Features

- **1K X 1 Serial EEPROM with Security Logic**
- **One Application Zone**
- **Stores and Validates Security Codes**
- **Maximum of Eight Incorrect Security Code Attempts**
- **Provides Transport Code Security**
- **Low Voltage Operation: 2.7V to 5.5V**
- **Manufactured using Low Power CMOS Technology**
- **Supports ISO/IEC 7816-3 Synchronous Protocol.**
- **V_{PP} Internally Generated**
- **2 µs Read Access Time; 2 ms Write Cycle Time**
- **Temperature Range from -40°C to 85°C**
- **ESD Protection 4,000V Minimum**
- **High Reliability:**
  - **100,000 Program/Erase Cycles Guaranteed**
  - **Data Retention of 10 years**

1K EEPROM - Security Logic with One Application Zone

AT88SC101

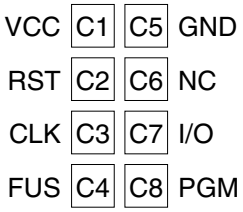
Description

The AT88SC101 device is a low-cost, synchronous, secure memory integrated circuit designed for use in prepaid and loyalty smart card applications. The AT88SC101 provides 1024 bits of serial Electrically Erasable and Programmable Read Only Memory (EEPROM) within one application zone, plus 64 bits in a code protected zone. Additional EEPROM memory and security logic provide security for smart card applications. Space is provided in the EEPROM memory for manufacturing records for both the smart card manufacturer and card issuer. After personalization, these records, and the state of the bit which enables the Erase Counter function, are locked and protected from modification for the lifetime of the product.

ISO Card Contact Descriptions

ISO Contact	Pad Name	Description
C1	VCC	Operating Voltage
C2	RST	Address Reset
C3	CLK	Clock and Address Control
C4	FUS	Fuse
C5	GND	Ground
C6	NC	No Connect
C7	I/O	Bidirectional Data
C8	PGM	Programming Control

Card Module Contacts



Rev. 1418B–11/99

Terminology

The following terms have specific definitions for the AT88SC101.

ERASE: A program operation which results in an EEPROM data bit being set to a logic “1” state. Outside the Application Zone, all Erase operations are performed on 16-bit words. An erase operation performed on any bit within a word will execute an erase of the entire word. Inside the Application zone, erase operations are controlled by the SV Flag, EZ passwords and the EC_EN fuse. These operations are defined in the “Device Operation” section of the data sheet.

WRITE: A program operation which results in an EEPROM bit, or word being set to a logic “0” state. An unwritten bit is defined as erased, or set to a logic “1” state. Write operations in the AT88SC101 may be performed on individual bits after security code validation. In Security Level 2, write operations also require that the P1 bit within the Application Zone is set to “1”.

PROGRAM: An EEPROM function which activates internally timed, high voltage circuitry and results in a data bit, or word being set to either a logic “0” or “1” state.

BIT: A single data element set to either a logic “0” or “1” state. All bit addresses within the Application Zone (AZ) may be written individually.

BYTE: Eight consecutive data bits. A byte boundary will begin on an address that is evenly divisible by eight. The AT88SC101 has no capability for byte write operations.

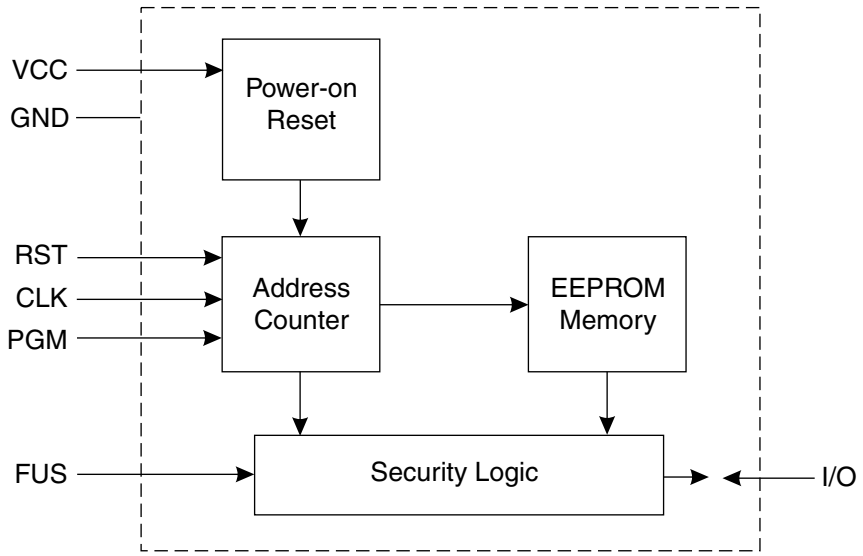
WORD: Sixteen consecutive data bits. A Word boundary will begin on an address that is evenly divisible by 16. Erase operations will always operate on 16-bit words when applied to addresses outside the Application Zone. In Security Level 1, erase operations within the Application Zone also operate on 16-bit words. In Security Level 2, erase operations within the Application Zone operate on the entire zone. Write operations function on single bits, not words, in both security levels.

BLOWN: In reference to an AT88SC101 internal EEPROM fuse, the blown state is a logic “0”.

UNBLOWN: In reference to an AT88SC101 internal EEPROM fuse, the unblown state is a logic “1”.

VERIFICATION: AT88SC101 operations are controlled by the state of several internal flags. The flags SV, and E1 are set after verification of an associated password (security code or EZ respectively). Verification is accomplished by executing an INC/CMP operation, which correctly matches the password bit by bit as the CLK increments the address through the password memory addresses.

Block Diagram



The AT88SC101 is manufactured using low-power CMOS technology and features its own internal high-voltage pump for single voltage supply operation. The devices are guaranteed to 100,000 erase/write cycles and 10-year data retention. The AT88SC101 supports the ISO/IEC 7816-3 synchronous protocol.

Security Features

The Security Features of Atmel's AT88SC101 include:

- Data access only after validation of the security code.
- Permanent invalidation of the device after eight consecutive false Security Code presentations.
- Read/write protection of certain memory zones.
- Secure transport of devices using transport code compare sequence.
- Unique customer identification number written and locked into every device for protection against duplication or counterfeiting.

Security Levels and Memory Access to AT88SC101

Access to the memory is controlled by the state of the Issuer Fuse and by the voltage supply applied on the FUS pad.

FUS Pad	Issuer Fuse	Security Level
Logic "0"	X	2
Logic "1"	1 (unblown)	1
Logic "1"	0 (unblown)	2

Level 1: (Security During Personalization)

Conditions:

ISSUER FUES = "1" (not blown)

FUS PIN = "1" (required)

AT88SC101 die and modules are delivered with the Issuer Fuse intact (unblown). Issuer personalization is completed at this level. Security code validation is required to allow access to personalize the EEPROM memory. The FUS PIN must be held at a logic "1" for Security Level 1. The function of the FUS PIN enables the card issuer to simulate Security Level 2 during application development, without permanently blowing the Issuer fuse.

See "Memory Access Rules During Personalization".

Level 2: (Security After Personalization)

Conditions:

Issuer Fuse = "0" (blown)

FUS PIN = "X" (don't care)

Customer release. The EEPROM memory zone is protected by the various flags and passwords. After issuer personalization, Security Level 2 is implemented by blowing the Issuer Fuse. The device can also be placed in Security Level 2 by taking FUS pin low, independent of the state of Issuer Fuse.

See "Memory Access Rules After Personalization".

Memory Map

AT88SC101 Memory Diagram

Bit Address	Description	Bits	Words
0 - 15	Fabrication Zone (FZ)	16	1
16 - 79	Issuer Zone (IZ)	64	4
80 - 95	Security Code (SC)	16	1
96 - 111	Security Code Attempts Counter (SCAC)	16	1
112 - 175	Code Protected Zone (CPZ)	64	4
176 - 1199	Application Zone (AZ)	1024	64
1200 - 1231	Application Zone Erase Key (EZ)	32	2
1232 - 1359	Application Zone Erase Counter (EC)	128	8
1360 - 1375	Memory Test Zone (MTZ)	16	1
1376 - 1391	Manufacturer's Zone (MFZ)	16	1
1392 - 1407	Block Write/Erase	16	1
1408 - 1423	MANUFACTURER'S FUSE	16	1
1481	EC_EN FUSE (controls use of EC)	1	
1504 - 1519	ISSUER FUSE	16	1

Memory Zones

Zone	Definition
Fabrication Zone **FZ** (16 bits)	The 16-bit Fabrication Zone is programmed when the chip is manufactured and cannot be changed. The data held in the Fabrication Zone is specific to each Atmel customer, and cannot be modified. Application software may check this Fabrication Zone Code to assure that the device was manufactured by Atmel specifically for the intended application. Devices containing codes assigned to specific customers will not be sold to unauthorized customers. Fraudulent cards will not contain the correct code.
Issuer Zone **IZ** (64 bits)	The 64-bit Issuer Zone is programmed by the card issuer during the personalization phase. It will contain issuer-specific information, such as serial numbers and dates. This area becomes read-only after the ISSUER FUSE has been blown. Read access is always allowed in the Issuer Zone.
Security Code **SC** (16 bits)	The card Security Code is initially set by Atmel, to protect the card during transportation to the card issuer. During personalization, this code must be verified by the AT88SC101 to allow access to the EEPROM memory. After the security code has been verified, the code itself may be changed in either security mode. While in personalization mode (Security Level 1), the Security Code gives ERASE and WRITE access to both the Application Zone and the Code Protected Zone. In Security Level 2, the Security Code gives WRITE access to both the Application Zone and the Code Protected Zone. ERASE access requires verification of both the Security Code and the Erase Key (EZ). Verification of the Security Code will set the internal flag SV to “1”. Atmel ships the device with a Security Code (transportation code) pre-programmed. This protects against the unauthorized use of an unpersonalized device, and should be written to a new value during initialization.
Security Code Attempts Counter **SCAC** (16 bits)	The protocol for verification of the Security Code requires that the user write one of the first eight bits of the SCAC to a logic “0”. This allows the SCAC to count the number of consecutive incorrect presentations of the Security Code. After eight consecutive incorrect Security Code presentations, the first eight bits of the SCAC will all be written to “0”, and the user is permanently blocked from access to the Application Zone, as well as other areas controlled by the Security Code. After a successful presentation of the Security Code, the entire 16-bit SCAC, including the eight active bits, should be erased. This verifies that the correct Security Code has been presented, since an erase operation in this area is not allowed without SC verification. It also clears the SCAC bits in preparation for the next use of the card. This erase operation will also clear the remaining eight bits of the 16-bit SCAC word. These eight bits may be used in an application, although the entire 16-bit word will be erased if any bit in the SCAC is erased.
Code Protected Zone **CPZ** (64 bits)	READ access to this area is always allowed, and does not require SC validation. The Security Code must be correctly presented to allow WRITE or ERASE access to the Code Protected Zone.
Application Zone **AZ** (1024 bits)	The Application Zone (AZ) is intended to hold user application data. P1 (address 176) controls WRITE access, and R1 (address 177) controls READ access within AZ. In Security Level 1, an entire 16-bit word will be erased if an erase is performed on any single bit within that word. In Security Level 2, erase operations are controlled by both the SV flag and the Erase Key (EZ). See the Device Operation ERASE definition for specific details. The number of erase operations performed in AZ may be limited by leaving the EC_EN Fuse set to “1”.
Application Zone Erase Key **EZ** (32 bits)	(Enabled in Security Level 2 only.) The Erase Key is a password used to control ERASE operations within the Application Zone, after the Issuer Fuse has been blown (Security Level 2). The Erase Key password is written by the Issuer during personalization (Security Level 1) after verification of the Security Code. EZ can not be changed after the Issuer Fuse is blown. In Security Level 2, the AT88SC101 allows only block erasure of the entire Application Zone. AZ can be erased only after both the Security Code and the EZ password have been validated. Verification of EZ will set the internal flag E1 to “1”.

Memory Zones (Continued)

Zone	Definition
Application Zone Erase Counter **EC** (128 bits)	(Enabled in Security Level 2 only) The Erase Counter (EC) is enabled only in Security Mode 2 and only when the EC_EN fuse is set to “1”. If both of these conditions are true, the user will be limited to 128 erase operations in the Application Zone. EC is used to count these erase cycles. The erase protocol for the AT88SC101 Application Zone requires one bit in EC to be written to “0”. After 128 erase operations, all 128 bits in EC will be “0” and the user will be blocked from erasing AZ. The Erase Counter is only writeable and cannot be erased. When the EC_EN fuse = “0”, the EC operation is disabled. In that case there is no limit to the number of times AZ can be erased, and EC has no function.
Memory Test Zone **MTZ** (16 bits)	All operations are allowed for this zone (WRITE, ERASE, READ). The purpose of this zone is to provide an area in the product memory which is not restricted by security logic. It is used for testing purposes during the manufacturing process, and may also be used in the product application if desired, although no security protection exists for the MTZ.
Manufacturer’s Zone **MFZ** (16 bits)	The MFZ is intended to hold data specific to the smart card manufacturer (like assembly lot codes, dates, etc.). Read operations within this zone are always allowed. Write or Erase operations within this zone are allowed after the Security Code has been verified. After the data is entered by the Card Manufacturer, the Manufacturer’s Fuse can be blown and the data within the MFZ will become read-only. Blowing the Issuer Fuse will also lock the data in the MFZ.
EC_EN Fuse (1 bit)	This single bit EEPROM fuse selects whether the EC counter is used to limit the number of AZ erase operations in Security Mode 2. If the EC_EN Fuse is unblown (“1”), the number of erase operations allowed in AZ is limited to 128. If the EC_EN Fuse is blown (“0”), there is no limit to the number of erase operations in AZ. After the Issuer Fuse is blown, the state of the EC_EN Fuse is locked and cannot be changed.
Issuer Fuse (16 bits)	This EEPROM fuse is used to change the security mode of the AT88SC101 from Security Mode 1 (“1”) to Security Mode 2 (“0”). Initialization of the AT88SC101 for use by the end customer occurs in Security Mode 1. Access conditions in Security Mode 1 are described in Table 1. Access conditions in Security Mode 2 are described in Table 2.
Manufacturer’s Fuse (1 bit)	This single bit EEPROM fuse is used to lock the data stored in the Manufacturer’s Zone after personalization has been completed.

Definition of AT88SC101 Internal Flags

Zone	Definition
SV	Security Validation Flag **OPERATION:** The SV flag is set by correctly matching the 16-bit Security Code bit-by-bit from address 80 through 95, as CLK increments the address counter. The security code matching operation must be followed immediately by a validation operation within the Security Code Attempts Counter (SCAC). This validation operation requires the user to find a bit in the first eight bits of the SCAC (addresses 96 - 103) which is a logic “1”. A WRITE operation is performed, followed by an ERASE. The AT88SC101 will validate that the comparison was correct by outputting a logic “1”, and SV will be set. After the ERASE, all 16 bits in the SCAC will also be erased. The SV flag remains set until power to the card is turned off. If the comparison was in error, or part of the validation was not performed correctly, the AT88SC101 will output a logic “0”, showing that the SV flag has not been set. After eight consecutive incorrect Security Code presentations, the card is permanently locked. **FUNCTION:** This flag is the master protection for the memory zones. See Tables 1 and 2.
P1	Application Zone Write Flag **OPERATION:** If bit 176 has been programmed to a logic “1” this flag is set after bit 176 has been addressed. The flag remains set until power to the device is turned off, even if this bit is written to “0” by a subsequent operation. **FUNCTION:** P1 and SV must both be set in order to enable a WRITE command in the Application Zone (Security Mode 2).
R1	Application Zone Read Flag **OPERATION:** If bit 177 has been programmed to a logic “1” this flag is set after bit 177 has been addressed. The flag remains set until power to the device is turned off, even if this bit is written to “0” by a subsequent operation. **FUNCTION:** R1 or SV must be set in order to enable the Application Zone to be read
E1 EC Enabled	Application Zone Erase Flag with Erase Counter operation enabled (EC_EN FUSE = “1”) **OPERATION:** This flag is set by correctly matching the Application Zone Erase Key (EZ) bit by bit as pin CLK increments the address counter. Then a validation operation must be completed. This operation requires the user to find a bit in the Application Zone Erase Counter (EC), addresses 1232 - 1359, which is a logic “1”. A WRITE must then be performed, followed by an ERASE. The AT88SC101 will validate that the comparison was correct and the Application Zone will be erased. This flag is also reset when the address counter = 0. **FUNCTION:** The Application Zone (bits 176 -1199) is erased when E1 is set and an ERASE is performed after the validation operation in EC described above. This operation erases all bits in the Application Zone.
E1 EC Disabled	Application Zone Erase Flag with Erase counter operation disabled (EC_EN FUSE = “0”) **OPERATION:** E1 is set when the Application Zone Erase Key comparison is valid. It is reset when the address counter = 0. **FUNCTION:** The Application Zone (bits 176 - 1199) is erased when E1 is set and an ERASE is performed on bit 1232. This operation erases all bits in the Application Zone but does not affect the word containing bit 1232.

Definition of AT88SC101 Passwords

Password	Definition
Security Code (**SC**) bits 80 - 95 (16 bits)	This password is used to set the SV (Security Validation) flag and is used in determining what operations are allowed in each zone (See tables 1 and 2).
Erase Key (**EZ**) bits 1200 - 1231 (32 bits)	This password must be programmed during issuer personalization. It is used to erase the Application Zone in Security Level 2. Verification of EZ will set the internal flag E1 to “1”.

Definition of AT88SC101 Fuses

MANUFACTURER FUSE: This fuse is used to control writes and erases of the Manufacturer Zone (MFZ). When the security code has been validated and both the Issuer Fuse and the Manufacturer Fuse are unblown, writes and erases of the MFZ are allowed. Blowing the Issuer Fuse will also disable the Manufacturer Fuse if it has not been blown previously.

EC_EN FUSE: This fuse selects whether the EC counter is used to limit the number of Application Zone erases allowed in security mode 2. If EC_EN FUSE is “unblown”, then the Application Zone erases are limited to 128. If the EC_EN FUSE is “blown” the Application Zone erases are unlimited. After the Issuer Fuse is blown the state of the EC_EN FUSE is locked and cannot be changed.

ISSUER FUSE: This fuse is used to personalize the AT88SC101 for end use. It is an additional EEPROM bit which can be programmed to a logic “0”. This is its “blown” state. Security of the device when Issuer Fuse is a logic “1” is described in table 1. The device is in Security Level 2 when the Issuer Fuse is blown. The device can also be placed in Security Level 2 by taking the FUS pin low independent of the state of Issuer Fuse. Memory access rules of the device in Security Level 2 are described in Table 2.

Memory Access Rules During Personalization - Security Mode 1[1]

Table 1. Access Conditions During Personalization (Issuer Fuse not blown).

Zone	SV[2]	R1[3]	MF[4]	Read	Erase	Write	Compare
FZ	x	x	x	yes	no	no	no
IZ	0 1	x x	x x	yes yes	no yes	no yes	no no
SC	0 1	x x	x x	no yes	no yes	no yes	yes no
SCAC	0 1	x x	x x	yes yes	no yes	yes yes	no no
CPZ	0 1	x x	x x	yes yes	no yes	no yes	no no
AZ	0 0 1	0 1 x	x x x	no yes yes	no no yes	no no yes	no no no
EZ	0 1	x x	x x	no yes	no yes	no yes	no no
EC	0 1	x x	x x	yes yes	no yes	yes yes	no no
MTZ	x	x	x	yes	yes	yes	no
MFZ	0 1 1	x x x	x 0 1	yes yes yes	no no yes	no no yes	no no no

Notes: 1. Security Mode 1 Conditions:
EC_EN = “1” or “0”
ISSUER FUSE = “1”
FUS PIN = “1” (required)

2. SV: SV = “1” after validation of the security code
3. R1: 2nd bit of the Application Zone (bit 177)
4. MF: MANUFACTURER FUSE = “0” when blown

Memory Access Rules After Personalization - Security Mode 2[1]

Table 2. Access Conditions after Personalization (Issuer Fuse blown).

Zone	SV[2]	P1[3]	R1[4]	E1[5]	Read	Erase	Write	Compare
FZ	x	x	x	x	yes	no	no	no
IZ	x	x	x	x	yes	no	no	no
SC	0 1	x x	x x	x x	no no	no yes	no yes	yes no
SCAC	0 1	x x	x x	x x	yes yes	no yes	yes yes	no no
CPZ	0 1	x x	x x	x x	yes yes	no yes	no yes	no no
AZ	0 0 1 1 1 1	x x 0 0 1 1	0 1 x x x x	x x 0 1 0 1	no yes yes yes yes yes	no no no yes no yes	no no no no yes yes	no no no no no no
EZ	x	x	x	x	no	no	no	yes
EC	x	x	x	x	yes	no	yes	no
MTZ	x	x	x	x	yes	yes	yes	no
MFZ	x	x	x	x	yes	no	no	no

Notes: 1. Security Mode 2 Conditions:
MANUFACTURER FUSE = “X”
EC_EN FUSE = “1” or “0”
ISSUER FUSE = “0”
FUS PIN = “X”

2. SV: SV = “1” after validation of the security code
3. P1: 1st bit of the Application Zone (Bit 176)
4. R1: 2nd bit of the Application Zone (Bit 177)
5. E1: E1 = “1” after a valid presentation of the erase key EZ

Micro Operations

The AT88SC101 circuit operation modes are selected by the input logic levels on the control pins PGM, CLK and RST and by the internal address. Timing for these operations is specified in the AC Characteristics section.

Operation	PGM	RST	CLK	Definition
RESET	X		0	This operation will reset the internal address to 0. After the falling edge of RST, the first bit of the Fabrication Zone (Address 0) will be driven on the I/O contact. The erase flag (E1) will be reset.
INC/READ	0	0		The address is incremented on the falling edge of CLK. If READ operations are enabled, the addressed bit will be driven on the I/O pin after the falling edge of CLK. When READ operations are disabled, the I/O will be disabled and pulled to a high state by the external system pull-up resistor.
INC/CMP	0	0		The INC/CMP operation will compare the value of the data driven by the system host on the I/O pin, to the value of the bit already written into the EEPROM memory at that address location. This process is used during validation of the AT88SC101 Security Code and Erase Key. The data must be stable on the I/O pin before the rising edge of CLK, when the data will be latched internally. Comparison occurs on the next falling edge of CLK. The internal address is also incremented on the falling edge of CLK.
ERASE/WRITE	1	0		The I/O pin must be driven to a “1” for an ERASE, and to a “0” for a WRITE operation before the rising edge of CLK (see t_{DS})
STANDBY	0	1	X	The device is placed in standby mode when FUS pin = “0” and RST = “1”. The address will not increment when RST is high.

Notes:
1. The output is disabled (hi-state) on all addresses where the READ operation is disabled.
2. The two instructions INC/READ and INC/CMP share the same control signal states.
3. The circuit will distinguish between the INC/READ and INC/CMP instructions by testing the internal address counter. (CMP can only be done with the addresses corresponding to the Security Code or to the Erase Key).
4. The internal address counter counts up to 1519. An additional CLK pulse resets the address to 0.

Device Functional Operation

Function	Functional Operation Sequence
POR	**OPERATION:** POR (power-on reset) is initiated as the device power supply ramps from 0V up to a valid operating voltage. **FUNCTION:** POR resets all flags, and the address is reset to 0.
RESET	**OPERATION:** With CLK low, a falling edge on the RST pin will reset the address counter to address 0. **FUNCTION:** The address is reset to 0, and the first bit of the memory is driven by the AT88SC101 on I/O after a reset. Only E1 is reset when the address is reset to 0. The RESET operation has no affect on any of the other flags (SV, P1, R1).
ADDRESSING	**OPERATION:** Addressing is handled by an internal address counter. The address is incremented on the falling edge of CLK. RESET must be low while incrementing the address. A falling edge of RESET clears the counter to address 0. **FUNCTION:** Addressing of the AT88SC101 is sequential. Specific bit addresses may be reached by completing a RESET, then clocking the device (INC/READ) until the desired address is reached. The AT88SC101 will determine which operations are allowed at specific address locations. These operations are specified in Tables 1 and 2. **EXAMPLE:** To address the Issuer Zone (IZ) execute a RESET operation, then clock the device 16 times. The device now outputs the first bit of the Issuer Zone (IZ). After the address counter counts up to 1519 the next CLK pulse resets the address to 0.
READ	**OPERATION**: RST and PGM pins must be low. If a READ operation is allowed, the state of the memory bit which is being addressed is output on the I/O pin. The I/O buffer is an open drain and the output of a logic “0” therefore causes the device to pull the pin to ground. The output of a logic “1” causes the device to place the pin in a high impedance state. Therefore in order to sense a logic “1”, an external pullup must be placed between the I/O pin and VCC. The address counter is incremented on the falling edge of CLK. **FUNCTION:** NON-APPLICATION ZONES: As the address counter is incremented, the contents of the memory are read out on the I/O pin. The READ operation is inhibited for addresses where security prevents a READ operation (See Table 1 and Table 2). APPLICATION ZONE: The Application Zones can be read when: SV = “1” or R1 = “1”.

Device Functional Operation (Continued)

Function	Functional Operation Sequence
WRITE	A WRITE operation sets the bit(s) to a logic “0”. **OPERATION:** CLK = “0” PGM “0” → “1” (I/O switches to an input) I/O = “0” (input = “0” for WRITE operation) CLK “0” → “1” (rising edge of CLK starts the WRITE operation.) PGM “1” → “0” I/O “0” → “Z” (high-impedance) Wait t_{CHP} (see “AC Electrical Characteristics”) CLK “1” → “0” (falling edge of CLK ends the WRITE operation). Note: The falling edge of CLK which ends the WRITE operation does not increment the address counter. **FUNCTION:** NON-APPLICATION ZONES: The WRITE operation is inhibited for addresses where security prevents a WRITE operation (See Tables 1 and 2). APPLICATION ZONE: The Application Zone can be written when: Security level 1: SV = “1” Security level 2: SV = “1” and P1 = “1”
ERASE Operation Sequence	CLK = “0” PGM “0” → “1” (I/O switches to an input) I/O = “1” (input = “1” for ERASE Operation) CLK “0” → “1” (rising edge of CLK starts the ERASE operation.) PGM “1” → “0” I/O “1” → “Z” (high-impedance) Wait t_{CHP} (see “AC Electrical Characteristics”) CLK “1” → “0” (falling edge of CLK ends the ERASE operation.) Note: The falling edge of CLK which ends the ERASE operation does not increment the address counter.
ERASE (Non-Application Zones)	An ERASE operation sets the bits to logic “1”. The EEPROM memory is organized into 16 bit words. Although erases are performed on single bits the ERASE operation clears an entire word in the memory (except for the Application Zone in Security Level 2). Therefore, performing an ERASE on any bit in the word will clear ALL 16 bits of that word to logic “1”. **OPERATION**: Perform “ERASE Operation Sequence” as specified above. **FUNCTION:** The ERASE operation is inhibited for addresses where security prevents an ERASE operation. (see Tables 1 and 2).
ERASE (Application Zone) **Security Level 1**	Security level 1: (ISSUER FUSE = “1” and FUS pin = “0”) The Application Zone can only be erased when SV = 1. **OPERATION:** Increment address counter to any bit within AZ. Perform “ERASE Operation Sequence” as specified above. **FUNCTION:** This operation will erase the entire 16-bit word containing the bit.

Device Functional Operation (Continued)

Function	Functional Operation Sequence
ERASE (Application Zone) **Security Level 2** **EC Mode Enabled**	Security level 2: (ISSUER FUSE = “0” or FUS pin = “0”) EC Mode is Enabled. Erase Operations within AZ are limited to 128. The Application Zone can only be erased when SV = “1” and E1 = “1”. **OPERATION:** Set SV = “1” by validating the Security Code (see definition of SV internal flag). Increment address counter to the first bit of the Application Zone Erase Key (EZ = bit 1200). Execute 32 INC/CMP operations, correctly verifying each bit of the 32-bit Erase Key. Increment the address counter through the Application Zone Erase Counter (EC = bits 1232 - 1359) until a bit is found which is set to “1”. Perform a WRITE operation on this bit (this WRITE will not increment the address counter). Perform an ERASE operation on the same bit. **FUNCTION:** This operation will erase the entire Application Zone. One additional bit of the Erase Counter will now be written to “0”. The ERASE operation in EC will initiate the AZ erase but will not affect the state of the bits within EC.
ERASE (Application Zone) **Security Level 2** **EC Mode Disabled**	Security Level 2: (ISSUER FUSE = “0” or FUS pin = “0”) EC Mode is Disabled. Unlimited Erase Operations in AZ. The Application Zone can only be erased when SV = “1” and E1 = “1”. **OPERATION:** Set SV = “1” by validating the Security Code (see definition of SV internal flag). Increment address counter to the first bit of the Application Zone Erase Key (EZ = bit 1200). Execute 32 INC/CMP operations, correctly verifying each bit of the 32-bit Erase Key. Increment the address counter to the next bit (bit 1232, the first bit of the Application Zone Erase Counter). Perform an ERASE operation on this bit. **FUNCTION:** This operation will erase the entire Application Zone, but does not affect the word containing bit 1232.
Block Write/Erase	Enabled in Security Level 1 only. **OPERATION:** Set address counter between address 1392 and 1407. SV must be set. FUS pin must be high. Perform a WRITE or ERASE operation. **FUNCTION:** The entire memory excluding the Fabrication Zone (FZ), Memory Test Zone (MTZ) and Manufacturer’s Zone (MFZ) will be written to “0” (WRITE) or “1” (ERASE). The BLOCK WRITE/ERASE modes are used to quickly personalize the device.
Blowing Manufacturer Fuse	Valid in Security Level 1. **OPERATION:** Set address counter between address 1408 and 1423. SV must be set. The FUS pin can be either a “0” or a “1”. RST pin = “1” Perform a WRITE operation. **FUNCTION:** The MANUFACTURER FUSE will be at a logic “0” state. Note: The address will not change as long as RST is high. CLK should be low when RST is brought low. This will reset the address counter to 0.

Device Functional Operation (Continued)

Function	Functional Operation Sequence
Blowing EC_EN Fuse	The EC_EN FUSE must be blown before the Issuer Fuse is blown. **OPERATION:** Set the address counter to address 1481. FUS pin = “1” RST pin = “1” Perform a WRITE operation **FUNCTION:** EC_EN Fuse will be written to a logic “0” state. Note: The address will not change as long as RST is high. CLK should be low when RST is brought low This will reset the address counter to 0.
Blowing Issuer Fuse	**OPERATION:** Set address counter between address 1504 and 1519. SV must be set. The FUS pin can be either a “0” or a “1”. RST pin = “1” Perform a WRITE operation **FUNCTION:** ISSUER FUSE will be set to a logic “0” state. This operation will convert the AT88SC101 from Security Level 1 to Security Level 2. The action is irreversible. Note: The address will not change as long as RST is high. CLK should be low when RST is brought low. This will reset the address counter to 0.
Function of FUS and RST Pins	
FUS	Used for personalizing the device. FUS must be high to be able to personalize the device when Issuer Fuse is unblown. In Security Level 1, the FUS pin may be forced low to simulate Security Level 2. In Security Level 2, the FUS pin has no function.
RST	This pin is used to reset the address counter address to 0. It is also used in writing the Issuer Fuse and the EC_EN FUSE low. When the FUS pin is low and the RST pin is high, the part is in stand by mode.

Absolute Maximum Ratings*

Operating Temperature	-55°C to +125°C
Storage Temperature	-65°C to +150°C
Voltage on Any Pin with Respect to Ground	-0.3V to V_{CC} + 0.7V
Maximum Operating Voltage	6.25V
DC Output Current	5.0 mA

*NOTICE: Stresses beyond those listed under "Absolute Maximum Ratings" may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of this specification is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

DC Characteristics

Applicable over recommended operating range from: V_{CC} = 2.7V to 5.5V and T_A = -25°C to +85°C (unless otherwise noted).

Symbol	Characteristics	Min	Type	Max	Unit
I_{CC}	Supply Current on V_{CC} during Read (T_{AMB} = +25°C)			2	mA
I_{CCP}	Supply Current on V_{CC} during Program (T_{AMB} = +25°C)			5	mA
I_{SB}	Standby Current on V_{CC} RST @ V_{CC}; FUS, CLK, PGM @ GND; I_{OL} = 0 µA; F_{CLK} = 0 kHz)			50	µA
V_{IL}	Input Low Level	-0.3		V_{CC} x 0.3	V
V_{IH}	Input High Level	V_{CC} x 0.7		V_{CC} + 0.3	V
V_{OL}	Output Low Level (I_{OL} = 1 mA)			0.4	V
I_{IL}	Input Leakage Current			20	µA
I_{IH}	I/O Leakage Current (V_{OH} = V_{CC} Open Drain)			20	µA

AC Characteristics

T_A = -25°C to +85°C, V_{CC} = 5V ± 10%, GND = 0V (unless otherwise noted).

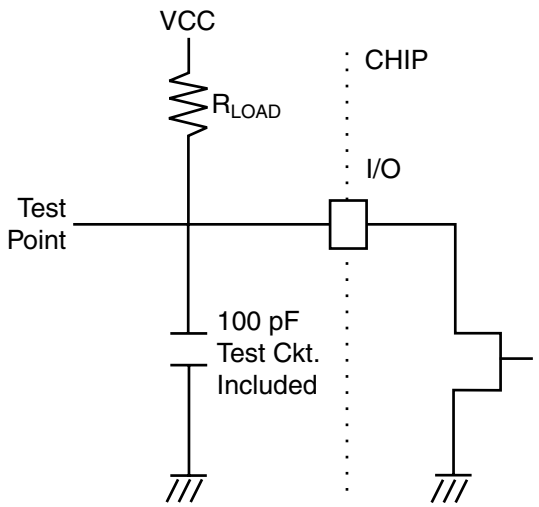
Symbol	Characteristics	Min	Typ	Max	Unit
t_{CLK}	Clock Cycle time	3.3			µs
t_{RH}	RST Hold Time	0.1			µs
t_{DVR}	Data Valid Reset to Address “0”			2.0	µs
t_{CH}	CLK Pulse Width (High)	0.2			µs
t_{CL}	CLK Pulse Width (Low)	0.2			µs
t_{DV}	Data Access			2.0	µs
t_{OH}	Data Hold	0			µs
t_{SC}	Data In Setup (CMP Instruction)	0			µs
t_{HC}	Data In Hold (CMP Instruction)	0.2			µs
t_{CHP}	CLK Pulse Width (High in Programming)	2.0			ms
t_{DS}	Data In Setup	0.2			µs
t_{DH}	Data In Hold	0			µs
t_{SPR}	PGM Setup	2.2			µs
t_{HPR}	PGM Hold	0.2			µs

Conditions of Dynamic Tests

The circuit has an output with open drain. An external resistor is necessary between VCC and I/O in order to load the output.

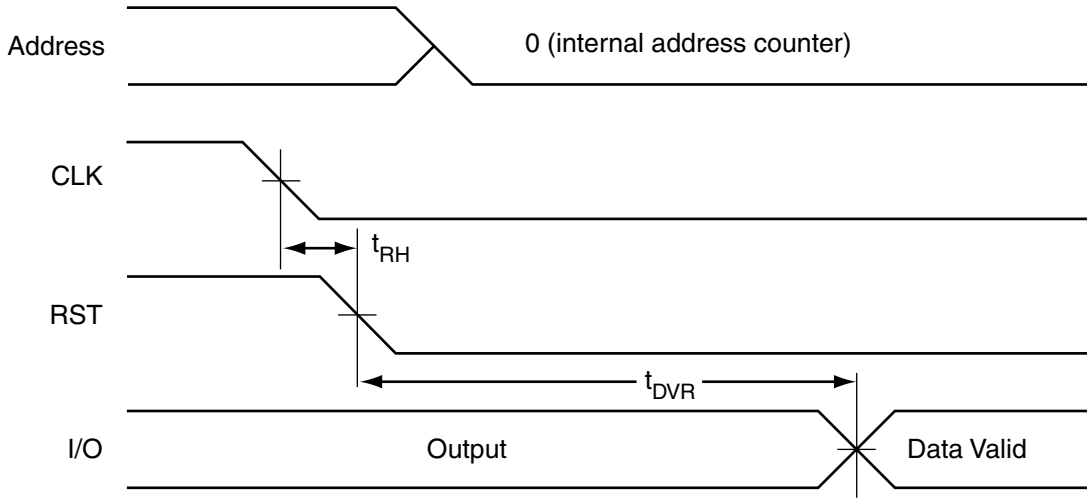
Pulse Levels of the Input	GND to V_{CC}
Reference Levels in Input	V_{CC} x 0.3 and V_{CC} x 0.7
Reference Levels in Output	1.5V
Rising and Falling Time of Signals	5 ns

AC Load Circuit



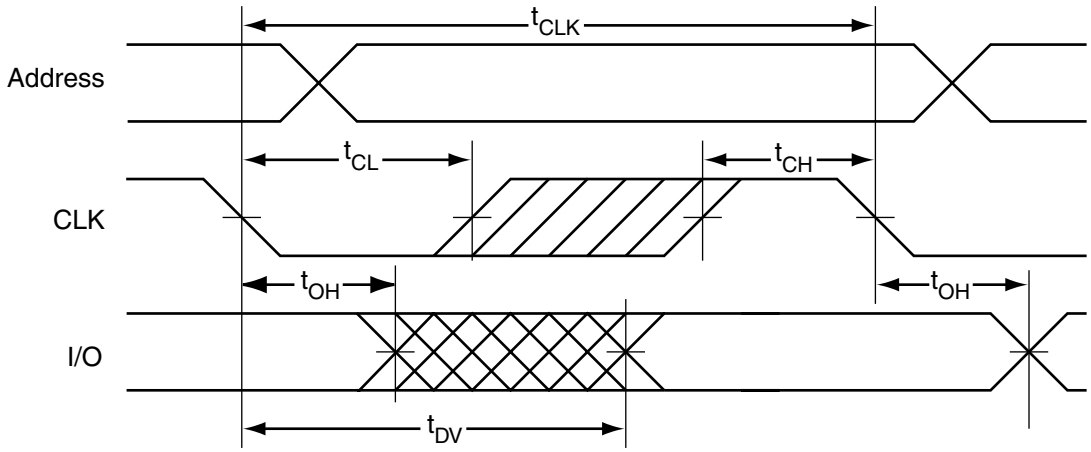
Timing Diagrams

Reset



Note: CLK should be low on the falling edge of RST. CLK may remain low while RST is pulsed.

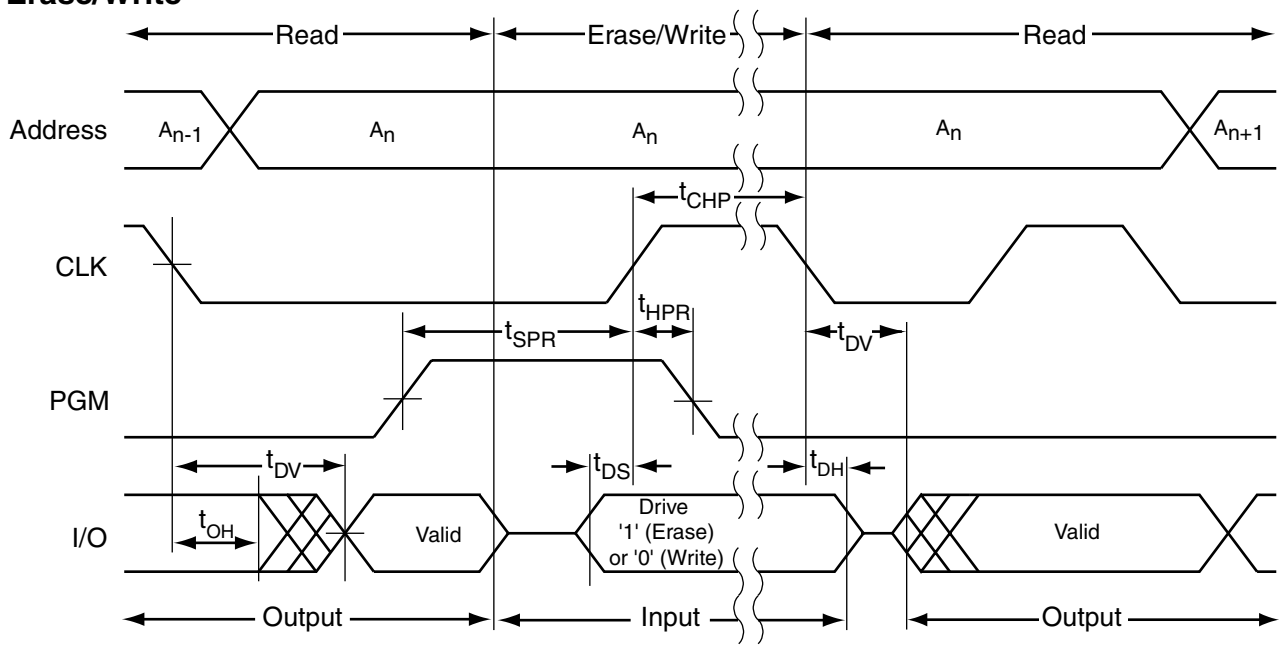
Read



Note: PGM and RST must both be low during a read cycle.
I/O should not be driven (except by the external pullup resistor).

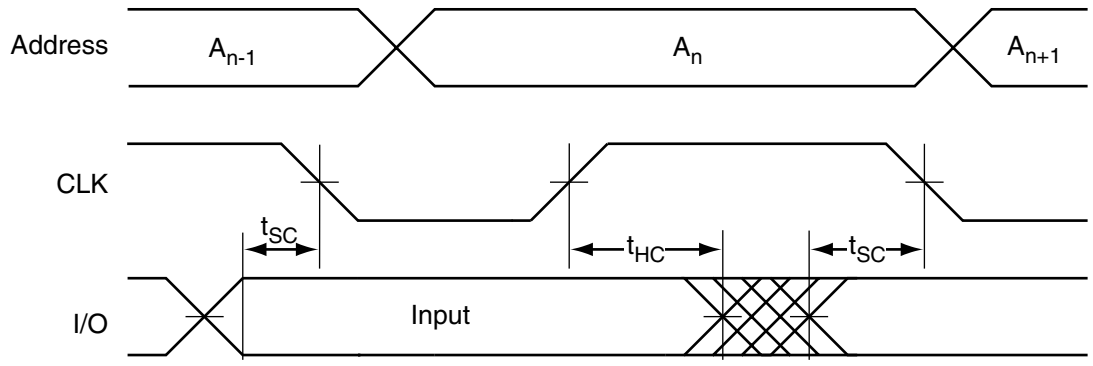
Program

Erase/Write



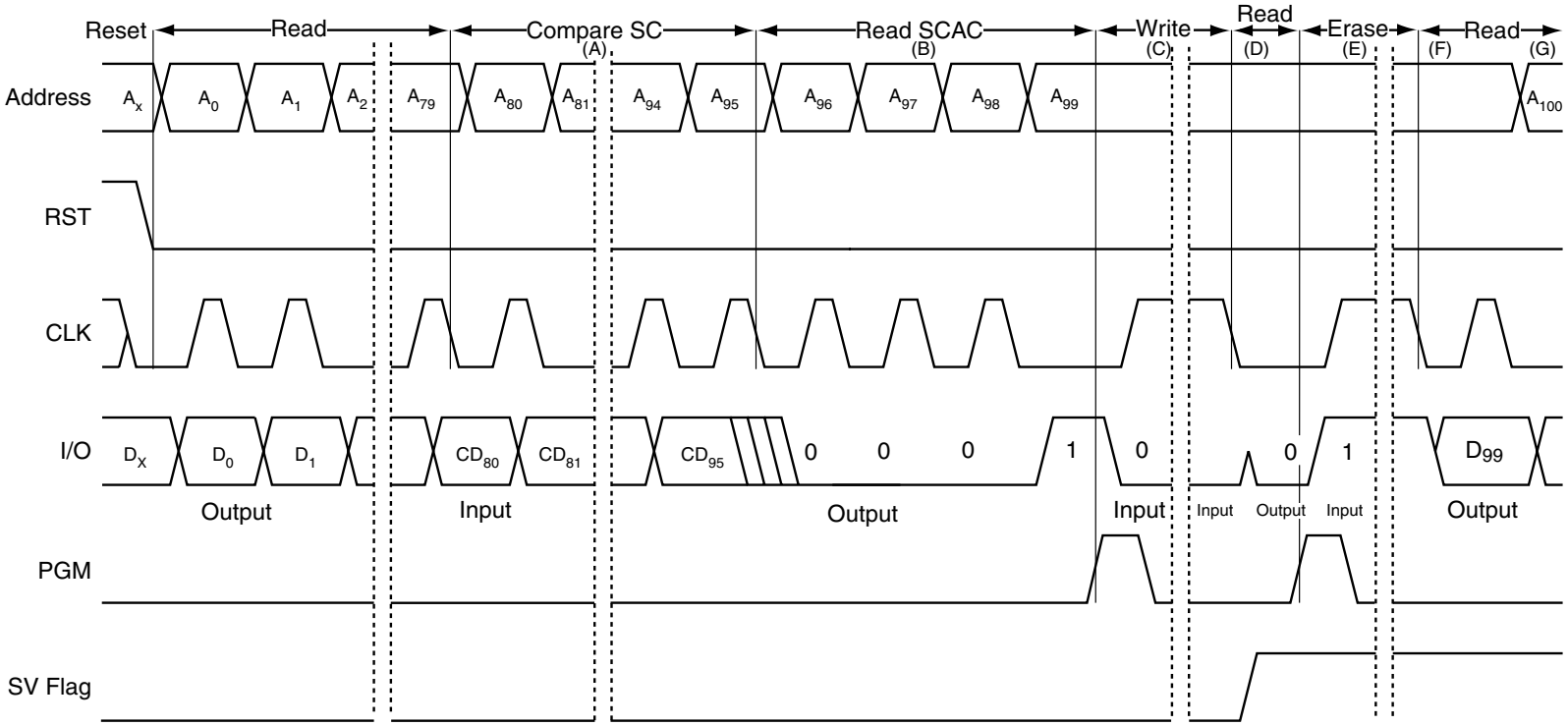
Notes: During any Erase or Write operation, PGM must fall before the falling edge of CLK at the end of t_{CHP} (recommend a minimum setup time of 1 µsec).
After the rising edge of PGM to initiate the Erase/write operation, delay at least t_{DV} (2 µsec) before driving data on the I/O contact.

Compare



Note: Input Data is latched on the rising edge of CLK. Comparison occurs on the next falling edge of CLK. The address counter is incremented on the falling edge of CLK. During a compare operation of the first bit following a read (i.e. the first bit of the SC, or erase keys), data driven to the I/O may be delayed by t_{DV} after the the falling edge of CLK.

Security Code Validation

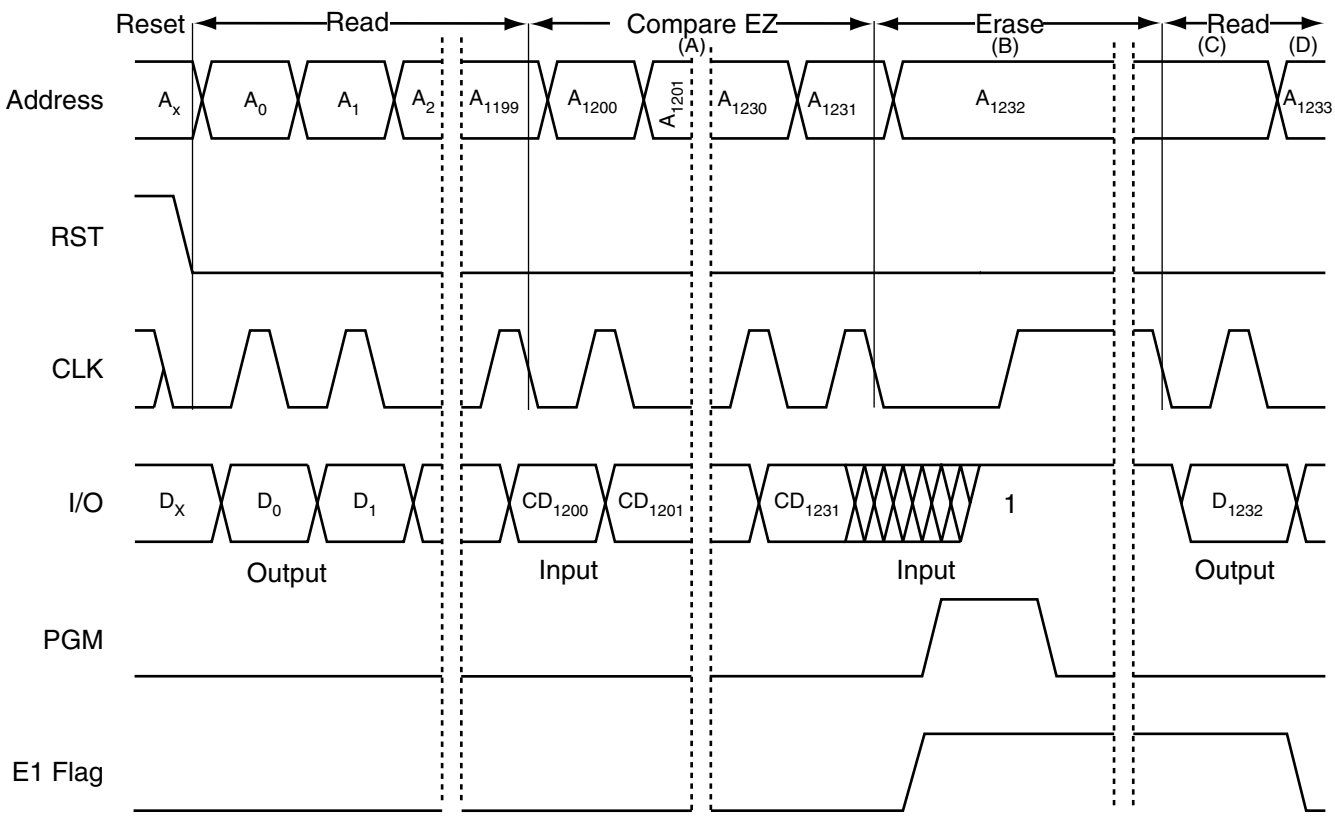


Notes:

1. A_n = Address, D_n = Read data (output), CD_n = Compare data (input)
2. Security level 2 (Issuer fuse blown)

A. Compare sequence of the Security Code.
B. This diagram shows an example in which the first three bits of the Security Code Attempts Counter (96 - 98) are previously set to 0. Bit 99 in this example is a 1, so the Write/Erase sequence is begun with that bit.
C. WRITE operation of a "0" over the existing "1".
D. The AT88SC101 will output a '0' following the WRITE operation. If the comparison is successful, the SV flag is set on the falling edge of CLK and the SCAC zone can be erased.
E. Erase operation
F. The AT88SC101 will output a "0" following the ERASE operation if the Security Code verification is successful. If invalid, the device will output a "1".
G. On the falling edge of CLK, the address is incremented and the state of the next bit is driven on the I/O pin.

Erase Operation Application Zone (AZ), EC Function Disabled

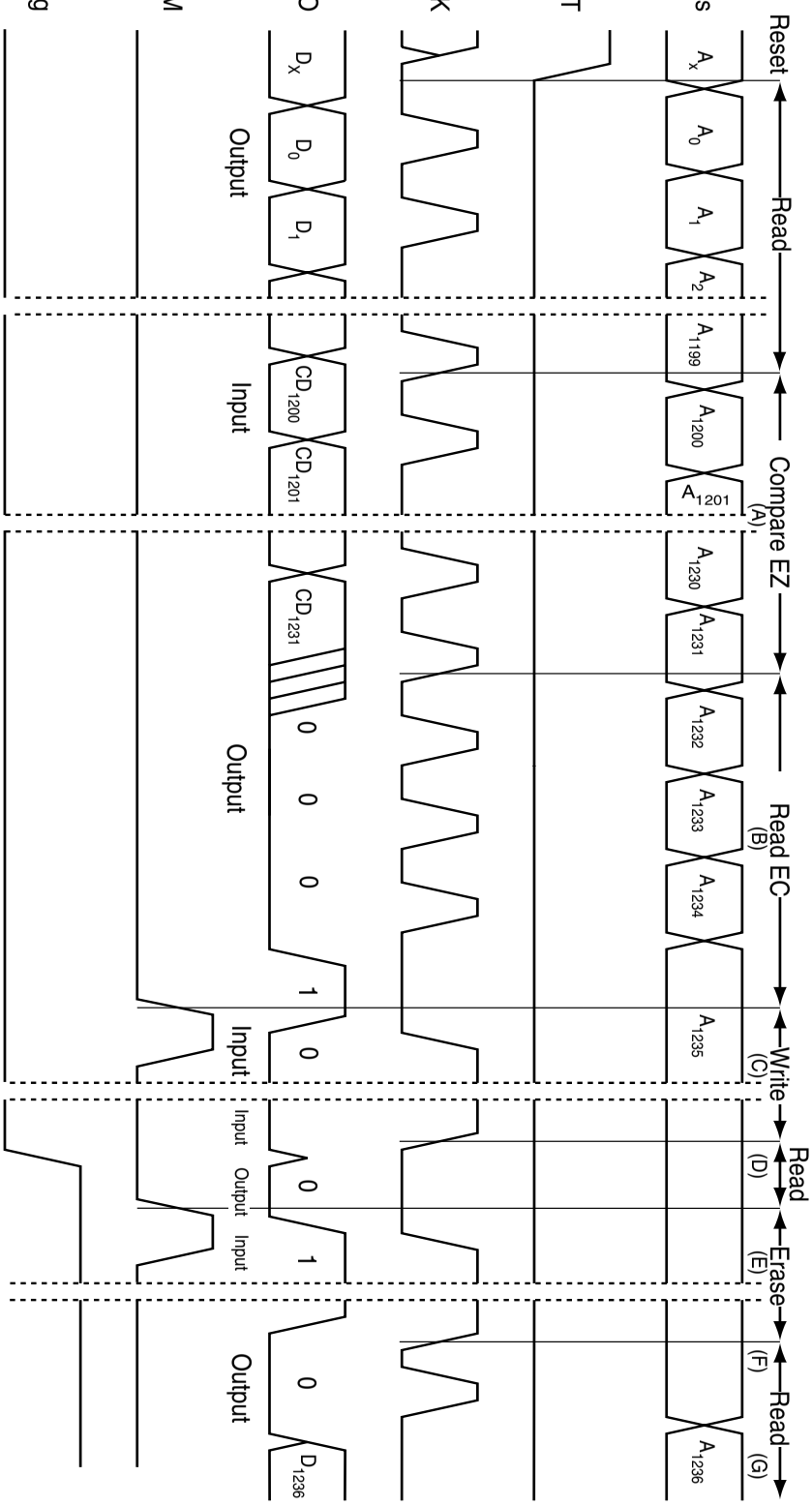


Notes:

1. A_n = Internal Address, D_n = Read data (output), CD_n = Compare data (input).
2. This diagram illustrates the protocol for setting the E1 flag in Security level 2 (Issuer fuse blown). Erase operations in Security Level 1 within the Application Zone do not require setting of the E1 flag. In Security Level 1, an erase operation on any bit in the Application Zone will erase the entire 16-bit word containing the bit.
3. EC_EN Fuse = "0" (disabled)

A. Compare sequence of EZ. If the comparison is valid, the E1 flag is set to "1", enabling erasure of AZ.
B. If E1 is set to "1", an erase operation on bit 1232 will erase bits 176 - 1199 (AZ) (Security Level 1).
C. After the falling edge of CLK, the device will drive the I/O contact to the logic state of the existing data in bit 1232. The state of this bit is not affected by the AZ erase operation.
D. After the falling edge of CLK, the address is incremented and the state of the next bit is driven on the I/O contact.

Erase Operation Application Zone (AZ) EC Function Enabled



Notes:

1. A_n = Internal Address, D_n = Read data (output), CD_n = Compare data (input)
2. EC_EN fuse = "1" (enabled)
3. Security Level 2 (Issuer fuse blown)

A. Compare sequence of the Erase Key (EZ).

B. This diagram shows an example in which the first three bits of the EC Erase Counter (bits 1232 - 1234) are previously set to "0". The WRITE/ERASE operation should be performed on the first bit in EC which is found to be a "1". Bit 1235 in this example is a "1", so the Write/Erase sequence is begun with that bit.

C. WRITE operation of a "0" over the existing "1".

D. The AT88SC101 will output a "0" following the WRITE operation. If the comparison is successful, the E1 flag is set and the AZ zone can be erased.

E. Erase operation

F. The AT88SC101 will output a "0" following the ERASE operation regardless of the success of the compare operation.

G. On the falling edge of CLK, the address is incremented and the state of the next bit is driven on the I/O pin.

Ordering Information

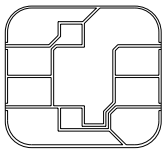
Ordering Code[1]	Package[2]	Voltage Range	Temperature Range
AT88SC101 - 09AT - xx - 2.7	M2 - A Module	2.7V to 3.3V	Commercial 0°C to 70°C
AT88SC101 - 09BT - xx - 2.7	M2 - B Module		
AT88SC101 - 09CT - xx - 2.7	M4 - C Module		
AT88SC101 - 09DT - xx - 2.7	M4 - D Module		
AT88SC101 - 09ET - xx - 2.7	M2 - E Module		
AT88SC101 - 09GT - xx - 2.7	M3 - G Module		
AT88SC101 - 09HT - xx - 2.7	M3 - H Module		
AT88SC101 - 09AT - xx	M2 - A Module	4.5V to 5.5V	Commercial 0°C to 70°C
AT88SC101 - 09BT - xx	M2 - B Module		
AT88SC101 - 09CT - xx	M4 - C Module		
AT88SC101 - 09DT - xx	M4 - D Module		
AT88SC101 - 09ET - xx	M2 - E Module		
AT88SC101 - 09GT - xx	M3 - G Module		
AT88SC101 - 09HT - xx	M3 - H Module		

Package Type[2]	
M2 - A Module	M2 ISO 7816 Smart Card Module
M2 - B Module	M2 ISO 7816 Smart Card Module with Atmel Logo
M4 - C Module	M4 ISO 7816 Smart Card Module
M4 - D Module	M4 ISO 7816 Smart Card Module with Atmel Logo
M2 - E Module	M2 ISO 7816 Smart Card Module
M3 - G Module	M3 ISO 7816 Smart Card Module
M3 - H Module	M3 ISO 7816 Smart Card Module with Atmel Logo

Notes: 1. “xx” must be replaced by a security code. Contact an Atmel Sales Office for the security code.
2. Formal drawings may be obtained from an Atmel Sales Office.

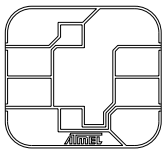
Smart Card Modules

M2 - A Module - Ordering Code: 09AT



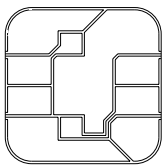
Module Size: M2
Dimension(1): 12.6 x 11.4 mm
Glob Top: Black, Square: 8.6 x 8.6 mm
Thickness: 0.58 mm max.
Pitch: 14.25 mm

M2 - B Module - Ordering Code: 09BT



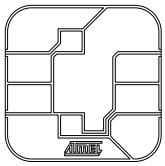
Module Size: M2
Dimension(1): 12.6 x 11.4 mm
Glob Top: Black, Square: 8.6 x 8.6 mm
Thickness: 0.58 mm max.
Pitch: 14.25 mm

M4 - C Module - Ordering Code: 09CT



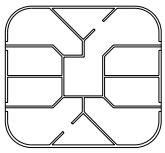
Module Size: M4
Dimension(1): 12.6 x 12.6 mm
Glob Top: Black, Square: 8.6 x 8.6 mm
Thickness: 0.58 mm
Pitch: 14.25 mm

M4 - D Module - Ordering Code: 09DT



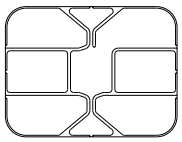
Module Size: M4
Dimension(1): 12.6 x 12.6 mm
Glob Top: Black, Square: 8.6 x 8.6 mm
Thickness: 0.58 mm max.
Pitch: 14.25 mm

M2 - E Module - Ordering Code: 09ET



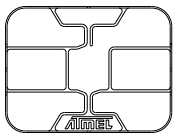
Module Size: M2
Dimension(1): 12.6 x 11.4 mm
Glob Top: Clear, Round: Ø 7.5 mm max.
Thickness: 0.58 mm max.
Pitch: 14.25 mm

M3 - G Module - Ordering Code: 09GT



Module Size: M3
Dimension(1): 10.6 x 8.0 mm
Glob Top: Clear, Round: Ø 6.5 mm max.
Thickness: 0.58 mm max.
Pitch: 9.5 mm

M3 - H Module - Ordering Code: 09HT



Module Size: M3
Dimension(1): 10.6 x 8.0 mm
Glob Top: Clear, Round: Ø 6.5 mm max.
Thickness: 0.58 mm max.
Pitch: 9.5 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).

Atmel Headquarters

Corporate Headquarters
2325 Orchard Parkway
San Jose, CA 95131
TEL (408) 441-0311
FAX (408) 487-2600

Europe
Atmel U.K., Ltd.
Coliseum Business Centre
Riverside Way
Camberley, Surrey GU15 3YL
England
TEL (44) 1276-686-677
FAX (44) 1276-686-697

Asia
Atmel Asia, Ltd.
Room 1219
Chinachem Golden Plaza
77 Mody Road Tsimhatsui
East Kowloon
Hong Kong
TEL (852) 2721-9778
FAX (852) 2722-1369

Japan
Atmel Japan K.K.
9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
Japan
TEL (81) 3-3523-3551
FAX (81) 3-3523-7581

Atmel Operations

Atmel Colorado Springs
1150 E. Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906
TEL (719) 576-3300
FAX (719) 540-1759

Atmel Rousset
Zone Industrielle
13106 Rousset Cedex
France
TEL (33) 4-4253-6000
FAX (33) 4-4253-6001

Fax-on-Demand
North America:
1-(800) 292-8635
International:
1-(408) 441-0732

e-mail
literature@atmel.com

Web Site
http://www.atmel.com

BBS
1-(408) 436-4309

1418B–11/99/xM