Features

- **Secure Computation of Public Key Signatures**
- **Secure Storage and Decryption of Symmetric Keys**
- **On-chip Cache for Frequently Used Keys**
- **SMBus Communications Port**
- **On-board Public Key Computation Engine and Microprocessor**
- **Physical and Logical Security Measures to Inhibit Attacks**
- **20-lead SOIC Package, 0°C to +70°C Operating Range**
- **3.3V ±10% Supply Voltage**

Secure Signature Generation Chip

AT90SP0801

Summary

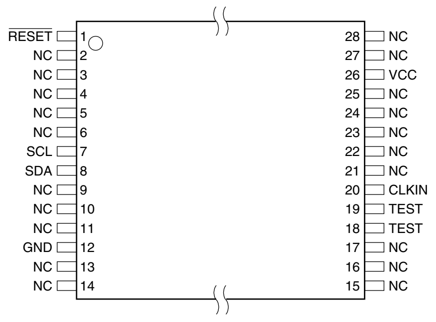
Description

The AT90SP0801 is used to perform cryptographic operations, using asymmetric private keys stored in its internal EEPROM. An arbitrary number of private keys can be stored externally and decrypted by the chip when required. Communication to the system processor is via the SMBus.

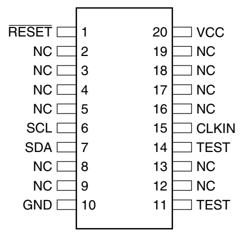
Figure 1. Pin Configuration

Name	Description
$\overline{\text{RESET}}$	Reset Input, Active-low
SCL	SMBus Clock
SDA	SMBus Data
GND	Ground
CLKIN	Input Clock
VCC	Operating Voltage
TEST	Do Not Connect

28-lead TSSOP



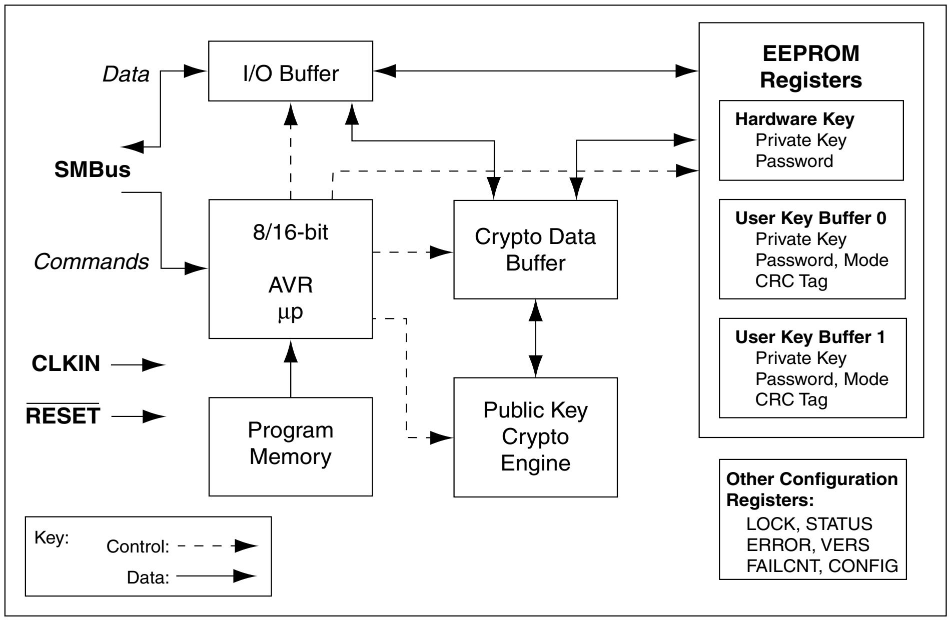
28-lead SOIC



Rev. 1495AS–01/02

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

Figure 2. Block Diagram



Serial Interface

Data is transferred to or from the I/O buffer on the chip using the SMBus interface, in a manner similar but not identical to that of standard two-wire serial EEPROMs.

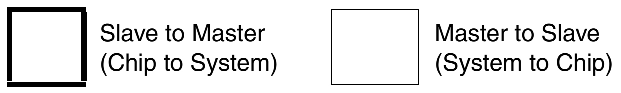
All bits are sent to or read from the chip most significant bit first, in a manner consistent with standard serial EEPROMs. Bit fields listed in this document are correspondingly listed with the MSB on the left and the LSB on the right. Hex numbers are specified with the “0x” prefix.

Multi-byte information sent to the chip is sent most significant byte first, following typical conventions. Within the chip, the first byte sent to the chip is stored in memory at the lowest address, and the address is incremented for subsequent bytes. When a message digest (hash) is sent to the chip, the first byte of the hash value is the first byte to be sent to the chip.

In both the text and graphics, the chip is the slave and the system is the master. The following abbreviations apply:

A	Acknowledge (bus pulled low, master or slave)
N	Not Acknowledge (bus left high, master or slave)
S	Start (High-to-low on SDA with SCL high, master)
P	Stop (Low-to-high on SDA with SCL high, master)

For the graphical representations, the direction of the data flow is indicated as below:



SMBus Standard Usage

Data transfer to and from the chip follows the SMBus V1.1 standard, using only some of the command protocols.

The “write” command of this chip uses the “Block Write” protocol of the SMBus spec. Note that in this chip the count value can exceed 32. This chip does not support the “Write Byte” and “Write Word” protocols of the SMBus spec.

The “Read” command of this chip uses the “Block Read” protocol of the SMBus spec. Note that in this chip the “Read” command can be optionally executed without the preceding partial block write command. This chip does not support the “Receive Byte”, “Read Byte” and “Read Word” protocols of the SMBus spec.

All other commands of this chip use the “Send Byte” protocol of the SMBus spec. Note that the “Quick Command” and “Process Call” protocols of the SMBus spec are not supported by this chip.

Two-wire Serial EEPROM Comparison

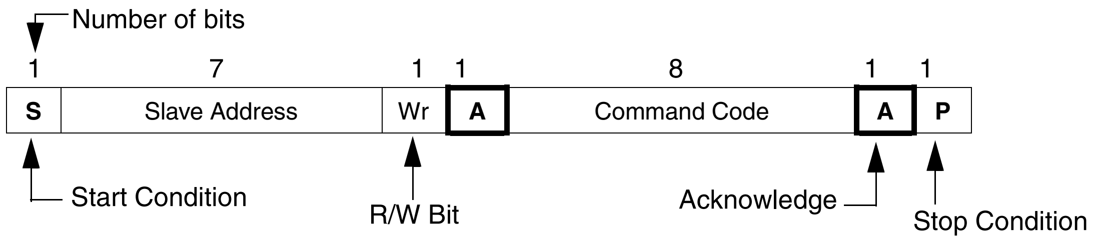
Some of the differences between this chip and a standard two-wire serial EEPROM are:

1. The slave address of this chip is different from the A0-AF (hex) standard for EEPROMs.
2. The maximum clock rate is 100 kHz and Tdh is 300 ns. These specs are part of SMbus.
3. The supply voltage is 3.0V to 3.7V.
4. The read address is not specified in the aborted read command.
5. Multi-byte reads and writes are preceded by the number of bytes that will be transferred.

6. Multi-byte writes longer than the maximum size of the register (i.e., containing more bytes) cause an error.

Commands Without Data Transfer

There are a number of commands (described within the following Commands sections) that perform various internal operations on the chip, using data already stored in either the I/O buffer or the internal memories of the chip. All such commands are composed of two bytes sent to the chip according to the following flow:



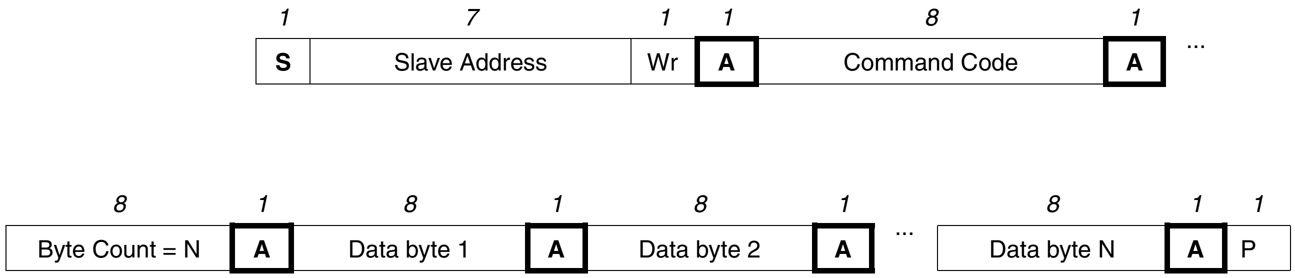
Write Commands

The write commands permit data to be transferred to the I/O buffer located within the SRAM on the chip. Only block writes are supported, so transfers of 1 or 2 bytes require the same basic sequence as 32 bytes.

The commands are encoded as follows:

Slave Address	Command Code	Description
0 1 0 1 0 0 0 0	$s_1 s_0$ 0 0 0 0 0 0	Write buffer, (+data)
0 1 0 1 0 0 1 0	0 1 1 1 1 1 1 1	Write command, ignored
0 1 0 1 0 0 0 0	0 1 1 1 1 1 1 1	Write command, ignored

The following figure shows the structure for block write operations:



The write buffer command is followed by up to 255 bytes of data. All bytes are sourced by the host and are formatted as follows:

01010000	$s_1s_0$000000	count	data0	data1	…	dataN	crc0	crc1

Count denotes the total number of bytes that follows the command, including any CRC bytes. A 0 value is illegal. 255 is the max. number of bytes that may be written per command.

Data is sent least significant byte first. In some circumstances, there may be no *data*, only *crc*.

Depending on the value of ss, the *crc* bytes may or may not be included.

The two sequence bits s_{1-0} within the command code tell the chip how to relate this transfer to previous and subsequent transfers.

S_0 if set to a 1 indicates that this is the first transfer to the buffer and that *data0* should go into buffer address 0 and so on. If this bit is set to a 0, then *data0* will be stored in the next location within the buffer after that from the previous transfer. When set, this bit also resets the CRC generator.

S_1 if set to a 1 indicates that this is the last transfer to the buffer. If set to a 0, the chip must have previously executed a command where s_0 was set to a 1. When s_1 is set to a 1, the last two bytes of the information transferred in this block are a CRC value. The chip will NACK the *crc1* byte, if the value sent does not match that computed on the incoming data. The CRC bytes may not be split across two blocks.

For instance, to write password information (64 bytes) to the chip, the following sequence of three write commands would be used (assuming 32 byte loads). The ACKs, NACKs and STOP conditions have been ignored for clarity.

S	01010000	01000000	00100000	data0	data1	data2	...	data31
S	01010000	00000000	00100000	data32	data33	data34	...	data63
S	01010000	10000000	00000010	crc0	crc1			

For shorter data transfer values, it is perfectly legal for both s_0 and s_1 to be set. This indicates that the entire transfer is taking place in a single block access. As an example of this, the following command would write a single byte to the buffer:

S	01010000	11000000	00000011	data0	crc0	crc1

The chip will NACK writes that attempt to write into the chip beyond the internal buffer, which may be as short as 320 bytes.

Read Commands

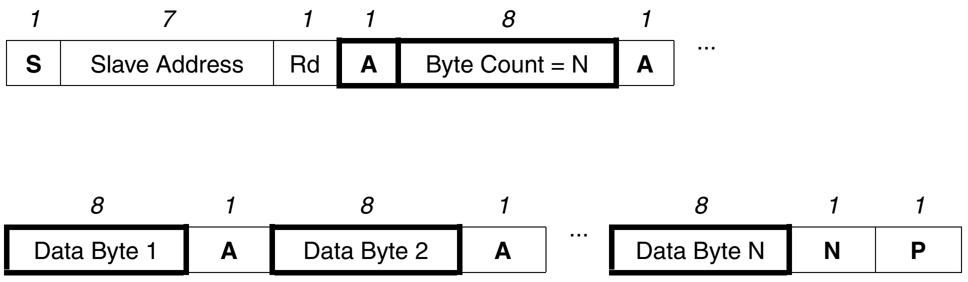
Block read commands are slightly different than writes and are encoded as follows:

Slave Address	Command Code	Description
0 1 0 1 0 0 1 1	- - - - - - - -	Read buffer, first block
0 1 0 1 0 0 0 1	- - - - - - - -	Read, subsequent blk

The read command is only one byte long, and the chip (not the host) sends back the count information. The count value will always be the smaller of MAXBLK_R or the (remaining) number of bytes in the register that have not been read yet.

When there are a large number of bytes in the buffer, multiple read commands must be executed to read all the bytes out of the chip. Using the slave address of 0x53 will cause the chip to start reading at the beginning of the buffer. Using the slave address of 0x51 will cause the chip to continue reading information that is subsequent to the information last read by the chip from the buffer. After a load or crypto operation, the first command may also be a 0x51, which will have the same effect as 0x53.

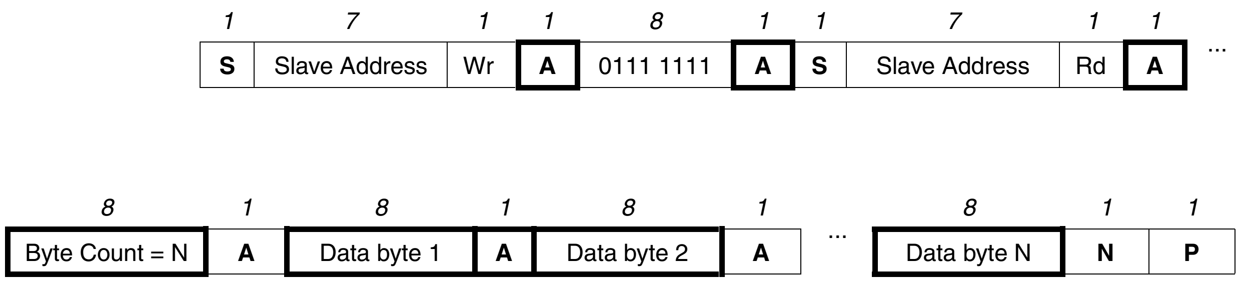
Block Reads are formatted as follows:


1 7 1 1 8 1
S | Slave Address | Rd | A | Byte Count = N | A ...
8 1 8 1 ... 8 1 1
Data Byte 1 | A | Data Byte 2 | A ... Data Byte N | N | P

After the last byte has been read from the register, the read pointer is reset back to the beginning of the register, and the system may continue to read from the beginning of the buffer again, if desired. There is no indication from the chip as to when the read pointer has been reset (other than as may be inferred from the values in the count field).

To be compatible with the SMBus specification, the read command may optionally be preceded by the first two bytes of either of the “ignored write” commands, which are then aborted with a new start bit for the read. The two bytes of the write command are completely ignored by the chip in this case, and a different encoding for the second byte (01111111, or 0x7F) must be used. Execution of a block read sequence using a legal write command code for the second byte (00, 0x40, 0x80 or 0xC) is undefined.

The protocol for this is shown below:


1 7 1 1 8 1 1 7 1 1
S | Slave Address | Wr | A | 0111 1111 | A | S | Slave Address | Rd | A ...
8 1 8 1 8 1 ... 8 1 1
Byte Count = N | A | Data byte 1 | A | Data byte 2 | A ... Data byte N | N | P

As an example of the read block command, the following would take place to read four bytes of data from the buffer (assuming that the load VERS_R command had previously been executed).

S	01010011	00000100	data0	data1	data2	data3

or

S	01010010	01111111	**S**	01010011	00000100	data0	data1	data2	data3

As an example of multiple read block command, the following would take place to read the 1040 bits (130 bytes) of signature data from the buffer (assuming that the “sign” command had previously been executed). As earlier, the two-byte aborted write is an option on each command. Note that the first byte read (data0) is the most significant byte of the signature, while data128 is the most significant byte of the CRC.

S	01010010	01111111	**S**	01010011	00100000	data0	data1	...	data31
S	01010000	01111111	**S**	01010001	00100000	data32	data33	...	data63
S	01010000	01111111	**S**	01010001	00100000	data64	data65	...	data95
S	01010000	01111111	**S**	01010001	00100000	data96	data97	...	data127
S	01010000	01111111	**S**	01010001	00000010	data128	data129	...	

Absolute Maximum Ratings

Operating Temperature	0°C to +70°C
Storage Temperature (without bias)	0°C to +70°C
Votage on I/O Pins	-0.1 to V_{CC} +0.3V
Voltage on VCC with Respect to Ground	6.0V
Maximum ESD Voltage	2000V

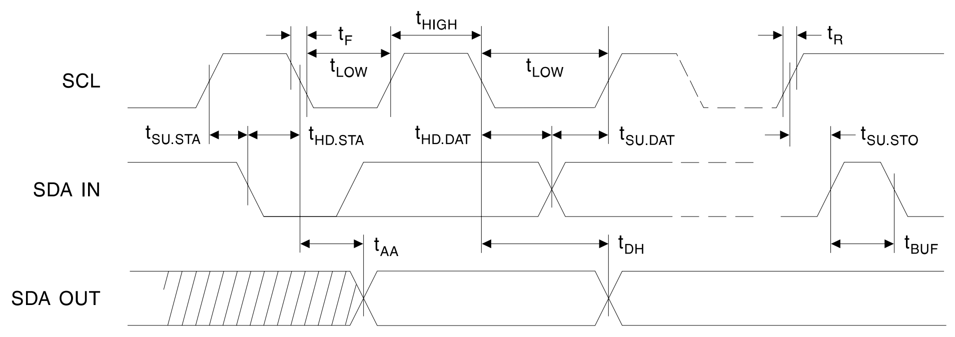
*NOTICE: Stresses beyond those listed under "Absolute Maximum Ratings" may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of this specification may cause temporary or permanent failure. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

Serial Interface AC Specifications

C_L = 1 TTL Gate and 100 pF, except as noted. V_{CC} = 3.0V to 3.7V.

Name	Min	Max	Units	Notes
t_{SCL}		100	kHz	Clock (SCL) Frequency
t_{LOW}	4.7		µs	Clock (SCL) Pulse Low-width
t_{HIGH}	4.0		µs	Clock (SCL) Pulse High-width
t_I		100	ns	Noise Suppression, Not Tested
t_{AA}	0.1	4.5	µs	Clock low to Data out valid
t_{BUF}	4.7		µs	Bus free before Transmission, Not Tested
$t_{HD.STA}$	4.0		µs	Start Hold Time
$t_{SU.STA}$	4.7		µs	Start Set-up Time
$t_{HD.DAT}$	0		µs	Data In Hold Time
$t_{SU.DAT}$	200		ns	Data In Set-up Time
t_R		1.0	µs	Inputs Rise Time, Not Tested
t_F		300	ns	Inputs Fall time, Not Tested
$t_{SU.STO}$	4.7		µs	Stop Set-up Time
t_{DH}	300		ns	Data Out Hold Time
t_{WR}		10	ms	Write Cycle Time, EEPROM Write
t_{CLKIN}	69	100	ns	CLKIN Period
t_{CLKO}, t_{CKH1}	34	50	ns	CLKIN Low or CLKIN High

Figure 3. Timing Diagram for Serial Interface AC Specification



Serial Interface DC Specifications

Operating Temperature Range = 0° to 70°C.

Name	Min	Typ	Max	Units	Notes
V_{CC}	3.0		3.7	V	Operating Voltage, V_{CC} Pin
I_{CC}(1)		18	25	mA	At V_{CC} = 3.7V, f_{SDA} = 100 kHz
I_{SB}(1)		50	100	µA	At V_{CC} = 3.3V, CLKIN = V_{SS}
I_{LIO}		0.1	3.0	µA	SDA, SCL. V_{IN} = V_{CC} or V_{SS}
V_{IL}	–0.1		V_{CC} x 0.3	V	
V_{IH}	V_{CC} x 0.7		V_{CC}	V	
V_{OL}			0.4	V	I_{OL} = 2.1 mA
C_{IO}				pF	SCL, SDA, Not Tested
f_{CLKIN}	1	14.318	15	MHz	Duty cycle >48% and <52%

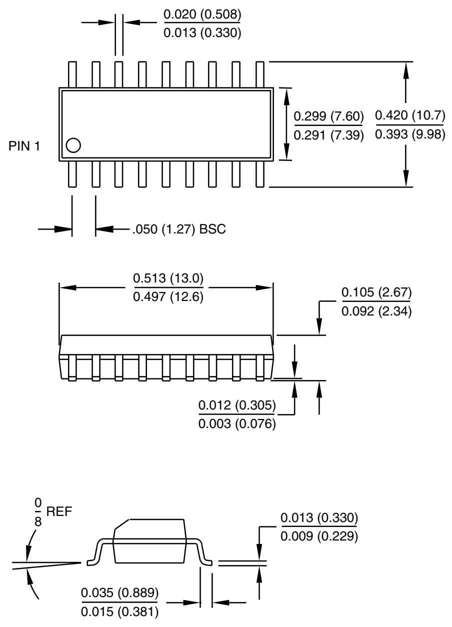
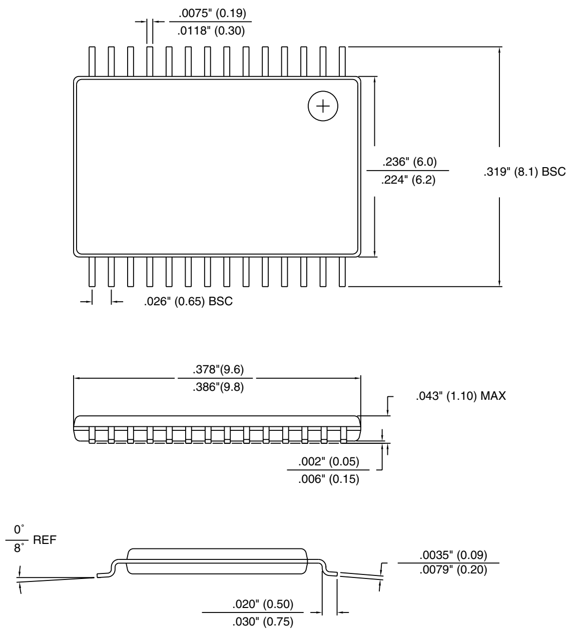
Notes: 1. The specifications noted as “not tested” denote parameters that are characterized and not 100% tested.
2. Preliminary data, subject to change.

Ordering Information

Ordering Code	Package	Operation Range
AT90SP0801-01SC	20S, 20-lead SOIC	Commercial (0°C to 70°C)

Package Type	
20S	20-lead, 0.300 Wide, Plastic Gull Wing Small Outline (SOIC)

Packaging Information

20S, 20 Lead, 0.300" Wide, Plastic Gull Wing Small Outline (SOIC) Dimensions in Inches and (Millimeters)	**28A**, 28-lead, 6.1mm Wide, Thin Shrink Small Outline Package (TSSOP) Dimensions in Inches and (Millimeters)
 0.020 (0.508) 0.013 (0.330) 0.299 (7.60) 0.291 (7.39) 0.420 (10.7) 0.393 (9.98) PIN 1 .050 (1.27) BSC 0.513 (13.0) 0.497 (12.6) 0.105 (2.67) 0.092 (2.34) 0.012 (0.305) 0.003 (0.076) 0 8 REF 0.013 (0.330) 0.009 (0.229) 0.035 (0.889) 0.015 (0.381)	 .0075" (0.19) .0118" (0.30) .236" (6.0) .224" (6.2) .319" (8.1) BSC .026" (0.65) BSC .378"(9.6) .386"(9.8) .043" (1.10) MAX .002" (0.05) .006" (0.15) 0˚ 8˚ REF .0035" (0.09) .0079" (0.20) .020" (0.50) .030" (0.75)

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
Casa Postale 80
CH-1705 Fribourg
Switzerland
TEL (41) 26-426-5555
FAX (41) 26-426-5500

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

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

Atmel Operations

Memory
Atmel Corporate
2325 Orchard Parkway
San Jose, CA 95131
TEL 1(408) 436-4270
FAX 1(408) 436-4314

Microcontrollers
Atmel Corporate
2325 Orchard Parkway
San Jose, CA 95131
TEL 1(408) 436-4270
FAX 1(408) 436-4314

Atmel Nantes
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
Atmel Rousset
Zone Industrielle
13106 Rousset Cedex, France
TEL (33) 4-42-53-60-00
FAX (33) 4-42-53-60-01

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

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

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

Atmel Colorado Springs
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
Atmel Grenoble
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