

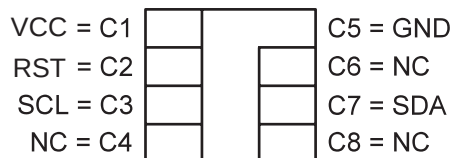
## Features

- One 64 x 8 (512-bit) Configuration Zone
- Three 64 x 8 (512-bit) User Zones
- Programmable Chip Select
- Low-voltage Operation: 2.7V to 5.5V
- Two-wire Serial Interface
- 8-byte Page Write Mode
- Self-timed Write Cycle (10 ms max)
- Answer-to-reset Register
- High-security Memory Including Anti-wiretapping
  - 64-bit Authentication Protocol (under exclusive patent license from ELVA)
  - Secure Checksum
  - Configurable Authentication Attempts Counter
  - Two Sets of Two 24-bit Passwords
  - Specific Passwords for Read and Write
  - Four Password Attempts Counters
  - Selectable Access Rights by Zone
- ISO Compliant Packaging
- High Reliability
  - Endurance: 100,000 Cycles
  - Data Retention: 100 Years
  - ESD Protection: 4,000V min
- Low-power CMOS

**Table 0-1.** Pin Configuration

| Name | Description              | ISO Module Contact | Standard Package Pin |
|------|--------------------------|--------------------|----------------------|
| VCC  | Supply Voltage           | C1                 | 8                    |
| GND  | Ground                   | C5                 | 1                    |
| SCL  | Serial Clock Input       | C3                 | 6                    |
| SDA  | Serial Data Input/Output | C7                 | 3                    |
| RST  | Reset Input              | C2                 | 7                    |

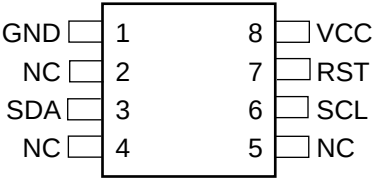
**Figure 0-1.** Card Module Contact



## 3 x 64 x 8 Secure Memory with Authentication

**AT88SC153**

**Figure 0-2.** 8-pin SOIC or, PDIP

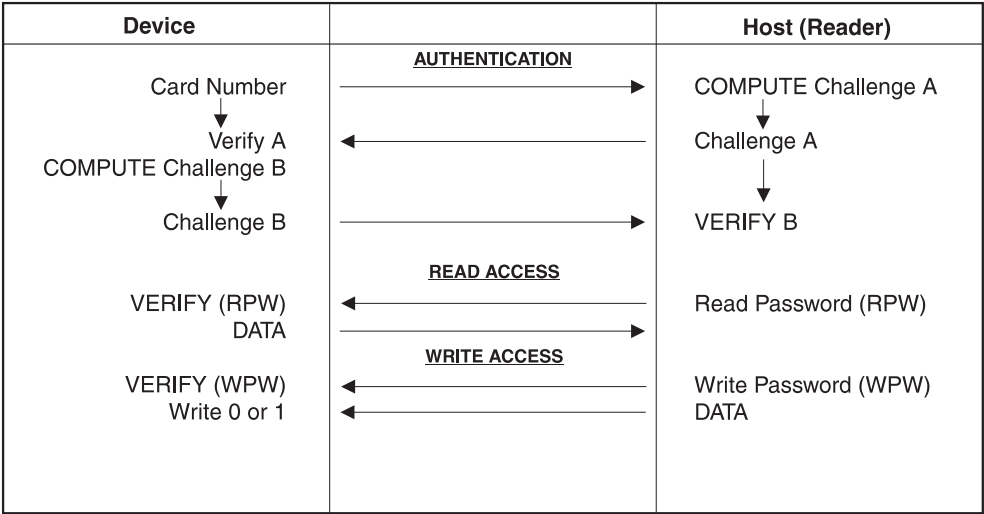


## 1. Description

The AT88SC153 provides 2,048 bits of serial EEPROM memory organized as one configuration zone of 64 bytes and three user zones of 64 bytes each. This device is optimized as a “secure memory” for multiapplication smart card markets, secure identification for electronic data transfer, or components in a system without the requirement of an internal microprocessor.

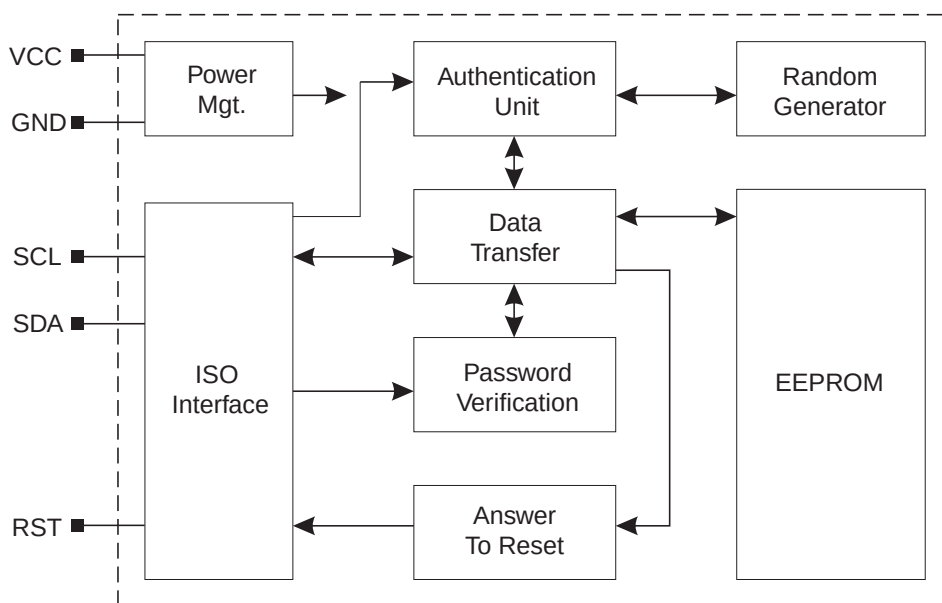
The embedded authentication protocol allows the memory and the host to authenticate each other. When this device is used with a host that incorporates a microcontroller (e.g., AT89C51, AT89C2051, AT90S1200), the system provides an “anti-wiretapping” configuration. The device and the host exchange “challenges” issued from a random generator and verify their values through a specific cryptographic function included in each part. When both agree on the same result, the access to the memory is permitted.

**Figure 1-1.** Security Methodology



## 2. Memory Access

Depending on the device configuration, the host might carry out the authentication protocol and/or present different passwords for each operation, read or write. Each user zone may be configured for free access for read and write or for password-restricted access. To insure security between the different user zones (multiapplication card), each zone can use a different set of passwords. A specific attempts counter for each password and for the authentication provides protection against “systematic attacks.” When the memory is unlocked, the two-wire serial protocol is effective, using SDA and SCL. The memory includes a specific register providing a 32-bit data stream conforming to the ISO 7816-10 synchronous answer-to-reset.

**Figure 2-1. Block Diagram**


## 3. Pin Descriptions

### 3.1 Supply Voltage (VCC)

The VCC input is a 2.7V-to-5.5V positive voltage supplied by the host.

### 3.2 Serial Clock (SCL)

The SCL input is used to positive edge clock data into the device and negative edge clock data out of the device.

### 3.3 Serial Data (SDA)

The SDA pin is bidirectional for serial data transfer. This pin is open-drain driven and may be wire-ORed with any number of other open-drain or open-collector devices. An external pull-up resistor should be connected between SDA and VCC. The value of this resistor and the system capacitance loading the SDA bus will determine the rise time of SDA. 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.

### 3.4 Reset (RST)

When the RST input is pulsed high, the device will output the data programmed into the 32-bit answer-to-reset register. All password and authentication access will be reset. Following a reset, device authentication and password verification sequences must be presented to re-establish user access.

## 4. Memory Mapping

The 2,048 bits of the memory are divided in four zones of 64 bytes each.

**Table 4-1.** Memory Map

| Zone                             | \$0      | \$1 | \$2 | \$3 | \$4 | \$5 | \$6 | \$7 | @    |
|----------------------------------|----------|-----|-----|-----|-----|-----|-----|-----|------|
| User 0<br>zz <sup>(1)</sup> = 00 |          |     |     |     |     |     |     |     | \$00 |
|                                  | 64 bytes |     |     |     |     |     |     |     | -    |
|                                  |          |     |     |     |     |     |     |     | -    |
|                                  |          |     |     |     |     |     |     |     | \$38 |
| User 1<br>zz = 01                |          |     |     |     |     |     |     |     | \$00 |
|                                  | 64 bytes |     |     |     |     |     |     |     | -    |
|                                  |          |     |     |     |     |     |     |     | -    |
|                                  |          |     |     |     |     |     |     |     | \$38 |
| User 2<br>zz = 10                |          |     |     |     |     |     |     |     | \$00 |
|                                  | 64 bytes |     |     |     |     |     |     |     | -    |
|                                  |          |     |     |     |     |     |     |     | -    |
|                                  |          |     |     |     |     |     |     |     | \$38 |
| Configuration<br>zz = 11         |          |     |     |     |     |     |     |     | \$00 |
|                                  | 64 bytes |     |     |     |     |     |     |     | -    |
|                                  |          |     |     |     |     |     |     |     | -    |
|                                  |          |     |     |     |     |     |     |     | \$38 |

Note: 1. zz = zone number

The last 64 bytes of the memory is a configuration zone with specific system data, access rights, and read/write commands; it is divided into four subzones.

**Table 4-2.** Configuration Zone

| Configuration  | \$0                | \$1                        | \$2 | \$3 | \$4              | \$5    | \$6 | \$7 | @    |
|----------------|--------------------|----------------------------|-----|-----|------------------|--------|-----|-----|------|
| Fabrication    | Answer-to-Reset    |                            |     |     | Lot History Code |        |     |     | \$00 |
|                | Fab Code           |                            | CMC |     | AR0              | AR1    | AR2 | MTZ | \$08 |
| Identification | Issuer Code        |                            |     |     |                  |        |     |     | \$10 |
|                | DCR                | Identification Number (Nc) |     |     |                  |        |     |     | \$18 |
|                | AAC <sup>(1)</sup> | Cryptogram (Ci)            |     |     |                  |        |     |     | \$20 |
| Secret         | Secret Seed (Gc)   |                            |     |     |                  |        |     |     | \$28 |
| Passwords      | PAC                | Write 0                    |     |     | PAC              | Read 0 |     |     | \$30 |
|                | PAC                | Secure Code/Write 1        |     |     | PAC              | Read 1 |     |     | \$38 |

Note: 1. Address \$20 also serves as the virtual address of the Checksum Authentication Register (CAR) during checksum mode.

Note: CMC: Card Manufacturer Code  
 AR0–2: Access Register for User Zone 0 to 2  
 MTZ: Memory Test Zone  
 DCR: Device Configuration Register  
 AAC: Authentication Attempts Counter  
 PAC: Password Attempts Counter

## 5. Fuses

FAB, CMA, and PER are nonvolatile fuses blown at the end of each card life step. Once blown, these EEPROM fuses can not be reset.

- The FAB fuse is blown by Atmel prior to shipping wafers to the card manufacturer.
- The CMA fuse is blown by the card manufacturer prior to shipping cards to the issuer.
- The PER fuse is blown by the issuer prior to shipping cards to the end user.

The device responds to a read fuse command with *fuse byte*.

**Table 5-1.** Fuse Byte

| Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
|-------|-------|-------|-------|-------|-------|-------|-------|
| 0     | 0     | 0     | 0     | 0     | PER   | CMA   | FAB   |

When the fuses are all “1”s, read and write are allowed in the entire memory. Before blowing the FAB fuse, Atmel writes the entire memory to “1” and programs the fabrication subzone (except CMC and AR) and the secure code.

**Table 5-2.** Access Rights

| Zone                                    | Access | FAB = 0     | CMA = 0     | PER = 0   |
|-----------------------------------------|--------|-------------|-------------|-----------|
| Fabrication<br>(Except CMC, MTZ and AR) | Read   | Free        | Free        | Free      |
|                                         | Write  | Forbidden   | Forbidden   | Forbidden |
| Card Manufacturer<br>Code               | Read   | Free        | Free        | Free      |
|                                         | Write  | Secure Code | Forbidden   | Forbidden |
| Access Registers                        | Read   | Free        | Free        | Free      |
|                                         | Write  | Secure Code | Secure Code | Forbidden |
| Memory Test Zone                        | Read   | Free        | Free        | Free      |
|                                         | Write  | Free        | Free        | Free      |
| Identification                          | Read   | Free        | Free        | Free      |
|                                         | Write  | Secure Code | Secure Code | Forbidden |
| Secret                                  | Read   | Secure Code | Secure Code | Forbidden |
|                                         | Write  | Secure Code | Secure Code | Forbidden |
| Passwords                               | Read   | Secure Code | Secure Code | Write PW  |
|                                         | Write  | Secure Code | Secure Code | Write PW  |
| PAC                                     | Read   | Free        | Free        | Free      |
|                                         | Write  | Secure Code | Secure Code | Write PW  |
| User Zones                              | Read   | AR          | AR          | AR        |
|                                         | Write  | AR          | AR          | AR        |

Note: CMC: Card Manufacturer Code  
 AR: Access Rights as defined by the access registers  
 PW: Password

## 6. Configuration Zone

### 6.1 Answer-to-reset

32-bit register defined by Atmel

### 6.2 Lot History Code

32-bit register defined by Atmel

### 6.3 Fab Code

16-bit register defined by Atmel

### 6.4 Card Manufacturer Code

16-bit register defined by the card manufacturer

### 6.5 Issuer Code

64-bit register defined by the card issuer

### 6.6 Access Registers

Three 8-bit access registers defined by the issuer, one for each user zone (active low)

**Table 6-1.** Access Registers

| Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
|-------|-------|-------|-------|-------|-------|-------|-------|
| WPE   | RPE   | ATE   | AOW   | PWS   | WLM   | MDF   | PGO   |

**Write Password Enable (WPE):** If enabled (WPE = “0”), the user is required to verify the write password to allow write operations in the user zone. If disabled (WPE = “1”), all write operations are allowed within the zone. Verification of the write password also allows the read and write passwords to be changed.

**Read Password Enable (RPE):** If enabled (RPE = “0”), the user is required to verify either the read password or write password to allow read operations in the user zone. Read operations initiated without a verified password will return \$00 (or the status of the fuse bits, if either CMA or PER are still intact). Verification of the write password will always allow read access to the zone. RPE = “0” and WPE = “1” is allowed but is not recommended.

**Authentication Enable (ATE):** If enabled (ATE = “0”), a valid authentication sequence is required for both read and write and must be completed before access is allowed to the user zone. If disabled (ATE = “1”), authentication is not required for access.

**Authentication Only for Write (AOW):** If enabled (AOW = “0”), a valid authentication sequence must be completed before write access is allowed to the user zone. Read access to this zone is allowed without authentication. This bit is ignored if ATE is enabled.

**Password Select (PWS):** This bit defines which of the two password sets must be presented to allow access to the user zone. Each access register may point to a unique password set, or access registers for multiple zones may point to the same password set. In this case, verification of a single password will open several zones, combining the zones into a single larger zone.

**Write Lock Mode (WLM):** If enabled (WLM = “0”), the 8 bits of the first byte of each user zone page will define the locked/unlocked status for each byte in the page. Write access is forbidden to a byte if its associated bit in byte 0 is set to “0”. Bit 7 controls byte 7, bit 6 controls byte 6, etc.

**Modify Forbidden (MDF):** If enabled (MDF = “0”), no write access is allowed in the zone at any time. The user zone must be written before the PER is blown.

**Program Only (PGO):** If enabled (PGO = “0”), data within the zone may be changed from “1” to “0” but never from “0” to “1”.

## 6.7 Identification Number (Nc)

An identification number with up to 56 bits is defined by the issuer and should be unique for each device.

## 6.8 Cryptogram (Ci)

The 56-bit cryptogram is generated by the internal random generator and modified after each successful verification of the cryptogram by the chip, on host request. The initial value, defined by the issuer, is diversified as a function of the identification number. The 64 bits used in the authentication protocol consist of the 56-bit cryptogram and the 8-bit Authentication Attempts Counter (AAC). Note that any change in the AAC status will change Ci for the next authentication attempt.

## 6.9 Secret Seed (Gc)

The 64-bit secret seed, defined by the issuer, is diversified as a function of the identification number.

## 6.10 Memory Test Zone

The memory test zone is an 8-bit free access zone for memory and protocol test.

## 6.11 Password Set

The password set consists of two sets of two 24-bit passwords for read and write operations, defined by the issuer. The write password allows modification of the read and write passwords of the same set. By default, Password 1 is selected for all user zones.

**Secure Code:** The secure code is a 24-bit password defined by Atmel and is different for each card manufacturer. The Write 1 Password is used as the secure code until the personalization is over (PER = 0).

**Attempts Counters:** There are four 8-bit password attempts counters (PACs), one for each password, and one other 8-bit attempts counter for the authentication protocol (AAC). The attempts counters limit the number of consecutive incorrect code presentations allowed (currently four).

## 6.12 Device Configuration Register

This 8-bit register allows the issuer to select the device configuration options (active-low) shown in [Figure .](#)

**Table 6-2.** Device Configuration Options

| Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
|-------|-------|-------|-------|-------|-------|-------|-------|
| SME   | UCR   | UAT   | ETA   | CS3   | CS2   | CS1   | CS0   |

**Programmable Chip Select (CS0–CS3):** The four most significant bits (b4–b7) of every command comprise the chip select address. All AT88SC153 devices will respond to the default chip select address of \$B (1011). Each device will also respond to a second chip select address programmed into CS0–CS3 of the device configuration register. By programming each device to a unique chip select address, it is possible to connect up to 15 devices on the same serial data bus. The Write EEPROM and Verify Password commands can be used globally to all devices sharing the bus by using the default chip select address \$B.

**Eight Trials Allowed (ETA):** If enabled (ETA = “0”), the ETA extends the trials limit to eight incorrect presentations allowed (passwords or authentication). If disabled (ETA = “1”), the PAC and AAC will allow only four incorrect attempts.

**Unlimited Authentication Trials (UAT):** If enabled (UAT = “0”), the AAC is disabled, allowing an unlimited number of authentication attempts. The PACs are not affected by the UAT bit.

**Unlimited Checksum Reads (UCR):** If enabled (UCR = “0”), the device will allow an unlimited number of checksums without requiring a new authentication.

**Supervisor Mode Enable (SME):** If enabled (SME = “0”), verification of the Write 1 password will allow the user to write and read the entire passwords zone (including the PACs).

## 6.13 Checksum Authentication Register

After a valid authentication has been completed, the internal pseudo-random generator (PRG) will compute a secure checksum after one write command or several consecutive write commands. This checksum certifies that the data sent by the host during the write commands were received and therefore written in the memory. For every write command, the device clocks the data bytes into the PRG and its output is the Checksum Authentication Register (CAR), which is a function of Ci, Gc, Q, and the data bytes written.

After a valid authentication, any write command will enable the checksum mode and cause AAC to become the virtual location of the 8-byte CAR. When all data have been transmitted, the host may perform a *Read CAR* command by sending a read command with the AAC address (\$20). The first 8 bytes transmitted by the device form the secure checksum.

The checksum mode allows only a single *Read CAR* operation for each valid authentication. The checksum mode is disabled at the end of the *Read CAR* command, whatever the number of bytes transmitted, or by a read command with any other address. The checksum mode can only be enabled once for a given authentication.

**Note:** During the *Read CAR* command, the internal address counter is incremented just as in a normal read command. Once 8 bytes have been transmitted, the checksum mode is automatically disabled, and if the host continues to request data, the device responds as to a normal read command, from the address \$28.



## 7. User Zones

Three zones are dedicated to the user data. The access rights of each zone are programmable separately via the access registers. If several zones share the same password set, this set will be entered only once (after the part is powered up), so several zones might be combined in one larger zone.

## 8. Security Operations

### 8.1 Write Lock

If a user zone is configured in the write lock mode (access register bit 2), the lowest address byte of a page constitutes a write access byte for the bytes of that page.

**Table 8-1.** Write Lock

| \$0 - WLB | \$1         | \$2         | \$3 | \$4 | \$5         | \$6 | \$7 | @    |
|-----------|-------------|-------------|-----|-----|-------------|-----|-----|------|
| 11011001  | x x<br>Lock | x x<br>Lock | x x | x x | x x<br>Lock | x x | x x | \$00 |

Example: The write lock byte (WLB) at \$00 controls the bytes from \$00 to \$07.

The WLB can also lock itself by writing its least significant (right most) bit to "0". The WLB can only be programmed, i.e., bits written to "0" cannot return to "1".

In the write lock configuration, only one byte of the page can be written at a time. Even if several bytes are received, only the first byte will be taken into account by the device.

### 8.2 Password Verification

Compare the operation password presented with the stored one, and write a new bit in the corresponding attempts counter for each wrong attempt. A valid attempt erases the attempts counter and allows the operation to be carried out as long as the chip is powered.

The current password is memorized and active until power is turned off, unless a new password is presented or RST becomes active. Only one password is active at a time. The AT88SC153 requires that the Verify Password command be transmitted twice in sequence to successfully verify a write or read password. (This two-pass method of password verification was implemented in the AT88SC153 to protect the device from attacks on the password security system.) The first Verify Password command can be considered an initialization command. It will write a new bit ("0") in the corresponding PAC. The data bits in this initialization command are ignored. The second Verify Password command will compare the 3-byte password data presented with the corresponding password value stored in memory. If the comparison is valid, the PAC will be cleared. A successful password verification will allow authorized operations to be carried out as long as the chip is powered. The current password is memorized and active until power is turned off, a new password is presented, or RST becomes active. Only one password is active at a time. If a new user zone is selected that points to a different password set, the new password must be verified and the old password becomes invalid.

### 8.3 Authentication Protocol

The access to an user zone may be protected by an authentication protocol in addition to password-dependent rights.

The 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 has lost its previous authentication and it should be presented again. Only the last request is memorized.

The authentication verification protocol requires the host to perform an Initialize Authentication command, followed by a Verify Authentication command.

The password and authentication may be presented at any time and in any order. If the trials limit has been reached, i.e., the 8 bits of the attempts counter have been written, the password verification or authentication process will not be taken into account.

## 9. Command Definitions and Protocols

The communications protocol is based on the popular two-wire serial interface. Note that the *most* significant bit is transmitted first.

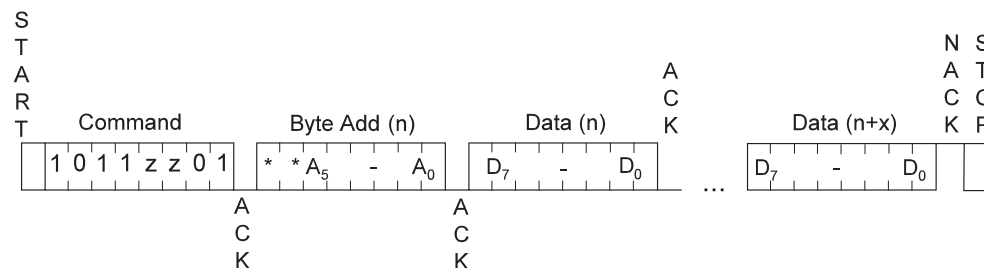
**Table 9-1.** Device Commands

| Description               | Command     |     |     |     |             |    |    |    |
|---------------------------|-------------|-----|-----|-----|-------------|----|----|----|
|                           | Chip Select |     |     |     | Instruction |    |    |    |
|                           | b7          | b6  | b5  | b4  | b3          | b2 | b1 | b0 |
| Write EEPROM              | CS3         | CS2 | CS1 | CS0 | z           | z  | 0  | 0  |
| Read EEPROM               | CS3         | CS2 | CS1 | CS0 | z           | z  | 0  | 1  |
| Verify Password           | CS3         | CS2 | CS1 | CS0 | r           | p  | 1  | 1  |
| Initialize Authentication | CS3         | CS2 | CS1 | CS0 | 0           | 0  | 1  | 0  |
| Verify Authentication     | CS3         | CS2 | CS1 | CS0 | 0           | 1  | 1  | 0  |
| Write Fuse                | CS3         | CS2 | CS1 | CS0 | 1           | 0  | 1  | 0  |
| Read Fuse                 | CS3         | CS2 | CS1 | CS0 | 1           | 1  | 1  | 0  |

Note: r : Read/write password  
p : Password set

## 9.1 Read EEPROM

Figure 9-1. Read EEPROM

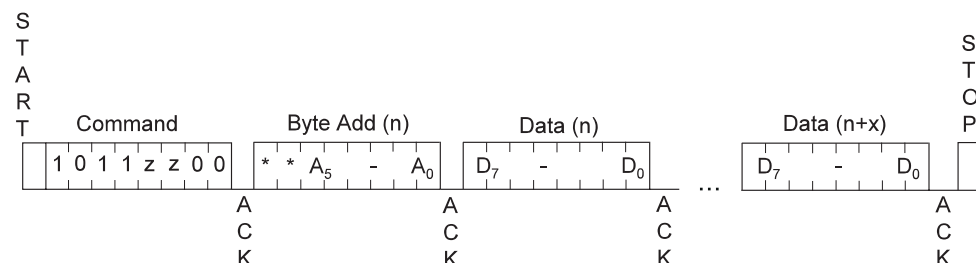


Note: \*don't care bit  
zz: Zone number

The data byte address is internally incremented following the transmission of each data byte. During a read operation, the address “roll over” is from the last byte of the current zone to the first byte of the same zone. If the host is not allowed to read at the specified address, the device will transmit the corresponding data byte with all bits equal to “0”.

## 9.2 Write EEPROM

Figure 9-2. Write EEPROM

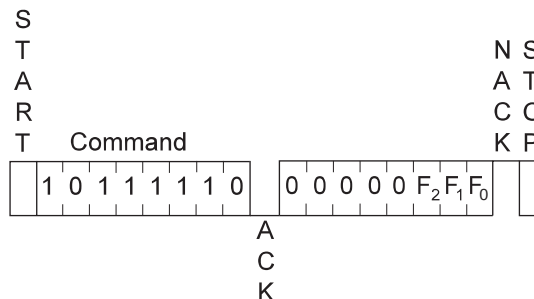


Note: \*don't care bit  
zz: Zone number

The data byte address lower three bits are internally incremented following the receipt of each data byte. The higher data byte address bits are not incremented, retaining the 8-byte write page address. Each data byte within a page must only be loaded once. Once a stop condition is issued to indicate the end of the host's write operation, the device initiates the internal nonvolatile write cycle. An ACK polling sequence can be initiated immediately. After a write command, if the host is not allowed to write at some address locations, a nonvolatile write cycle will still be initiated, but the device will only modify data at the allowed addresses. When write lock mode is enabled (WLM = “0”), the write cycle is initiated automatically after the first data byte has been transmitted.

## 9.3 Read Fuses

**Figure 9-3.** Read Fuses

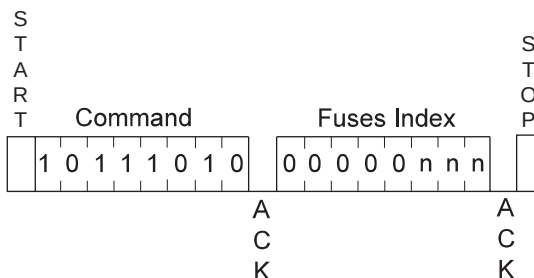


Note: F<sub>x</sub> = 1: fuse is not blown  
F<sub>x</sub> = 0: fuse is blown

The Read Fuses operation is always allowed. The AT88SC153 will continuously transmit the fuse byte if the host continues to transmit an ACK. The command is terminated when the host transmits a NACK and STOP bit.

## 9.4 Write Fuses

**Figure 9-4.** Write Fuses



Note: nnn = 001 : Blow FAB  
nnn = 010 : Blow CMA  
nnn = 100 : Blow PER

The Write Fuses operation is only allowed under secure code control; no data byte is transmitted by the host. The fuses are blown sequentially: CMA is blown if FAB is equal to "0", and PER is blown if CMA is equal to "0". If the fuses are all "0"s, the operation is canceled and the device waits for a new command.

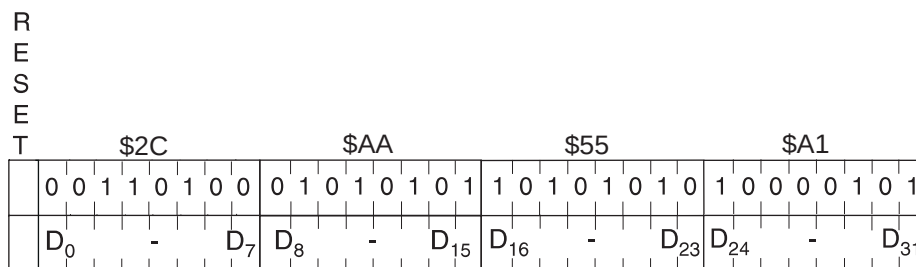
Once a stop condition is issued to indicate the end of the host's write operation, the device initiates the internal nonvolatile write cycle. An ACK polling sequence can be initiated immediately.

## 9.5 Answer-to-reset

If RST is high during SCL clock pulse, the reset operation occurs according to the ISO 7816-10 synchronous answer-to-reset. The four bytes of the answer-to-reset register are transmitted least significant bit first, on the 32 clock pulses provided on SCL.

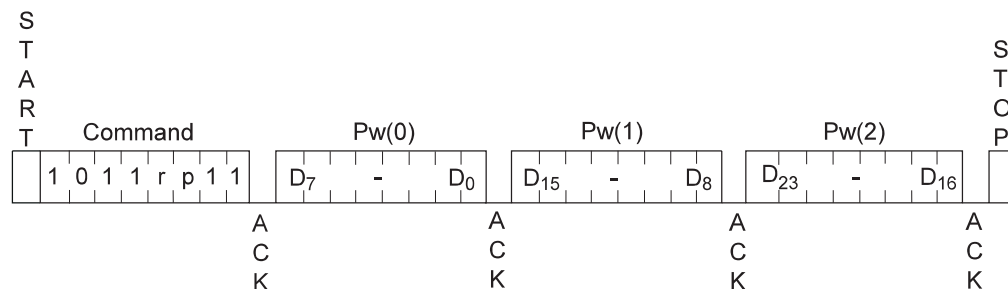
The values programmed by Atmel are shown in [Figure 9-5](#) below.

Figure 9-5. Answer-to-reset Values



## 9.6 Verify Password

Figure 9-6. Verify Password

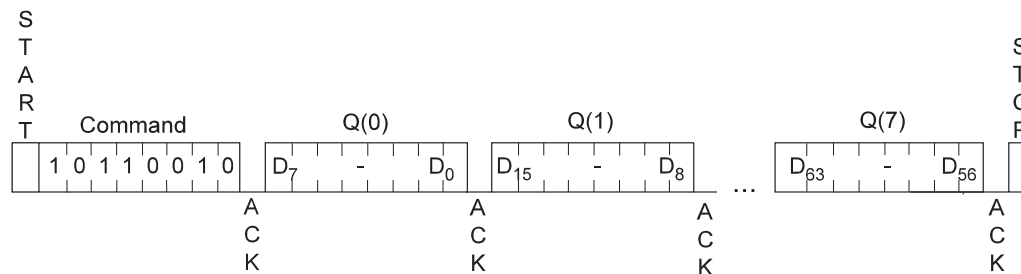


Note: Pw: Password, 3 bytes.  
 The two bits "rp" indicate the password to compare:  
 r = 0: Write password  
 r = 1: Read password  
 p: Password set number  
 rp = 01 for the secure code

This command must be transmitted twice in sequence to successfully verify a write or read password. The first Verify Password command can be considered an initialization command. It will write a new bit ("0") in the PAC corresponding to the "r" and "p" bits. The data bits in this initialization command are ignored. The second Verify Password command will compare the 3-byte password data presented with the corresponding password value stored in memory. If the comparison is valid, the PAC will be cleared. For both commands, once the command sequence is completed and a stop condition is issued, a nonvolatile write cycle is initiated to update the associated attempts counter. After the stop condition is issued, an ACK polling sequence with the specific command byte of \$BD will indicate the end of the write cycle and will read the attempts counter in the configuration zone. The initialization command will result in a "0" bit in the PAC. The second Verify Password command will read \$FF in the PAC if the verification was successful.

## 9.7 Initialize Authentication

**Figure 9-7.** Initiatize Authentication

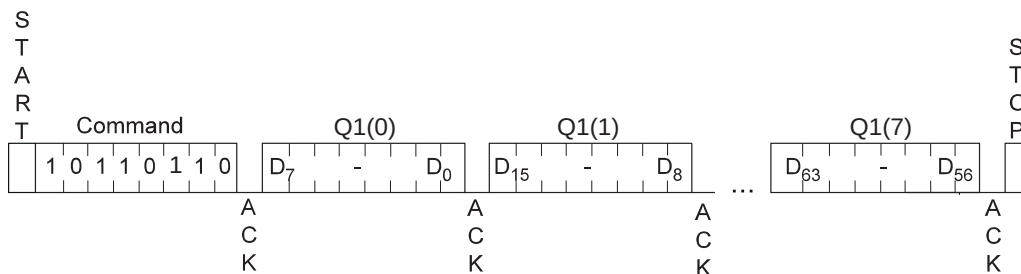


Note: Q: Host random number, 8 bytes

The Initialize Authentication command sets up the random generator with the cryptogram (Ci), the secret seed (Gc), and the host random number (Q). Once the sequence is completed and a stop condition is issued, there is a nonvolatile write cycle to clear a new bit of the AAC. In order to complete the authentication protocol, the device requires the host to perform an ACK polling sequence with the specific command byte of \$B6, corresponding to the Verify Authentication command.

## 9.8 Verify Authentication

**Figure 9-8.** Verify Authentication



Note: Q1: Host challenge, 8 bytes

If Q1 is equal to Ci + 1, then the device writes Ci + 2 in memory in place of Ci; this must be preceded by the Initialize Authentication command. Once the sequence is completed and a stop condition is issued, there is a nonvolatile write cycle to update the associated attempts counter. In order to know whether or not the authentication was correct, the device requires the host to perform an ACK polling sequence with the specific command byte of \$BD, to read the corresponding attempts counter in the configuration zone. A valid authentication will result in the AAC cleared to \$FF. An invalid authentication attempt will initiate a nonvolatile write cycle, but no clear operation will be performed on the AAC.

## 10. Device Operation

### 10.1 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 ([Figure 10-2 on page 16](#)). Data changes during SCL-high time periods will indicate a start or stop condition as defined below.

### 10.2 Start Condition

A high-to-low transition of SDA with SCL high is a start condition that must precede any other command ([Figure 10-1 on page 15](#)).

### 10.3 Stop Condition

A low-to-high transition of SDA with SCL high is a stop condition. After a read sequence, the stop command will place the device in a standby power mode ([Figure 10-1 on page 15](#)).

### 10.4 Acknowledge

All addresses and data are serially transmitted to and from the device in 8-bit words. The device sends a “0” to acknowledge that it has received each byte. This happens during the ninth clock cycle.

### 10.5 Standby Mode

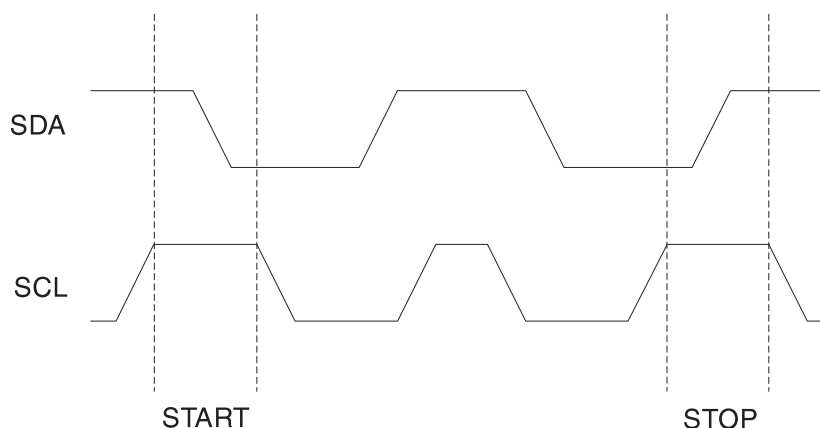
The AT88SC153 features a low-power standby mode that is enabled upon power-up and after the receipt of the stop bit and the completion of any internal operations.

### 10.6 Acknowledge Polling

Once the internally-timed write cycle has started and the device inputs are disabled, acknowledge polling can be initiated. This involves sending a start condition followed by the command byte representative of the operation desired. Only if the internal write cycle has completed will the device respond with a “0”, allowing the sequence to continue.

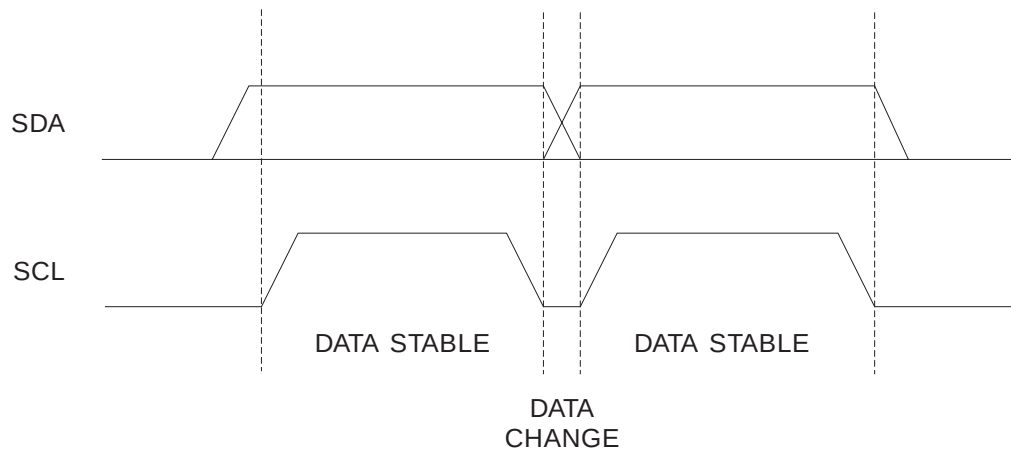
### 10.7 Device Timing

**Figure 10-1.** Start and Stop Definition

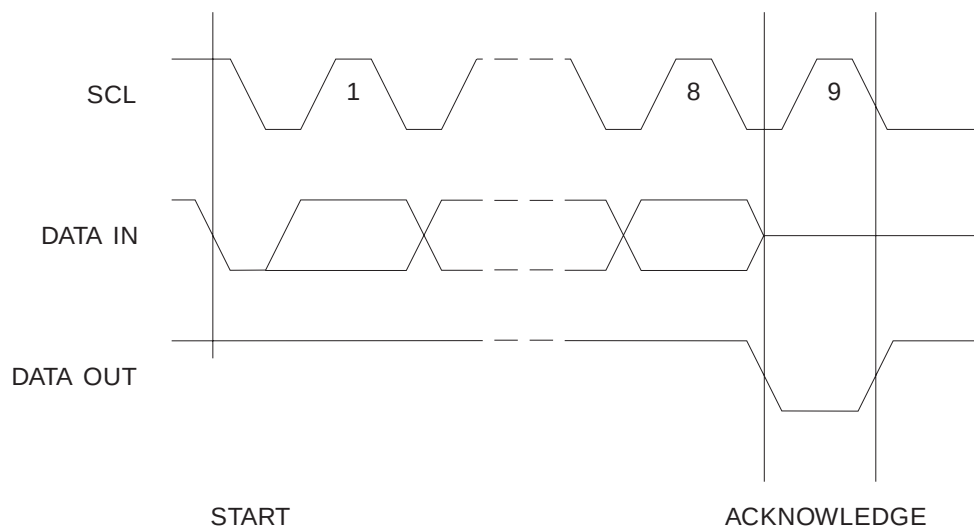


Note: The SCL input should be low when the device is idle. Therefore, SCL is low before a start condition and after a stop condition.

**Figure 10-2.** Data Validity



**Figure 10-3.** Output Acknowledge



Note: To transmit a NACK (no acknowledge), hold data (SDA) high during the entire ninth clock cycle.



## 11. Absolute Maximum Ratings

|                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operating Temperature: 0°C to +70°C<br>Storage Temperature: – 65°C to +150°C<br>Voltage on Any Pin with Respect to Ground: – 0.7V to $V_{CC} + 0.7V$<br>Maximum Voltage: 6.25V<br>DC Output Current: 5.0 mA | <b>*NOTICE:</b> Stresses beyond those listed under “Absolute Maximum Ratings” may cause permanent damage to the device. This is a stress rating only; functional operation of the device at these or any other conditions 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 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 12. DC Characteristics

**Table 12-1.** DC Characteristics

Applicable over recommended operating range from:  $V_{CC} = +2.7V$  to 5.5V,  $T_{AC} = 0^{\circ}C$  to +70°C (unless otherwise noted).

| Symbol          | Parameter                            | Test Condition               | Min                 | Typ | Max                 | Units |
|-----------------|--------------------------------------|------------------------------|---------------------|-----|---------------------|-------|
| $V_{CC}^{(1)}$  | Supply Voltage                       |                              | 2.7                 |     | 5.5                 | V     |
| $I_{CC}$        | Supply Current ( $V_{CC} = 5.0V$ )   | READ at 1 MHz <sup>(2)</sup> |                     |     | 5.0                 | mA    |
| $I_{CC}$        | Supply Current ( $V_{CC} = 5.0V$ )   | WRITE at 1 MHz               |                     |     | 5.0                 | mA    |
| $I_{SB1}^{(1)}$ | Standby Current ( $V_{CC} = 2.7V$ )  | $V_{IN} = V_{CC}$ or GND     |                     |     | 1.0                 | μA    |
| $I_{SB2}$       | Standby Current ( $V_{CC} = 5.0V$ )  | $V_{IN} = V_{CC}$ or GND     |                     |     | 5.0                 | μA    |
| $I_{LI}$        | Input Leakage Current                | $V_{IN} = V_{CC}$ or GND     |                     |     | 1.0                 | μA    |
| $I_{LI}$        | RST Input Leakage Current            | $V_{IN} = V_{CC}$ or GND     |                     |     | 20.0                | μA    |
| $I_{LO}$        | Output Leakage Current               | $V_{OUT} = V_{CC}$ or GND    |                     |     | 1.0                 | μA    |
| $V_{IL}$        | Input Low Level <sup>(3)</sup>       |                              | -0.3                |     | $V_{CC} \times 0.3$ | V     |
| $V_{IH}$        | Input High Level <sup>(3)</sup>      |                              | $V_{CC} \times 0.7$ |     | $V_{CC} + 0.5$      | V     |
| $V_{OL2}$       | Output Low Level ( $V_{CC} = 2.7V$ ) | $I_{OL} = 2.1$ mA            |                     |     | 0.4                 | V     |

- Notes:
1. This parameter is preliminary; Atmel may change the specifications upon further characterization.
  2. Output not loaded.
  3.  $V_{IL}$  min and  $V_{IH}$  max are reference only and are not tested.

## 13. AC Characteristics

**Table 13-1.** AC Characteristics

Applicable over recommended operating range from  $T_A = 0^\circ\text{C}$  to  $+70^\circ\text{C}$ ,  $V_{CC} = +2.7\text{V}$  to  $+5.5\text{V}$ ,  $CL = 1$  TTL Gate and 100 pF (unless otherwise noted).

| Symbol       | Parameter                                                                         | 5.0 Volt |     | Units |
|--------------|-----------------------------------------------------------------------------------|----------|-----|-------|
|              |                                                                                   | Min      | Max |       |
| $f_{SCL}$    | Clock Frequency, SCL                                                              |          | 1.0 | MHz   |
| $t_{LOW}$    | Clock Pulse Width Low                                                             | 400      |     | ns    |
| $t_{HIGH}$   | Clock Pulse Width High                                                            | 400      |     | ns    |
| $t_{AA}$     | Clock Low to Data Out Valid                                                       |          | 550 | 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                                                                 | 0        |     | ns    |
| $t_{SU,DAT}$ | Data In Set-up Time                                                               | 100      |     | ns    |
| $t_R$        | Inputs Rise Time <sup>(1,2)</sup>                                                 |          | 300 | ns    |
| $t_F$        | Inputs Fall Time <sup>(1,2)</sup>                                                 |          | 100 | ns    |
| $t_{SU,STO}$ | Stop Set-up Time                                                                  | 200      |     | ns    |
| $t_{DH}$     | Data Out Hold Time                                                                | 0        |     | ns    |
| $t_{WR}$     | Write Cycle Time                                                                  |          | 10  | ms    |
| $t_{RST}$    | Reset Width High                                                                  | 600      |     | ns    |
| $t_{SU,RST}$ | Reset Set-up Time                                                                 | 50       |     | ns    |
| $t_{HD,RST}$ | Reset Hold Time                                                                   | 50       |     | ns    |
| $t_{BUF}$    | Period of time the bus must be free before a new command can start <sup>(1)</sup> |          | 500 | ns    |
| $t_{VCC}$    | Power On Reset Time                                                               |          | 2.0 | ms    |

Notes: 1. This parameter is characterized and is not 100% tested.

2. Input rise and fall transitions must be monotonic.

## 14. Pin Capacitance

**Table 14-1.** Pin Capacitance

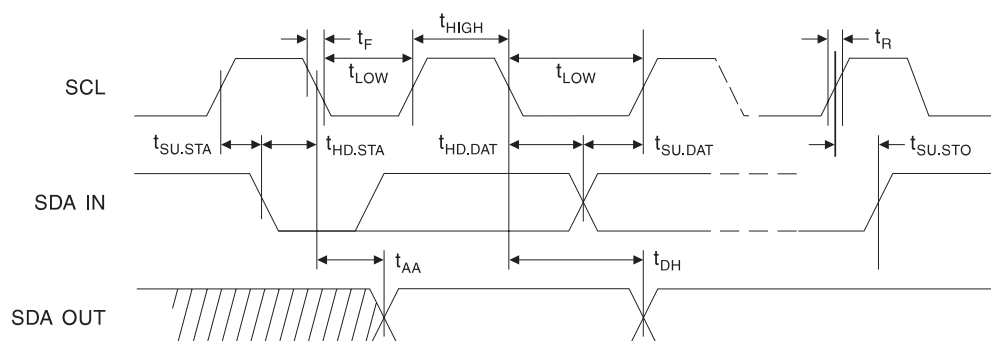
Applicable at recommended operating conditions:  $T_A = 25^\circ\text{C}$ ,  $f = 1.0$  MHz,  $V_{CC} = +2.7\text{V}$ .

| Symbol    | Test Condition                                | Max | Units | Conditions            |
|-----------|-----------------------------------------------|-----|-------|-----------------------|
| $C_{I/O}$ | Input/Output Capacitance (SDA) <sup>(1)</sup> | 8   | pF    | $V_{I/O} = 0\text{V}$ |
| $C_{IN}$  | Input Capacitance (RST, SCL) <sup>(1)</sup>   | 6   | pF    | $V_{IN} = 0\text{V}$  |

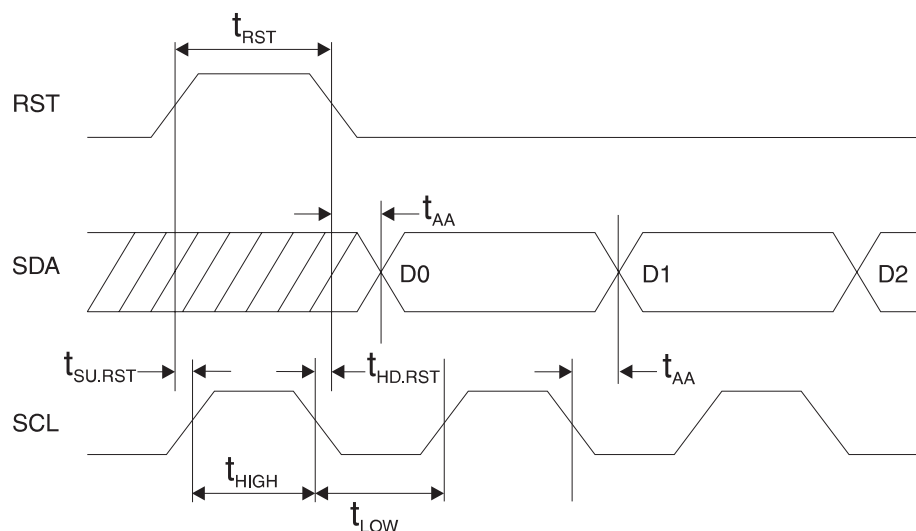
Notes: 1. This parameter is characterized and is not 100% tested.

## 15. Timing Diagrams

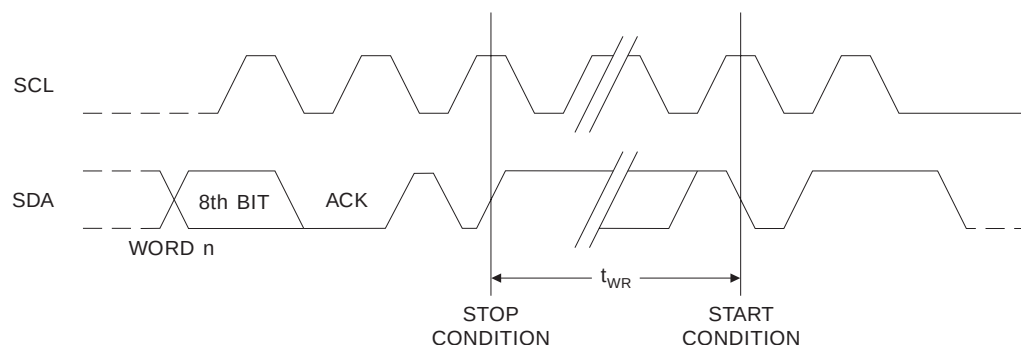
**Figure 15-1.** Bus Timing (SCL: Serial Clock; SDA: Serial Data I/O)



**Figure 15-2.** Synchronous Answer-to-reset Timing



**Figure 15-3.** Write Cycle (SCL: Serial Clock; SDA: Serial Data I/O)



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

## 16. Ordering Information

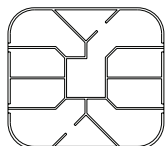
| Ordering Code     | Package       | Voltage Range | Temperature Range        |
|-------------------|---------------|---------------|--------------------------|
| AT88SC153-09ET-00 | M2 – E Module | 2.7V–5.5V     | Commerical (0°C–70°C)    |
| AT88SC153-09PT-00 | M2 – P Module | 2.7V–5.5V     | Commerical (0°C–70°C)    |
| AT88SC153-10PU-00 | 8P3           | 2.7V–5.5V     | Industrial (– 40°C–85°C) |
| AT88SC153-10SU-00 | 8S1           | 2.7V–5.5V     | Industrial (– 40°C–85°C) |
| AT88SC153-10WU-00 | 7 mil Wafer   | 2.7V–5.5V     | Industrial (– 40°C–85°C) |

| Package Type <sup>(1)</sup> | Description                                                               |
|-----------------------------|---------------------------------------------------------------------------|
| M2 – P Module               | M2 ISO 7816 Smart Card Module with Atmel Logo                             |
| M2 – E Module               | M2 ISO 7816 Smart Card Module                                             |
| 8S1                         | 8-lead, 0.150" Wide, Plastic Gull Wing Small Outline Package (JEDEC SOIC) |
| 8P3                         | 8-lead, 0.300" Wide, Plastic Dual Inline Package (PDIP)                   |

Notes: 1. Formal drawings may be obtained from an Atmel Sales Office.

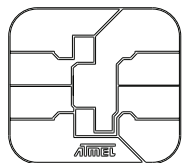
## 17. Smart Card Modules

### Ordering Code: 09ET-00



Module Size: **M2-00**  
 Dimension\*: 12.6 x 11.4 [mm]  
 Glob Top: Clear, Round:  $\varnothing$  8.0 [mm] max  
 Thickness: 0.58 [mm] max  
 Pitch: 14.25 [mm]

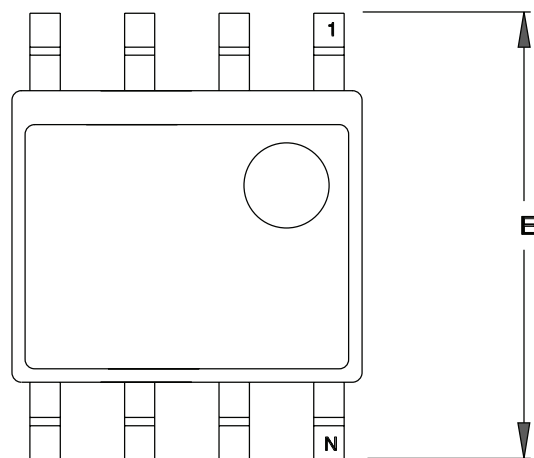
### Ordering Code: 09PT-00



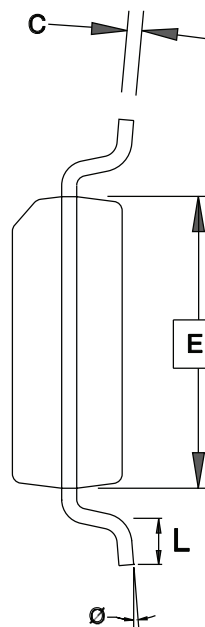
Module Size: **M2**  
 Dimension\*: 12.6 x 11.4 [mm]  
 Glob Top: Square: 8.8 x 8.8 [mm]  
 Thickness: 0.58 [mm]  
 Pitch: 14.25 [mm]

\*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 0.4 mm greater in both directions (i.e., a punched M2 module will yield 13.0 x 11.8 mm).

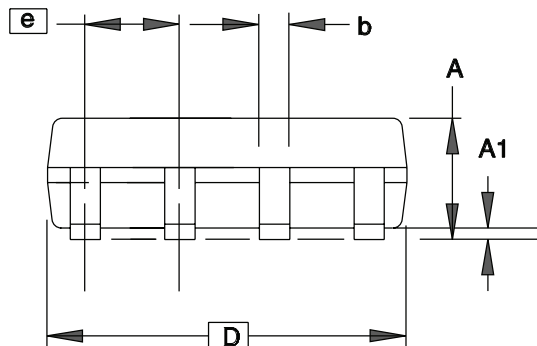
**Ordering Code: 10SU-00**  
**8-lead SOIC**



**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 |      |
| θ      | 0°       | —   | 8°   |      |

Note: These drawings are for general information only. Refer to JEDEC Drawing MS-012, Variation AA for proper dimensions, tolerances, datums, etc.

3/17/05



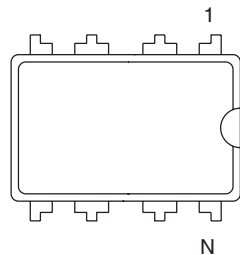
1150 E. Cheyenne Mtn. Blvd.  
 Colorado Springs, CO 80906

**TITLE**  
**8S1**, 8-lead (0.150" Wide Body), Plastic Gull Wing  
 Small Outline (JEDEC SOIC)

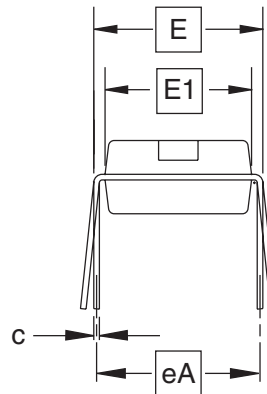
**DRAWING NO.**  
 8S1

**REV.**  
 C

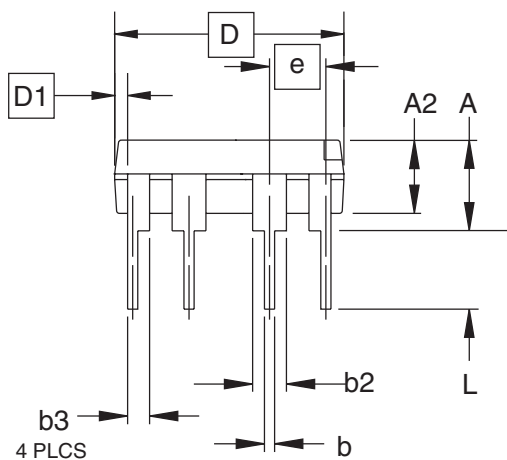
# Ordering Code: 10PU-00 8-lead PDIP



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).

01/09/02



2325 Orchard Parkway  
San Jose, CA 95131

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

**DRAWING NO.**  
8P3

**REV.**  
B

## Revision History

| Lit Number | Date    | Comment                                                                                                                                                                                                         |
|------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1016E      | 12/2007 | Adjusted Absolute Maximum Ratings<br>Adjusted Ordering Codes<br>Removed LAP<br>Fixed spacing on minus signs<br>Updated to new template<br>Modified Ordering Codes<br>Replaced 8-lead SOIC figure with version C |



## Headquarters

---

**Atmel Corporation**  
2325 Orchard Parkway  
San Jose, CA 95131  
USA  
Tel: 1(408) 441-0311  
Fax: 1(408) 487-2600

## International

---

**Atmel Asia**  
Room 1219  
Chinachem Golden Plaza  
77 Mody Road Tsimshatsui  
East Kowloon  
Hong Kong  
Tel: (852) 2721-9778  
Fax: (852) 2722-1369

**Atmel Europe**  
Le Krebs  
8, Rue Jean-Pierre Timbaud  
BP 309  
78054 Saint-Quentin-en-  
Yvelines Cedex  
France  
Tel: (33) 1-30-60-70-00  
Fax: (33) 1-30-60-71-11

**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

## Product Contact

---

**Web Site**  
[www.atmel.com/products/securemem](http://www.atmel.com/products/securemem)

**Technical Support**  
[securememories@atmel.com](mailto:securememories@atmel.com)

**Sales Contact**  
[www.atmel.com/contacts](http://www.atmel.com/contacts)

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

---

**Disclaimer:** The information in this document is provided in connection with Atmel products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Atmel products. **EXCEPT AS SET FORTH IN ATMEL'S TERMS AND CONDITIONS OF SALE LOCATED ON ATMEL'S WEB SITE, ATMEL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ATMEL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ATMEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.** Atmel makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Unless specifically provided otherwise, Atmel products are not suitable for, and shall not be used in, automotive applications. Atmel's products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.

© 2007 Atmel Corporation. All rights reserved. Atmel®, logo 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.