ATECC108

Atmel CryptoAuthentication

SUMMARY DATASHEET

Features

- Secure authentication and product validation device
- High-Speed Public Key Algorithm (PKI) Crypto Engine
  - FIPS186-3 Elliptic Curve Digital Signature Algorithm (ECDSA)
- NIST Standard P256, B283, and K283 Elliptic Curve support
- Superior SHA-256 Hash Algorithm; HMAC option
- Integrated capability for both Host and Client operations
- Best in class 256/283-bit key length, storage for up to 16 keys
- Guaranteed unique 72-bit serial number
- Internal high-quality FIPS Random Number Generator (RNG)
- 8.5Kb EEPROM memory for keys, certificates, and data
- 512 One Time Programmable (OTP) bits for fixed information or consumption logging
- Multiple I/O options
  - High-Speed single pin interface, with one GPIO pin
  - 1MHz standard I^2C interface
- Integrated temperature sensor
  - Uncalibrated accuracy, -40°C to +85°C (±3°C)
- 2.0V – 5.5V supply voltage range
- 1.8V – 5.5V communications
- <150nA sleep current
- Extended multi-level hardware security
- 8-lead SOIC, 8-pad UDFN, and 3-lead CONTACT packages

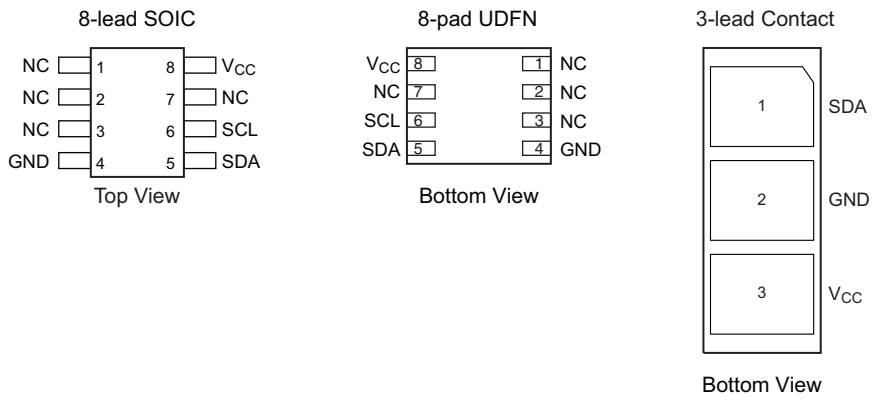
Applications

- Anti-clone for accessories, daughter cards, and consumables
- Secure boot validation — software anti-piracy
- Network and computer access control and password handling
- Authenticated/encrypted network communications

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

Figure 1. Pin Configurations

Pin Name	Function
NC	No Connect
GND	Ground
SDA	Serial Data
SCL	Serial Clock Input
V_{CC}	Power Supply



1. Introduction

1.1 Applications

The Atmel® ATECC108 is a member of the Atmel CryptoAuthentication™ family of high-security hardware authentication devices. It has a flexible command set that allows use for many applications, including the following:

- **Anti-Counterfeiting —** Validates that a removable, replaceable, or consumable client is authentic. Examples of clients could be system accessories, electronic daughter cards, or other spare parts. It can also be used to validate a software/firmware module or memory storage element.
- **Protection for Firmware or Media —** Validate code stored in flash memory at boot to prevent unauthorized modifications, encrypt downloaded program files as a common broadcast, or uniquely encrypt code images to be usable on a single system only.
- **Secure Data Storage —** Store secret keys for use by crypto accelerators in standard microprocessors. ATECC108 can also be used to store small quantities of data necessary for configuration, calibration, ePurse value, consumption data, or other secrets. Programmable protection is available using encrypted/authenticated reads and writes.
- **User Password Checking —** Validates user entered passwords without letting the expected value become known, map memorable passwords to random number, and securely exchange password values with remote system.

1.2 Device Features

ATECC108 includes an EEPROM array that can be used for storage of up to 16 keys, miscellaneous read/write, read-only or secret data, consumption logging, and security configuration. Access to the various sections of memory can be restricted in a variety of ways and then the configuration locked to prevent changes.

ATECC108 features a wide array of defensive mechanisms specifically designed to prevent physical attacks on the device itself or logical attacks on the data transmitted between the device and the system. Hardware restrictions on the ways in which keys are used or generated provide further defense against certain styles of attack.

Access to the device is through a standard I^2C Interface at speeds up to 1Mb/sec. It is compatible with standard Serial EEPROM I^2C interface specifications. The device also supports a Single-Wire Interface that can reduce the number of GPIOs required on the system processor and/or reduce the number of pins on connectors. Additionally, the device supports an alternative Single-Wire Interface compatible with other single-wire devices. If either Single-Wire Interface is enabled, the remaining pin is available for use as a GPIO. Contact Atmel for more details.

Using either the I^2C or Single-Wire Interface, multiple ATECC108 devices can share the same bus which saves processor GPIO usage in system with multiple clients such as different color ink tanks or multiple spare parts.

Each ATECC108 ships with a guaranteed unique 72-bit serial number. Using the cryptographic protocols supported by the device, a Host system or remote server can verify a signature to prove that the serial number is both authentic and not a copy. Serial numbers are often stored in a standard Serial EEPROM but these can be easily copied, and there is no way for the Host to know if the serial number is authentic or if it's a clone.

ATECC108 can generate high-quality FIPS random numbers and employ them for any purpose, including usage as part of the device's crypto protocols. Because each random number is guaranteed to be essentially unique from all numbers ever generated on this or any other device, their inclusion in the protocol calculation ensures that replay attacks (re-transmitting a previously successful transaction) always fails.

System integration is eased with a wide supply voltage range (2.0V – 5.5V) and an ultra-low sleep current of <150nA.

1.3 Cryptographic Operation

ATECC108 implements a complete asymmetric (public/private) key cryptographic signature solution based on Elliptic Curve Cryptography and the ECDSA signature protocol. The device features hardware acceleration for the NIST standard P256, B283, and K283 binary curves and supports the complete key life cycle from high quality private key generation, ECDSA signature generation and public key signature verification. The hardware accelerator can implement these asymmetric cryptographic operations 10 to 1,000 times faster than software running on standard microprocessors without the usual high risk of key exposure.

The device is designed to be able to securely store multiple private keys along with their public keys and the signature components of the corresponding certificates. The signature verification command can use any stored or external ECC public key. Public keys stored within the device can be configured to require validation via a certificate chain to speed up future device authentication.

Random private key generation is supported internally within the device to ensure that the private key can never be known outside the device. The public key corresponding to a stored private key is always returned when the key is generated and may optionally be computed at a later time.

ATECC108 also supports a standard hash-based challenge response protocol to simplify programming. At its most basic, the system sends a challenge to the device which combines that challenge with a secret key via the `MAC` command from the system, and sends the response back to the system. The device uses a SHA-256 cryptographic hash algorithm for the combination such that an observer on the bus cannot derive the value of the secret key, but the recipient can verify that the response is correct by performing the same calculation with a stored copy of the secret.

Due to the flexible command set of the ATECC108, these two basic operation sets (ECDSA signatures and SHA-256 challenge-response) can be expanded in many ways. Using the `GenDig` command, the values in other slots can be included in the response digest or signature, which provides an effective way of proving that a data read really did come from the device, as opposed to being inserted by a man-in-the-middle attacker. This same command can be used to combine two keys with the challenge, which is useful when there are multiple layers of authentication to be performed.

The `DeriveKey` command implements a key rolling scheme. Depending on the command mode parameter, the resulting operation can be similar to that implemented in a remote-controlled garage door opener. Each time the key is used, the current value of the key is cryptographically combined with a value specific to that system, and the result forms the key for the next cryptographic operation. Even if an attacker gets the value of one key, with the next use, that key will be gone forever.

The `DeriveKey` command can also be used to generate new random keys that might be valid only for a particular Host ID, for a particular time period, or for some other restricted environment. Each generated key is different than any other key ever generated on any device. By activating a Host-Client pair in the field in this manner, a clone of a single client will not work on any other Host.

In a Host-Client configuration, where the Host (for instance a mobile phone) needs to verify a client (for instance an OEM battery), there is a need to store the secret in the Host in order to validate the response from the client. The `CheckMac` command allows the device to securely store the secret in the Host system and hides the correct response value from the pins, returning only a *yes* or *no* answer to the system.

Where a user entered password is required, the `CheckMac` command also provides a way to both verify the password without exposing it on the communications bus, as well as, mapping the password into a stored value that can have a much higher entropy.

Finally, the hash combination of a challenge and secret key can be kept on the device and XOR'd with the contents of a slot to implement an encrypted `Read` command, or it can be XOR'd with encrypted input data to implement an encrypted `Write` command.

All hashing functions are implemented using the industry-standard SHA-256 secure hash algorithm, which is part of the latest set of high-security cryptographic algorithms recommended by various governments and cryptographic experts. If desired, the SHA-256 algorithm can also be included in a HMAC sequence. ATECC108 employs full-sized 256 bit secret keys to prevent any kind of exhaustive attack.

2. Electrical Characteristics

2.1 Absolute Maximum Ratings*

Operating Temperature . . . . . -40°C to 85°C

Storage Temperature . . . . . -65°C to 150°C

Maximum Operating Voltage 6.0V

DC Output Current. 5.0mA

Voltage on any pin. . . . . -0.5V to (V_{CC} + 0.5V)

*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 condition beyond those indicated in the operational sections of this specification is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

2.2 Reliability

ATECC108 is fabricated with the high reliability of the Atmel CMOS EEPROM manufacturing technology.

Table 2-1. EEPROM Reliability

Parameter	Min	Typical	Max	Units
Write Endurance (each byte)	100,000			Write Cycles
Data Retention (at 55°C)	10			Years
Data Retention (at 35°C)	30	50		Years
Read Endurance	Unlimited			Read Cycles

3. Ordering Information

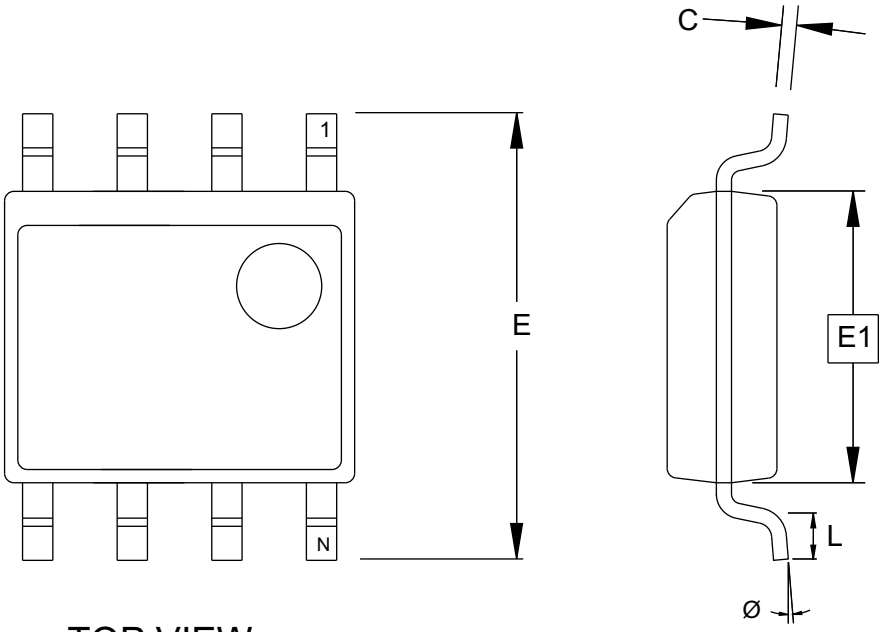
Ordering Code	Package	Interface Configuration
ATECC108-SSHCZ-T	SOIC, Tape and Reel(2)	Single-Wire
ATECC108-SSHCZ-B	SOIC, Bulk in Tubes(1)	Single-Wire
ATECC108-SSHDA-T	SOIC, Tape and Reel(2)	I^2C
ATECC108-SSHDA-B	SOIC, Bulk in Tubes(1)	I^2C
ATECC108-MAHCZ-T	UDFN, Tape and Reel(2)	Single-Wire
ATECC108-MAHDA-T	UDFN, Tape and Reel(2)	I^2C
ATECC108-RBHCZ-T(3)	3-lead CONTACT, Tape and Reel(2)	Single-Wire

Notes:
1. B = Bulk
2. T = Tape and reel
   - SOIC = 4K per reel
   - UDFN and CONTACT = 5K per reel
3. Please contact Atmel for availability.

8S1	8-lead 0.150” wide, Plastic Gull Wing Small Outline (JEDEC SOIC)
8MA2	8-pad, 2.0mm x 3.0mm x 0.6mm body, Thermally Enhanced Plastic Ultra Thin Dual Flat No Lead (UDFN)
3RB	3-lead 2.5mm x 6.5mm body, 2.0mm pitch, CONTACT (Sawn)

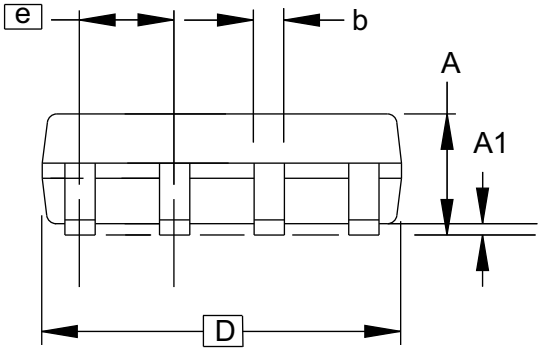
4. Package Drawings

4.1 8S1 — 8-lead SOIC



TOP VIEW

END VIEW



SIDE VIEW

COMMON DIMENSIONS
(Unit of Measure = mm)

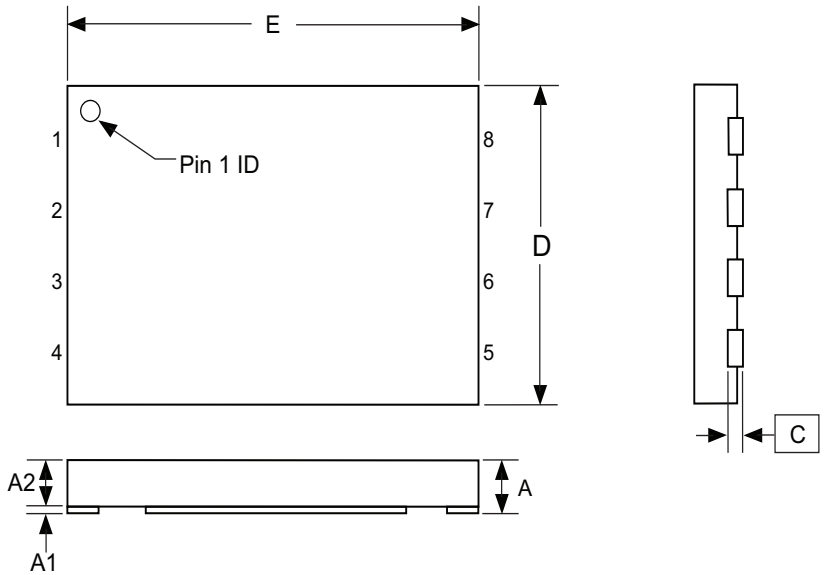
SYMBOL	MIN	NOM	MAX	NOTE
A	1.35	–	1.75	
A1	0.10	–	0.25	
b	0.31	–	0.51	
C	0.17	–	0.25	
D	4.80	–	5.05	
E1	3.81	–	3.99	
E	5.79	–	6.20	
e	1.27 BSC			
L	0.40	–	1.27	
Ø	0°	–	8°	

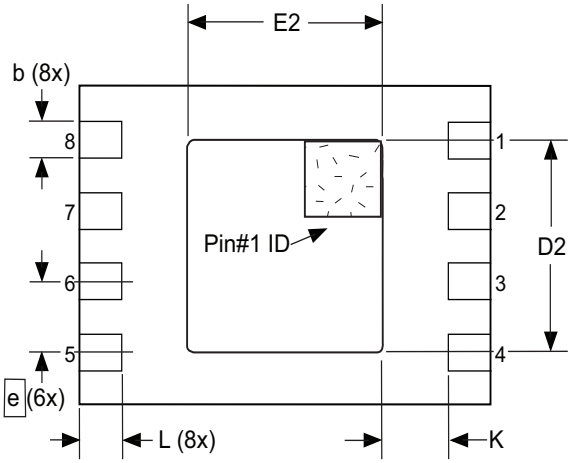
Notes: This drawing is for general information only. Refer to JEDEC Drawing MS-012, Variation AA for proper dimensions, tolerances, datums, etc.

6/22/11

Atmel Package Drawing Contact: packagedrawings@atmel.com	TITLE 8S1, 8-lead (0.150” Wide Body), Plastic Gull Wing Small Outline (JEDEC SOIC)	GPC SWB	DRAWING NO. 8S1	REV. G

4.2 8MA2 — 8-pad UDFN





COMMON DIMENSIONS
(Unit of Measure = mm)

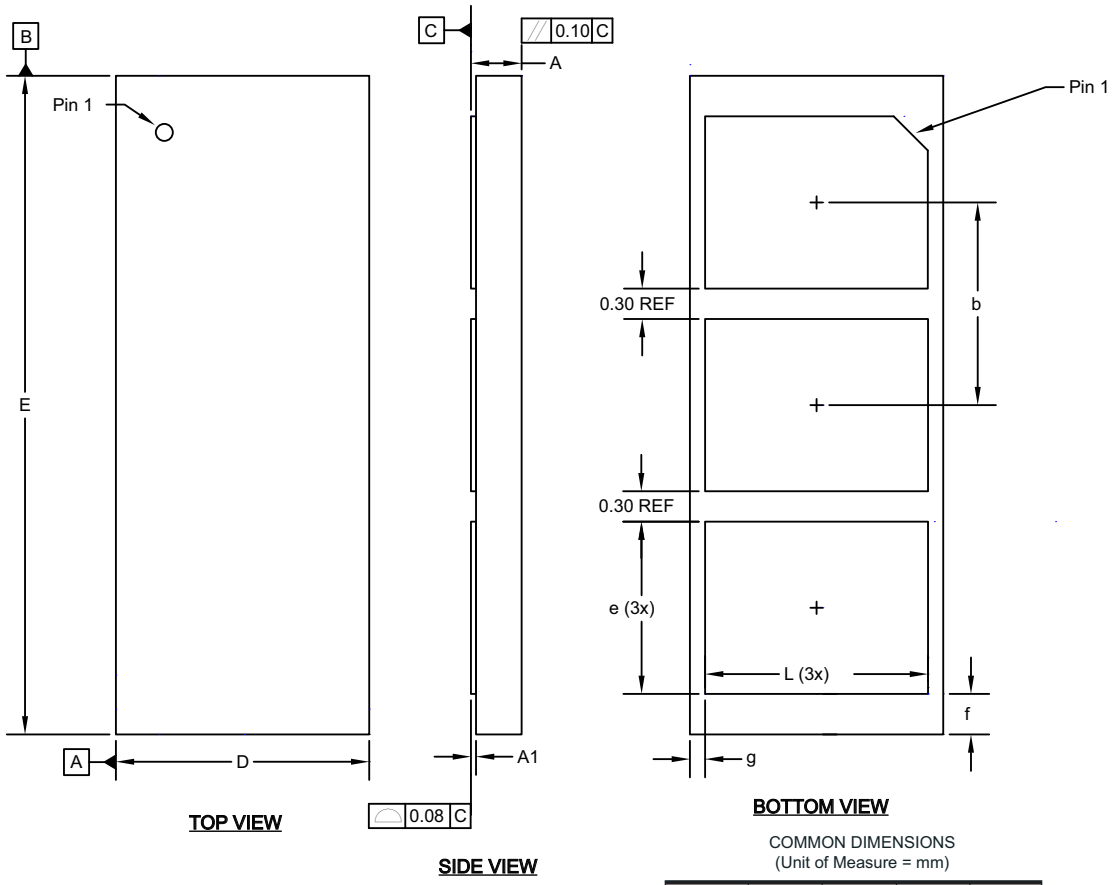
SYMBOL	MIN	NOM	MAX	NOTE
D	1.90	2.00	2.10	
E	2.90	3.00	3.10	
D2	1.40	1.50	1.60	
E2	1.20	1.30	1.40	
A	0.50	0.55	0.60	
A1	0.0	0.02	0.05	
A2	–	–	0.55	
C	0.152 REF			
L	0.30	0.35	0.40	
e	0.50 BSC			
b	0.18	0.25	0.30	3
K	0.20	–	–	

Notes:
1. This drawing is for general information only. Refer to JEDEC Drawing MO-229, for proper dimensions, tolerances, datums, etc.
2. The terminal #1 ID is a laser-marked feature.
3. 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.

9/6/12

Atmel Package Drawing Contact: packagedrawings@atmel.com	TITLE 8MA2, 8-pad, 2 x 3 x 0.6 mm Body, Thermally Enhanced Plastic Ultra Thin Dual Flat No Lead Package (UDFN)	GPC YNZ	DRAWING NO. 8MA2	REV. C

4.3 3RB — 3-lead CONTACT



COMMON DIMENSIONS
(Unit of Measure = mm)

SYMBOL	MIN	NOM	MAX	NOTE
D	2.40	2.50	2.60	
E	6.40	6.50	6.60	
A	0.45	0.50	0.55	
A1	0.0	-	0.05	
e	1.60	1.70	1.80	
b	2.00 BSC			
L	2.10	2.20	2.30	
f	0.30	0.40	0.50	
g	0.05	0.15	0.25	

12/16/11

Atmel Package Drawing Contact: packagedrawings@atmel.com	TITLE 3RB, 3-lead 2.5x6.5mm Body, 2.0 mm pitch, CONTACT PACKAGE. (Sawn)	GPC RHB	DRAWING NO. 3RB	REV. A

5. Revision History

Doc. Rev.	Date	Comments
8873BS	10/2013	Update UDFN and CONTACT ordering codes' note references.
8873AS	06/2013	Initial summary 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**

© 2013 Atmel Corporation. All rights reserved. / Rev.: Atmel-8873BS-CryptoAuth-ATECC108-Datasheet-Summary_102013.

Atmel®, Atmel logo and combinations thereof, Enabling Unlimited Possibilities®, 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.

SAFETY-CRITICAL, MILITARY, AND AUTOMOTIVE APPLICATIONS DISCLAIMER: Atmel products are not designed for and will not be used in connection with any applications where the failure of such products would reasonably be expected to result in significant personal injury or death (“Safety-Critical Applications”) without an Atmel officer's specific written consent. Safety-Critical Applications include, without limitation, life support devices and systems, equipment or systems for the operation of nuclear facilities and weapons systems. Atmel products are not designed nor intended for use in military or aerospace applications or environments unless specifically designated by Atmel as military-grade. Atmel products are not designed nor intended for use in automotive applications unless specifically designated by Atmel as automotive-grade.