEC Drawing MO-153, Variation AE for additional information.

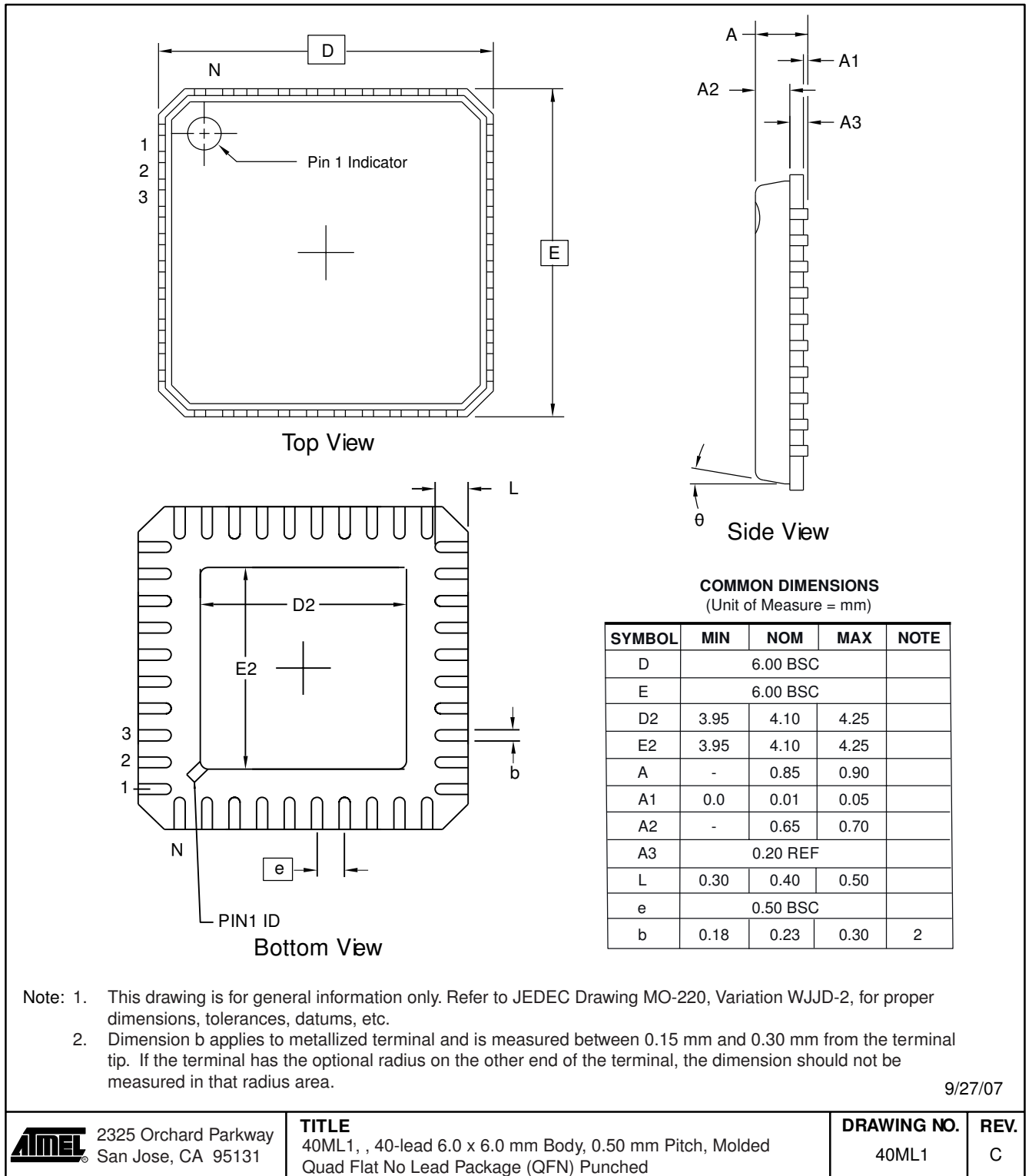
6/17/08

	Package Drawing Contact: packagedrawings@atmel.com	TITLE 28A2, 28-lead, 4.4x9.7 mm Body, 0.65 pitch, Thin Shrink Small Outline Package (TSSOP)	GPC TFL	DRAWING NO. 28A2	REV. B

28A3 – TSSOP



40ML1 – QFN



5. Revision history

Doc. rev.	Date	Comments
5295CS	03/2011	Corrected header and footers
5295BS	10/2010	Added Industrial Grade support detail
5295AS	01/2008	Initial document release

**Atmel Corporation**

2325 Orchard Parkway
San Jose, CA 95131
USA

Tel: (+1) (408) 441-0311

Fax: (+1) (408) 487-2600

www.atmel.com

Atmel Asia Limited

Unit 01-5 & 16, 19F
BEA Tower, Millennium City 5
418 Kwun Tong Road
Kwun Tong, Kowloon
HONG KONG

Tel: (+852) 2245-6100

Fax: (+852) 2722-1369

Atmel Munich GmbH

Business Campus
Parkring 4
D-85748 Garching b. Munich
GERMANY

Tel: (+49) 89-31970-0

Fax: (+49) 89-3194621

Atmel 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

© 2011 Atmel Corporation. All rights reserved. / Rev.: 5295CS-TPM-3/11

Atmel[®], logo and combinations thereof, CryptoAuthentication[™] and others are registered trademarks or trademarks of Atmel Corporation or its subsidiaries. Other terms and product names may be trademarks of others.

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 THE ATMEL TERMS AND CONDITIONS OF SALES LOCATED ON THE ATMEL WEBSITE, 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 AND 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 products descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Unless specifically provided otherwise, Atmel products are not suitable for, and shall not be used in, automotive applications. Atmel products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.