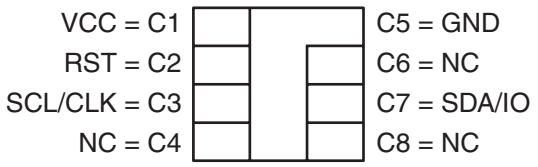
2-wireFeatures

- One of a Family of Devices with User Memories from 1-Kbit to 1-Mbit
- 128-Kbit (16-Kbyte) EEPROM User Memory
  - Sixteen 1-Kbyte (8-Kbit) Zones
  - Self-timed Write Cycle (5 ms)
  - Single Byte or 128-byte Page Write Mode
  - Programmable Access Rights for Each Zone
- 2-Kbit Configuration Zone
  - 37-byte OTP Area for User-defined Codes
  - 160-byte Area for User-defined Keys and Passwords
- High Security Features
  - 64-bit Patented Dynamic Symetric Mutual Authentication Protocol (under exclusive patent license from ELVA)
  - Encrypted Checksum
  - Stream Encryption
  - Four Key Sets for Authentication and Encryption
  - Eight Sets of Two 24-bit Passwords
  - Anti-tearing Function
  - Voltage and Frequency Monitor
- Smart Card Features
  - ISO 7816 Class A (5V) or Class B (3V) Operation
  - ISO 7816-3 Asynchronous T = 0 Protocol
  - Supports Protocol and Parameters Selection for Faster Operation
  - Multiple Zones, Key Sets and Passwords for Multi-application Use
  - Synchronous 2-wire Serial Interface for Faster Device Initialization
  - Programmable 8-byte Answer-to-reset Register
  - ISO 7816-2 Compliant Modules
- Embedded Application Features
  - Low Voltage Operation: 2.7V to 5.5V
  - Secure Nonvolatile Storage for Sensitive System or User Information
  - 2-wire Serial Interface
  - 1.5 MHz Compatibility for Fast Operation
  - Standard 8-lead Plastic Packages
  - Same Pinout as 2-wire Serial EEPROMs
- High Reliability
  - Endurance: 100,000 Cycles
  - Data Retention: 10 years
  - ESD Protection: 4,000V min

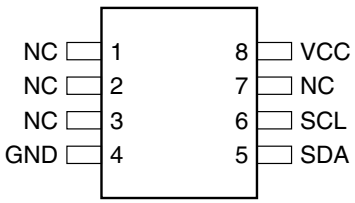
Table 1. Pin Configuration

Pad	Description	ISO Module Contact	Standard Package Pin
VCC	Supply Voltage	C1	8
GND	Ground	C5	4
SCL/CLK	Serial Clock Input	C3	6
SDA/IO	Serial Data Input/Output	C7	5
RST	Reset Input	C2	NC

Card Module Contact



8-lead SOIC, PDIP or LAP



CryptoMemory® 128 Kbit

AT88SC12816C

Summary

Rev. 5016BS–SMEM–04/03

Note: This is a summary document. A complete document is available under NDA. For more information, please contact your local Atmel sales office.

Description

The AT88SC12816C member of the CryptoMemory family is a high-performance secure memory providing 128 Kbits of user memory with advanced security and cryptographic features built in. The user memory is divided into 16 1-Kbyte zones, each of which may be individually set with different security access rights or combined together to provide space for one to four data files.

Smart Card Applications

The AT88SC12816C provides high security, low cost, and ease of implementation without the need for a microprocessor operating system. The embedded cryptographic engine provides for dynamic, symmetric-mutual authentication between the device and host, as well as performing stream encryption for all data and passwords exchanged between the device and host. Up to four unique key sets may be used for these operations. The AT88SC12816C offers the ability to communicate with virtually any smart card reader using the asynchronous T = 0 protocol defined in ISO 7816-3. Communication speeds up to 153,600 baud are supported by utilizing ISO 7816-3 Protocol and Parameter Selection.

Embedded Applications

Through dynamic, symmetric-mutual authentication, data encryption, and the use of encrypted checksums, the AT88SC12816C provides a secure place for storage of sensitive information within a system. With its tamper detection circuits, this information remains safe even under attack. A 2-wire serial interface running at 1.5 MHz is used for fast and efficient communications with up to 15 devices that may be individually addressed. The AT88SC12816C is available in industry standard 8-lead packages with the same familiar pinout as 2-wire serial EEPROMs.

Figure 1. Block Diagram

Pin Descriptions

Supply Voltage (V_{CC})

The V_{CC} input is a 2.7V to 5.5V positive voltage supplied by the host.

Clock (SCL/CLK)

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

When the synchronous protocol is used, the SCL/CLK input is used to positive edge clock data into the device and negative edge clock data out of the device.

Serial Data (SDA/IO)

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

Reset (RST)

The AT88SC12816C provides an ISO 7816-3 compliant asynchronous answer to reset sequence. When the reset sequence is activated, the device will output the data programmed into the 64-bit answer-to-reset register. An internal pull-up on the RST input pad allows the device to be used in synchronous mode without bonding RST. The AT88SC12816C does not support the synchronous answer-to-reset sequence.

Device Architecture

User Zones

The EEPROM user memory is divided into 16 zones of 8,192 bits each. Multiple zones allow for different types of data or files to be stored in different zones. Access to the user zones is allowed only after security requirements have been met. These security requirements are defined by the user during the personalization of the device in the configuration zone. If the same security requirements are selected for multiple zones, then these zones may effectively be accessed as one larger zone.

Table 2. User Zones

ZONE	$0	$1	$2	$3	$4	$5	$6	$7	
User 0									$000
	1024 bytes								–
									–
									$3F8
User 1 - - - User 14									$000
									–
									–
									–
									$3F8
User 15									$000
	1024 bytes								–
									–
									$3F8

Control Logic

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

Configuration Zone

The configuration zone consists of 2048 bits of EEPROM memory used for storing passwords, keys and codes and defining security levels to be used for each user zone. Access rights to the configuration zone are defined in the control logic and may not be altered by the user.

Table 3. Configuration Zone

Component	Address
Answer to Reset	$00
Fab Code	
Memory Test Zone	
Card Manufacturers Code	
Lot History Code	
Device Configuration Register	$18
Identification Number	
Access Registers	
Password/Key Registers	
Issuer Code	
Authentication Attempts Counters	$50
Cryptograms	
Session Encryption Keys	
Secret Seeds	
Password Attempts Counters	$B0
Write Passwords	
Read Passwords	
Reserved	

Security Fuses

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

Protocol Selection

The AT88SC12816C supports two different communication protocols.

- **Smart Card Applications**: The asynchronous T = 0 protocol defined by ISO 7816-3 is used for compatibility with the industry's standard smart card readers.
- **Embedded Applications**: A 2-wire serial interface is used for fast and efficient communication with logic or controllers.

The power-up sequence determines which of the two communication protocols will be used.

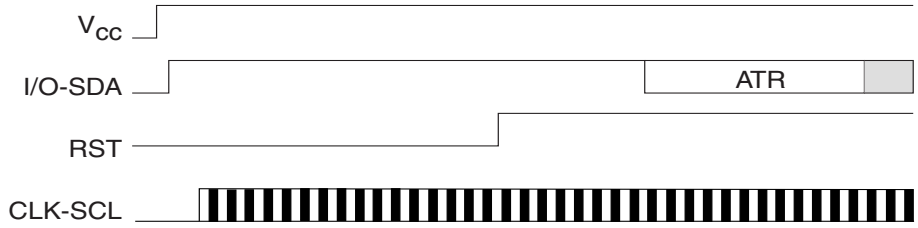
Asynchronous T = 0 Protocol

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

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

The device will respond with a 64-bit ATR code, including historical bytes to indicate the memory density within the CryptoMemory family. Once the asynchronous mode has been selected, it is not possible to switch to the synchronous mode without powering off the device.

Figure 2. Asynchronous T = 0 Protocol



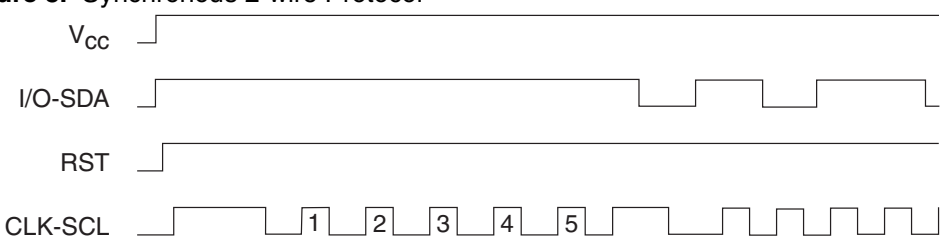
After a successful ATR, the Protocol and Parameter Selection (PPS) protocol, as defined by ISO 7816-3, may be used to negotiate the communications speed with CryptoMemory devices 32 Kbits and larger. CryptoMemory supports D values of 1, 2, 4, 8, 12, and 16 for an F value of 372. Also supported are D values of 8 and 16 for F = 512. This allows selection of 8 communications speeds ranging from 9600 baud to 153,600 baud.

Synchronous 2-wire Serial Interface

The synchronous mode is the default after powering up V_{CC} due to the internal pull-up on RST. For embedded applications using CryptoMemory in standard plastic packages, this is the only communication protocol.

- Power-up V_{CC}, RST goes high also.
- After stable V_{CC}, CLK-SCL and I/O-SDA may be driven.

Figure 3. Synchronous 2-wire Protocol



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

Communication Security Modes

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

Table 4. Communication Security Modes[1]

Mode	Configuration Data	User Data	Passwords	Data Integrity Check
Standard	Clear	Clear	Clear	MDC
Authentication	Clear	Clear	Encrypted	MAC
Encryption	Clear	Encrypted	Encrypted	MAC

Note: 1. Configuration data include viewable areas of the Configuration Zone except the passwords:
MDC: Modification Detection Code
MAC: Message Authentication Code.

Security Options

Anti-tearing

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

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

In 2-wire mode, the host is required to perform ACK polling for up to 20 ms after write commands when anti-tearing is active. At power-up, the host is required to perform ACK polling, in some cases for up to 10 ms, in the event that the device needs to carry out the data recovery process.

Write Lock

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

Example: The write lock byte at $080 controls the bytes from $080 to $087.

$080	$081	$082	$083	$084	$085	$086	$087	@
11011001	xxxx xxxx locked	xxxx xxxx locked	xxxx xxxx	xxxx xxxx	xxxx xxxx locked	xxxx xxxx	xxxx xxxx	$80

The write lock byte may also be locked by writing its least significant (rightmost) bit to "0". Moreover, when write lock mode is activated, the write lock byte can only be programmed – that is, bits written to "0" cannot return to "1".

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

Password Verification

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

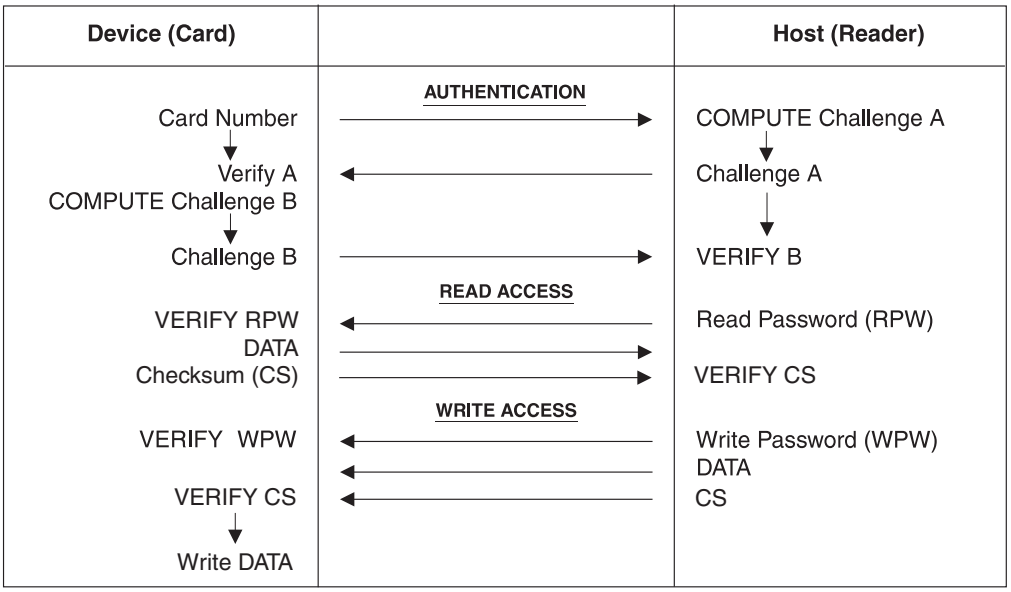
Authentication Protocol

The access to a user zone may be protected by an authentication protocol. Any one of four keys may be selected to use with a user zone.

The authentication success is memorized and active as long as the chip is powered, unless a new authentication is initialized or RST becomes active. If the new authentication request is not validated, the card loses its previous authentication and it should be presented again. Only the last request is memorized.

Note: Password and authentication may be presented at any time and in any order. If the trials limit has been reached (after four consecutive incorrect attempts), the password verification or authentication process will not be taken into account.

Figure 4. Password and Authentication Operations



Checksum

The AT88SC12816C implements a data validity check function in the form of a checksum, which may function in standard, authentication or encryption modes.

In the standard mode, the checksum is implemented as a Modification Detection Code (MDC), in which the host may read a MDC from the device in order to verify that the data sent was received correctly.

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

Encryption

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

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

Supervisor Mode

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

Modify Forbidden

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

Program Only

For a user zone protected by this feature, data within the zone may be changed from a “1” to a “0”, but never from a “0” to a “1”.

Ordering Information

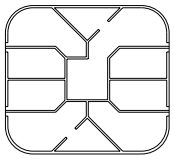
Ordering Code	Package	Voltage Range	Temperature Range
AT88SC12816C-MF	M2 – F Module	2.7V–5.5V	Commercial (0°C–70°C)
AT88SC12816C-MB	M2 – B Module	2.7V–5.5V	Commercial (0°C–70°C)
AT88SC12816C-PI	8P3	2.7V–5.5V	Industrial (–40°C–85°C)
AT88SC12816C-SI	8S1	2.7V–5.5V	Industrial (–40°C–85°C)
AT88SC12816C-CI	8C	2.7V–5.5V	Industrial (–40°C–85°C)
AT88SC12816C-WI	7 mil wafer	2.7V–5.5V	Industrial (–40°C–85°C)

Package Type[1]	Description
M2 – F Module	M2 ISO 7816 Smart Card Module
M2 – B Module	M2 ISO 7816 Smart Card Module with Atmel Logo
8P3	8-lead, 0.300” Wide, Plastic Dual Inline Package (PDIP)
8S1	8-lead, 0.150” Wide, Plastic Gull Wing Small Outline Package (JEDEC SOIC)
8CN1	8-lead, 8 x 5 x 1.04 mm Body, Leadless Array Package (LAP)

Note: 1. Formal drawings may be obtained from an Atmel sales office.

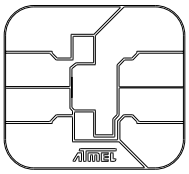
Packaging Information

Ordering Code: ME



Module Size: **M2**
Dimension*: 12.6 x 11.4 [mm]
Glob Top: Round - ∅ 8.0 [mm]
Thickness: 0.58 [mm]
Pitch: 14.25 mm

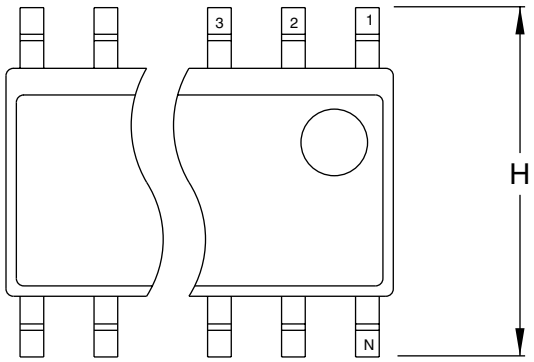
Ordering Code: MP



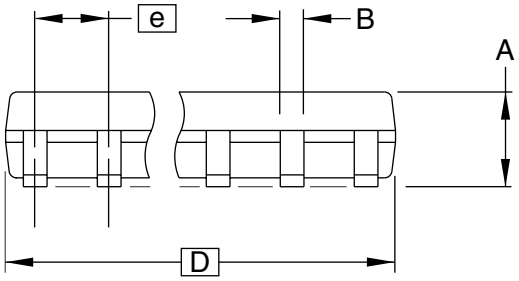
Module Size: **M2**
Dimension*: 12.6 x 11.4 [mm]
Glob Top: Square - 8.8 x 8.8 [mm]
Thickness: 0.58 [mm]
Pitch: 14.25 mm

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

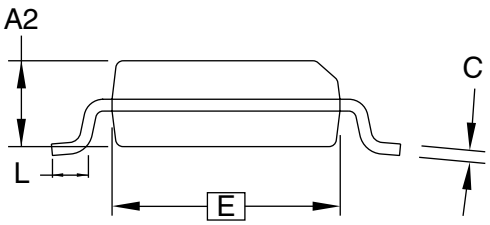
Ordering Code: SI
8-lead SOIC



Top View



Side View



End View

COMMON DIMENSIONS
(Unit of Measure = mm)

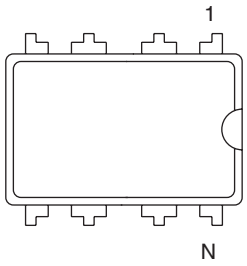
SYMBOL	MIN	NOM	MAX	NOTE
A	–	–	1.75	
B	–	–	0.51	
C	–	–	0.25	
D	–	–	5.00	
E	–	–	4.00	
e		1.27 BSC		
H	–	–	6.20	
L	–	–	1.27	

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

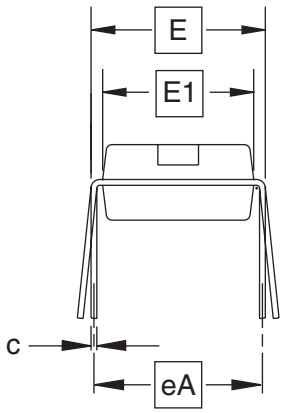
10/10/01

	TITLE	DRAWING NO.	REV.
2325 Orchard Parkway San Jose, CA 95131	**8S1**, 8-lead (0.150" Wide Body), Plastic Gull Wing Small Outline (JEDEC SOIC)	8S1	A

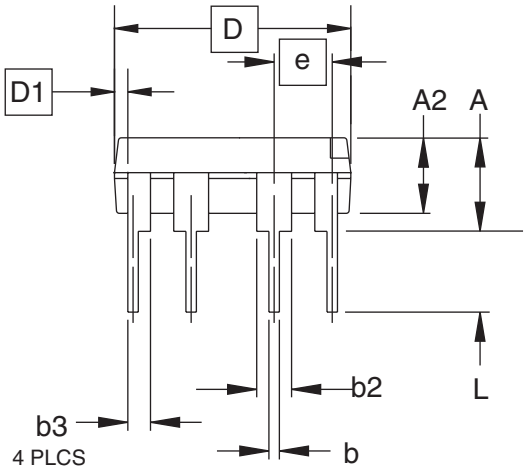
Ordering Code: PI
8-lead PDIP



Top View



End View



Side View

COMMON DIMENSIONS
(Unit of Measure = inches)

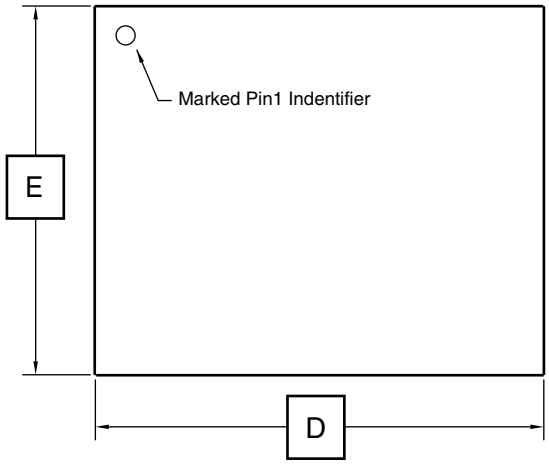
SYMBOL	MIN	NOM	MAX	NOTE
A			0.210	2
A2	0.115	0.130	0.195	
b	0.014	0.018	0.022	5
b2	0.045	0.060	0.070	6
b3	0.030	0.039	0.045	6
c	0.008	0.010	0.014	
D	0.355	0.365	0.400	3
D1	0.005			3
E	0.300	0.310	0.325	4
E1	0.240	0.250	0.280	3
e	0.100 BSC			
eA	0.300 BSC			4
L	0.115	0.130	0.150	2

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

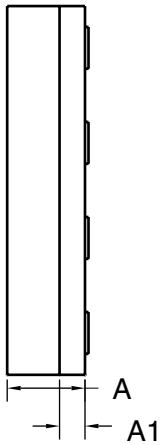
01/09/02

	TITLE	DRAWING NO.	REV.
2325 Orchard Parkway San Jose, CA 95131	**8P3**, 8-lead, 0.300" Wide Body, Plastic Dual In-line Package (PDIP)	8P3	B

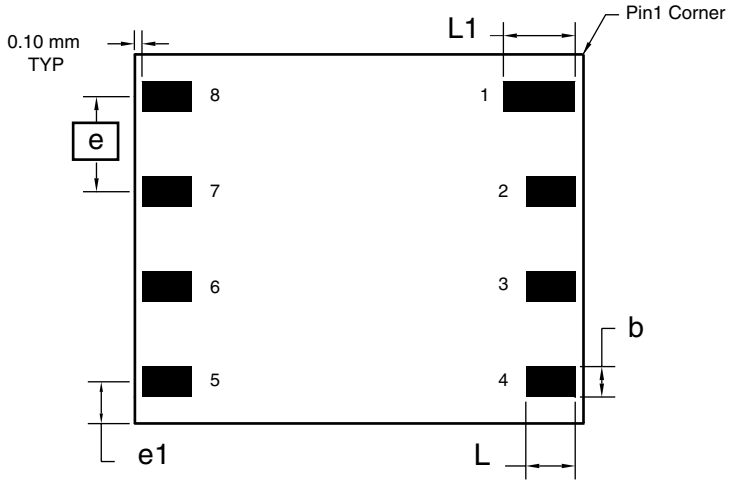
Ordering Code: CI
8-lead LAP



Top View



Side View



Bottom View

COMMON DIMENSIONS
(Unit of Measure = mm)

SYMBOL	MIN	NOM	MAX	NOTE
A	0.94	1.04	1.14	
A1	0.30	0.34	0.38	
b	0.36	0.41	0.46	1
D	7.90	8.00	8.10	
E	4.90	5.00	5.10	
e	1.27 BSC			
e1	0.60 REF			
L	0.62	.0.67	0.72	1
L1	0.92	0.97	1.02	1

Note: 1. Metal Pad Dimensions.

11/13/01

2325 Orchard Parkway San Jose, CA 95131	**TITLE** **8CN1**, 8-lead (8 x 5 x 1.04 mm Body), Lead Pitch 1.27 mm, Leadless Array Package (LAP)	**DRAWING NO.** 8CN1	**REV.** A

Atmel Headquarters

Corporate Headquarters
2325 Orchard Parkway
San Jose, CA 95131
TEL 1(408) 441-0311
FAX 1(408) 487-2600

Europe
Atmel Sarl
Route des Arsenaux 41
Case Postale 80
CH-1705 Fribourg
Switzerland
TEL (41) 26-426-5555
FAX (41) 26-426-5500

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

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

Atmel Operations

Memory
2325 Orchard Parkway
San Jose, CA 95131
TEL 1(408) 441-0311
FAX 1(408) 436-4314

Microcontrollers
2325 Orchard Parkway
San Jose, CA 95131
TEL 1(408) 441-0311
FAX 1(408) 436-4314

La Chantrerie
BP 70602
44306 Nantes Cedex 3, France
TEL (33) 2-40-18-18-18
FAX (33) 2-40-18-19-60

ASIC/ASSP/Smart Cards
Zone Industrielle
13106 Rousset Cedex, France
TEL (33) 4-42-53-60-00
FAX (33) 4-42-53-60-01

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906
TEL 1(719) 576-3300
FAX 1(719) 540-1759

Scottish Enterprise Technology Park
Maxwell Building
East Kilbride G75 0QR, Scotland
TEL (44) 1355-803-000
FAX (44) 1355-242-743

RF/Automotive
Theresienstrasse 2
Postfach 3535
74025 Heilbronn, Germany
TEL (49) 71-31-67-0
FAX (49) 71-31-67-2340

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906
TEL 1(719) 576-3300
FAX 1(719) 540-1759

Biometrics/Imaging/Hi-Rel MPU/
High Speed Converters/RF Datacom
Avenue de Rochepleine
BP 123
38521 Saint-Egreve Cedex, France
TEL (33) 4-76-58-30-00
FAX (33) 4-76-58-34-80

---

e-mail
literature@atmel.com

Web Site
http://www.atmel.com

5016BS–SMEM–04/03