

Atmel CryptoAuthentication Device

SUMMARY DATASHEET

CryptoAuthentication

Ensures Things and Code are Real, Untampered, and Confidential



Secure Download and Boot

Authentication and Protect Code In-transit

Ecosystem Control

Ensure Only OEM/Licensed Nodes and Accessories Work

Anti-cloning

Prevent Building with Identical BOM or Stolen Code

Message Security

Authentication, Message Integrity, and Confidentiality of Network Nodes (IoT)

Features

- Cryptographic Co-processor with Secure Hardware-based Key Storage
- Performs High-Speed Public Key (PKI) Algorithms
 - ECDSA: FIPS186-3 Elliptic Curve Digital Signature Algorithm
 - ECDH: FIPS SP800-56A Elliptic Curve Diffie-Hellman Algorithm
- NIST Standard P256 Elliptic Curve Support
- SHA-256 Hash Algorithm with HMAC Option
- Host and Client Operations
- 256-bit Key Length
- Storage for up to 16 Keys
- Two high-endurance monotonic counters
- Guaranteed Unique 72-bit Serial Number
- Internal High-quality FIPS Random Number Generator (RNG)
- 10Kb EEPROM Memory for Keys, Certificates, and Data
- Storage for up to 16 Keys
- Multiple Options for Consumption Logging and One Time Write Information
- Intrusion Latch for External Tamper Switch or Power-on Chip Enablement.
- Multiple I/O Options:
 - High-speed Single Pin Interface, with One GPIO Pin
 - 1MHz Standard I²C Interface
- 2.0V to 5.5V Supply Voltage Range
- 1.8V to 5.5V IO levels
- <150nA Sleep Current
- 8-pad UDFN, 8-lead SOIC, and 3-lead CONTACT Packages

Applications

- IoT Node Security and ID
- Secure Download and Boot
- Ecosystem Control
- Message Security
- Anti-Cloning

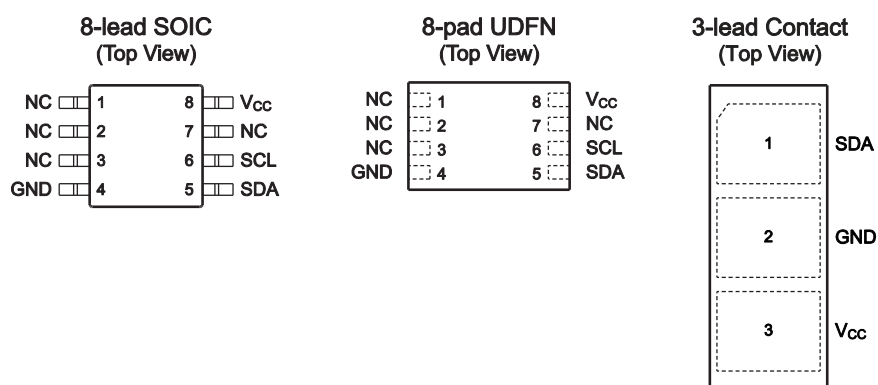
**This is a summary document.
The complete document is
available under NDA. For more
information, please contact
your local Atmel sales office.**

Pin Configuration and Pinouts

Table 1. Pin Configuration

| Pin | Function |
|-----------------|--------------------|
| NC | No Connect |
| GND | Ground |
| SDA | Serial Data |
| SCL | Serial Clock Input |
| V _{CC} | Power Supply |

Figure 1. Pinouts



1 Introduction

1.1 Applications

The Atmel® ATECC508A is a member of the Atmel CryptoAuthentication™ family of crypto engine authentication devices with highly secure hardware-based key storage.

The ATECC508A has a flexible command set that allows use in many applications, including the following, among many others:

- **Network/IoT Node Protection**
Authenticates node IDs, ensures the integrity of messages, and supports key agreement to create session keys for message encryption.
- **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.
- **Protecting Firmware or Media**
Validates 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.
- **Storing Secure Data**
Store secret keys for use by crypto accelerators in standard microprocessors. Programmable protection is available using encrypted/authenticated reads and writes.
- **Checking User Password**
Validates user-entered passwords without letting the expected value become known, maps memorable passwords to a random number, and securely exchanges password values with remote systems.

1.2 Device Features

The ATECC508A includes an EEPROM array which can be used for storage of up to 16 keys, certificates, miscellaneous read/write, read-only or secret data, consumption logging, and security configurations. Access to the various sections of memory can be restricted in a variety of ways and then the configuration can be locked to prevent changes.

The ATECC508A features a wide array of defense 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 made through a standard I²C Interface at speeds of up to 1Mb/s. The interface is compatible with standard Serial EEPROM I²C interface specifications. The device also supports a Single-Wire Interface (SWI), which can reduce the number of GPIOs required on the system processor, and/or reduce the number of pins on connectors. If the Single-Wire Interface is enabled, the remaining pin is available for use as a GPIO, an authenticated output or tamper input.

Using either the I²C or Single-Wire Interface, multiple ATECC508A devices can share the same bus, which saves processor GPIO usage in systems with multiple clients such as different color ink tanks or multiple spare parts, for example.

Each ATECC508A 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 of the serial number to prove that the serial number is authentic and not a copy. Serial numbers are often stored in a standard Serial EEPROM; however, these can be easily copied with no way for the host to know if the serial number is authentic or if it is a clone.

The ATECC508A 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 (i.e. re-transmitting a previously successful transaction) will always fail.

System integration is easy due to a wide supply voltage range (of 2.0V to 5.5V) and an ultra-low sleep current (of <150nA). Multiple package options are available.

See Section 3 for information regarding compatibility with the Atmel ATSHA204 and ATECC108.

1.3 Cryptographic Operation

The ATECC508A implements a complete asymmetric (public/private) key cryptographic signature solution based upon Elliptic Curve Cryptography and the ECDSA signature protocol. The device features hardware acceleration for the NIST standard P256 prime curve and supports the complete key life cycle from high quality private key generation, to ECDSA signature generation, ECDH key agreement, and ECDSA public key signature verification.

The hardware accelerator can implement such asymmetric cryptographic operations from ten to one-thousand times faster than software running on standard microprocessors, without the usual high risk of key exposure that is endemic to standard microprocessors.

The device is designed to securely store multiple private keys along with their associated public keys and certificates. The signature verification command can use any stored or an external ECC public key. Public keys stored within the device can be configured to require validation via a certificate chain to speed-up subsequent device authentications.

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

The ATECC508A also supports a standard hash-based challenge-response protocol in order to simplify programming. In its most basic instantiation, the system sends a challenge to the device, which combines that challenge with a secret key and then sends the response back to the system. The device uses a SHA-256 cryptographic hash algorithm to make that combination so that an observer on the bus cannot derive the value of the secret key, but preserving that ability of a recipient to verify that the response is correct by performing the same calculation with a stored copy of the secret on the recipient's system.

Due to the flexible command set of the ATECC508A, these basic operation sets (i.e. ECDSA signatures, ECDH key agreement and SHA-256 challenge-response) can be expanded in many ways.

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.

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 government agencies and cryptographic experts. The ATECC508A 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 | 5mA |
| 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 conditions beyond those indicated in the operational sections of this specification are not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

2.2 Reliability

The ATECC508A is fabricated with the Atmel high reliability of the CMOS EEPROM manufacturing technology.

Table 2-1. EEPROM Reliability

| Parameter | Min | Typical | Max | Units |
|-------------------------------------|-----------|---------|-----|--------------|
| Write Endurance at 85°C (Each Byte) | 400,000 | | | Write Cycles |
| Data Retention at 55°C | 10 | | | Years |
| Data Retention at 35°C | 30 | 50 | | Years |
| Read Endurance | Unlimited | | | Read Cycles |

2.3 AC Parameters: All I/O Interfaces

Figure 2-1. AC Parameters: All I/O Interfaces

| Parameter ⁽¹⁾ | Symbol | Direction | Min | Typ | Max | Unit | Notes |
|-----------------------------------|------------------------|--------------------------|-------------------|-----|-----|------|---|
| Power-Up Delay | t _{PU} | To Crypto Authentication | 100 | | — | μs | Minimum time between V _{CC} > V _{CC} min prior to measurement of t _{WLO} . |
| Wake Low Duration | t _{WLO} | To Crypto Authentication | 60 | | — | μs | |
| Wake High Delay to Data Comm. | t _{WHI} | To Crypto Authentication | 500 | | | μs | SDA should be stable high for this entire duration. |
| High Side Glitch Filter at Active | t _{HIGNORE_A} | To Crypto Authentication | 45 ⁽¹⁾ | | | ns | Pulses shorter than this in width will be ignored by the device, regardless of its state when active. |
| Low Side Glitch Filter at Active | t _{LIGNORE_A} | To Crypto Authentication | 45 ⁽¹⁾ | | | ns | Pulses shorter than this in width will be ignored by the device, regardless of its state when active. |
| Low Side Glitch Filter at Sleep | t _{LIGNORE_S} | To Crypto Authentication | 15 ⁽¹⁾ | | | μs | Pulses shorter than this in width will be ignored by the device when in sleep mode. |
| Watchdog Timeout | t _{WATCHDOG} | To Crypto Authentication | 0.7 | 1.3 | 1.7 | s | Maximum time from wake until device is forced into sleep mode. |

Note: 1. These parameters are guaranteed through characterization, but not tested.

2.3.1 AC Parameters: Single-Wire Interface

Table 2-2. AC Parameters: Single-Wire Interface

Applicable from $T_A = -40^{\circ}\text{C}$ to $+85^{\circ}\text{C}$, $V_{CC} = +2.0\text{V}$ to $+5.5\text{V}$, $C_L = 100\text{pF}$ (unless otherwise noted).

| Parameter | Symbol | Direction | Min | Typ | Max | Unit | Notes |
|------------------------------|-------------------------|----------------------------|------|------|------|---------------|---|
| Start Pulse Duration | t_{START} | To Crypto Authentication | 4.10 | 4.34 | 4.56 | μs | |
| | | From Crypto Authentication | 4.60 | 6 | 8.60 | μs | |
| Zero Transmission High Pulse | t_{ZHI} | To Crypto Authentication | 4.10 | 4.34 | 4.56 | μs | |
| | | From Crypto Authentication | 4.60 | 6 | 8.60 | μs | |
| Zero Transmission Low Pulse | t_{ZLO} | To Crypto Authentication | 4.10 | 4.34 | 4.56 | μs | |
| | | From Crypto Authentication | 4.60 | 6 | 8.60 | μs | |
| Bit Time ⁽¹⁾ | t_{BIT} | To Crypto Authentication | 37 | 39 | — | μs | If the bit time exceeds t_{TIMEOUT} then ATECC508A may enter the sleep mode. |
| | | From Crypto Authentication | 41 | 54 | 78 | μs | |
| Turn Around Delay | $t_{\text{TURNAROUND}}$ | From Crypto Authentication | 64 | 96 | 131 | μs | ATECC508A will initiate the first low going transition after this time interval following the initial falling edge of the start pulse of the last bit of the transmit flag. |
| | | To Crypto Authentication | 93 | | | μs | After ATECC508A transmits the last bit of a group, system must wait this interval before sending the first bit of a flag. It is measured from the falling edge of the start pulse of the last bit transmitted by ATECC508A. |
| IO Timeout | t_{TIMEOUT} | To Crypto Authentication | 45 | 65 | 85 | ms | ATECC508A may transition to the sleep mode if the bus is inactive longer than this duration. |

Note: 1. START, ZLO, ZHI, and BIT are designed to be compatible with a standard UART running at 230.4Kbaud for both transmit and receive. The UART should be set to seven data bits, no parity and one Stop bit.

2.3.2 AC Parameters: I²C Interface

Table 2-3. AC Characteristics of I²C Interface

Applicable over recommended operating range from TA = -40°C to + 85°C, V_{CC} = +2.0V to +5.5V, CL = 1 TTL Gate and 100pF (unless otherwise noted).

| Symbol | Parameter | Min | Max | Units |
|----------------------|---|-----|-----|-------|
| f _{SCK} | SCK Clock Frequency | 0 | 1 | MHz |
| t _{HIGH} | SCK High Time | 400 | | ns |
| t _{LOW} | SCK Low Time | 400 | | ns |
| t _{SU.STA} | Start Setup Time | 250 | | ns |
| t _{HD.STA} | Start Hold Time | 250 | | ns |
| t _{SU.STO} | Stop Setup Time | 250 | | ns |
| t _{SU.DAT} | Data In Setup Time | 100 | | ns |
| t _{HD.DAT} | Data In Hold Time | 0 | | ns |
| t _R | Input Rise Time ⁽¹⁾ | | 300 | ns |
| t _F | Input Fall Time ⁽¹⁾ | | 100 | ns |
| t _{AA} | Clock Low to Data Out Valid | 50 | 550 | ns |
| t _{DH} | Data Out Hold Time | 50 | | ns |
| t _{TIMEOUT} | SMBus Timeout Delay | 25 | 75 | ms |
| t _{BUF} | Time bus must be free before a new transmission can start. ⁽¹⁾ | 500 | | ns |

Note: 1. Values are based on characterization and are not tested.

AC measurement conditions:

- RL (connects between SDA and V_{CC}): 1.2k (for V_{CC} +2.0V to +5.0V)
- Input pulse voltages: 0.3V_{CC} to 0.7V_{CC}
- Input rise and fall times: ≤ 50ns
- Input and output timing reference voltage: 0.5V_{CC}

2.4 DC Parameters: All I/O Interfaces

Table 2-4. DC Parameters on All I/O Interfaces

| Parameter | Symbol | Min | Typ | Max | Unit | Notes |
|-------------------------------|---------------|-----|-----|-----|------|---|
| Ambient Operating Temperature | T_A | -40 | | 85 | °C | |
| Power Supply Voltage | V_{CC} | 2.0 | | 5.5 | V | |
| Active Power Supply Current | I_{CC} | | 3 | 6 | mA | Waiting for I/O during I/O transfers or execution of non-ECC commands when ChipMode:3 is zero. |
| | | | — | 16 | mA | During ECC command execution. |
| Idle Power Supply Current | I_{IDLE} | | 800 | | µA | When device is in idle mode, V_{SDA} and $V_{SCL} < 0.4V$ or $> V_{CC} - 0.4$ |
| Sleep Current | I_{SLEEP} | | 30 | 150 | nA | When device is in sleep mode, $V_{CC} \leq 3.6V$, V_{SDA} and $V_{SCL} < 0.4V$ or $> V_{CC} - 0.4$, $T_A \leq 55^\circ C$ |
| | | | | 2 | µA | When device is in sleep mode. |
| Output Low Voltage | V_{OL} | | | 0.4 | V | When device is in active mode, $V_{CC} = 2.5 - 5.5V$ |
| Output Low Current | I_{OL} | | | 4 | mA | When device is in active mode, $V_{CC} = 2.5 - 5.5V$, $V_{OL} = 0.4V$ |
| Theta JA | Θ_{JA} | | 166 | | °C/W | SOIC (SSH) |
| | | | 173 | | °C/W | UDFN (MAH) |
| | | | 146 | | °C/W | RBH |

2.4.1 V_{IH} and V_{IL} Specifications

The input voltage thresholds when in sleep or idle mode are dependent on the V_{CC} level as shown in the graph below. When the device is active (i.e. not in sleep or idle mode), the input voltage thresholds are different depending upon the state of TTLenable (bit 1) within the ChipMode byte in the Configuration zone of the EEPROM. When a common voltage is used for the ATECC508A V_{CC} pin and the input pull-up resistor, then this bit should be set to a one, which permits the input thresholds to track the supply.

If the voltage supplied to the V_{CC} pin of the ATECC508A is different than the system voltage to which the input pull-up resistor is connected, then the system designer may choose to set TTLenable to zero, which enables a fixed input threshold according to the following table. The following applies only when the device is active:

Table 2-5. V_{IL} , V_{IH} on All I/O Interfaces

| Parameter | Symbol | Min | Typ | Max | Unit | Notes |
|--------------------|----------|------|-----|----------------|------|---|
| Input Low Voltage | V_{IL} | -0.5 | | 0.5 | V | When device is active and TTLenable bit in configuration memory is zero; otherwise see above. |
| Input High Voltage | V_{IH} | 1.5 | | $V_{CC} + 0.5$ | V | When device is active and TTLenable bit in configuration memory is zero; otherwise see above. |

3 Compatibility

3.1 Atmel ATSHA204

ATECC508A is fully compatible with the ATSHA204 and ATSHA204A devices. If properly configured, it can be used in all situations where the ATSHA204 or ATSHA204A is currently employed. Because the Configuration zone is larger, the personalization procedures for the device must be updated when personalizing the ATSHA204 or ATSHA204A.

3.2 Atmel ATECC108

ATECC508A is designed to be fully compatible with the ATECC108 and ATECC108A devices. If properly configured, can be used in all situations where ATECC108 is currently employed. In many situations, the ATECC508A can also be used in an ATECC108 application without change. The new revisions provide significant advantages as outlined below:

New Features in ATECC108A vs. ATECC108

- Intrusion Detection Capability, Including Gating Key Use
- New SHA Command, Also Computes HMAC
- X.509 Certificate Verification Capability
- Programmable Watchdog Timer Length
- Programmable Power Reduction
- Shared Random Nonce and Key Configuration Validation (Gendig Command)
- Larger Slot 8 which is Extended to 416 bytes

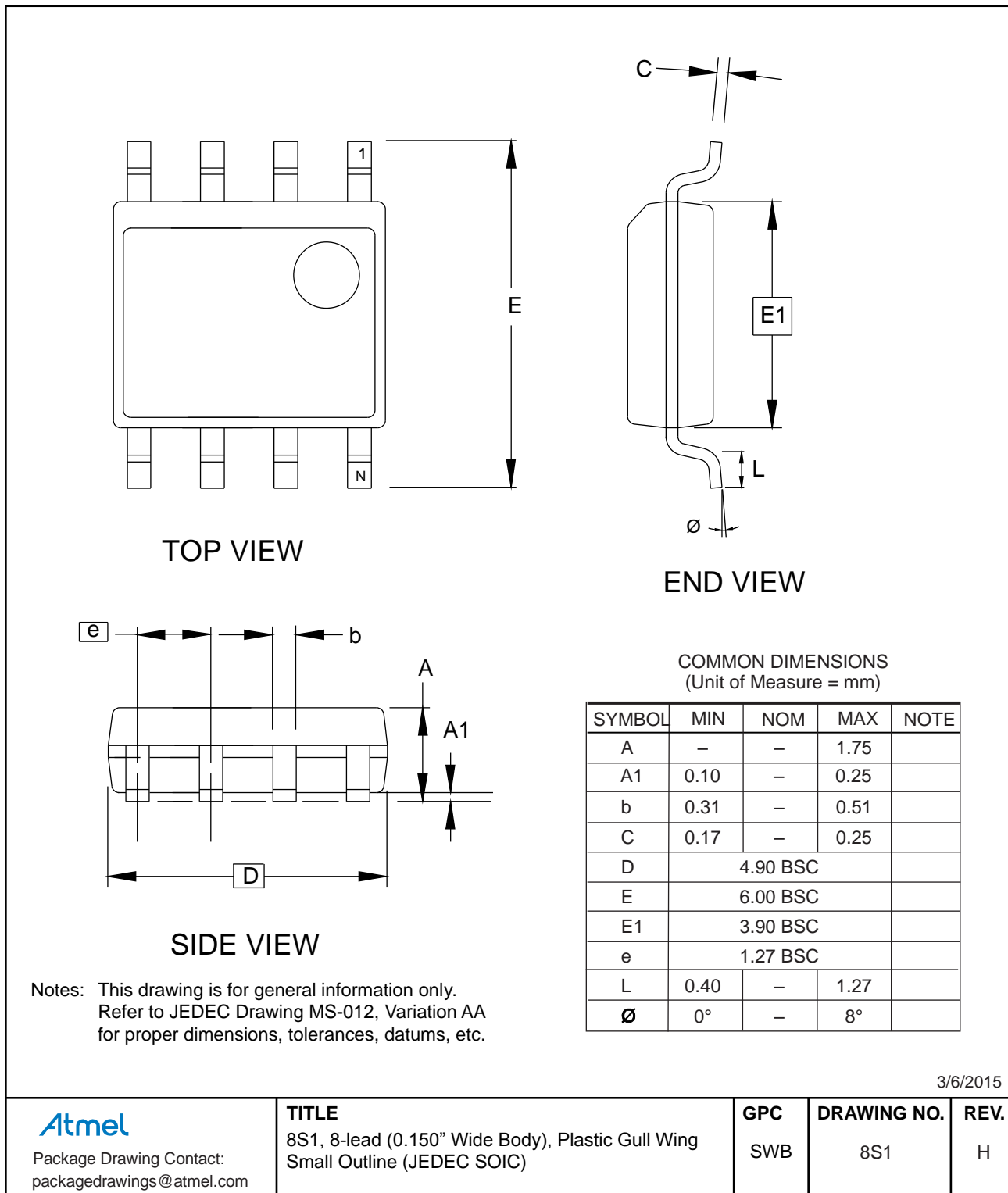
4 Ordering Information

| Atmel Ordering Code ⁽²⁾ | Package | Delivery Information | | Interface Configuration |
|------------------------------------|----------------|----------------------|-----------------|-------------------------|
| | | Form | Quantity | |
| ATECC508A-SSHCZ-T | 8-lead SOIC | Tape and Reel | 4,000 per Reel | Single-Wire |
| ATECC508A-SSHCZ-B | | Bulk in Tubes | 100 per Tube | |
| ATECC508A-SSHDA-T | | Tape and Reel | 4,000 per Reel | I ² C |
| ATECC508A-SSHDA-B | | Bulk in Tubes | 100 per Tube | |
| ATECC508A-MAHCZ-T | 8-pad UDFN | Tape and Reel | 15,000 per Reel | Single-Wire |
| ATECC508A-MAHDA-T | | | | I ² C |
| ATECC508A-MAHCZ-S | | | 3,000 per Reel | Single-Wire |
| ATECC508A-MAHDA-S | | | | I ² C |
| ATECC508A-RBHCZ-T ⁽¹⁾ | 3-lead CONTACT | Tape and Reel | 5,000 per Reel | Single-Wire |

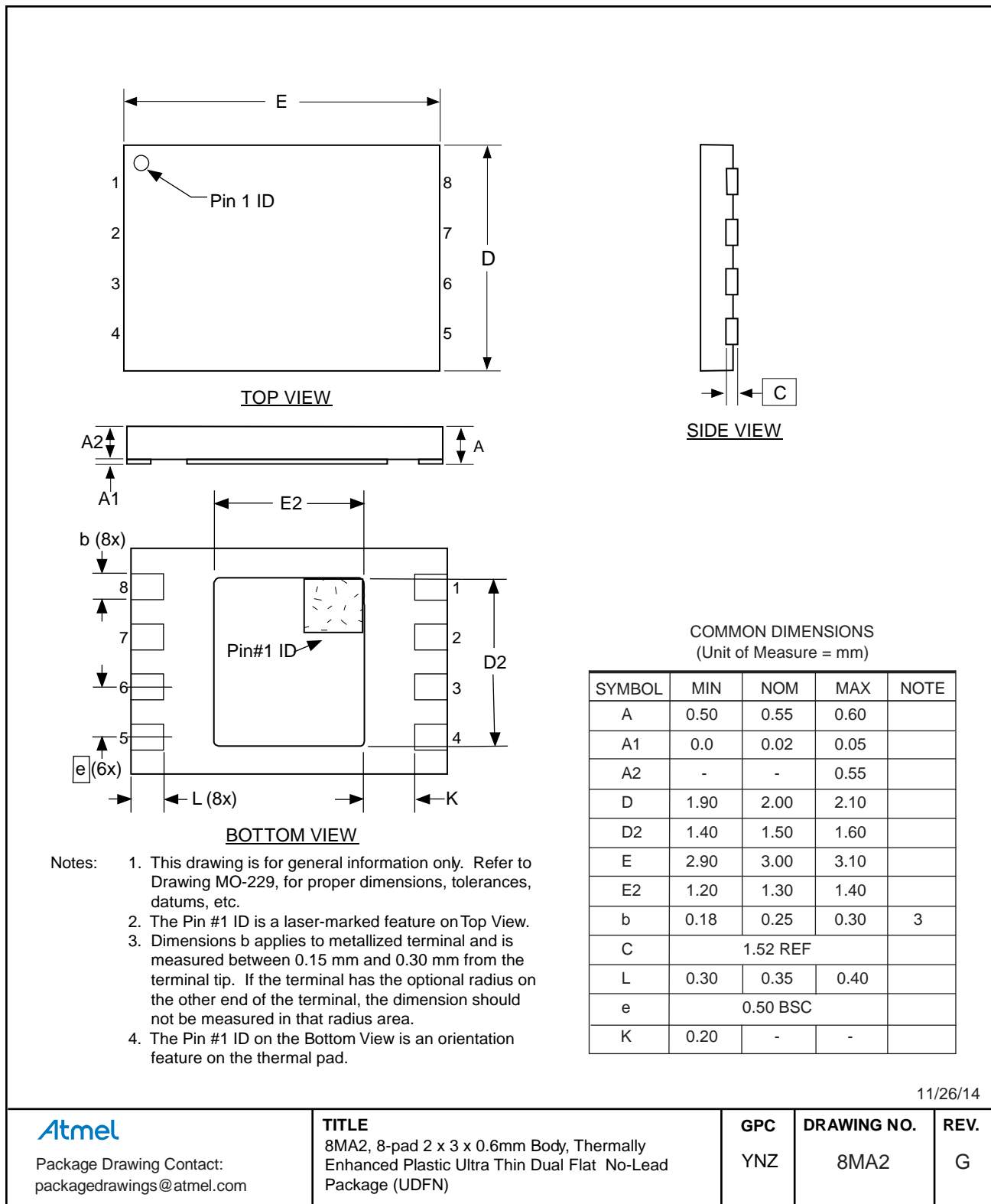
Notes: 1. Please contact Atmel for availability.
2. Please contact Atmel for thinner packages.

5 Package Drawings

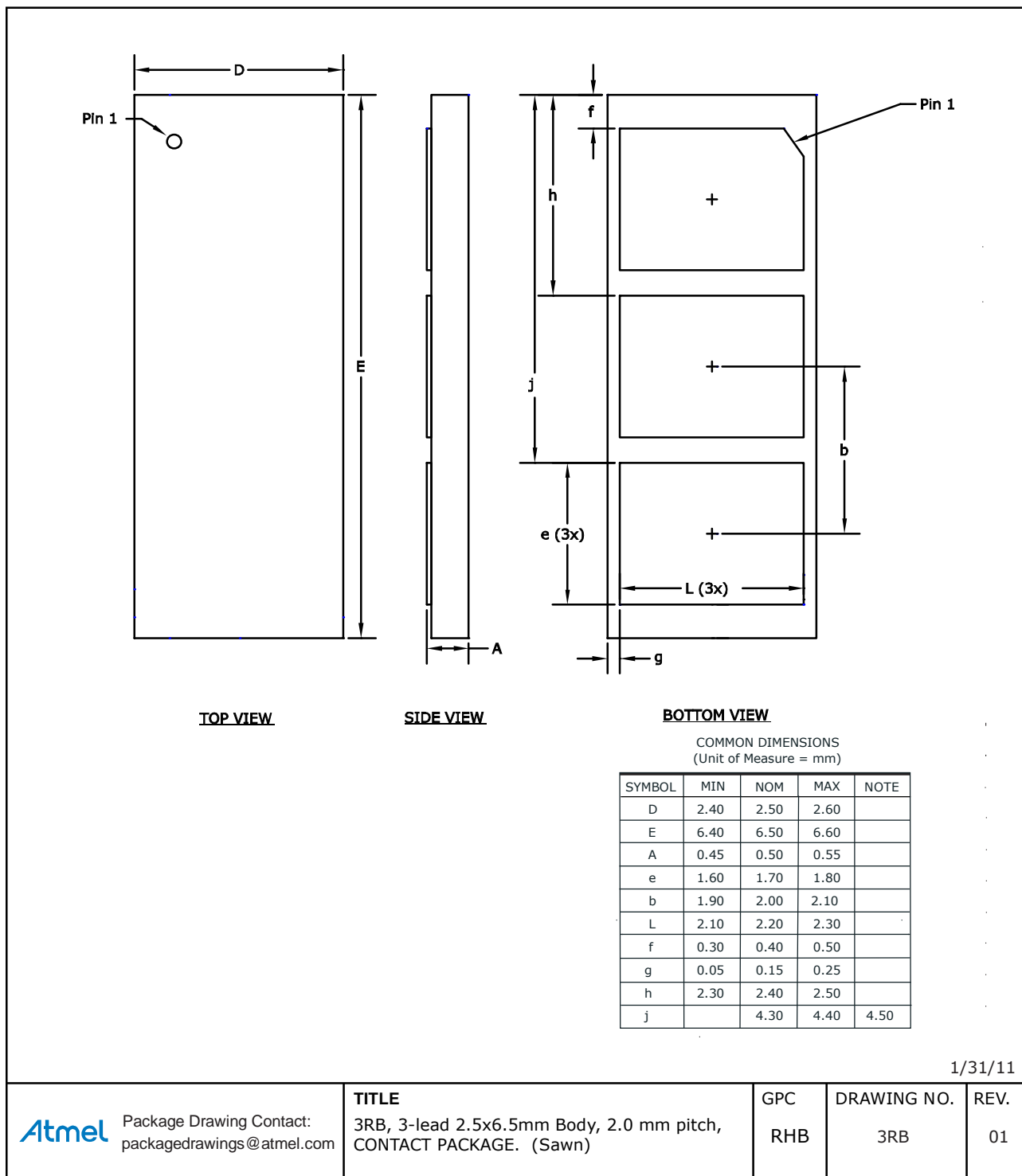
5.1 8-lead SOIC



5.2 8-pad UDFN



5.3 3-lead CONTACT



6 Revision History

| Doc. Rev. | Date | Comments |
|-----------|---------|--|
| 8922BX | 10/2015 | Updated introduction and applications, EEPROM Reliability – Write Endurance, 8S1 package drawing, and ordering information. Added MAHCZ-S and MAHDA-S UDFN options. |
| 8922AX | 02/2015 | Initial summary document release. |

Security at our Core

Atmel Has You Covered



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

© 2015 Atmel Corporation. / Rev.:Atmel-8923BS-CryptoAuth-ATECC508A-Datasheet-Summary_102015.

Atmel®, Atmel logo and combinations thereof, Enabling Unlimited Possibilities®, CryptoAuthentication™, and others are registered trademarks or trademarks of Atmel Corporation in U.S. and other countries.

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.