



#### Features

- One of a family of devices with user memories from 1Kbit to 8Kbit
- 2Kbit (256-byte) EEPROM user memory
  - Four 512-bit (64-byte) zones
  - Self-timed write cycle
  - Single byte or 16-byte page write mode
  - Programmable access rights for each zone
- 2Kbit configuration zone
  - 37-byte OTP (One-time Programmable) area for user-defined codes
  - 160-byte area for user-defined keys and passwords
- High security features
  - 64-bit mutual authentication protocol (under license of ELVA)
  - Cryptographic Message Authentication Codes (MAC)
  - Stream encryption
  - Four key sets for authentication and encryption
  - Eight sets of two 24-bit passwords
  - Anti-tearing function
  - Voltage and frequency monitors
- Smart card features
  - ISO 7816 Class B (3V) operation
  - ISO 7816-3 asynchronous T=0 protocol (Gemplus® Patent) \*
  - Multiple zones, key sets and passwords for multi-application use
  - Synchronous two-wire serial interface for faster device initialization \*
  - Programmable 8-byte answer-to-reset register
  - ISO 7816-2 compliant modules
- Embedded application features
  - Low voltage supply: 2.7V – 3.6V
  - Secure nonvolatile storage for sensitive system or user information
  - Two-wire serial interface (TWI, 5V compatible)
  - 1.0MHz compatibility for fast operation
  - Standard 8-lead plastic packages, green compliant (exceeds RoHS)
  - Same pin configuration as Atmel® AT24CXXX Serial EEPROM in SOIC and PDIP packages
- High reliability
  - Endurance: 100,000 cycles
  - Data retention: 10 years
  - ESD protection: 2,000V min

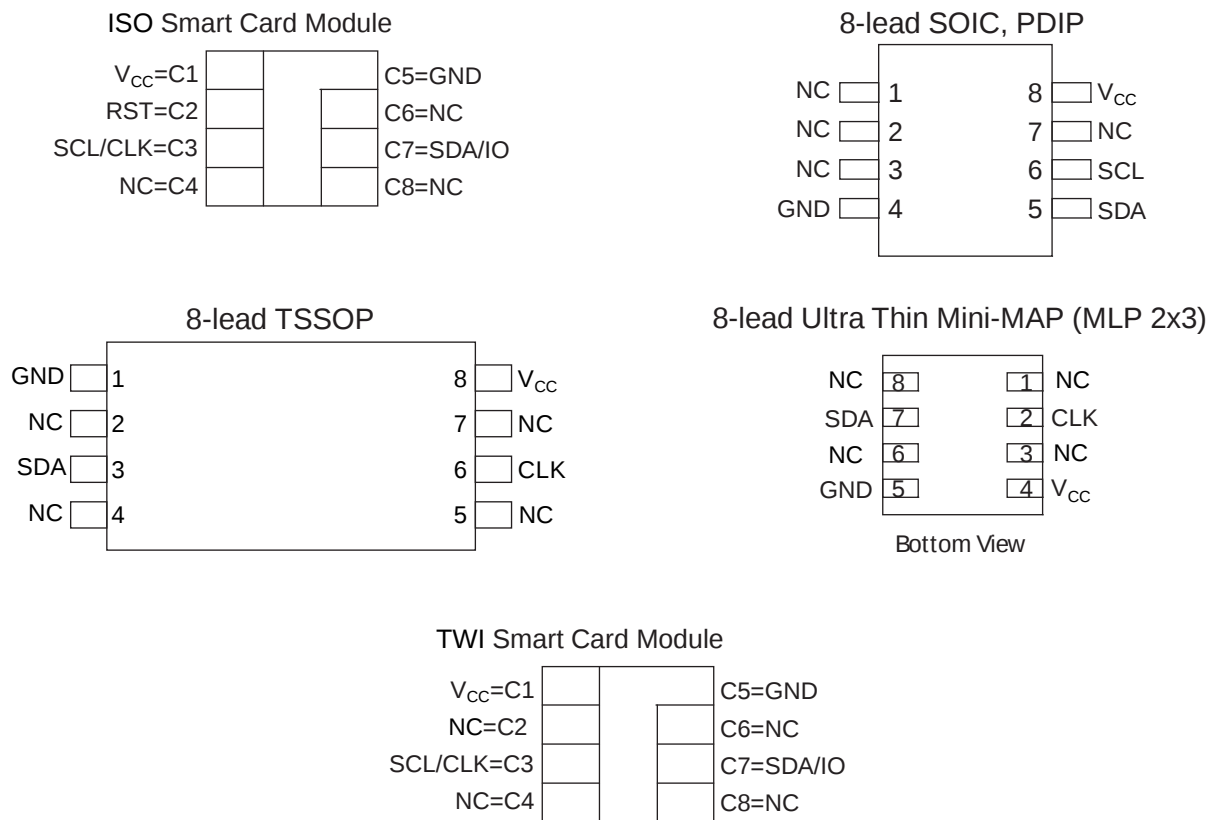
This is a summary document.  
The complete document is  
available on the Atmel website  
at [www.atmel.com](http://www.atmel.com).

\* Note: Modules available with either T = 0 / 2-wire modes or 2-wire mode only

**Table 1. Pin Assignments**

| Pad             | Description              | ISO Module | TWI Module | “SOIC, PDIP” | TSSOP | Mini-MAP |
|-----------------|--------------------------|------------|------------|--------------|-------|----------|
| V <sub>CC</sub> | Supply Voltage           | C1         | C1         | 8            | 8     | 4        |
| GND             | Ground                   | C5         | C5         | 4            | 1     | 5        |
| SCL/CLK         | Serial Clock Input       | C3         | C3         | 6            | 6     | 2        |
| SDA/IO          | Serial Data Input/Output | C7         | C7         | 5            | 3     | 7        |
| RST             | Reset Input              | C2         | NC         | NC           | NC    | NC       |

**Figure 1. Pin Configuration**



## 1. Description

The Atmel AT88SC0204CA member of the Atmel CryptoMemory® family is a high-performance secure memory providing 2Kbit of user memory with advanced security and cryptographic features built in. The user memory is divided into four 64-byte zones, each of which may be individually set with different security access rights or effectively combined together to provide space for one to four data files. The AT88SC0204CA features an enhanced command set that allows direct communication with microcontroller hardware two-wire interface thereby allowing for faster firmware development with reduced code space requirements.

### 1.1 Smart Card Applications

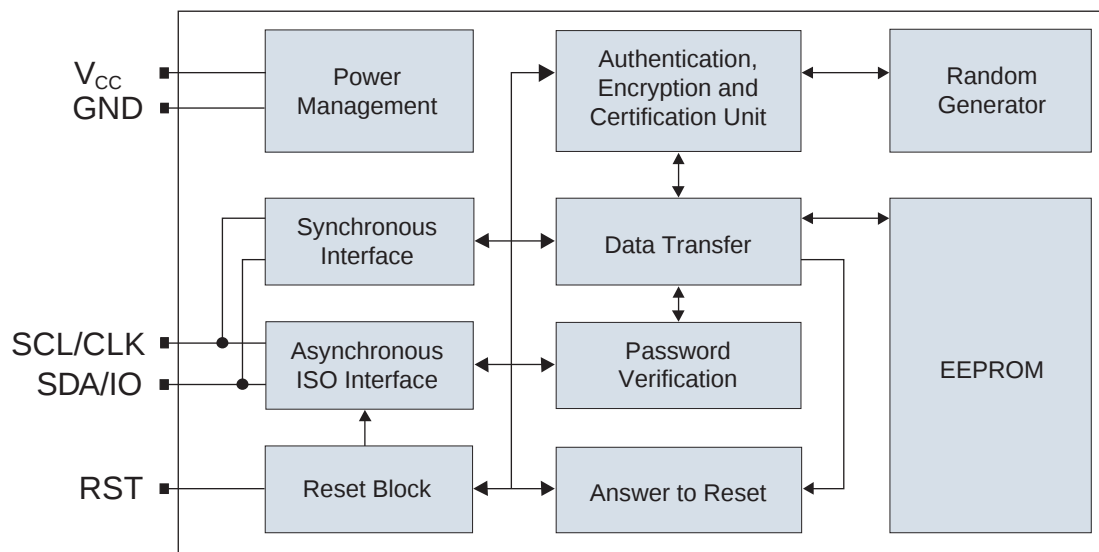
The AT88SC0204CA provides high security, low cost, and ease of implementation without the need for a microprocessor operating system. The embedded cryptographic engine provides for dynamic, symmetric-mutual authentication between the device and host, as well as performing stream encryption for all data and passwords exchanged between the device and host. Up to four unique key sets may be used for these operations. The AT88SC0204CA offers the ability to communicate with virtually any smart card reader using the asynchronous T = 0 protocol (Gemplus Patent) defined in ISO 7816-3.

### 1.2 Embedded Applications

Through dynamic, symmetric-mutual authentication, data encryption, and the use of cryptographic Message Authentication Codes (MAC), the AT88SC0204CA provides a secure place for storage of sensitive information within a system. With its tamper detection circuits, this information remains safe even under attack. A two-wire serial interface running at speeds up to 1.0MHz provides fast and efficient communications with up to 15 individually addressable devices. The AT88SC0204CA is available in industry standard 8-lead packages with the same familiar pin configuration as AT24CXXX Serial EEPROM devices.

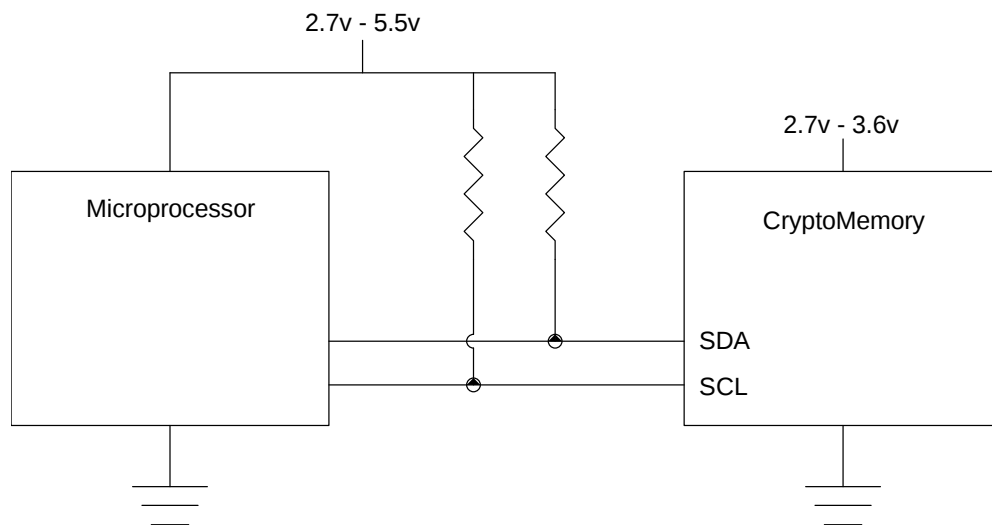
Note: Does not apply to either the TSSOP or the Ultra Thin Mini-Map pinouts

Figure 1-1. Block Diagram



## 2. Connection Diagram

Figure 2-1. Connection Diagram



## 3. Pin Descriptions

### 3.1 Supply Voltage ( $V_{CC}$ )

The  $V_{CC}$  input is a 2.7V to 3.6V positive voltage supplied by the host.

### 3.2 Clock (SCL/CLK)

When using the asynchronous  $T = 0$  protocol, the CLK (SCL) input provides the device with a carrier frequency  $f$ . The nominal length of one bit emitted on I/O is defined as an “elementary time unit” (ETU) and is equal to  $372/f$ .

When using the synchronous protocol, data clocking is done on the positive edge of the clock when writing to the device and on the negative edge of the clock when reading from the device.

### 3.3 Reset (RST)

The AT88SC0204CA provides an ISO 7816-3 compliant asynchronous answer-to-reset (ATR) sequence. Upon activation of the reset sequence, the device outputs bytes contained in the 64-bit ATR register. An internal pull-up on the RST input pad allows the device to operate in synchronous mode without bonding RST. The AT88SC0204CA does not support an ATR sequence in the synchronous mode of operation.

### 3.4 Serial Data (SDA/IO)

The SDA/IO pin is bidirectional for serial data transfer. This pin is open-drain driven and may be wired with any number of other open-drain or open-collector devices. An external pull-up resistor should be connected between SDA/IO and  $V_{CC}$ . The value of this resistor and the system capacitance loading the SDA/IO bus will determine the rise time of SDA/IO. This rise time will determine the maximum frequency during read operations. Low value pull-up resistors will allow higher frequency operations while drawing higher average power supply current. SDA/IO information applies to both asynchronous and synchronous protocols.

## 4. \*Absolute Maximum Ratings

|                                                    |                         |
|----------------------------------------------------|-------------------------|
| Operating temperature.....                         | -40°C to +85°C          |
| Storage temperature .....                          | -65°C to + 150°C        |
| Voltage on any pin<br>with respect to ground ..... | - 0.7 to $V_{CC}$ +0.7V |
| Maximum operating voltage.....                     | 4.0V                    |
| DC output current .....                            | 5.0mA                   |

**\*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 of time may affect device reliability.

**Table 4-1. DC Characteristics**

Applicable over recommended operating range from  $V_{CC} = +2.7$  to 3.6V,  $T_{AC} = -40^{\circ}\text{C}$  to  $+85^{\circ}\text{C}$  (unless otherwise noted)

| Symbol         | Parameter                  | Test Conditions                       | Min                 | Typ | Max                  | Units         |
|----------------|----------------------------|---------------------------------------|---------------------|-----|----------------------|---------------|
| $V_{CC}^{(1)}$ | Supply Voltage             |                                       | 2.7                 |     | 3.6                  | V             |
| $I_{CC}$       | Supply Current             | Async read at 3.57MHz                 |                     |     | 5                    | mA            |
| $I_{CC}$       | Supply Current             | Async write at 3.57MHz                |                     |     | 5                    | mA            |
| $I_{CC}$       | Supply Current             | Synch read at 1MHz                    |                     |     | 5                    | mA            |
| $I_{CC}$       | Supply Current             | Synch write at 1MHz                   |                     |     | 5                    | mA            |
| $I_{SB}$       | Standby Current            | $V_{IN} = V_{CC}$ or GND              |                     |     | 100                  | $\mu\text{A}$ |
| $V_{IL}$       | SDA/IO Input Low Voltage   |                                       | 0                   |     | $V_{CC} \times 0.2$  | V             |
| $V_{IL}$       | CLK Input Low Voltage      |                                       | 0                   |     | $V_{CC} \times 0.2$  | V             |
| $V_{IL}$       | RST Input Low Voltage      |                                       | 0                   |     | $V_{CC} \times 0.2$  | V             |
| $V_{IH}^{(1)}$ | SDA/IO Input High Voltage  |                                       | $V_{CC} \times 0.7$ |     | 5.5                  | V             |
| $V_{IH}^{(1)}$ | SCL/CLK Input High Voltage |                                       | $V_{CC} \times 0.7$ |     | 5.5                  | V             |
| $V_{IH}^{(1)}$ | RST Input High Voltage     |                                       | $V_{CC} \times 0.7$ |     | 5.5                  | V             |
| $I_{IL}$       | SDA/IO Input Low Current   | $0 < V_{IL} < V_{CC} \times 0.15$     |                     |     | 15                   | $\mu\text{A}$ |
| $I_{IL}$       | SCL/CLK Input Low Current  | $0 < V_{IL} < V_{CC} \times 0.15$     |                     |     | 15                   | $\mu\text{A}$ |
| $I_{IL}$       | RST Input Low Current      | $0 < V_{IL} < V_{CC} \times 0.15$     |                     |     | 50                   | $\mu\text{A}$ |
| $I_{IH}$       | SDA/IO Input High Current  | $V_{CC} \times 0.7 < V_{IH} < V_{CC}$ |                     |     | 20                   | $\mu\text{A}$ |
| $I_{IH}$       | SCL/CLK Input High Current | $V_{CC} \times 0.7 < V_{IH} < V_{CC}$ |                     |     | 100                  | $\mu\text{A}$ |
| $I_{IH}$       | RST Input High Current     | $V_{CC} \times 0.7 < V_{IH} < V_{CC}$ |                     |     | 150                  | $\mu\text{A}$ |
| $V_{OH}$       | SDA/IO Output High Voltage | 20K ohm external pull-up              | $V_{CC} \times 0.7$ |     | $V_{CC}$             | V             |
| $V_{OL}$       | SDA/IO Output Low Voltage  | $I_{OL} = 1\text{mA}$                 | 0                   |     | $V_{CC} \times 0.15$ | V             |
| $I_{OH}$       | SDA/IO Output High Current | $V_{OH}$                              |                     |     | 20                   | $\mu\text{A}$ |
| $I_{OL}$       | SDA/IO Output Low Current  | $V_{OL}$                              |                     |     | 10                   | mA            |

Note: 1. To prevent latch up conditions from occurring during power up of the AT88SC0204CA,  $V_{CC}$  must be turned on before applying  $V_{IH}$ . For powering down,  $V_{IH}$  must be removed before turning  $V_{CC}$  off.

**Table 4-2 AC Characteristics**

Applicable over recommended operating range from  $V_{CC} = +2.7$  to  $3.6V$ ,  $T_{AC} = -40^{\circ}C$  to  $+85^{\circ}C$ ,  $CL = 30pF$   
(unless otherwise noted)

| Symbol       | Parameter                   | Min | Max         | Units   |
|--------------|-----------------------------|-----|-------------|---------|
| $f_{CLK}$    | Async Clock Frequency       | 1   | 4           | MHz     |
| $f_{CLK}$    | Synch Clock Frequency       | 0   | 1           | MHz     |
|              | Clock Duty cycle            | 40  | 60          | %       |
| $t_R$        | "Rise Time - SDA/IO, RST"   |     | 1           | $\mu S$ |
| $t_F$        | "Fall Time - SDA/IO, RST"   |     | 1           | $\mu S$ |
| $t_R$        | Rise Time - SCL/CLK         |     | 9% x period | $\mu S$ |
| $t_F$        | Fall Time - SCL/CLK         |     | 9% x period | $\mu S$ |
| $t_{AA}$     | Clock Low to Data Out Valid |     | 250         | nS      |
| $t_{HD,STA}$ | Start Hold Time             | 200 |             | nS      |
| $t_{SU,STA}$ | Start Set-up Time           | 200 |             | nS      |
| $t_{HD,DAT}$ | Data In Hold Time           | 10  |             | nS      |
| $t_{SU,DAT}$ | Data In Set-up Time         | 100 |             | nS      |
| $t_{SU,STO}$ | Stop Set-up Time            | 200 |             | nS      |
| $t_{DH}$     | Data Out Hold Time          | 20  |             | nS      |
| $t_{WR}$     | Write Cycle Time            |     | 5           | mS      |

## 5. Device Operations for Synchronous Protocols

### 5.1 Clock and Data Transitions

The SDA pin is normally pulled high with an external device. Data on the SDA pin may change only during SCL low time periods (see Figure 5-3 on page 8). Data changes during SCL high periods will indicate a start or stop condition as defined below.

#### 5.1.1 Start condition

A high-to-low transition of SDA with SCL high defines a start condition which must precede all commands (see Figure 5-4 on page 8).

#### 5.1.2 Stop condition

A low-to-high transition of SDA with SCL high defines a stop condition. After a read sequence, the stop condition will place the EEPROM in a standby power mode (see Figure 5-4 on page 8).

#### 5.1.3 Acknowledge

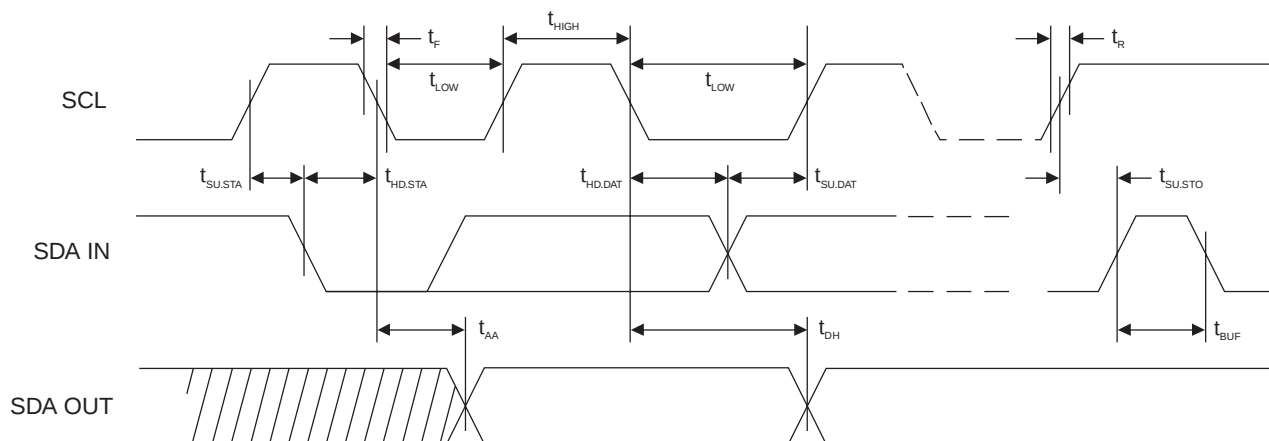
All addresses and data words are serially transmitted to and from the EEPROM in 8-bit words. The EEPROM sends a zero to acknowledge that it has received each word. This happens during the ninth clock cycle (see Figure 5-5 on page 8).

## 5.2 Memory Reset

After an interruption in communication due to protocol errors, power loss or any reason, perform "Acknowledge Polling" to properly recover from the condition. Acknowledge polling consists of sending a start condition followed by a valid CryptoMemory command byte and determining if the device responded with an ACKNOWLEDGE.

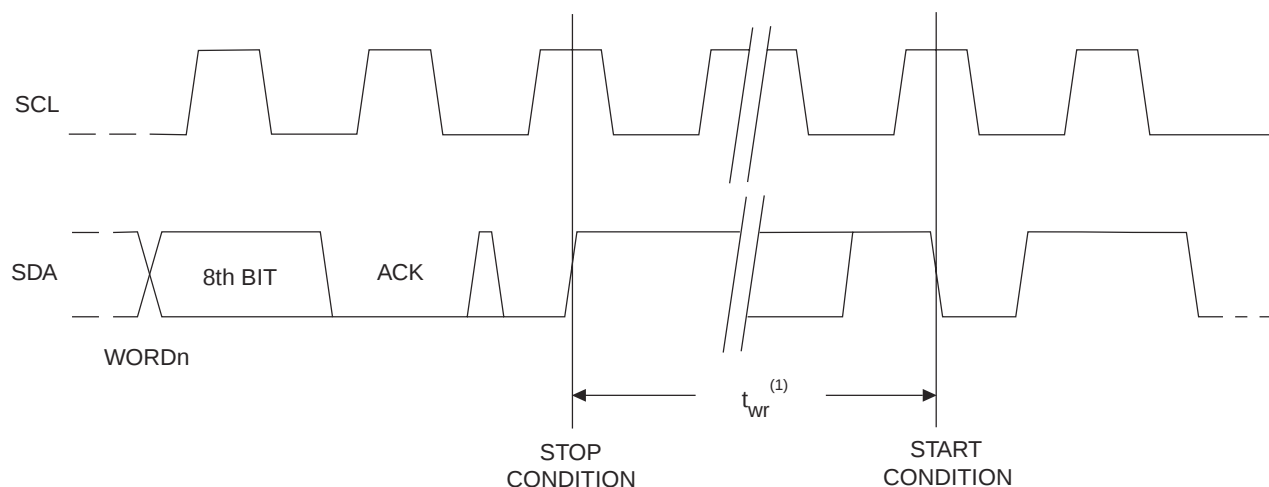
**Figure 5-1. Bus Time for Two-wire Serial Communications**

SCL: Serial Clock, SDA: Serial Data I/O



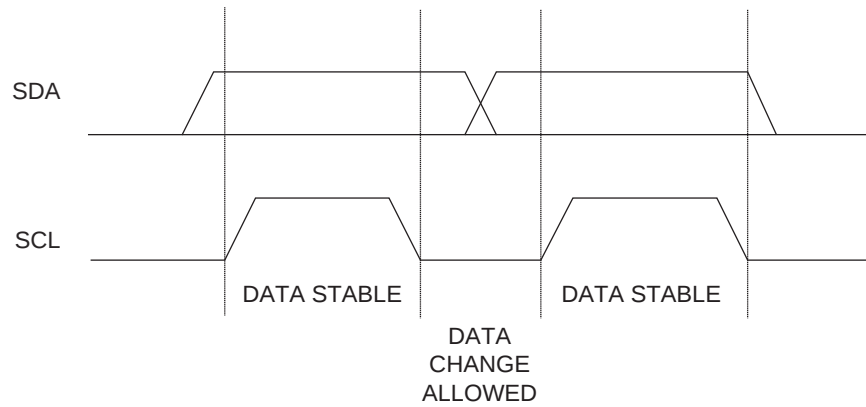
**Figure 5-2. Write Cycle Timing**

SCL: Serial Clock, SDA: Serial Data I/O

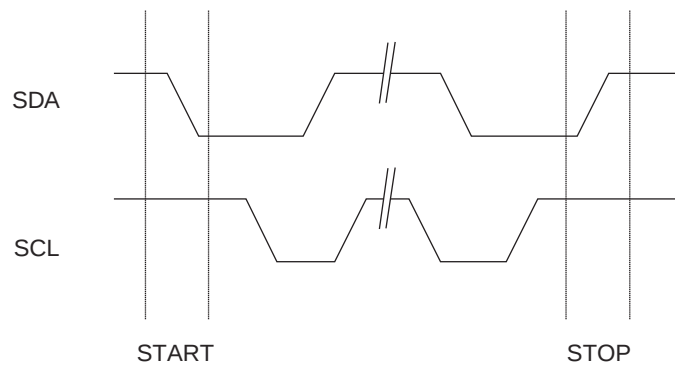


**Note:** The write cycle time  $t_{wr}$  is the time from a valid stop condition of a write sequence to the end of the internal clear/write cycle

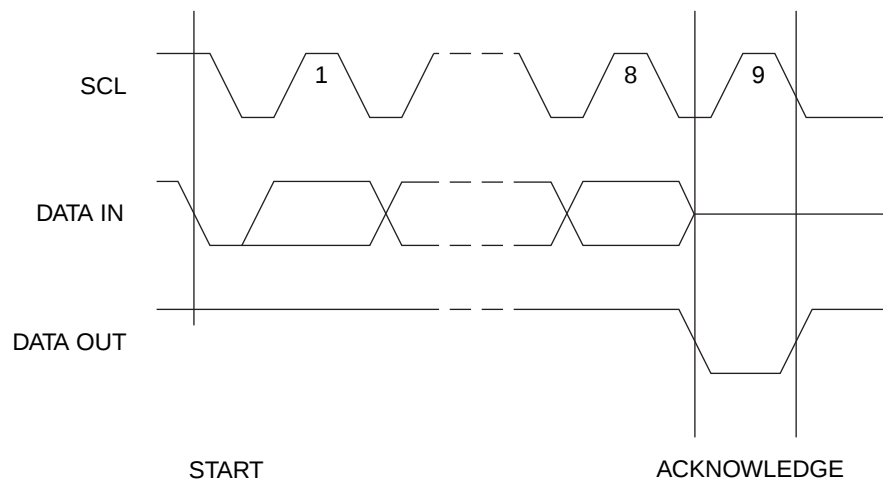
**Figure 5-3. Data Validity**



**Figure 5-4. START and STOP Definitions**



**Figure 5-5. Output Acknowledge**



## 6. Device Architecture

### 6.1 User Zones

The EEPROM user memory is divided into four zones of 512 bits each. Multiple zones allow for storage of different types of data or files in different zones. Access to user zones is permitted only after meeting proper security requirements. These security requirements are user definable in the configuration memory during device personalization. If the same security requirements are selected for multiple zones, then these zones may effectively be accessed as one larger zone.

**Figure 6-1. User Zones**

| Zone   |      | \$0      | \$1 | \$2 | \$3 | \$4 | \$5 | \$6 | \$7 |
|--------|------|----------|-----|-----|-----|-----|-----|-----|-----|
| User 0 | \$00 |          |     |     |     |     |     |     |     |
|        | -    | 64 bytes |     |     |     |     |     |     |     |
|        | -    |          |     |     |     |     |     |     |     |
|        | \$38 |          |     |     |     |     |     |     |     |
| User 1 | \$00 |          |     |     |     |     |     |     |     |
|        | -    | 64 bytes |     |     |     |     |     |     |     |
|        | -    |          |     |     |     |     |     |     |     |
|        | \$38 |          |     |     |     |     |     |     |     |
| User 2 | \$00 |          |     |     |     |     |     |     |     |
|        | -    | 64 bytes |     |     |     |     |     |     |     |
|        | -    |          |     |     |     |     |     |     |     |
|        | \$38 |          |     |     |     |     |     |     |     |
| User 3 | \$00 |          |     |     |     |     |     |     |     |
|        | -    | 64 bytes |     |     |     |     |     |     |     |
|        | -    |          |     |     |     |     |     |     |     |
|        | \$38 |          |     |     |     |     |     |     |     |

## 7. Control Logic

Access to the user zones occur only through the control logic built into the device. This logic is configurable through access registers, key registers and keys programmed into the configuration memory during device personalization. Also implemented in the control logic is a cryptographic engine for performing the various higher-level security functions of the device.

## 8. Configuration Memory

The configuration memory consists of 2048 bits of EEPROM memory used for storage of passwords, keys, codes, and also used for definition of security access rights for the user zones. Access rights to the configuration memory are defined in the control logic and are not alterable by the user after completion of personalization.

**Figure 8-1. Configuration Memory**

|      | \$0                                   | \$1                      | \$2 | \$3 | \$4                    | \$5    | \$6 | \$7          |                |
|------|---------------------------------------|--------------------------|-----|-----|------------------------|--------|-----|--------------|----------------|
| \$00 | Answer To Reset                       |                          |     |     |                        |        |     |              | Identification |
| \$08 | Fab Code                              |                          | MTZ |     | Card Manufacturer Code |        |     |              |                |
| \$10 | Lot History Code                      |                          |     |     |                        |        |     |              | Read Only      |
| \$18 | DCR                                   | Identification Number Nc |     |     |                        |        |     |              | Access Control |
| \$20 | AR0                                   | PR0                      | AR1 | PR1 | AR2                    | PR2    | AR3 | PR3          |                |
| \$28 | Reserved                              |                          |     |     |                        |        |     |              |                |
| \$30 |                                       |                          |     |     |                        |        |     |              |                |
| \$38 |                                       |                          |     |     |                        |        |     |              |                |
| \$40 | Issuer Code                           |                          |     |     |                        |        |     |              |                |
| \$48 |                                       |                          |     |     |                        |        |     |              |                |
| \$50 | For Authentication and Encryption use |                          |     |     |                        |        |     | Cryptography |                |
| \$58 |                                       |                          |     |     |                        |        |     |              |                |
| \$60 |                                       |                          |     |     |                        |        |     |              |                |
| \$68 |                                       |                          |     |     |                        |        |     |              |                |
| \$70 |                                       |                          |     |     |                        |        |     |              |                |
| \$78 |                                       |                          |     |     |                        |        |     |              |                |
| \$80 |                                       |                          |     |     |                        |        |     |              |                |
| \$88 |                                       |                          |     |     |                        |        |     |              |                |
| \$90 | For Authentication and Encryption use |                          |     |     |                        |        |     | Secret       |                |
| \$98 |                                       |                          |     |     |                        |        |     |              |                |
| \$A0 |                                       |                          |     |     |                        |        |     |              |                |
| \$A8 |                                       |                          |     |     |                        |        |     |              |                |
| \$B0 | PAC                                   | Write 0                  |     |     | PAC                    | Read 0 |     |              | Password       |
| \$B8 | PAC                                   | Write 1                  |     |     | PAC                    | Read 1 |     |              |                |
| \$C0 | PAC                                   | Write 2                  |     |     | PAC                    | Read 2 |     |              |                |
| \$C8 | PAC                                   | Write 3                  |     |     | PAC                    | Read 3 |     |              |                |
| \$D0 | PAC                                   | Write 4                  |     |     | PAC                    | Read 4 |     |              |                |
| \$D8 | PAC                                   | Write 5                  |     |     | PAC                    | Read 5 |     |              |                |
| \$E0 | PAC                                   | Write 6                  |     |     | PAC                    | Read 6 |     |              |                |
| \$E8 | PAC                                   | Write 7                  |     |     | PAC                    | Read 7 |     |              |                |
| \$F0 | Reserved                              |                          |     |     |                        |        |     | Forbidden    |                |
| \$F8 |                                       |                          |     |     |                        |        |     |              |                |

## 8.1 Security Fuses

There are three fuses on the device that must be blown during the device personalization process. Each fuse locks certain portions of the configuration zone as OTP (One-Time Programmable) memory. Fuses are designed for the module manufacturer, card manufacturer and card issuer and should be blown in sequence, although all programming of the device and blowing of the fuses may be performed at one final step.

## 9. Communication Security Modes

Communications between the device and host operate in three basic modes. Standard mode is the default mode for the device after power-up. Authentication mode is activated by a successful authentication sequence. Encryption mode is activated by a successful encryption activation following a successful authentication.

**Table 9-1. Communication Security Modes<sup>(1)</sup>**

| Mode           | Configuration Data | User Data | Passwords | Data Integrity Check |
|----------------|--------------------|-----------|-----------|----------------------|
| Standard       | Clear              | Clear     | Clear     | MDC <sup>(1)</sup>   |
| Authentication | Clear              | Clear     | Encrypted | MAC <sup>(1)</sup>   |
| Encryption     | Clear              | Encrypted | Encrypted | MAC <sup>(1)</sup>   |

Note: 1. Configuration data include viewable areas of the configuration zone except the passwords:

- MDC: Modification Detection Code
- MAC: Message Authentication Code

## 10. Security Options

### 10.1 Anti-tearing

In the event of a power loss during a write cycle, the integrity of the device's stored data is recoverable. This function is optional: the host may choose to activate the anti-tearing function, depending on application requirements. When anti-tearing is active, write commands take longer to execute, since more write cycles are required to complete them, and data is limited to a maximum of eight bytes for each write request.

Data is written first into a buffer zone in EEPROM instead of the intended destination address, but with the same access conditions. The data is then written in the required location. If this second write cycle is interrupted due to a power loss, the device will automatically recover the data from the system buffer zone at the next power-up. Non-volatile buffering of the data is done automatically by the device.

During power-up in applications using anti-tearing, the host is required to perform ACK polling in the event that the device needs to carry out the data recovery process.

### 10.2 Write Lock

If a user zone is configured in the write lock mode, the lowest address byte of an 8-byte page constitutes a write access byte for the bytes of that page.

**Example:** The write lock byte at \$080 controls the bytes from \$081 to \$087

**Table 10-1. Write Lock Example**

| Address | \$0      | \$1       | \$2       | \$3       | \$4       | \$5       | \$6       | \$7       |
|---------|----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| \$080   | 11011001 | xxxx xxxx | xxxx xxxx | xxxx xxxx | xxxx xxxx | xxxx xxxx | xxxx xxxx | xxxx xxxx |
|         |          | locked    | locked    |           |           | locked    |           |           |

In the write lock configuration, write operations are limited to writing only one byte at a time. Attempts to write more than one byte will result in writing of just the first byte into the device.

Passwords may be used to protect read and/or write access of any user zone. When a valid password is presented, it is memorized and active until power is turned off, unless a new password is presented or RST becomes active. There are eight password sets that may be used to protect any user zone. Only one password is active at a time.

## 10.4 Authentication Protocol

Authentication success is memorized and active as long as the chip is powered, unless a new authentication is initialized or RST becomes active. If the new authentication request is not validated, the card loses its previous authentication which must be presented again to gain access. Only the latest request is memorized.

```

sequenceDiagram
    participant Device as Device (Card)
    participant Host as Host (Reader)

    Device->>Host: AUTHENTICATION
    Host->>Device: 
    Device->>Host: 
    Host->>Device: 
    Device->>Host: READ ACCESS
    Host->>Device: 
    Device->>Host: WRITE ACCESS
    Host->>Device: 
    Device->>Host: 
    Host->>Device: 
    
```

The diagram illustrates the interaction between a **Device (Card)** and a **Host (Reader)** during an authentication and access control process. The process is divided into three main phases: **AUTHENTICATION**, **READ ACCESS**, and **WRITE ACCESS**.

**AUTHENTICATION Phase:**

- The **Device (Card)** sends **Card Number** to the **Host (Reader)**.
- The **Host (Reader)** sends **COMPUTE Challenge A** to the **Device (Card)**.
- The **Device (Card)** sends **VERIFY A** to the **Host (Reader)**.
- The **Host (Reader)** sends **Challenge A** to the **Device (Card)**.
- The **Device (Card)** sends **COMPUTE Challenge B** to the **Host (Reader)**.
- The **Host (Reader)** sends **Challenge B** to the **Device (Card)**.
- The **Device (Card)** sends **VERIFY B** to the **Host (Reader)**.

**READ ACCESS Phase:**

- The **Device (Card)** sends **VERIFY RPW** to the **Host (Reader)**.
- The **Host (Reader)** sends **Read Password (RPW)** to the **Device (Card)**.
- The **Device (Card)** sends **DATA** to the **Host (Reader)**.
- The **Host (Reader)** sends **Checksum (CS)** to the **Device (Card)**.
- The **Device (Card)** sends **VERIFY CS** to the **Host (Reader)**.

**WRITE ACCESS Phase:**

- The **Device (Card)** sends **VERIFY WPW** to the **Host (Reader)**.
- The **Host (Reader)** sends **Write Password (WPW)** to the **Device (Card)**.
- The **Device (Card)** sends **DATA** to the **Host (Reader)**.
- The **Host (Reader)** sends **CS** to the **Device (Card)**.
- The **Device (Card)** sends **VERIFY CS** to the **Host (Reader)**.
- The **Host (Reader)** sends **Write DATA** to the **Device (Card)**.



## 10.5 Cryptographic Message Authentication Codes

AT88SC0204CA implements a data validity check function in the standard, authentication or encryption modes of operation.

In the standard mode, data validity check is done through a Modification Detection Code (MDC), in which the host may read an MDC from the device in order to verify that the data sent was received correctly.

In authentication and encryption modes, the data validity check becomes more powerful since it provides a bidirectional data integrity check and data origin authentication capability in the form of a Message Authentication Codes (MAC). Only the host/device that carried out a valid authentication is capable of computing a valid MAC. While operating in the authentication or encryption modes, the use of MAC is required. For an ingoing command, if the device calculates a MAC different from the MAC transmitted by the host, not only is the command abandoned but the security privilege is revoked. A new authentication and/or encryption activation will be required to reactivate the MAC.

## 10.6 Encryption

The data exchanged between the device and the host during read, write and verify password commands may be encrypted to ensure data confidentiality.

The issuer may choose to require encryption for a user zone by settings made in the configuration memory. Any one of four keys may be selected for use with a user zone. In this case, activation of the encryption mode is required in order to read/write data in the zone and only encrypted data will be transmitted. Even if not required, the host may still elect to activate encryption provided the proper keys are known.

## 10.7 Supervisor Mode

Enabling this feature allows the holder of one specific password to gain full access to all eight password sets, including the ability to change passwords.

## 10.8 Modify Forbidden

No write access is allowed in a user zone protected with this feature at any time. The user zone must be written during device personalization prior to blowing the security fuses.

## 10.9 Program Only

For a user zones protected by this feature, data can only be programmed (bits change from a “1” to a “0”), but not erased (bits change from a “0” to a “1”).

## 11. Protocol Selection

The AT88SC0204CA supports two different communication protocols.

- **Smartcard Applications:**

Smartcard applications use ISO 7816-B protocol in asynchronous T = 0 mode for compatibility and interoperability with industry standard smartcard readers.

- **Embedded Applications:**

A two-wire serial interface provides fast and efficient connectivity with other logic devices or microcontrollers.

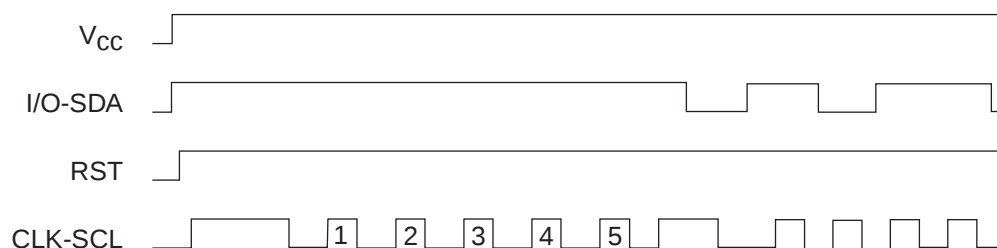
The power-up sequence determines establishes the communication protocol for use within that power cycle. Protocol selection is allowed only during power-up.

### 11.1 Synchronous Two-wire Serial Interface

The synchronous mode is the default mode after power up. This is due to the presence of an internal pull-up on RST. For embedded applications using CryptoMemory in standard plastic packages, this is the only available communication protocol.

- Power-up  $V_{CC}$ , RST goes high also
- After stable  $V_{CC}$ , SCL (CLK) and SDA(I/O) may be driven
- Once synchronous mode has been selected, it is not possible to switch to asynchronous mode without first powering off the device

**Figure 11-1. Synchronous Two-wire Protocol**



Note: Five clock pulses must be sent before the first command is issued

## 11.2 Asynchronous T = 0 Protocol

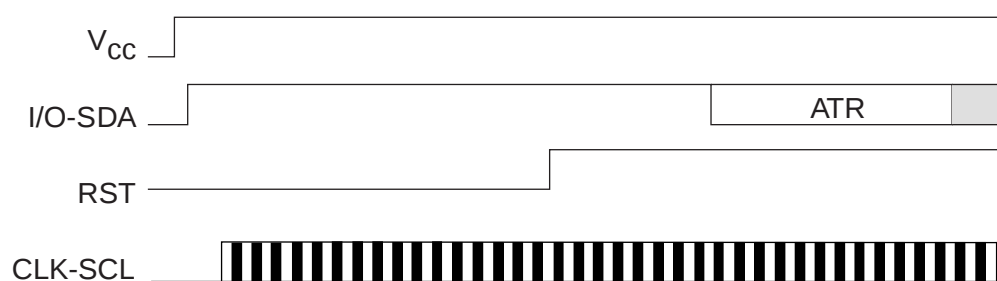
This power-up sequence complies to ISO 7816-3 for a cold reset in smart card applications.

- $V_{CC}$  goes high; RST, I/O (SDA) and CLK (SCL) are low
- Set I/O (SDA) in receive mode
- Provide a clock signal to CLK (SCL)
- RST goes high after 400 clock cycles

The device will respond with a 64-bit ATR code, including historical bytes to indicate the memory density within the CryptoMemory family.

Once asynchronous mode has been selected, it is not possible to switch to synchronous mode without first powering off the device.

Figure 11-2. Asynchronous T = 0 Protocol (Gemplus Patent)



## 12. Initial Device Programming

Enabling the security features of CryptoMemory requires prior personalization. Personalization entails setting up of desired access rights by zones, passwords and key values, programming these values into the configuration memory with verification using simple write and read commands, and then blowing fuses to lock this information in place.

Gaining access to the configuration memory requires successful presentation of a secure (or transport) code. The initial signature of the secure (transport) code for the AT88SC0204CA device is \$E5 47 47. This is the same as the Write 7 password. The user may elect to change the signature of the secure code anytime after successful presentation.

After writing and verifying data in the configuration memory, the security fuses *must* be blown to lock this information in the device. For additional information on personalizing CryptoMemory, please see the application notes *Programming CryptoMemory for Embedded Applications* and *Initializing CryptoMemory for Smart Card Applications* from the product page at [www.atmel.com/products/securemem](http://www.atmel.com/products/securemem).

## 13. Ordering Information

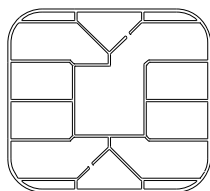
| Atmel Ordering Code                                                          | Package                                                                                  | Voltage Range | Temperature Range                                              |
|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|---------------|----------------------------------------------------------------|
| AT88SC0204CA-MJ<br>AT88SC0204CA-MP<br>AT88SC0204CA-MJTG<br>AT88SC0204CA-MPTG | M2 – J Module - ISO<br>M2 – P Module - ISO<br>M2 – J Module - TWI<br>M2 – P Module - TWI | 2.7V–3.6V     | Commercial (0°C to 70°C)                                       |
| AT88SC0204CA-PU<br>AT88SC0204CA-SH<br>AT88SC0204CA-TH<br>AT88SC0204CA-Y6H-T  | 8P3<br>8S1<br>8A2<br>8Y6                                                                 | 2.7V–3.6V     | Green compliant (exceeds RoHS) /<br>Industrial (–40°C to 85°C) |
| AT88SC0204CA-WI                                                              | 7 mil wafer                                                                              | 2.7V–3.6V     | Industrial (–40°C to 85°C)                                     |

| Package Type <sup>(1) (2)</sup>   | Description                                                                                |
|-----------------------------------|--------------------------------------------------------------------------------------------|
| <b>M2 – J Module : ISO or TWI</b> | M2 ISO 7816 smart card module                                                              |
| <b>M2 – P Module: ISO or TWI</b>  | M2 ISO 7816 smart card module with Atmel® logo                                             |
| <b>8P3</b>                        | 8-lead, 0.300" wide, Plastic Dual Inline (PDIP)                                            |
| <b>8S1</b>                        | 8-lead, 0.150" wide, Plastic Gull Wing Small Outline (JEDEC SOIC)                          |
| <b>8A2</b>                        | 8-lead, 4.4mm body, Plastic Thin Shrink Small Outline (TSSOP)                              |
| <b>8Y6</b>                        | 8-lead, 2.0 x 3.0mm body, 0.50mm pitch, Ultra Thin Mini-map, Dual No Lead (DFN), (MLP 2x3) |

- Notes:
1. Formal drawings may be obtained from an Atmel sales office
  2. Both the J and P module packages are used for either ISO (T=0 / 2-wire mode) or TWI (2-wire mode only)

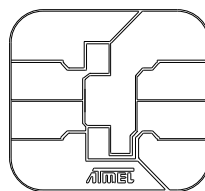
## 14. Package Information

### Ordering Code: MJ or MJTG



Module Size: **M2**  
Dimension\*: 12.6 x 11.4 [mm]  
Glob Top: Round - Ø 8.5 [mm]  
Thickness: 0.58 [mm]  
Pitch: 14.25mm

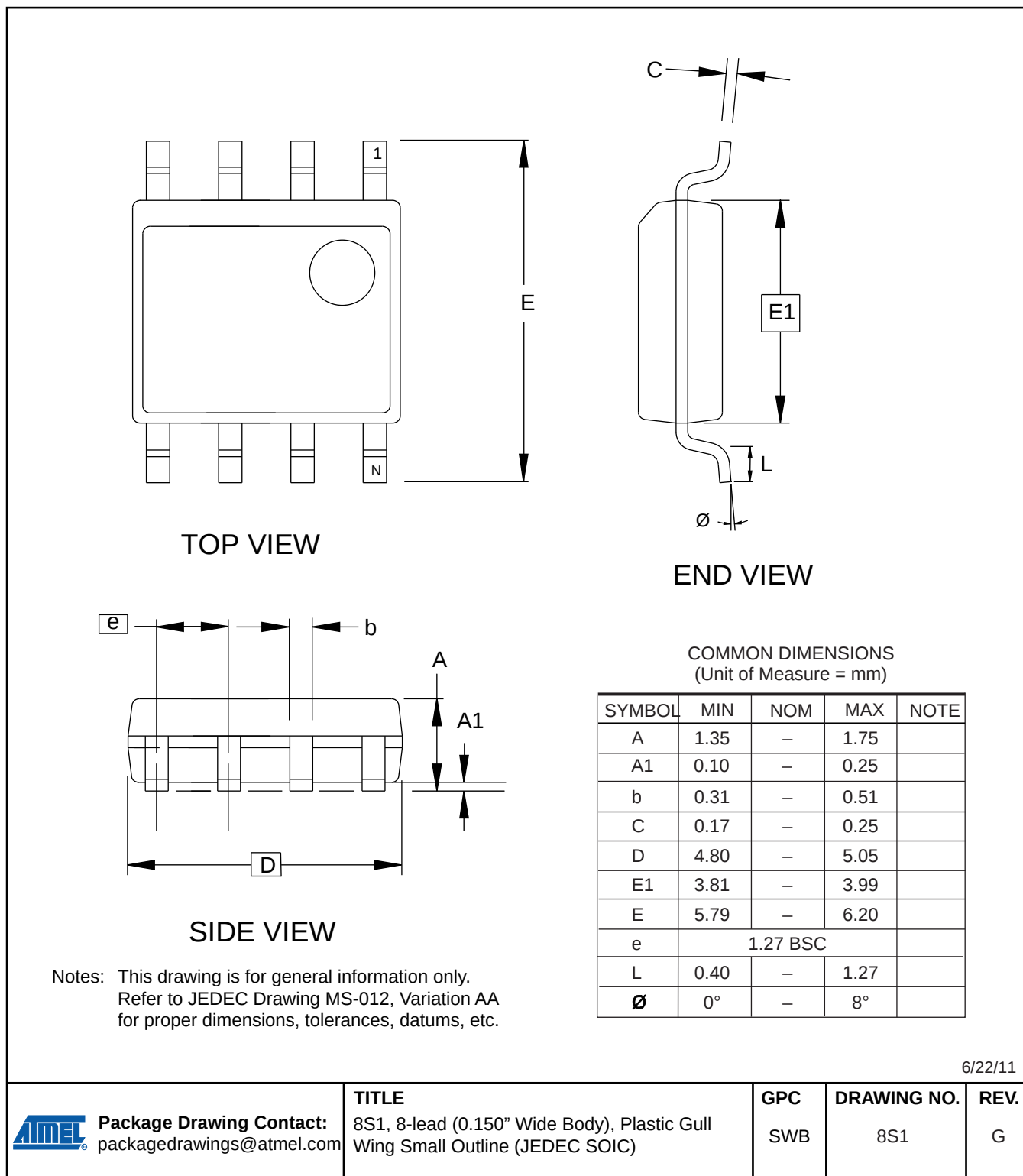
### Ordering Code: MP or MPTG



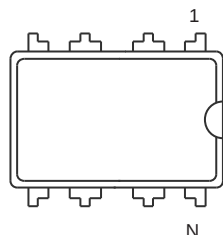
Module Size: **M2**  
Dimension\*: 12.6 x 11.4 [mm]  
Glob Top: Square - 8.8 x 8.8 [mm]  
Thickness: 0.58 [mm]  
Pitch: 14.25mm

Note: \* The module dimensions listed refer to the dimensions of the exposed metal contact area. The actual dimensions of the module after excise or punching from the carrier tape are generally 0.4mm greater in both directions (i.e., a punched M2 module will yield 13.0 x 11.8mm).

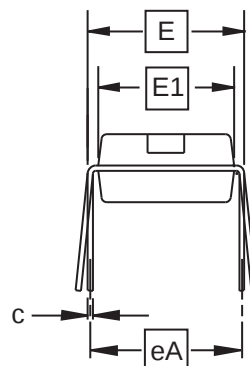
15. Ordering Code: SH  
8S1 – 8-lead SOIC



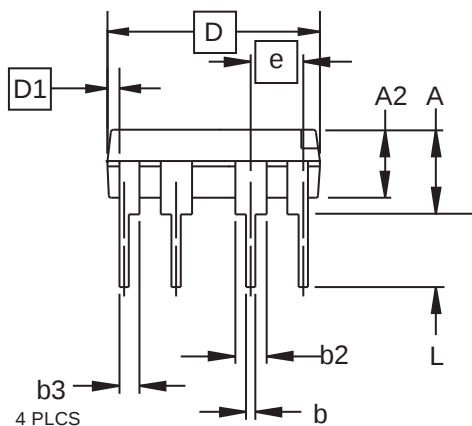
## 16. Ordering Code: PU 8P3 – 8-lead PDIP



Top View



End View



Side View

COMMON DIMENSIONS  
(Unit of Measure = inches)

| SYMBOL | MIN       | NOM   | MAX   | NOTE |
|--------|-----------|-------|-------|------|
| A      |           |       | 0.210 | 2    |
| A2     | 0.115     | 0.130 | 0.195 |      |
| b      | 0.014     | 0.018 | 0.022 | 5    |
| b2     | 0.045     | 0.060 | 0.070 | 6    |
| b3     | 0.030     | 0.039 | 0.045 | 6    |
| c      | 0.008     | 0.010 | 0.014 |      |
| D      | 0.355     | 0.365 | 0.400 | 3    |
| D1     | 0.005     |       |       | 3    |
| E      | 0.300     | 0.310 | 0.325 | 4    |
| E1     | 0.240     | 0.250 | 0.280 | 3    |
| e      | 0.100 BSC |       |       |      |
| eA     | 0.300 BSC |       |       | 4    |
| L      | 0.115     | 0.130 | 0.150 | 2    |

- Notes:
1. This drawing is for general information only; refer to JEDEC Drawing MS-001, Variation BA for additional information.
  2. Dimensions A and L are measured with the package seated in JEDEC seating plane Gauge GS-3.
  3. D, D1 and E1 dimensions do not include mold Flash or protrusions. Mold Flash or protrusions shall not exceed 0.010 inch.
  4. E and eA measured with the leads constrained to be perpendicular to datum.
  5. Pointed or rounded lead tips are preferred to ease insertion.
  6. b2 and b3 maximum dimensions do not include Dambar protrusions. Dambar protrusions shall not exceed 0.010 (0.25 mm).

06/21/11



Package Drawing Contact:  
packagedrawings@atmel.com

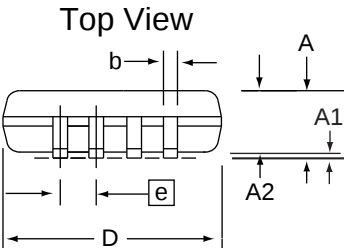
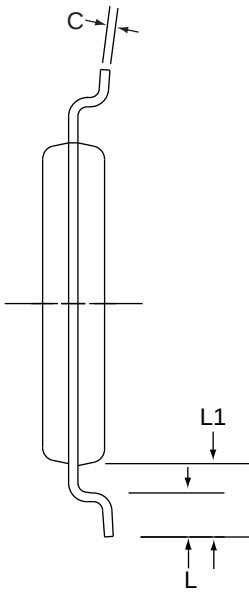
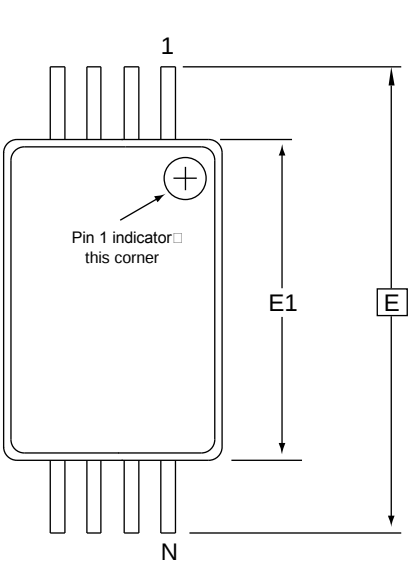
TITLE  
8P3, 8-lead, 0.300" Wide Body, Plastic Dual  
In-line Package (PDIP)

GPC  
PTC

DRAWING NO.  
8P3

REV.  
D

17.   **Ordering Code: TH**  
      **8X – 8-lead TSSOP**



| COMMON DIMENSIONS<br>(Unit of Measure = mm) |          |      |      |      |
|---------------------------------------------|----------|------|------|------|
| SYMBOL                                      | MIN      | NOM  | MAX  | NOTE |
| A                                           | -        | -    | 1.20 |      |
| A1                                          | 0.05     | -    | 0.15 |      |
| A2                                          | 0.80     | 1.00 | 1.05 |      |
| D                                           | 2.90     | 3.00 | 3.10 | 2, 5 |
| E                                           | 6.40 BSC |      |      |      |
| E1                                          | 4.30     | 4.40 | 4.50 | 3, 5 |
| b                                           | 0.19     | -    | 0.30 | 4    |
| e                                           | 0.65 BSC |      |      |      |
| L                                           | 0.45     | 0.60 | 0.75 |      |
| L1                                          | 1.00 REF |      |      |      |
| C                                           |          | 0.09 | -    | 0.20 |

- Notes:
- 1. This drawing is for general information only. Refer to JEDEC Drawing MO-153, Variation AA, for proper dimensions, tolerances, datums, etc.
  - 2. Dimension D does not include mold Flash, protrusions or gate burrs. Mold Flash, protrusions and gate burrs shall not exceed 0.15mm (0.006in) per side.
  - 3. Dimension E1 does not include inter-lead Flash or protrusions. Inter-lead Flash and protrusions shall not exceed 0.25mm (0.010in) per side.
  - 4. 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. Dambar cannot be located on the lower radius of the foot. Minimum space between protrusion and adjacent lead is 0.07mm.
  - 5. Dimension D and E1 to be determined at Datum Plane H.

6/22/11



**Package Drawing Contact:**  
packagedrawings@atmel.com

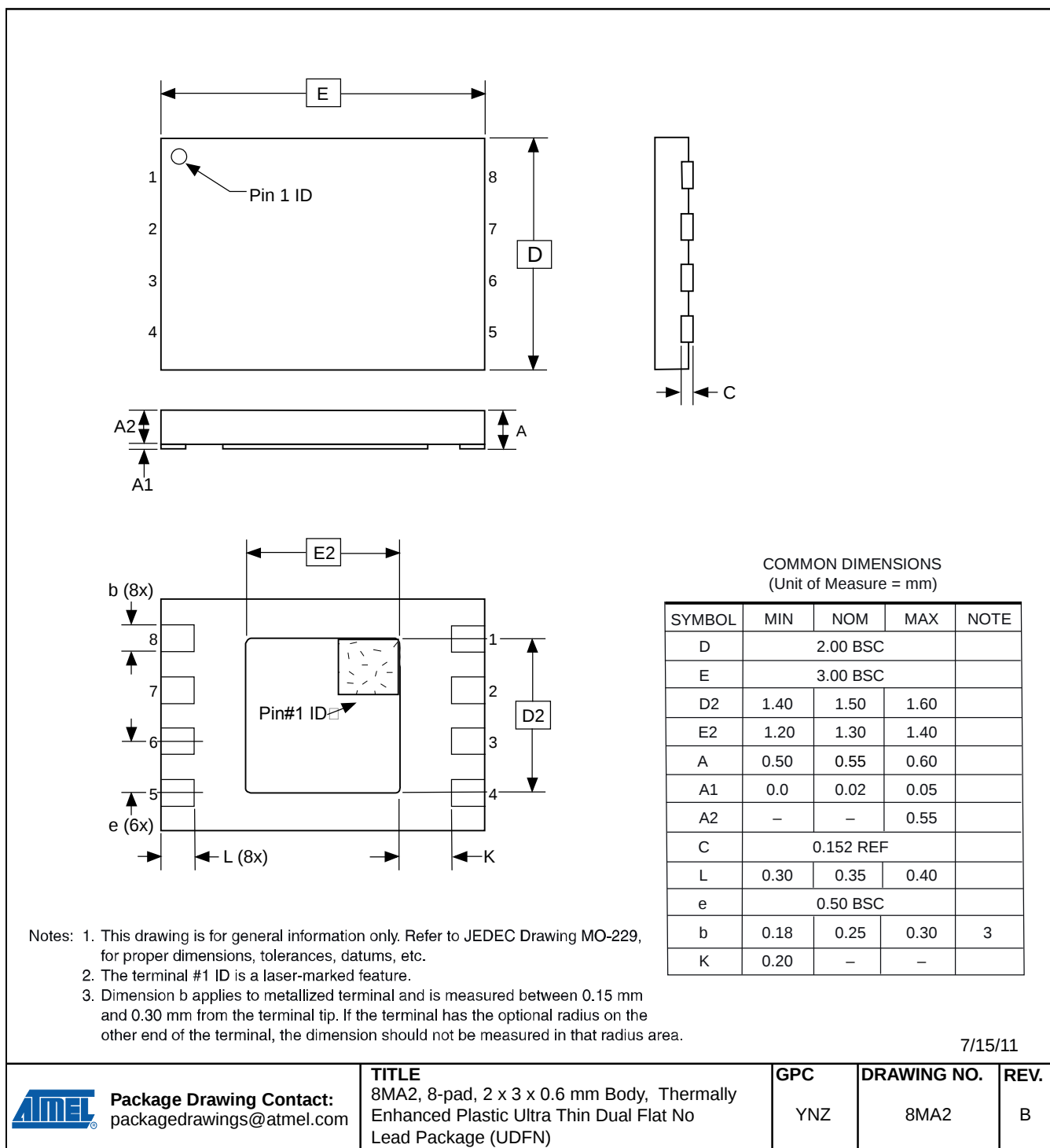
**TITLE**  
8X, 8-lead 4.4mm Body, Plastic Thin  
Shrink Small Outline Package (TSSOP)

**GPC**  
TNR

**DRAWING NO.**  
8X

**REV.**  
D

# 18. Ordering Code: Y6H-T 8MA2 – 8-lead Ultra Thin Mini-Map



## 19. Revision History

| Doc. Rev. | Date    | Comments                                                                                                                                        |
|-----------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 5202FS    | 12/2011 | Update Template<br>Update package drawings and<br>- Replace 8A2 with 8X<br>- Replace 8Y6 with 8MA2<br>Change AT88SC0204CA-SU to AT88SC0204CA-SH |
| 5202ES    | 08/2009 |                                                                                                                                                 |
| 5202DS    | 08/2009 | Minor edits and TWI module updates                                                                                                              |
| 5202DS    | 07/2009 | Minor updates to package drawing information and ordering information.                                                                          |
| 5202CS    | 05/2009 | Added Mini-MAP column to Table 1-1 and Mini-MAP pin-out drawing.                                                                                |
| 5202BS    | 02/2009 | Connection Diagram inserted; DC Characteristics table updated.                                                                                  |
| 5202AS    | 07/2008 | Initial document release.                                                                                                                       |



Enabling Unlimited Possibilities™

**Atmel Corporation**

2325 Orchard Parkway  
San Jose, CA 95131  
USA

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

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

[www.atmel.com](http://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  
Parking 4  
D-85748 Garching b. Munich  
GERMANY

**Tel:** (+49) 89-31970-0

**Fax:** (+49) 89-3194621

**Atmel Japan G.K.**

16F Shin-Osaki Kangyo Bldg.  
1-6-4 Osaki, Shinagawa-ku  
Tokyo 141-0032  
JAPAN

**Tel:** (+81)(3) 6417-0300

**Fax:** (+81)(3) 6417-0370

© 2011 Atmel Corporation. All rights reserved. / Rev.: 5202FS-CRYPTO-12/11

Atmel®, Atmel logos and combinations thereof, 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.