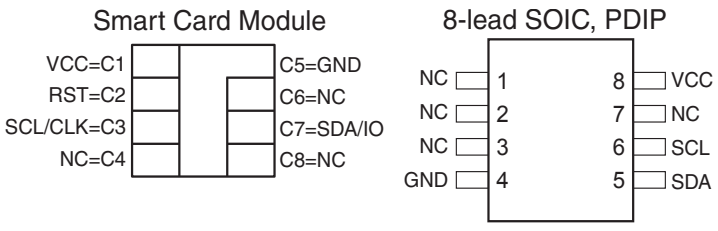
Features

- One of a Family of 9 Devices with User Memories from 1 Kbit to 256-Kbit
- 1-Kbit (128-byte) EEPROM User Memory
  - Four 32 byte (256 bit) Zones
  - Self-timed Write Cycle
  - Single Byte or 16-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 Mutual Authentication Protocol (Under License of 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 (Gemplus® Patent)
  - 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
  - 1.0 MHz Compatibility for Fast Operation
  - Standard 8-lead Plastic Packages
  - Same Pinout as 2-wire Serial EEPROM's
- 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

Figure 1. Package Options



CryptoMemory 1 Kbit

AT88SC0104C

Summary

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 AT88SC0104C member of the CryptoMemory® family is a high-performance secure memory providing 1 Kbit of user memory with advanced security and cryptographic features built in. The user memory is divided into four 32-byte zones, each of which may be individually set with different security access rights or effectively combined together to provide space for 1 to 4 data files.

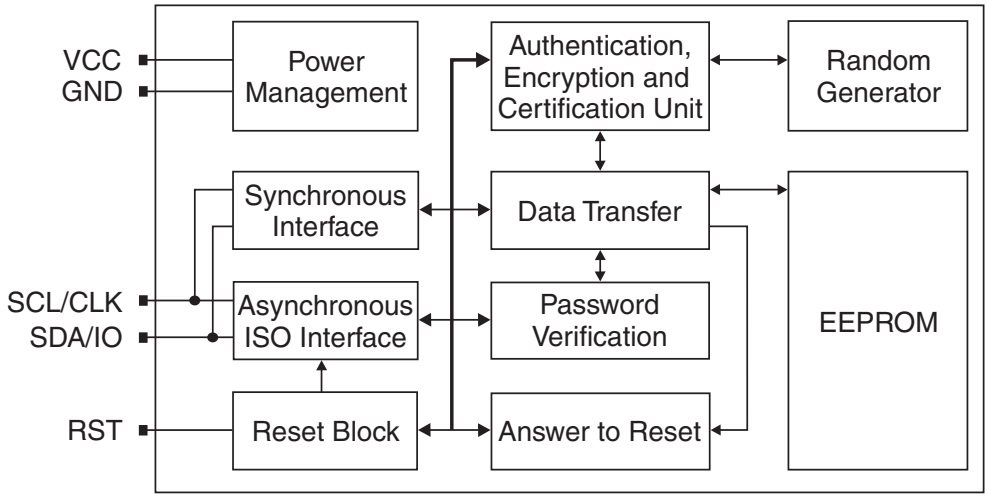
Smart Card Applications

The AT88SC0104C provides high security, low cost, and ease of implementation without the need for a microprocessor operating system. The embedded cryptographic engine provides for dynamic and 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 AT88SC0104C offers the ability to communicate with virtually any smart card reader using the asynchronous T = 0 protocol (Gemplus Patent) defined in ISO 7816-3.

Embedded Applications

Through dynamic and symmetric mutual authentication, data encryption, and the use of encrypted checksums, the AT88SC0104C 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 1.0 MHz is used for fast and efficient communications with up to 15 devices that may be individually addressed. The AT88SC0104C is available in industry standard 8-lead packages with the same familiar pinout as 2-wire serial EEPROMs.

Figure 2. 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.

Reset (RST) The AT88SC0104C 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 AT88SC0104C does not support the synchronous answer-to-reset sequence.

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. SDA/IO information applies to both asynchronous and synchronous protocols.

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.

Table 2. DC Characteristics

Applicable over recommended operating range from V_{CC} = +2.7 to 5.5V, T_{AC} = -40°C to +85°C (unless otherwise noted)

Symbol	Parameter	Test Condition	Min	Typ	Max	Units
V_{CC}	Supply Voltage		2.7		5.5	V
I_{CC}	Supply Current (V_{CC} = 5.5V)	Async READ at 3.57MHz			5	mA
I_{CC}	Supply Current (V_{CC} = 5.5V)	Async WRITE at 3.57MHz			5	mA
I_{CC}	Supply Current (V_{CC} = 5.5V)	Synch READ at 1MHz			5	mA
I_{CC}	Supply Current (V_{CC} = 5.5V)	Synch WRITE at 1MHz			5	mA
I_{SB}	Standby Current (V_{CC} = 5.5V)	V_{IN} = V_{CC} or GND			100	uA
V_{IL}	SDA/IO Input Low Threshold(1)		0		V_{CC} x 0.2	V
V_{IL}	SCL/CLK Input Low Threshold(1)		0		V_{CC} x 0.2	V
V_{IL}	RST Input Low Threshold(1)		0		V_{CC} x 0.2	V
V_{IH}	SDA/IO Input High Threshold(1)		V_{CC} x 0.7		V_{CC}	V
V_{IH}	SCL/CLK Input High Threshold(1)		V_{CC} x 0.7		V_{CC}	V
V_{IH}	RST Input High Threshold(1)		V_{CC} x 0.7		V_{CC}	V
I_{IL}	SDA/IO Input Low Current	0 < V_{IL} < V_{CC} x 0.15			15	uA
I_{IL}	SCL/CLK Input Low Current	0 < V_{IL} < V_{CC} x 0.15			15	uA
I_{IL}	RST Input Low Current	0 < V_{IL} < V_{CC} x 0.15			50	uA
I_{IH}	SDA/IO Input High Current	V_{CC} x 0.7 < V_{IH} < V_{CC}			20	uA
I_{IH}	SCL/CLK Input High Current	V_{CC} x 0.7 < V_{IH} < V_{CC}			100	uA
I_{IH}	RST Input High Current	V_{CC} x 0.7 < V_{IH} < V_{CC}			150	uA
V_{OH}	SDA/IO Output High Voltage	20K ohm external pull-up	V_{CC} x 0.7		V_{CC}	V
V_{OL}	SDA/IO Output Low Voltage	I_{OL} = 1mA	0		V_{CC} x 0.15	V
I_{OH}	SDA/IO Output High Current	V_{OH}			20	uA

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

Table 3. AC Characteristics

Applicable over recommended operating range from V_{CC} = +2.7 to 5.5V,

T_{AC} = -40°C to +85°C, CL = 30pF (unless otherwise noted)

Symbol	Parameter	Min	Max	Units
f_{CLK}	Async Clock Frequency (V_{CC} Range: +4.5 - 5.5V)	1	5	MHz
f_{CLK}	Async Clock Frequency (V_{CC} Range: +2.7 - 3.3V)	1	4	MHz
f_{CLK}	Synch Clock Frequency	0	1	MHz
	Clock Duty cycle	40	60	%
t_R	Rise Time - I/O, RST		1	uS
t_F	Fall Time - I/O, RST		1	uS
t_R	Rise Time - CLK		9% x period	uS
t_F	Fall Time - CLK		9% x period	uS
t_{AA}	Clock Low to Data Out Valid		35	nS
$t_{HD.STA}$	Start Hold Time	200		nS
$t_{SU.STA}$	Start Set-up Time	200		nS
$t_{HD.DAT}$	Data In Hold Time	10		nS
$t_{SU.DAT}$	Data In Set-up Time	100		nS
$t_{SU.STO}$	Stop Set-up Time	200		nS
t_{DH}	Data Out Hold Time	20		nS
t_{WR}	Write Cycle Time (at 25·C)		5	mS
t_{WR}	Write Cycle Time (-40° to +85°C)		7	mS

Device Operation For Synchronous Protocols

CLOCK and DATA TRANSITIONS: The SDA pin is normally pulled high with an external device. Data on the SDA pin may change only during SCL low time periods (see Figure 5 on page 5). Data changes during SCL high periods will indicate a start or stop condition as defined below.

START CONDITION: A high-to-low transition of SDA with SCL high is a start condition which must precede any other command (see Figure 6 on page 6).

STOP CONDITION: A low-to-high transition of SDA with SCL high is a stop condition. After a read sequence, the stop command will place the EEPROM in a standby power mode (see Figure 6 on page 6).

ACKNOWLEDGE: All addresses and data words are serially transmitted to and from the EEPROM in 8-bit words. The EEPROM sends a zero to acknowledge that it has received each word. This happens during the ninth clock cycle.

MEMORY RESET: After an interruption in protocol, power loss or system reset, any 2-wire part can be reset by following these steps:

1. Clock up to 9 cycles.
2. Look for SDA high in each cycle while SCL is high.
3. Create a start condition.

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 memory. 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”.

Initial Device Programming

To enable the security features of CryptoMemory, the device must first be personalized to set up several registers and load in the appropriate passwords and keys. This is accomplished through programming the configuration memory of CryptoMemory using simple write and read commands. To gain access to the configuration memory, the secure code must first be successfully presented. For the AT88SC0104C device, the secure code is $DD 42 97. After writing and verifying data in the configuration memory, the security fuses must be blown to lock this information in the device. For additional information on personalizing CryptoMemory, please see the application notes *Programming CryptoMemory for Embedded Applications* and *Initializing CryptoMemory for Smart Card Applications* (at www.Atmel.com).

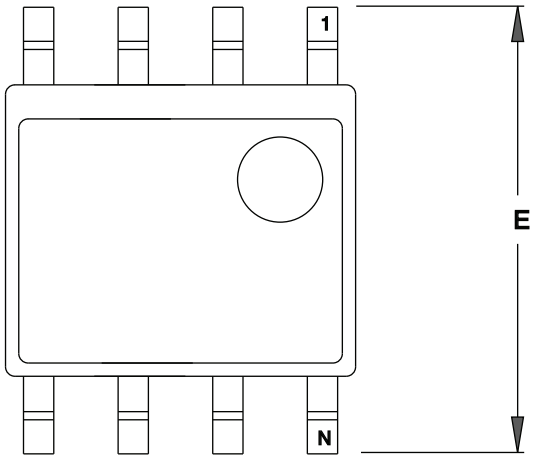
Ordering Information

Ordering Code	Package	Voltage Range	Temperature Range
AT88SC0104C-MJ AT88SC0104C-MP	M2 – J Module M2 – P Module	2.7V–5.5V	Commercial (0°C–70°C)
AT88SC0104C-PU AT88SC0104C-SU	8P3 8S1	2.7V–5.5V	Lead-free/Halogen-free/Industrial (–40°C–85°C)
AT88SC0104C-WI	7 mil wafer	2.7V–5.5V	Industrial (–40°C–85°C)

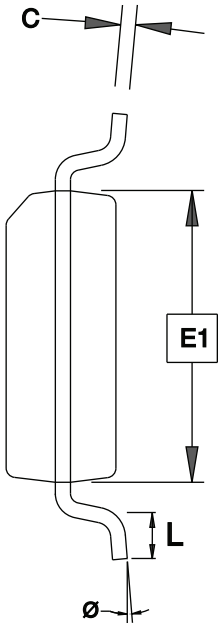
Package Type[1]	Description
M2 – J Module	M2 ISO 7816 Smart Card Module
M2 – P Module	M2 ISO 7816 Smart Card Module with Atmel® Logo
8P3	8-lead, 0.300” Wide, Plastic Dual Inline Package (PDIP)
8S1	8-lead, 0.150” Wide, Plastic Gull Wing Small Outline Package (JEDEC SOIC)

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

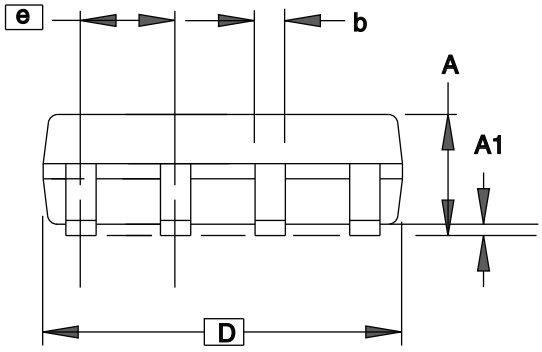
Ordering Code: SU
8-lead SOIC



TOP VIEW



END VIEW



SIDE VIEW

COMMON DIMENSIONS
(Unit of Measure = mm)

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

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

1150 E. Cheyenne Mtn. Blvd. Colorado Springs, CO 80906	**TITLE** **8S1**, 8-lead (0.150" Wide Body), Plastic Gull Wing Small Outline (JEDEC SOIC)	**DRAWING NO.** 8S1	**REV.** C