ATAES132

32Kb AES Serial EEPROM Specification

SPI SUMMARY DATASHEET

NOT RECOMMENDED FOR NEW DESIGNS

Replaced by ATAES132A

Features

- 32Kb standard Serial EEPROM User Memory
  - Compatible with the Atmel® AT2530B
  - 16 user zones of 2Kb each
- High-security features
  - AES algorithm with 128-bit keys
  - AES-CCM for authentication
  - Message Authentication Code (MAC) for cryptographic operations
  - Secure storage for sixteen 128-bit keys
  - Encrypted User Memory Read and Write
  - FIPS Random Number Generator
  - 16 high-endurance monotonic EEPROM counters
- Flexible, user-configurable security
  - User zone access rights independently configured
  - Authentication prior to zone access
- Read/Write, encrypted, or read-only user zone options
- 10MHz serial interface
- 2.5V to 5.5V supply, <250nA sleep
- Packages: SOIC or UDFN
  - Serial EEPROM compatible pinout
- -40°C to +85°C operating temperature

Benefits

Add security without retooling printed circuit board by just replacing an existing Serial EEPROM.

- Authenticate consumables
- Authenticate components
- Authenticate network access
- Protect sensitive firmware
- Secure confidential data
- Prevent enablement of unpaid for features
- Manage contract manufacturers from overbuilds
- Manage warranty claims
- Securely store complete identify including fingerprints and pictures

This is a summary document. The complete document is available on the Atmel website at www.atmel.com.

Description

The Atmel ATAES132 is a high-security, Serial Electrically Erasable and Programmable Read-Only Memory (EEPROM) providing both authentication, confidential, nonvolatile data storage capabilities. Access restrictions for the sixteen user zones are independently configured, and any key can be used with any zone. Keys can also be used for standalone authentication. This flexibility permits the ATAES132 to be used in a wide range of applications.

The AES-128 cryptographic engine operates in AES-CCM mode to provide authentication, stored data encryption/decryption, and message authentication codes. Both internally stored data and/or small quantities of external data can be protected by the ATAES132 device.

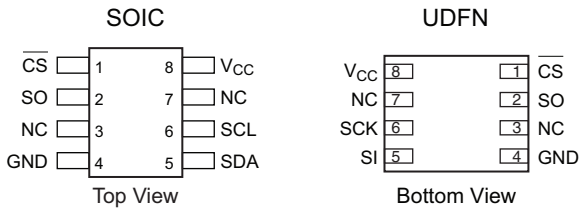
The ATAES132 pinout is compatible with standard Serial EEPROMs to allow placement on existing PC boards. The Serial EEPROM portion of the ATAES132 instruction set is identical to the Atmel Serial EEPROM instruction set. The ATAES132's extended security functions are accessed by sending command packets to the ATAES132 using standard Write instructions and reading responses using standard read instructions. The ATAES132 secure Serial EEPROM architecture allows it to be inserted into existing applications.

The ATAES132 device incorporates multiple physical security mechanisms to prevent release of the internally stored secrets. Secure personalization features are provided to facilitate third-party product manufacturing.

Table 1. Package Pin List

Pad	Description	SOIC	UDFN
V_{CC}	Supply Voltage	8	8
GND	Ground	4	4
SCK	Serial Clock Input	6	6
SI	Serial Data Input	5	5
$\overline{CS}$	SPI Chip Select Input	1	1
SO	Serial Data Output	2	2

Figure 1. Pin Configurations



Note: Drawings are not to scale.

1. Security

1.1 Advanced Encryption Standard (AES)

The ATAES132 cryptographic functions are implemented with a hardware cryptographic engine using the Advanced Encryption Standard (AES) in the CCM (Counter mode Cipher block chaining Message authentication code) mode with 128-bit keys. AES-CCM mode provides both confidentiality and integrity checking with a single key. The integrity MAC includes both the encrypted data and additional authenticate-only data bytes, as described in each command definition. Each MAC is unique due to inclusion of a nonce and an incrementing MacCount register in the MAC calculation.

1.2 Hardware Security Features

The ATAES132 device contains physical security features to prevent an attacker from determining the internal secrets. The ATAES132 includes tamper detectors for voltage, temperature, frequency, and light, as well as an active metal shield over the circuitry, internal memory encryption, and various other features. The ATAES132 physical design and cryptographic protocol are architected to prevent or significantly complicate most algorithmic, timing, and side-channel attacks.

2. Device Internal Regions

Seven distinct regions make up the internal organization of the ATAES132: User Memory, Information Region, Configuration Memory, Counters, Key Memory, SmallZone, and I/O Support regions.

Figure 2-1. Device Internal Regions

User Memory (32Kb)
Information Region (36 bytes)
Configuration Memory (165 bytes)
Counters (2Kb)
Key Memory (2Kb)
Small Zone (32 bytes)
Free Space (96 bytes)
I/O Support SRAM

2.1 User Memory

The User Memory is comprised of 32Kb of nonvolatile memory, segmented into 16 zones. Access to the zones is independently configurable to offer access restrictions, from open access, as in any standard Serial EEPROM, to full restrictions that preclude Read/Write operations and will only permit internal, authenticated use for such data as security keys.

2.2 Information Region

The information region holds read-only identification information, such as unique die serial numbers and other information pertaining to the ATAES132.

2.3 Configuration Memory

The Configuration Memory offers the ability to customize access rights to different resources of the device as a means to tailor the various security features of the device to one's specific application. This customizing, formally known as personalization, grants the application owner the ability to define custom access rights to device resources, from counters and key usage to memory. After personalization, the application owner issues lock commands to render the configuration permanent and to forever seal security keys and information in user zones configured to be confidential.

The Configuration Memory supports multi-step workflows to support the use of third-party services like programming without compromising the content or application security. In addition, Atmel offers optional, value-add programming services through the use of hardware security modules, which allow application owners to virtually inject their secrets into the ATAES132.

Table 2-1. Summary of Configuration Table Parameters, Sorted by Name

Name	Description	Write	Read	Bytes
Algorithm	Algorithm ID Code (0x0000).	Never	Always	2
ChipConfig	Device level cryptographic and power-up configuration options.	If Lockconfig = Unlocked	Always	1
Counters	16 monotonic counters, each capable of counting to 2M.	If Lockconfig = Unlocked	Always	128
CounterConfig	Configuration information for each counter.	If Lockconfig = Unlocked	Always	32
DeviceNum	Atmel device number code.	Never	Always	1
EEPageSize	Length in bytes of physical EEPROM page (32, 0x20).	Never	Always	1
EncReadSize	Maximum data length in bytes for EncRead (32, 0x20).	Never	Always	1
EncWriteSize	Maximum data length in bytes for EncWrite (32, 0x20).	Never	Always	1
FreeSpace	Free memory for customer data storage.	If Lockconfig = Unlocked	Always	96
JEDEC	Atmel JEDEC manufacturer code 0x001F.	Never	Always	2
KeyConfig	Configuration information for each key.	If Lockconfig = Unlocked	Always	64
LockConfig(1)	Controls Configuration Memory Write access except SmallZone. Default is the Unlocked state.	Via Lock Command Only	Always	1
LockKeys(1)	Controls Key Memory Write Access. Default is the 'unlocked' state.	Via Lock Command Only	Always	1
LockSmall(1)	Controls SmallZone Register Write access. Default is the 'unlocked' state.	Via Lock Command Only	Always	1
LotHistory	Atmel proprietary manufacturing information	Never	Always	8

Note: 1. Changes to most of the configuration registers take effect immediately which allows the functionality to be tested during the personalization process. Changes to the I2C Addr register take effect at the next Reset, Power-Up, or Wake-Up from the Sleep state.

Table 2-1. Summary of Configuration Table Parameters, Sorted by Name (Continued)

Name	Description	Write	Read	Bytes
ManufacturingID	Two byte manufacturing ID code	Never	Always	2
PermConfig	Atmel factory device configuration options	Never	Always	1
SerialNum	Guaranteed unique die serial number. SerialNum is optionally included in cryptographic calculations.	Never	Always	8
SmallZone	32 byte value. The first four bytes are optionally included in cryptographic calculations.	If Locksmall = Unlocked	Always	32
I2C Addr	Selects the serial interface mode and stores the I^2C device address.	If LockConfig = Unlocked	Always	1
ZoneConfig	Access and usage permissions for each user zone.	If LockConfig = Unlocked	Always	64

Note: 1. Changes to most of the configuration registers take effect immediately which allows the functionality to be tested during the personalization process. Changes to the I2C Addr register take effect at the next Reset, Power-Up, or Wake-Up from the Sleep state.

2.4 Counters

The Counters region contains 16 nonreversible monotonic counters. Counter operation is customized during personalization in the Configuration Memory to permit such features as free use, authenticated-only increments, and control of key usage.

2.5 Key Memory

Key Memory holds sixteen 128-bit keys targeting various AES and AES-CCM operations. Key usage is customized during personalization in the Configuration Memory to permit custom features like authentication-only, limited-use, counter increment, user zone access, key permissions, and many other uses. The Key Memory is writeable only during personalization, and is never readable under any circumstances. One may only use an authentication procedure to validate the content of a key; however, ATAES132 offers a set of commands which, when so configured during personalization, permits secure key creation, imports, and transfer of content from a confidential User Memory to key space.

2.6 SmallZone

SmallZone is a 32-byte, general-purpose memory separate from the 32Kb user memory and with special features to aid multi-step workflows. Configuration at personalization may make portions of this zone a mandatory input into cryptographic calculations.

2.7 I/O Support

The I/O Support regions contains a FIFO and other registers, which together provide a means to send the ATAES132 commands and receive responses, including status information.

3. Commands

The ATAES132 extends the command set of a standard Serial EEPROM to offer additional commands that solve various security challenges. Unrestricted memory regions are accessible using standard Serial EEPROM SPI commands. Restricted User Memory regions, as well as security features, are still accessible by using standard SPI commands to

send extended command bytes to a FIFO address. Responses are read using standard SPI commands from same FIFO address.

Table 3-1. ATAES132 Extended Command Set Summary

Opcode	Name	Description
0x03	Auth	Performs one-way or mutual authentication using the specified key.
0x15	AuthCheck	Checks the output MAC generated by the Auth command or by reading a counter using the Counter command on a second ATAES132 device.
0x14	AuthCompute	Computes the input MAC required to execute the Auth command or to increment a counter using the Counter command on a second ATAES132 device.
0x10	BlockRead	Reads 1 to 32 bytes of data from User Memory or the Configuration Memory. Returns cleartext data.
0x0A	Counter	Increments a monontonic counter and/or returns the counter value.
0x0B	Crunch	Processes a seed value through the internal crunch engine. This function is used to detect clones.
0x07	Decrypt	Decrypts 16 or 32 bytes of data provided by the Host after verifying the integrity MAC.
0x04	EncRead	Encrypts 1 to 32 bytes of data from User Memory and returns the encrypted data and integrity MAC.
0x06	Encrypt	Encrypts 16 or 32 bytes of plaintext data provided by the Host.
0x05	EncWrite	Writes 1 to 32 bytes of encrypted data into the User Memory or Key Memory after verifying the integrity MAC.
0x0C	Info	Returns device information: the MacCount, authentication status, or the hardware revision code.
0x08	KeyCreate	Generates a random number, stores it in Key Memory, and returns the encrypted key to the Host.
0x19	KeyImport	Decrypts and writes a key that was output by the KeyCreate command.
0x09	KeyLoad	Writes an encrypted key to Key Memory after verifying the integrity MAC.
0x1A	KeyTransfer	Transfers a key from User Memory to the Key Memory or to the VolatileKey Register.
0x0F	Legacy	Performs a single AES-ECB mode operation on 16 bytes of data provided by the Host.
0x0D	Lock	Permanently locks the Configuration Memory or Key Memory. Locked memory can never be unlocked.
0x01	Nonce	Generates a 128-bit nonce using the internal random number generator for use by the cryptographic commands. This command can also be used to write a host nonce directly into the Nonce Register.
0x13	NonceCompute	Generates a nonce in a manner that allows two ATAES132 devices to have identical nonce values.

Table 3-1. ATAES132 Extended Command Set Summary (Continued)

Opcode	Name	Description
0x02	Random	Returns a 128-bit random number from the internal random number generator.
0x00	Reset	Resets the device, clearing the cryptographic status.
0x11	Sleep	Places the device in the sleep state or standby state to reduce power consumption.

4. Power Management Features

The ATAES132 supports four power states that offer great flexibility in reducing its power consumption, especially in low-power embedded systems. These are the Active, Standby, Sleep, and Off sates. Power consumption ranges from less than 250nA in the Sleep state to10mA in the Active state. The ATAES132 can power-up into any of the powered states, if so configured. It can also enter the standby or sleep states after receipt of a Sleep command from the Host.

5. Electrical Characteristics

5.1 Absolute Maximum Ratings*

Operating Temperature	−40°C to +85°C
Storage Temperature	−65°C to + 150°C
Maximum Operating Voltage	6.0V
DC Output Current	5.0mA
Voltage on Any Pin	-0.7V to (V_{CC} + 0.7V)
HBM ESD	3kV minimum

*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 may affect device reliability.

5.2 Reliability

The ATAES132 is fabricated with Atmel high reliability CMOS EEPROM manufacturing technology. The reliability ratings in Table 5-1 apply to each byte of the EEPROM memory.

Table 5-1. EEPROM Reliability(1)

Parameter	Min	Typical	Max	Units
Write Endurance (Each byte)	100,000			Write Cycles
Data Retention (At 55°C)	10			Years
Data Retention (At 35°C)	30	50		Years
Read Endurance	Unlimited			Read Cycles

Note: 1. These specifications apply to every byte of the User Memory, Configuration Memory, and Key Memory. The Write Endurance specification also applies to the random number generator EEPROM Seed Register.

5.3 DC Characteristics

5.3.1 Supply Voltage and Current Characteristics

Applicable over recommended operating range from T_A = −40°C to +85°C, V_{CC} = +2.5V to +5.5V (unless otherwise noted).(1)

Symbol	Parameter	Test Conditions	Min	Typ	Max	Units
V_{CC}(1)	Supply Voltage		2.5		5.5	V
I_{CC1}	Supply Current	V_{CC} = 3.3V at fmax(4), SO = Open(3), Read, Write, or AES Operation.			6	mA
I_{CC2}	Supply Current	V_{CC} = 5.5V at fmax(4), SO = Open(3), Read, Write, or AES Operation.			10	mA
I_{CC3}	Idle Current	V_{CC} = 3.3V or 5.5V at fmax(4), SO = Open (3), Waiting for a Command.		600	800	µA
I_{SL1}	Sleep Current	V_{CC} = 3.3V, $\overline{CS}$ = V_{CC} (3), Sleep State		0.10	0.25	µA
I_{SL2}	Sleep Current	V_{CC} = 5.5V, $\overline{CS}$ = V_{CC} (3), Sleep State		0.25	0.50	µA
I_{SB1}	Standby Current	V_{CC} = 3.3V, $\overline{CS}$ = V_{CC} (3), Standby State		15	30	µA
I_{SB2}	Standby Current	V_{CC} = 5.5V, $\overline{CS}$ = V_{CC} (3), Standby State		20	40	µA

Notes:
1. Typical values are at 25°C, and are for reference only. Typical values are not tested or guaranteed
2. On power-up, V_{CC} must rise continuously from V_{SS} to the operating voltage, with a rise time no faster than 1V/µs.
3. All input pins must be held at either V_{SS} or V_{CC} during this measurement
4. Measurement is performed at the maximum serial clock frequency
5. The ATAES132 does not support hot swapping or hot plugging. Connecting or disconnecting this device to a system while power is energized can cause permanent damage to ATAES132

5.3.2 DC Characteristics

Applicable over recommended operating range from T_A = −40°C to +85°C, V_{CC} = +2.5V to +5.5V (unless otherwise noted).

Symbol	Parameter	Test Conditions	Min	Max	Units
I_{LI}	Input Current	V_{IN} = 0V or V_{CC}	−3.0	3.0	µA
I_{LO}	Output Leakage	V_{OUT} = 0V or V_{CC}	−3.0	3.0	µA
V_{IL}(1)	Input Low-voltage		−0.5	V_{CC} x 0.3	V
V_{IH}(1)	Input High-voltage		V_{CC} x 0.7	V_{CC} + 0.5	V
V_{OL1}	Output low-voltage, except SI	I_{OL} = 3.0mA	0	0.4	V
V_{OH1}	Output high-voltage, except SI	I_{OH} = −3.0mA	V_{CC} −0.8	V_{CC}	V
V_{OL2}	Output low-voltage, SI	I_{OL} = 3.0mA	0	0.4	V

Note: 1. V_{IL} min and V_{IH} max are for reference only, and are not tested.

5.4 AC Characteristics

Applicable over recommended operating range from T_A = −40°C to + 85°C, V_{CC} = +2.5V to +5.5V.

Symbol	Parameter	Min	Max	Units
t_{WC1}	User Zone Write Cycle Time(1)	6	9	ms
t_{WC2}	Key Zone Write Cycle Time(1)	12	16	ms

Note: 1. The Write Cycle Time includes the EEPROM Erase, Write, and Automatic Data Write Verification operations.

5.4.1 Power-up, Sleep, and Wake-up Timing Characteristics(1)

Applicable over recommended operating range from T_A = −40°C to + 85°C, V_{CC} = +2.5V to +5.5V

Symbol	Parameter	Min	Typ	Max	Units
$t_{PU.STATUS}$	Power-up Time, Status		500	600	µs
$t_{PU.RDY}$	Power-up Ready Time		1200	1500	µs
t_{SB}	Sleep Time, Entering the Standby State		65	100	µs
t_{SL}	Sleep Time, Entering the Sleep State		55	90	µs
$t_{WupSB.STATUS}$	Wake-up Status Time, Standby State		50	100	µs
$t_{WupSB.RDY}$	Wake-up Ready Time, Standby State		200	240	µs
$t_{WupSL.STATUS}$	Wake-up Status, Sleep State		500	600	µs
$t_{WupSL.RDY}$	Wake-up Ready Time, Sleep State		1000	1200	µs
$t_{CSS.Wup}$	$\overline{CS}$ Setup Time at Wake-up (see Section 6., “Part Markings”)	100			ns

Note: 1. All values are based on characterization, and are not tested. Typical values are at 25°C and are for reference only.

5.4.2 SPI Interface Timing

Applicable over recommended operating range from T_A = −40°C to + 85°C, V_{CC} = +2.5V to +5.5V, CL = 1 TTL Gate and 30pF (unless otherwise noted).

Symbol	Parameter	Min	Max	Units
f_{SCK}	SCK Clock Frequency	0	10	MHz
	SCK Clock Duty Cycle	30	70	Percent
t_{WH}	SCK High Time	40		ns
t_{WL}	SCK Low Time	40		ns
t_{CS}	$\overline{CS}$ High Time	50		ns
t_{CSS}	$\overline{CS}$ Setup Time	50		ns
t_{CSH}	$\overline{CS}$ Hold Time	50		ns
t_{SU}	Data in Setup Time	10		ns
t_H	Data in Hold Time	10		ns
t_{RI}	Input Rise Time(1)		2	µs
t_{FI}	Input Fall Time(1)		2	µs
t_V	Output Valid	0	40	ns
t_{HO}	Output Hold Time	0		ns
t_{DIS}	Output Disable Time		50	ns

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

Figure 5-1. SPI Synchronous Data Timing

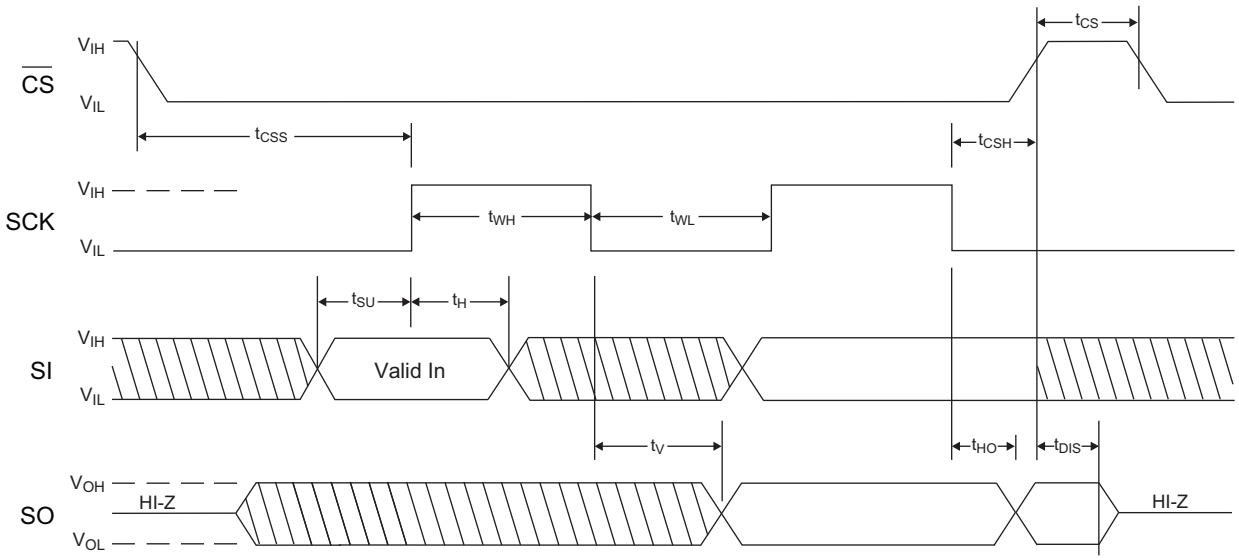
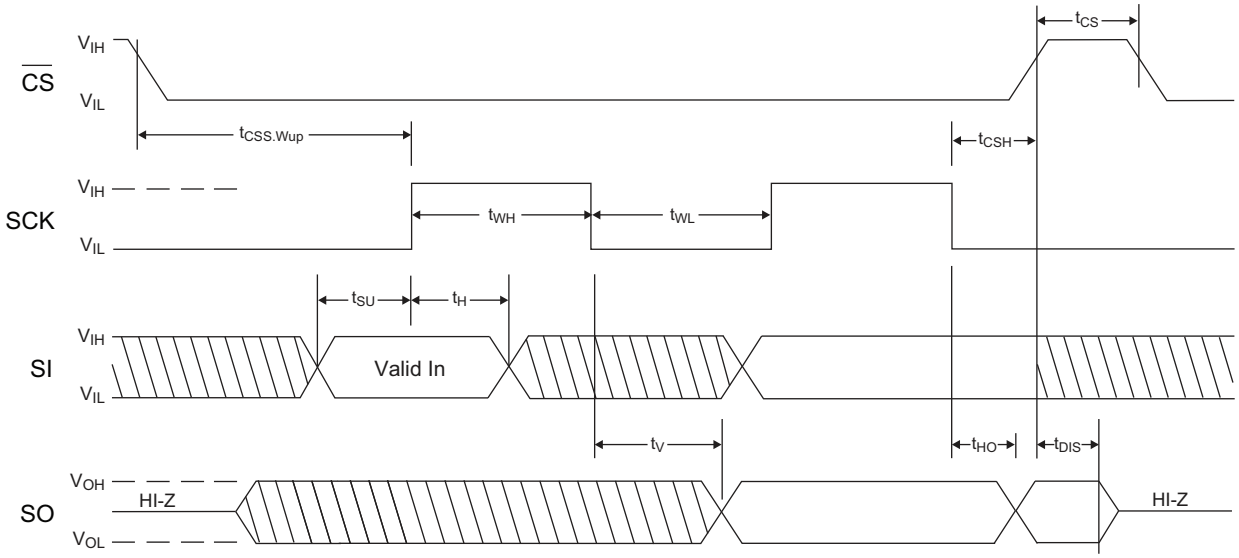


Figure 5-2. SPI Interface Timing, $\overline{CS}$ Setup Time at Wake-up



6. Part Markings

The part marking on the packages represents only variable manufacturing lot information and does not contain any reference to the part number. Each reel or shipment may have different markings. Do not use the marking on the IC package to determine product acceptance, instead, use the information on the shipment, reel, or box label.

7. Ordering Information

The ATAES132 production ordering codes are listed below. The ATAES132 packages are marked only with a lot trace code and *not* the ordering code.

7.1 Ordering Codes

ATAES132 Ordering Code	Package	Conditioning	Interface Configuration	Temperature Range
ATAES132-SH-EQ	SOIC	Bulk	SPI	-40°C to 85°C
ATAES132-SH-EQ-T(1)	SOIC	Tape and Reel		
ATAES132-MAH-EQ-T(1)	UDFN	Tape and Reel		

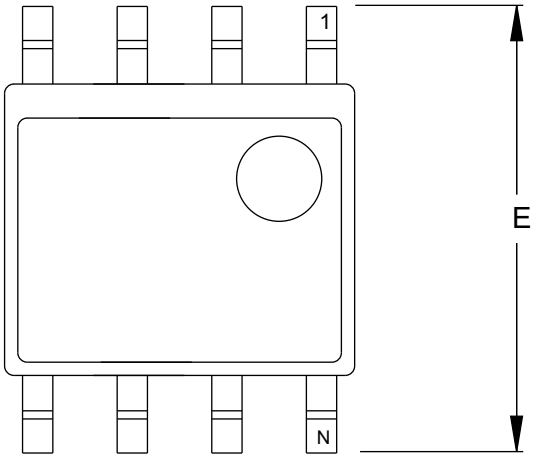
Note: 1. T = Tape and Reel
- SOIC = 4K per reel
- UDFN = 5K per reel

Package Type	
SOIC	8-pin SOIC, NiPdAu Lead Finish, Green(1)
UDFN	8-pin UDFN/USON 2.00mm x 3.00mm, NiPdAu Lead Finish, Green(1)

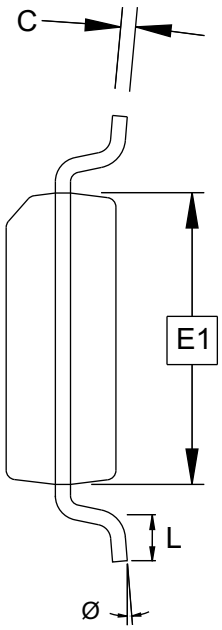
Note: 1. Lead-free, halogen-free package. Exceeds RoHS requirements.

7.2 Package Drawings

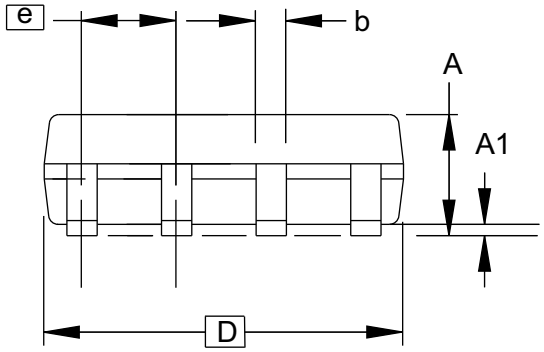
7.2.1 8S1 — 8-lead JEDEC SOIC



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.

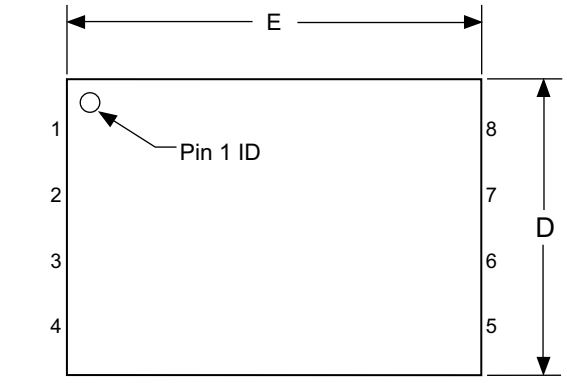
COMMON DIMENSIONS
(Unit of Measure = mm)

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°	

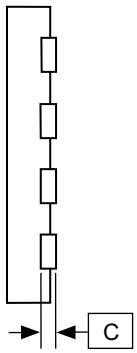
6/22/11

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

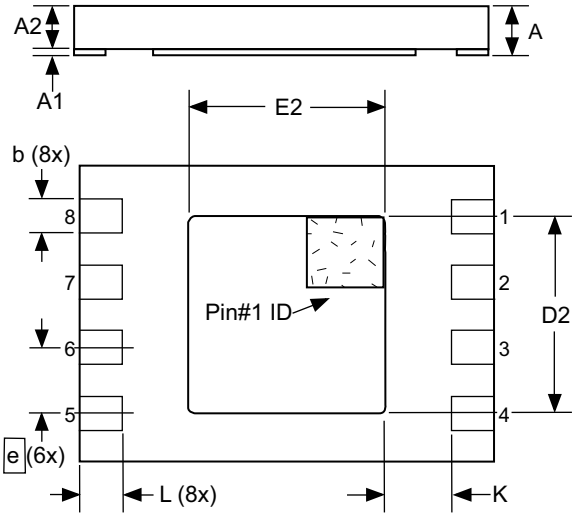
7.2.2 8MA2 — 8-pad UDFN



TOP VIEW



SIDE VIEW



BOTTOM VIEW

Notes:
1. This drawing is for general information only. Refer to Drawing MO-229, for proper dimensions, tolerances, datums, etc.
2. The Pin #1 ID is a laser-marked feature on Top View.
3. Dimensions b applies to metallized terminal and is measured between 0.15 mm and 0.30 mm from the terminal tip. If the terminal has the optional radius on the other end of the terminal, the dimension should not be measured in that radius area.
4. The Pin #1 ID on the Bottom View is an orientation feature on the thermal pad.

COMMON DIMENSIONS
(Unit of Measure = mm)

SYMBOL	MIN	NOM	MAX	NOTE
A	0.50	0.55	0.60	
A1	0.0	0.02	0.05	
A2	-	-	0.55	
D	1.90	2.00	2.10	
D2	1.20	-	1.60	
E	2.90	3.00	3.10	
E2	1.20	-	1.60	
b	0.18	0.25	0.30	3
C	1.52 REF			
L	0.30	0.35	0.40	
e	0.50 BSC			
K	0.20	-	-	

6/6/14

Atmel Package Drawing Contact: packagedrawings@atmel.com	**TITLE** 8MA2, 8-pad 2 x 3 x 0.6mm Body, Thermally Enhanced Plastic Ultra Thin Dual Flat No-Lead Package (UDFN)	**GPC** YNZ	**DRAWING NO.** 8MA2	**REV.** F

8. Revision History

Doc. Rev.	Date	Comments
8763DS	07/2014	03/2015 Not recommended for new designs. Replaced by ATAES132A. Update ESD from 2000V to 3kV and 8MA2 package drawing.
8763CS	10/2013	Remove DecRead and WriteCompute commands and TSSOP package option. Update KeyExport to KeyCreate. Add SOIC and UDFN package drawings. Update footers and disclaimer page.
8763BS	02/2013	Ordering code table: add package column, notes, and update ordering codes. Update Atmel logos and disclaimer/copy page.
8763AS	05/2011	Initial SPI summary document release.

Atmel Corporation 1600 Technology Drive, San Jose, CA 95110 USA **T:** (+1)(408) 441.0311 **F:** (+1)(408) 436.4200 | **www.atmel.com**