Atmel AT88SA100S

Atmel CryptoAuthentication Battery Authentication Chip

DATASHEET

Features

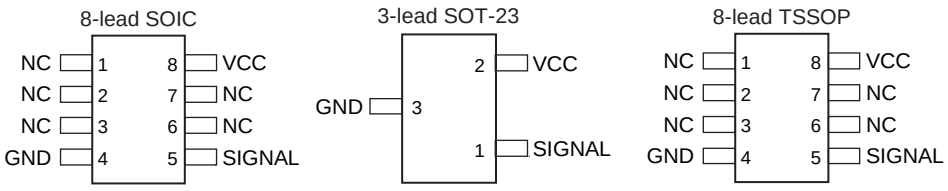
- Secure battery authentication
- Superior SHA-256 hash algorithm
- Best in class 256-bit key length
- Guaranteed unique 48-bit serial number
- High speed single wire interface
- Supply voltage: 2.7 – 5.25 V
- <150 nA sleep current
- Green compliant (exceeds RoHS) 3-pin SOT-23 package and 8-lead TSSOP or SOIC

Applications

- Cell phones
- PDA and smart phones
- Portable media players
- Digital cameras & camcorders
- Cordless tools
- Handheld devices

Figure 1. Pin configurations

Pin name	Function
SIGNAL	Serial data, single-wire clock, and data
GND	Ground
VCC	Power supply



1. Introduction

The Atmel® AT88SA100S is a small authentication chip that can be used to validate battery packs and other replaceable items that contain a power source. It uses the industry leading SHA-256 hash algorithm to provide the ultimate level of security.

An industry leading key length of 256-bits prevents exhaustive attacks while multiple physical security features prevent unauthorized disclosure of the secret key stored within the chip. This key is automatically erased when power is removed from the AT88SA100S.

It is shipped with a guaranteed unique 48-bit serial number that is used in combination with an input challenge and the stored secret key to generate a response that is unique for every individual AT88SA100S.

The chip also includes 80 one-time fuses that can be used to configure the system and/or retain permanent status. The values in these fuses can also be locked to prevent modification.

1.1 Memory Resources

Sram — 256-bits of SRAM are used for storage of a key. The LoadSram command provides a mechanism to securely initialize this block during personalization. This memory will retain its value when the chip is put/goes to sleep, so long as a supply voltage in excess of V_{RETAIN} is still supplied to the chip.

MemValid — A single bit that tells whether or not SRAM contains valid data. It's cleared when power is lost and set when the SRAM is loaded with a secret key.

Fuse — Block of 128-fuse bits that can be read and written through the one wire interface. The first 8-bits are lock bits that control burn ability on 16-bit words of the array. Fuse[88-95] are part of the manufacturing ID values fixed by Atmel. Fuse[96-127] are part of the serial number programmed by Atmel which is guaranteed to be unique. See Section 1.3 for more details on the Manufacturing ID and Serial Number.

ROM — Metal mask programmed memory. Unrestricted reads are permitted on the first 64-bits of this array. The physical ROM will be larger and will contain other information that cannot be read.

ROM MfrID — Two bytes of ROM that specifies part of the manufacturing ID code. This value is assigned by Atmel and is always the same for all chips of a particular model number. For the AT88SA100S, this value is 0x2301. (Appears on the bus: 0x0123), ROM MfrID can be read by accessing ROM bytes 0 and 1 of Address 0.

ROM SN — Two bytes of ROM that can be used to identify chips among others on the wafer. These bits reduce the number of fuses necessary to construct a unique serial number. The ROM SN is read by accessing ROM bytes 2 and 3 of Address 0. The serial number can always be read by the system and is optionally included in the message digested by the MAC command.

RevNum — Four bytes of ROM that are used by Atmel to identify the design revision of the AT88SA100S chip. These bytes can be freely read as the four bytes returned from ROM Address 1, however system code should not depend on this value as it may change from time to time.

1.2 Fuse Map

The AT88SA100S chip incorporates 128 one-time fuses within the chip. Once burned, there is no way to reset the value of a fuse. Fuses, with the exception of the manufacturing ID and serial number bits, which are initialized by Atmel, have a value of one when shipped from the Atmel factory and transition to a zero when they are burned.

Table 1-1. The 128 Fuses in the Atmel AT88SA100S Chip are Arranged in the Following Manner:

Fuse #	Name	Description
0 – 7	Fuse Lock Bits	Each bit, when zero, locks the current value of the corresponding 16-bit block of the fuse array, see below for more details
8 → 83	Status Fuses	These fuses can be written with the BurnFuse command and can always be read with the Read command. They are totally user-defined
84 → 87	Status Fuses	These fuses can be written with the BurnFuse command and can always be read with the Read command. They are user-defined, but have special significance for the Pause Long command. See Section 6.3
87	Fuse Disable	The MAC command ignores the values of Fuse[0-86] while this fuse is an one Once it is burned to zero, the BurnSecure command is disabled
88 → 95	Fuse MfrID	See Section 1.3. Set by Atmel, cannot be modified in the field
96 → 127	Fuse SN	See Section 1.3. Set by Atmel, cannot be modified in the field

Fuse Lock Bits These eight fuses can be used to prevent further writing of the status fuses. Bit 0, when burned, locks Fuse[0-15] from being modified, Bit[1] locks Fuse[16-31] and so on up through bit five, which locks Fuse[80-87]. Fuse[88-127] can never be modified with the BurnFuse command.

Note: Burning bit zero has the effect of preventing any changes to the current value of the lock bits

Status Fuses These fuses can be used to store various information which are not secret. Their value can always be determined using the Read command. They can be individually burned using the BurnFuse command. Two common usage models for these fuses are:

1. Consumption logging, i.e. burn one bit after every n uses, the host system keeps track of the number of uses so far for this serial number since the last fuse burn.
2. Model number information. In this situation, the bits are written at the factory and their value is locked to prevent modifications in the field. This method can also be used for feature enabling.

1.3 Chip Identification

The chip includes a total of 72-bits of information that can be used to distinguish between individual chips in a reliable manner. The information is distributed between the ROM and fuse blocks in the following manner.

Serial Number This 48-bit value is composed of ROM SN (16-bits) and Fuse SN (32-bits). Together they form a serial number that is guaranteed to be unique for all devices ever manufactured within the Atmel CryptoAuthentication™ family. This value is optionally included in the MAC calculation.

Manufacturing ID This 24-bit value is composed of ROM MfrID (16-bits) and Fuse MfrID (8-bits). Typically this value is the same for all chips of a given type. It is always included in the cryptographic computations.

1.4 SHA-256 Computation

This chip performs only one cryptographic calculation – a keyed digest of an input challenge using the SHA-256 algorithm, documented here:

http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

1.4.1 SHA Computation Example

In order to ensure that there is no ambiguity, the following example vector is provided in addition to the sample vectors in the NIST document. In this example, all values are listed in hex. For all but the key, bytes are listed in the order that they appear on the bus – first on the left. Key is listed in the same order, so the 01 at the left of the key string is the first byte passed to SHA-256.

SHA Computation Example

Key	01030507090B0D0F11131517191B1D1F21232527292B2D2F31333537393B3D3F
Challenge	020406080A0C0E10121416181A1C1E20222426282A2C2E30323436383A3C3E40
Opcode	08
Mode	40 (include serial number in message)
Param2	0000
Fuse MfrID	77
Fuse S/N	8899AABB
ROM MfrID	CCDD
ROM SN	EEFF

The 88-bytes over which the digest is calculated are:
0103…3D3F0204…3E4001400000…EEFF

Digest: 7D38245733717A488575B9F794F7BCAFE033A3848D39430DA25141FDEBEAA1C2

A read command executed on Address 0 of the ROM (ROM MfrID, ROM SN) would return CC DD EE FF, with CC being the first byte on the bus and FF being the last.

Throughout this document, the complete message processed by the SA100S chip is documented. According to the above specification, this always includes a single bit of ‘1’ pad after the message, followed by a 64-bit value representing the total number of bits being hashed (less pad and length). If the length is less than 447 (512-64-1) then the necessary number of ‘0’ bits are included between the ‘1’ pad and ‘length’ to stretch the last message block out to 512-bits.

When using standard libraries to calculate the SHA-256 digest, these pad and length bits should probably not be passed to the library as most standard software implementations of the algorithm add them in automatically.

1.5 Security Features

The AT88SA100S incorporates a number of physical security features designed to protect the key from unauthorized release. These include an active shield over the entire surface of the internal memory encryption, internal clock generation, glitch protection, voltage tamper detection and other physical design features.

Both the clock and logic supply voltage are internally generated, preventing any direct attack via the pins on these two signals.

2. IO Protocol

Communications to and from the AT88SA100S take place over a single asynchronously timed wire uses a pulse count scheme. The overall communications structure is a hierarchy:

Table 2-1. IO Hierarchy

Tokens	Implement a single data bit transmitted on the bus, or the wake-up event
Flags	Comprised of eight tokens (bits) which convey the direction and meaning of the next group of bits (if any) which may be transmitted
Blocks	of data follow the command and Transmit flags. They incorporate both a byte count and a checksum to ensure proper data transmission
Packets	of bytes form the core of the block without the count and CRC. They are either the input or output parameters of an Atmel AT88SA100S chip command or status information from the AT88SA100S chip

2.1 IO Tokens

There are a number of IO **tokens** that may be transmitted along the bus:

Input: (To AT88SA100S)

- Wake — Wake AT88SA100S up from sleep (low power) state
- Zero — Send a single bit from system to the AT88SA100S with a value of zero
- One — Send a single bit from system to the AT88SA100S with a value of one

Output: (From AT88SA100S)

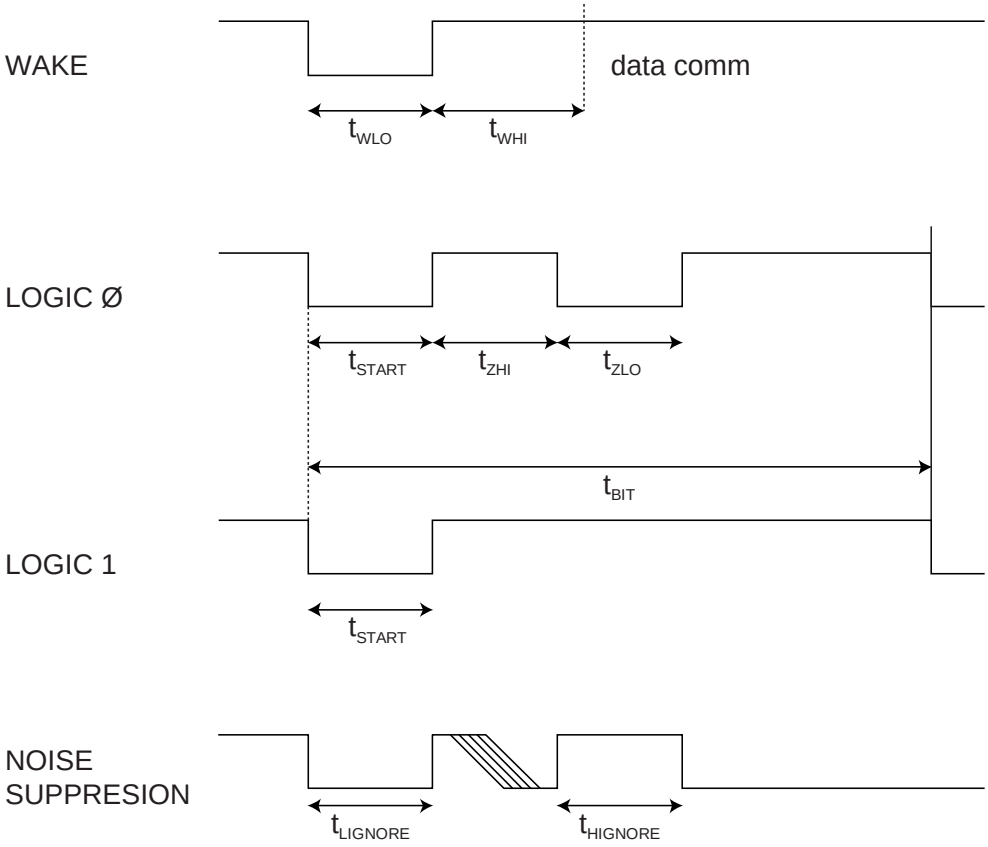
- ZeroOut — Send a single bit from the AT88SA100S to the system with a value of zero
- OneOut — Send a single bit from the AT88SA100S to the system with a value of one

The waveforms are the same in either direction, however there are some differences in timing based on the expectation that the host has a very accurate and consistent clock while the AT88SA100S has significant variation in its internal clock generator due to normal manufacturing and environmental fluctuations.

The bit timings are designed to permit a standard UART running at 230.4 K baud to transmit and receive the tokens efficiently. Each byte transmitted or received by the UART corresponds to a single bit received or transmitted by the AT88SA100S. Refer to applications notes on the Atmel website for more details describing how the UART should be controlled.

2.2 AC Parameters

Figure 2-2. AC Parameters



3. Absolute Maximum Ratings*

Operating temperature	−40°C to +85°C
Storage temperature	−65°C to + 150°C
Voltage on any pin with respect to ground	− 0.5 to V_{CC}+0.5 V

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

4. AC Parameters

Table 4-1. AC Parameters

Parameter	Symbol	Direction	Min	Typ	Max	Unit	Notes
Wake low duration	t_{WLO}	To Atmel CryptoAuthentication	60		-	µs	Signal can be stable in either high or low levels during extended sleep intervals.
Wake Delay to Data Comm.	t_{WHI}	To Atmel CryptoAuthentication	2.5		45	ms	Signal should be stable high for this entire duration. t_{WHI} must not exceed $t_{TIMEOUT}$ or the chip will transition to sleep.
Start pulse duration	t_{START}	To Atmel CryptoAuthentication	4.1	4.34	4.56	µs	
		From CryptoAuthentication	4.6	6.0	8.6	µs	
Zero transmission high pulse	t_{ZHI}	To Atmel CryptoAuthentication	4.1	4.34	4.56	µs	
		From Atmel CryptoAuthentication	4.6	6.0	8.6	µs	
Zero transmission low pulse	t_{ZLO}	To Atmel CryptoAuthentication	4.1	4.34	4.56	µs	
		From Atmel CryptoAuthentication	4.6	6.0	8.6	µs	
Bit time	t_{BIT}	To Atmel CryptoAuthentication	37	39	-	µs	If the bit time exceeds $t_{TIMEOUT}$ then the Atmel CryptoAuthentication will enter sleep mode and the Wake token must be resent.
		From Atmel CryptoAuthentication	41	54	78	µs	
Turn around delay	$t_{TURNAROUND}$	From Atmel CryptoAuthentication	28	60	95	µs	Atmel CryptoAuthentication will initiate the first low going transition after this time interval following the end of the Transmit flag
		To Atmel CryptoAuthentication	15µs		45ms		After Atmel CryptoAuthentication transmits the last bit of a block, system must wait this interval before sending the first bit of a flag
High side glitch filter @ active	$t_{HIGNORE\_A}$	To Atmel CryptoAuthentication	45			ns	Pulses shorter than this in width will be ignored by the chip, regardless of its state when active
Low side glitch filter @ active	$t_{LIGNORE\_A}$	To Atmel CryptoAuthentication	45			ns	Pulses shorter than this in width will be ignored by the chip, regardless of its state when active
Low side glitch filter @ sleep	$t_{LIGNORE\_S}$	To Atmel CryptoAuthentication	500			ns	Pulses shorter than this in width will be ignored by the chip when in sleep mode
Io timeout	$t_{TIMEOUT}$	To Atmel CryptoAuthentication	45	65	85	ms	Refer to Section 5.4.1
Watchdog reset	$t_{WATCHDOG}$	To Atmel CryptoAuthentication	3	4	5.7	s	Max. time from Wake until chip is forced into Sleep mode See Watchdog Failsafe, Section 5.5

5. DC Parameters

Table 5-1. DC Parameters

Parameter	Symbol	Min	Typ	Max	Unit	Notes
Operating temperature	T_A	-40		85	°C	
Power supply voltage	V_{CC}	2.7		5.25	V	
Fuse burning voltage	V_{BURN}	3.0		5.25	V	Voltage applied to V_{CC} pin. See Section 6.3
Active power supply current	I_{CC}		-	6	mA	
Sleep Power Supply Current @ -40 to 55 C	I_{SLEEP}			150	nA	When chip is in sleep mode, V_{CC} = 5.25 V, Vsig = 0.0 to 0.3 V, or Vsig = V_{CC} -0.3 V to V_{CC}
Sleep power supply current @ 85 c	I_{SLEEP}			1	µA	When chip is in sleep mode, V_{CC} = 5.25 V, Vsig = 0.0 to 0.3 V, or Vsig = V_{CC} -0.3 V to V_{cc}
Input low voltage @ V_{CC} = 5.25 v	V_{IL}	-0.5		0.75	V	Voltage levels for Wake token when chip is in sleep mode
Input low voltage @ V_{CC} = 2.7 v	V_{IL}	-0.5		0.5	V	Voltage levels for Wake token when chip is in sleep mode
Input high voltage @ V_{CC} = 5.25 v	V_{IH}	1.5		5.25	V	Voltage levels for Wake token when chip is in sleep mode
Input high voltage @ V_{CC} = 2.7 v	V_{IH}	1.25		3.0	V	Voltage levels for Wake token when chip is in sleep mode
Input low voltage when active	V_{IL}	-0.5		0.5	V	When chip is in active mode, V_{CC} = 2.7 – 5.25 V
Input high voltage when active	V_{IH}	1.2		5.25	V	When chip is in active mode, V_{CC} = 2.7 – 5.25 V
Output low voltage	V_{OL}			0.4	V	When chip is in active mode, V_{CC} = 2.7 – 5.25 V
Maximum input voltage	V_{MAX}			5.25	V	

5.1 IO Flags

The host system is always the bus master, so before any IO transaction, the system must first send an 8-bit **flag** to the chip to indicate the IO operation that is to be performed, as follows:

Value	*Name*	*Meaning*
0x77	Command	After this flag, the system starts sending a command block to the chip. The first bit of the block can follow immediately after the last bit of the flag.
0x88	Transmit	After a turn-around delay, the chip will start transmitting the response for a previously transmitted command block.
0xCC	Sleep	Upon receipt of a sleep flag, the chip will enter a low power mode until the next Wake token is received.

All other values are reserved and will be ignored.

5.1.1 Command Timing

After a command flag is transmitted, a command block should be sent to the chip. During parsing of the parameters and subsequent execution of a properly received command, the chip will be busy and not respond to transitions on the signal pin. The delays for these operations are listed in the table below:

Table 5-2. Command Timing (Guaranteed by design; not tested)

Parameter	Symbol	Max	Unit	Notes
ParsingDelay	t_{PARSE}	100	µs	Delay to check CRC and parse opcode and parameters before an error indication will be available
MemoryDelay	t_{EXEC_MEM}	3	ms	Delay to execute Read, Write and/or SramLock commands
FuseDelay	t_{EXEC_FUSE}	700	µs	Delay to execute BurnFuse command See Section 6.3 for more details
MacDelay	t_{EXEC_MAC}	30	ms	Delay to execute MAC command
PersonalizeDelay	t_{PERSON}	13	ms	Delay to execute GenPersonalizationKey or LoadSram

In this document, t_{EXEC} is used as shorthand for the delay corresponding to whatever command has been sent to the chip.

5.1.2 Transmit Flag

The Transmit flag is used to turn around the signal so that the AT88SA100S can send data back to the system, depending on its current state. The bytes that the AT88SA100S returns to the system, depending on its current state as follows:

Table 5-3. Return Codes

State Description	Error/Status	Description
After Wake, but prior to first command	0x11	Indication that a proper Wake token has been received by the AT88SA100S.
After successful command execution	–	Return bytes per “Output Parameters” in Section 6, Commands of this document. In some cases this is a single byte with a value of 0x00 indicating success. The Transmit flag can be resent to the AT88SA100S repeatedly if a re-read of the output is necessary.
Execution error	0x0F	Command was properly received but could not be executed by the AT88SA100S chip. Changes in the AT88SA100S chip state or the value of the command bits must happen before it is re-attempted.
After CRC or other parsing error	0xFF	Command was *not* properly received by AT88SA100S and should be re-issued by the system.

The AT88SA100S always transmits complete blocks to the system, so in the above table the status/error bytes result in 4-bytes going to the system – count, error, CRC x 2.

After receipt of a command block, the AT88SA100S will parse the command for errors, a process which takes t_{PARSE} (See Section 5.1.1). After this interval the system can send a transmit token to the AT88SA100S – if there was an error then the AT88SA100S will respond with an error code. If there is no error then the AT88SA100S internally transitions automatically from t_{PARSE} to t_{EXEC} and will not respond to any Transmit tokens until both delays are complete.

5.1.3 Sleep Flag

The sleep flag is used to transition the AT88SA100S to the low power state, which causes a complete reset of the AT88SA100S’ internal command engine and input/output buffer. It can be sent to the AT88SA100S at any time when the AT88SA100S will accept a flag.

To achieve the specified I_{SLEEP}, Atmel recommends that the input signal be brought below V_{IL} when the chip is asleep. To achieve I_{SLEEP} if the sleep state of the input pin is high, the voltage on the input signal should be within 0.3V of V_{CC} to avoid additional leakage on the input circuit of the chip.

5.1.4 Pause State

The pause state is entered via the PauseLong command and can be exited only when the watchdog timer has expired and the chip transitions to a sleep state. When in the pause state, the chip ignores all transitions on the signal pin but does not enter a low power consumption mode.

The pause state provides a mechanism for multiple AT88SA100S chips on the same wire to be selected and to exchange data with the host microprocessor. The PauseLong command includes an optional address field which is compared to the values in Fuses 84-87. If the two matches, then the chip enters the pause state, otherwise, it continues to monitor the bus for subsequent commands. The host would selectively put all but one AT88SA100S in the pause state before executing the MAC command on the active chip. After the end of the watchdog interval all the chips will have entered the sleep state and the selection process can be started with a Wake token (which will then be honored by all chips) and selection of a subsequent chip.

5.2 IO Blocks

Commands are sent to the chip, and responses received from the chip, within a block that is constructed in the following way:

Byte Number	*Name*	*Meaning*
0	Count	Number of bytes to be transferred to the chip in the block, including count, packet and checksum, so this byte should always have a value of (N+1). The maximum size block is 39 and the minimum size block is four. Values outside this range will cause unpredictable operation.
1 to (N-2)	Packet	Command, parameters and data, or response See Section 6 for more details
N-1, N	Checksum	CRC-16 verification of the count and packet bytes. The CRC polynomial is 0x8005, the initial register value should be zero and after the last bit of the count and packet have been transmitted the internal CRC register should have a value that matches that in the block. The first byte transmitted (N-1) is the least significant byte of the CRC value so the last byte of the block is the most significant byte of the CRC.

5.3 IO Flow

The general IO flow for a MAC command is as follows:

1. System sends wake token
2. System sends transmit flag
3. Receive 0x11 value from the AT88SA100S to verify proper wakeup synchronization
4. System sends command flag
5. System sends command block
6. System waits t_{PARSE} for the AT88SA100S to check for command formation errors
7. System sends transmit flag. If command format is OK, the AT88SA100S ignores this flag because the computation engine is busy. If there was an error, the AT88SA100S responds with an error code
8. System waits t_{EXEC}. See Section 5.1.1
9. System sends transmit flag
10. Receive output block from the AT88SA100S, system checks CRC
11. If CRC from the AT88SA100S is incorrect, indicating a transmission error, system resends transmit flag
12. System sends sleep flag to the AT88SA100S

All commands other than MAC have a short execution delay. In these cases the system should omit steps six, seven, and eight and replace this with a wait of duration t_{PARSE} + t_{EXEC}.

5.4 Synchronization

Because the communications protocol is half duplex, there is the possibility that the system and the AT88SA100S will fall out of synchronization with each other. In order to speed recovery, the AT88SA100S implements a timeout that forces the AT88SA100S to sleep. See Section 5.4.1.

5.4.1 IO Timeout

After a leading transition for any data token has been received, the AT88SA100S will expect the remaining bits of the token to be properly received by the chip within the $t_{TIMEOUT}$ interval. Failure to send enough bits or the transmission of an illegal token (a low pulse exceeding t_{ZLO}) will cause the chip to enter the sleep state after the $t_{TIMEOUT}$ interval.

The same timeout applies during the transmission of the command block. After the transmission of a legal command flag, the IO Timeout circuitry is enabled until the last expected data bit is received.

Note: The timeout counter is reset after every legal token, so the total time to transmit the command may exceed the $t_{TIMEOUT}$ interval while the time between bits may not

In order to limit the active current if the AT88SA100S is inadvertently awakened, the IO timeout circuitry is also enabled when the AT88SA100S receives a wake-up. If the first token does not come within the $t_{TIMEOUT}$ interval, then the AT88SA100S will go back to the sleep mode without performing any operations.

The IO timeout circuitry is disabled when the chip is busy executing a command.

5.4.2 Synchronization Procedures

When the system and the AT88SA100S fall out of synchronization, the system will ultimately end up sending a Transmit flag which will not generate a response from the AT88SA100S. The system should implement its own timeout which waits for $t_{TIMEOUT}$ during which time the AT88SA100S should go to sleep automatically. At this point, the system should send a Wake token and after $t_{WLO} + t_{WHI}$, a Transmit token. The 0x11 status indicates that the resynchronization was successful.

It may be possible that the system does not get the 0x11 code from the AT88SA100S for one of the following reasons:

1. The system did not wait a full $t_{TIMEOUT}$ delay with the IO signal idle in which case the AT88SA100S may have interpreted the Wake token and Transmit flag as a data bits. Recommended resolution is to wait twice the $t_{TIMEOUT}$ delay and re-issue the Wake token.
2. The AT88SA100S went into the sleep mode for some reason while the system was transmitting data. In this case, the AT88SA100S will interpret the next data bit as a Wake token, but ignore some of the subsequently transmitted bits during its wake-up delay. If any bytes are transmitted after the wake-up delay, they may be interpreted as a legal flag, though the following bytes would not be interpreted as a legal command due to an incorrect count or the lack of a correct CRC. Recommended resolution is to wait the $t_{TIMEOUT}$ delay and re-issue the Wake token.
3. There is some internal error condition within the AT88SA100S which will be automatically reset after a $t_{WATCHDOG}$ interval, see below. There is no way to externally reset the AT88SA100S – the system should leave the IO pin idle for this interval and issue the Wake token.

5.5 Watchdog Failsafe

After the Wake token has been received by the AT88SA100S, a watchdog counter is started within the chip. After $t_{WATCHDOG}$, the chip will enter sleep mode, regardless of whether it is in the middle of execution of a command and/or whether some IO transmission is in progress. There is no way to reset the counter other than to put the chip to sleep and wake it up again.

This is implemented as a fail-safe so that no matter what happens on either the system side or inside the various state machines of the AT88SA100S including any IO synchronization issue, power consumption will fall to the low sleep level automatically.

5.6 Byte and Bit Ordering

The AT88SA100S is a little-endian chip:

- All multi-byte aggregate elements within this spec are treated as arrays of bytes and are processed in the order received
- Data is transferred to/from the AT88SA100S least significant bit first on the bus
- In this document, the most significant bit appears towards the left hand side of the page

6. Commands

The command packet is broken down in the following way:

Byte	Name	Meaning
0	Opcode	The command code
1	Param1	The first parameter – always present
2-3	Param2	The second parameter – always present
4 +	Data	Optional remaining input data

If a command fails because the CRC within the block is incorrect, the opcode is invalid or one of the parameters is illegal, then immediately after t_{PARSE} the system will be able to retrieve an error response block containing a single byte packet. The value of that byte will be either 0x0F or 0xFF depending on the source of the error. See Section 5.1.2.

If a command is received successfully then after the appropriate execution delay the system will be able to retrieve the output block as described in the individual command descriptions below.

In the individual command description tables below, the size column describes the number of bytes in the parameter documented in each particular row. The total size of the block for each of the commands is fixed, though that value is different for each command. If the block size for a particular command is incorrect, the chip will not attempt the command execution and return an error.

6.1 MAC

Computes a SHA-256 digest of the key, challenge and other fixed information on the chip to generate an output response. If MemValid is not set, indicating that no valid key is stored in the SRAM, then this command will return an error. The hashed message includes the following bytes, concatenated in this order:

256-bits	Key (Stored in Sram)
256-bits	Challenge
8-bits	Opcode (always 0x08)
8-bits	Mode input
16-bits	Param2 input
88-bits	All zeros
8-bits	Fuse MfrID (Fuse[88-95])
32-bits	Fuse SN (Fuse[96-127]) or zeros
16-bits	ROM MfrID
16-bits	ROM SN or zeros
1-bit	1's – SHA-256 padding
255-bits	0's – SHA-256 padding
64-bits	Length (704) per SHA-256

Table 6-1. Input Parameters

	Name	Size	Notes
Opcode	MAC	1	0x08
Param1	Mode	1	See Table 6-6
Param2	Zero	2	Must be 0x0000
Data	Challenge	32	Input portion of message to be digested

Table 6-2. Output Parameters

Name	Size	Notes
Response	32	SHA-256 digest

Table 6-3. Mode Encoding

Bit	Notes
6	If set, then the four bytes of Fuse SN and the two bytes of ROM SN will be included in the message, otherwise these bits will be set to zero in the message
0-5, 7	Ignored, must be all zero

6.2 Read

Reads four bytes from Fuse, ROM or MemValid. Any attempt to present the chip with an illegal Fuse address will result in an error return.

Table 6-4. Input Parameters

	Name	Size	Notes
Opcode	READ	1	0x02
Param1	Mode	1	Fuse, ROM or MemValid. See to Table 12
Param2	Address	2	Which 4-bytes within array. Bits 2-15 are ignored by the chip and should be zeros
Data	–	0	

Table 6-5. Output Parameters

Name	Size	Notes
Contents	4	The contents of the specified memory location

Table 6-6. Mode Encoding

Name	Value	Notes
ROM	0x00	Reads four bytes from the ROM. Bit 1 of the address parameter must be zero
Fuse	0x01	Reads the value of 32-fuses
MemValid	0x03	Returns four bytes. The LSB of the first byte indicates whether or not the contents of the SRAM are valid. All other bits in all bytes have a value of zero. The address parameter is ignored

6.3 BurnFuse

Burns one of the 88 user accessible fuse bits.

The values in fuses #88-127 are reserved for Fuse MfrID and Fuse SN and cannot be blown via this command. All addresses above 0x57 (87) will result in an error.

Fuses, with the exception of those initialized by Atmel, have a value of one on shipment from the Atmel factory and transition to a zero when they are burned.

Fuse bits zero through seven of the fuse array are word lock bits. Burning one of these has the effect of locking the corresponding 16-bit word within Fuse. Bit 0 locks fuses 0-15, bit 1 locks fuses 16-31 and so on. If bit 0 is burned, then the value of the lock bits can no longer be changed. The values of lock bits six and seven are ignored by the chip.

The power supply pin must meet the V_{BURN} specification during the entire BurnFuse command in order to burn fuses reliably. If Vcc is greater than or equal to 3.7 V, then the BurnTime parameter should be set to 0x00 and the internal burn time will be 250µs. If Vcc is less than 3.7 V but greater than V_{BURN} then the BurnTime parameter should be set to 0xFFFF and the internal burn time will be up to 262ms. The chip does *not* internally check the supply voltage level.

There is a very small interval during t_{EXEC_BURN} when the fuse element is actually being burned. During this interval, the power supply must not be removed and the watchdog timer must not be allowed to expire or the fuse may end up in a state where it reads as un-burned but cannot be burned.

Table 6-7. Input Parameters

	Name	Size	Notes
Opcode	BURNFUSE	1	0x04
Param1	FuseNum	1	Which bit within fuse array, minimum value is 0, and maximum value is 87
Param2	BurnTime	2	Must be 0x0000 if Vcc >=3.7 V; must be 0xFFFF otherwise
Data	–	0	

Table 6-8. Output Parameters

Name	Size	Notes
Success	1	Upon successful completion, a value of 0 will be returned by the Atmel AT88SA100S

6.4 GenPersonalizationKey

This command generates a decryption digest that will be used by the subsequent command (LoadSram) to decrypt the key value that is to be written into the SRAM. This command must be run immediately prior to LoadSram within the same watchdog cycle.

This command loads a transport key from an internal secure storage location and then uses that key along with an input seed to generate a decryption digest using SHA-256. Neither the transport key nor the decryption digest can be read from the chip. Upon completion, an internal bit is set indicating that the decryption digest has been generated and is ready to use by LoadSram. This bit is cleared (and the digest lost) when the watchdog timer expires, the chip goes to sleep or the power is cycled.

Table 6-9. Input Parameters

	Name	Size	Notes
Opcode	GenPers	1	0x20
Param1	Zero	1	Must be 0x00
Param2	KeyID	2	Identification number of the personalization key to be loaded
Data	Seed	16	Seed for digest generation. The least significant bit of the last byte is ignored

Table 6-10. Output Parameter

Name	Size	Notes
Success	1	Upon successful execution, a value of 0 will be returned by the AT88SA100S chip

The SHA-256 message body used to create the decryption digest which is internally stored in the chip consists of the following 512-bits:

256-bits	Stored Key[KeyID]
64-bits	All ones
127-bits	Input seed
1-bit	‘1’ pad
64-bits	length of message in bits, fixed at 447

6.5 LoadSram

Writes 256-bits into the battery backed SRAM and locks this memory against further modification. The value in the battery backed SRAM cannot be read, it must be verified via the MAC command. If the secret value in the SRAM is already valid then this command will fail with an error response. The only way to unlock the SRAM is to remove power from the AT88SA100S.

The input data (secret key) is always decrypted using the decryption digest previously generated by GenPersonalizationKey prior to being written into the battery backed SRAM.

Note: Both the GenPersonalizationKey and LoadSram commands must be run consecutively within a single Wake cycle prior to the expiration of the watchdog timer. If any command is inserted between these two operations then LoadSram will fail.

Table 6-11. Input Parameters

	Name	Size	Notes
Opcode	LOADSRAM	1	0x10
Param1	Zero1	1	Must be 0x00
Param2	Zero2	2	Must be 0x0000
Data	Key	32	Encrypted value to be written into the SRAM

Table 6-12. Output Parameter

Name	Size	Notes
Success	1	Upon successful execution, a value of 0 will be returned by the AT88SA100S chip

The AT88SA100S chip executes the following sequence on receipt of this command.

1. If the internal flag (indicating that a personalization key has been loaded) is not set, then return error. If the MemValid flag is set, return error
2. Successively XOR each byte in the data (secret key) parameter with the corresponding byte from the personalization key generated by GenPersonalizationKey
3. Transfer the resulting bytes to the battery backed SRAM
4. Set MemValid (internal flag) to one

6.6 PauseLong

Forces the chip into the pause state until the watchdog timer expires, after which it will automatically enter into the sleep state. During execution of this command the chip will ignore all activity on the IO signal. This command is used to prevent bus conflicts in a system that also includes the CryptoAuthentication host chip sharing the same signal wire.

Table 6-13. Input Parameters

	Name	Size	Notes
Opode	PAUSELONG	1	0x01
Param1	Selector	1	Which chip to put into the pause state, 0x00 for all chips
Param2	Zero	2	Must be 0x0000
Data	Ignored	0	

Table 6-14. Output Parameter

Name	Size	Notes
Success	1	If the command indicates that some other chip should go into the pause state, a value of zero will be returned by this AT88SA100S chip. If this chip goes into the pause state no value will be returned.

The selector parameter provides a mechanism to select which AT88SA100S will pause if there are multiple devices on the bus:

- If the selector parameter is 0x00, then every chip receiving this command will go into the pause state and no chip will return a success code.
- If any of the bits of the selector parameter are set, then the chip will read the values of Fuse[84-87] and go to sleep only if those fuse values match the least significant four bits of the selector parameter. If the chip does *not* go into the pause state, it returns an error code of 0x0F. Otherwise, it goes into the pause state and never returns any code.

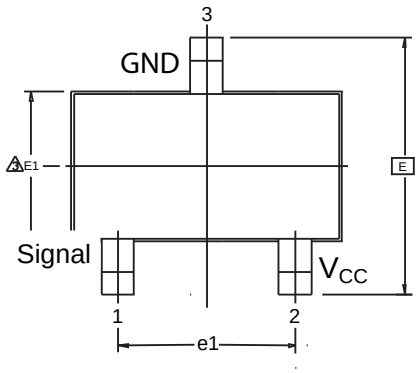
7. Pinout

Table 7-1. Pin Definitions

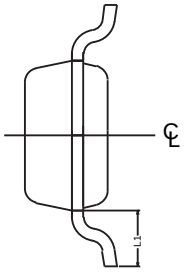
SOIC/TSSOP	SOT-23	Name	Description
5	1	Signal	IO channel to the system, open drain output. It is expected that an external pull-up resistor will be provided to pull this signal up to V_{CC} for proper communications. When the chip is not in use this pin can be pulled to either V_{CC} or GND.
8	2	V_{CC}	Power supply, 2.7 – 5.25 V. This pin should be bypassed with a high quality 0.1µF capacitor close to this pin with a short trace to GND Additional applications information at www.atmel.com
4	3	GND	Connect to system ground
1,2,3,6,7	--	NC	Not connected

8. Package Drawings

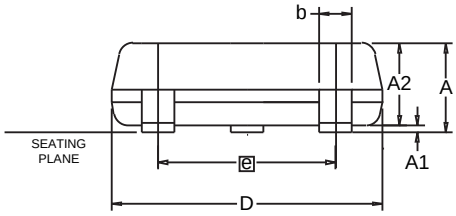
3TS1 – Shrink SOT



Top View



End View



Side View

Notes:
1. Dimension D does not include mold flash, protrusions or gate burrs. Mold flash, protrusions or gate burrs shall not exceed 0.25mm per end. Dimension E1 does not include interlead flash or protrusion. Interlead flash or protrusion shall not exceed 0.25mm per side.
2. The package top may be smaller than the package bottom. Dimensions D and E1 are determined at the outermost extremes of the plastic body exclusive of mold flash, tie bar burrs, gate burrs and interlead flash, but including any mismatch between the top and bottom of the plastic body.
3. These dimensions apply to the flat section of the lead between 0.08 mm and 0.15mm from the lead tip.

This drawing is for general information only. Refer to JEDEC Drawing TO-236, Variation AB for additional information.

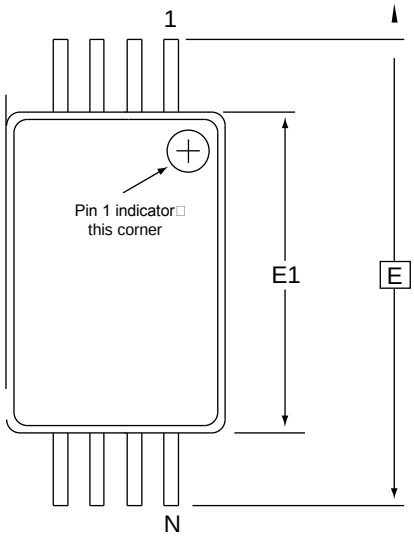
COMMON DIMENSIONS
(Unit of Measure = mm)

SYMBOL	MIN	NOM	MAX	NOTE
A	0.89	-	1.12	
A1	0.01	-	0.10	
A2	0.88	-	1.02	
D	2.80	2.90	3.04	1,2
E	2.10	-	2.64	
E1	1.20	1.30	1.40	1,2
L1		0.54 REF		
e1		1.90 BSC		
b	0.30	-	0.50	3

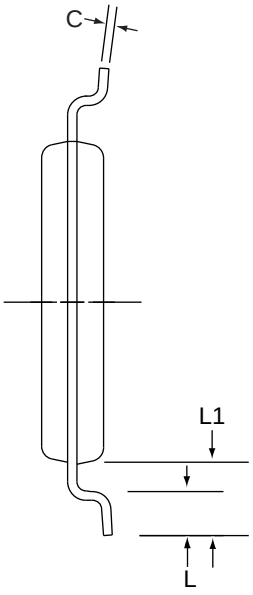
12/11/09

Package Drawing Contact: packagedrawings@atmel.com	**TITLE** **3TS1, 3-lead, 1.30mm Body, Plastic Thin** Shrink Small Outline Package (Shrink SOT)	**GPC** TBG	**DRAWING NO.** 3TS1	**REV.** B

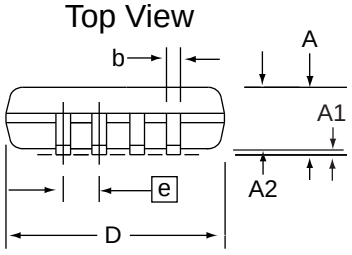
8X – TSSOP



Top View



End View



Side View

Notes:
1. This drawing is for general information only. Refer to JEDEC Drawing MO-153, VariationAA, for proper dimensions, tolerances, datums, etc.
2. Dimension D does not include mold Flash, protrusions or gate burrs. Mold Flash, protrusions and gate burrs shall not exceed 0.15mm (0.006in) per side.
3. Dimension E1 does not include inter-lead Flash or protrusions. Inter-lead Flash and protrusions shall not exceed 0.25mm (0.010in) per side.
4. Dimension b does not include Dambar protrusion. Allowable Dambar protrusion shall be 0.08 mm total in excess of the b dimension at maximum material condition. Dambar cannot be located on the lower radius of the foot. Minimum space between protrusion and adjacent lead is 0.07mm.
5. Dimension D and E1 to be determined at Datum Plane H.

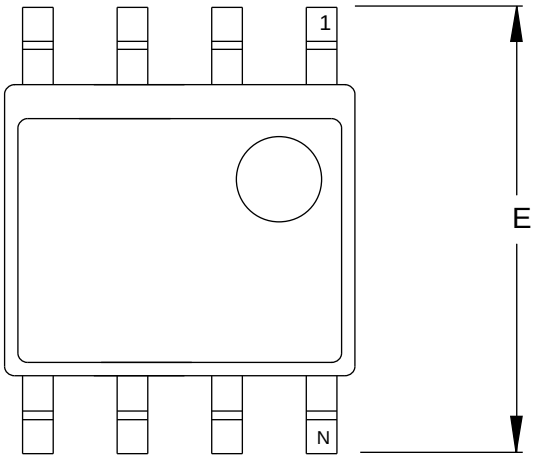
COMMON DIMENSIONS
(Unit of Measure = mm)

SYMBOL	MIN	NOM	MAX	NOTE
A	-	-	1.20	
A1	0.05	-	0.15	
A2	0.80	1.00	1.05	
D	2.90	3.00	3.10	2, 5
E		6.40 BSC		
E1	4.30	4.40	4.50	3, 5
b	0.19	–	0.30	4
e		0.65 BSC		
L	0.45	0.60	0.75	
L1		1.00 REF		
C		0.09	-	0.20

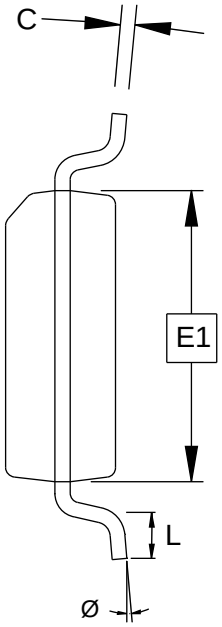
6/22/11

Package Drawing Contact: packagedrawings@atmel.com	TITLE 8X, 8-lead 4.4mm Body, Plastic Thin Shrink Small Outline Package (TSSOP)	GPC TNR	DRAWING NO. 8X	REV. D

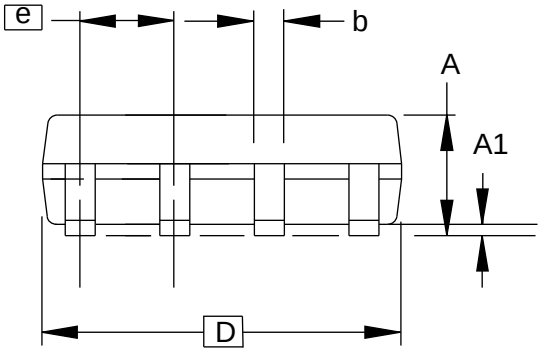
8S1 – JEDEC SOIC



TOP VIEW



END VIEW



SIDE VIEW

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

COMMON DIMENSIONS
(Unit of Measure = mm)

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

6/22/11

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

9. Ordering Information

Atmel AT88SA100S Ordering Information

Atmel Ordering Code	Package Type	Temperature Range
AT88SA100S-SH-CZ-T	SOIC, Tape and Reel	-40 °C to 85 °C
AT88SA100S -TH-CZ-T	TSSOP, Tape and Reel	-40 °C to 85 °C
AT88SA100S -TSU-T	3LD SOT23, Tape and Reel	-40 °C to 85 °C

10. Revision History

Doc. Rev.	Date	Comments
8558F	09/2011	Correct references and sections numbers Section 5.1.3, Sleep Flag, change " within 0.5V of V_{CC}" to "within 0.3V of V_{CC}"
8558E	08/2010	Update IO timeout description
8558D	06/2010	Update to Table 3: AC Parameters
8558C	05/2010	Expansion of IO Timeout specification
8558B	04/2010	Add TSSOP and SOIC packages
8558A	03/2009	Initial document release

Atmel Corporation
2325 Orchard Parkway
San Jose, CA 95131
USA
Tel: (+1)(408) 441-0311
Fax: (+1)(408) 487-2600
www.atmel.com

Atmel Asia Limited
Unit 01-5 & 16, 19F
BEA Tower, Millennium City 5
418 Kwun Tong Road
Kwun Tong, Kowloon
HONG KONG
Tel: (+852) 2245-6100
Fax: (+852) 2722-1369

Atmel Munich GmbH
Business Campus
Parkring 4
D-85748 Garching b. Munich
GERMANY
Tel: (+49) 89-31970-0
Fax: (+49) 89-3194621

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