Features

Companion Chip to CryptoRF and CryptoMemory

- Securely implements host algorithms
- Securely stores host secrets
- Verifies Host Firmware Digests

High Security Features in Hardware

- CryptoMemory and CryptoRF F2 Algorithm
- SHA-1 Standard Cryptographic Algorithm
- 64-bit Mutual Authentication Protocol (Under License of ELVA)
- Permanently Coded Serial Numbers
- High Quality Random Number Generator (RNG)
- Metal Shield Over Memory
- Data Scrambling in Nonvolatile Memory
- Delay Penalties to prevent Systematic Attacks
- Reset Locking to prevent Illegal Power Cycling
- Voltage and Frequency Monitors

Host-side Crypto Functions

- Authentication Challenge Generation
- Device Challenge Response
- Message Authentication Codes (MAC) Generation
- Data Encryption and Decryption
- Secure Authentication Key Management

Secure Storage and Key Management

- Up to 16 sets of 64-bits Diversified Host Keys
- Eight Sets of Two 24-bit Passwords
- Secure and Custom Personalization
- Up to 232-Byte Read/Write Configurable User Data Area

Nonvolatile Up Counters

- Four sets Unidirectional Counters
- 64 Million Maximum Counts Per Counter

Application Features

- Low Voltage Operation: 2.7V – 3.3V
- 2-Wire Serial Interface
- 1.0 MHz Compatibility for Fast Operation
- Standard 8-lead Plastic Packages

High Reliability

- Endurance : 100,000 Cycles
- Data Retention : 10 years
- ESD Protection : 3,000 min

CryptoCompanion Chip

AT88SC016

Summary

5277AS– CryptoCompanion –02/08

1. Product Overview

The CryptoCompanion™ Chip is designed to complement Atmel's CryptoRF® and CryptoMemory® chips, collectively referred to in the remainder of this document as CRF.

CryptoCompanion makes extensive use of the SHA-1 hash algorithm as specified in http://www.itl.nist.gov/fipspubs/fip180-1.htm and elsewhere. In this document, the nomenclature SHA-1(a, b, c) means to concatenate a, b & c in that order and then pad them to a block size of 64 bytes before computing the digest. CryptoCompanion generates SHA-1 digests of single round datasets at a time.

1.1. General Operation

The CRF chip contains secrets that must be known or derived by an outside entity in order to establish a trusted link between the two and permit communications to happen. CryptoCompanion stores these secrets in an obscured way in nonvolatile memory and contains all the circuitry necessary to compute the authentication, password and encryption/decryption actions specified in the CRF datasheet. In this manner, the secrets do not ever need to be revealed.

The general cryptographic strategy is as follows:

- Each CRF chip has a serial or identification number (ID) and authentication secret Gi stored in EEPROM. ID is freely readable while Gi can never be read and is unique for all tags.
- CryptoCompanion contains an EEPROM that holds a set of common secrets (Fn). CryptoCompanion combines Fn with ID and KID to compute a value of G that is expected to match that in the CRF chip. Specifically, G = SHA-1(Fn, ID, KID)
- G is further diversified by the inclusion of a number (KID) generated by the system in a manner of its choosing. Typically, it will be the result of a cryptographic operation on the CRF ID value calculated using other data, secrets and/or algorithms external to CryptoCompanion. This permits scenarios that offer varying degrees of additional security.
- CryptoCompanion includes a general purpose cryptographic quality random number generator which is used to seed a mutual authentication process between CryptoCompanion and CRF. If the CRF confirms the CryptoCompanion challenge, and the CryptoCompanion confirms the CRF response, then the host system proceeds with CRF operations. In this way the host system may use the CRF without knowing the CRF's secrets directly.

1.2. CryptoCompanion Benefits

The following is a partial list of the benefits of using this chip versus storing the algorithms and secrets in standard FLASH system memory.

- Keep confidential those core secrets that are used to authenticate with and communicate to/from CRF. (Store them in EEPROM, use them on-chip)
- Flexible system implementation – multiple secrets and policies for different CRF locations within the system. Multiple manufacturer setup options.
- Hardware encryption engines, avoids algorithm disclosure from reverse-compilation of system operating code.
- Full hardware security implementation makes it harder for an attacker (even with lab equipment) to get secrets stored on CryptoCompanion.
- Global secrets are protected using strong security, standard algorithm (SHA-1).
- Robust random number generation avoids accidental replay for all cryptographic operations using the system, not just with respect to CRF.
- Secure EEPROM storage for configuration information, etc. May permit reduction in the total BOM for the system.
- Easy to use – little programming required, no knowledge of security algorithms or protocols, fast time to market.

1.3. Package, Pin Definition & IO

1.3.1. Pin Definition

1.3.1.1. Vcc, Gnd

Power supply is 2.7 – 3.6V. Supply current less than 50mA.

CryptoCompanion will be available to accept commands 60ms after the later of Vcc rising above 2.7V or Reset being driven high if CryptoCompanion is in a security delay then this interval is significantly longer.

During Power Up, Vcc must exhibit a monotonic ramp at a minimum rate of 50 mV/mS until Vcc has crossed the 2.7V level. During Power Down, Vcc must exhibit a monotonic ramp at a minimum rate of 50 mV/mS once it has dropped below the 2.5V boundary.

Vcc must be bypassed with high quality surface mount capacitors that are properly located on the board. Atmel recommends two capacitors connected in parallel having a value of 1µF and 0.01µF. The capacitors should be manufactured using X5R or X7R dielectric material. These capacitors should be connected to CryptoCompanion using a total of no more than 1cm PC board traces. Atmel recommends the use of a ground plane and a trace length of less than 0.5cm between the capacitors and the Vcc pin. Failure to follow these recommendations may result in improper operation.

1.3.1.2. SDA

Two wire interface data pin, 5V tolerant. Minimum data setup time = 0.1µs, and minimum data hold time = 0µs min. The system board must include an external pull-up resistor.

1.3.1.3. SCL

Two wire interface clock pin, 5V tolerant. Maximum SCL rate is 400KHz, minimum T_{LOW} = 1.2□s, minimum T_{HIGH} = 0.6µs. The system board must include an external pull-up resistor.

1.3.1.4. Reset (RST)

This active low input will reset all states within CryptoCompanion. Honored regardless of the state of PowerDown.

1.3.1.5. PowerDown (PDN)

When held low, the part operates normally. When held high the part will go to sleep and ignore all transitions on SDA and SCL, power consumption will drop to less than 10uA. There is a 50ms delay between this pin falling and the first transition on SDA or SCL that will be accepted by the chip.

1.3.2. Package

CryptoCompanion is packaged in an 8 lead SOIC package with the following pin definition:

Table 1. 8 lead SOIC package pin definition

Pin Number	Pin Name
1	Vcc
5	Gnd
7	SDA
8	SCL
4	RST
3	PDN
2,6	NC

Pins 2 & 6 are NC and should be connected to ground on the PC board.

1.3.3. Environmental

CryptoCompanion is guaranteed to operate over the commercial temperature range of 0° to 70° C. ESD is rated at 3KV, Human Body Model.

1.3.4. TWI Input/Output Operation

CryptoCompanion communicates to the system using a two wire interface (TWI), which is similar to SMBus. The chip operates as a slave and does not support clock stretching. This two wire protocol is identical to that supported by the Atmel AT24C16A serial EEPROM chips. Please see that datasheet on the Atmel web site for detailed timing and protocol information.

The system processor is expected to properly format commands for CryptoCompanion (which may include information from the CRF chip), and then process the outputs of CryptoCompanion (which may include sending some of the outputs to the CRF chip).

CryptoCompanion cannot directly communicate with CRF chips. Both CRF and CryptoCompanion are slave devices. The bus master may use one or two busses to communicate with them. Separate TWI addresses must be used if both chips are on the same bus.

All communications packets sent to or from CryptoCompanion use the following naming conventions. The column labeled "*TWI name*" provides the name of the byte as described in the AT24C16A datasheet.

2. AC & DC Characteristics (Preliminary)

Table 2. DC Characteristics

Applicable over recommended operating range from V_{CC} = +2.7 to 3.3V,

T_{AC} = 0°C to 70°C (unless otherwise noted)

Symbol	Parameter	Test Condition	Min	Typ	Max	Units
V_{CC}	Supply Voltage		2.7		3.3	V
Icc	Supply Current	1MHz			5	mA
I_{SB}	Standby Current	V_{IN} = VCC or GND			100	uA
V_{IL}	SDA Input Low Voltage		0		V_{CC} x 0.2	V
V_{IL}	CLK Input Low Voltage		0		V_{CC} x 0.2	V
V_{IL}	RST Input Low Voltage		0		V_{CC} x 0.2	V
V_{IH}	SDA Input High Voltage		V_{CC} x 0.7		V_{CC}	V
V_{IH}	SCL Input High Voltage		V_{CC} x 0.7		V_{CC}	V
V_{IH}	RST Input High Voltage		V_{CC} x 0.7		V_{CC}	V
I_{IL}	SDA Input Low Current	0 < V_{IL} < V_{CC} x 0.15			15	uA
I_{IL}	SCL 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 Input High Current	V_{CC} x 0.7 < V_{IH} < V_{CC}			*20*	uA
I_{IH}	SCL 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 Output High Voltage	20K ohm external pull-up	V_{CC} x 0.7		V_{CC}	V
V_{OL}	SDA Output Low Voltage	I_{OL} = 1mA	0		V_{CC} x 0.15	V
I_{OH}	SDA Output High Current	VOH			20	uA

Table 3. AC Characteristics

Applicable over recommended operating range from V_{CC} = +2.7 to 3.3V,

T_{AC} = -0°C to 70°C, CL = 30pF (unless otherwise noted)

Symbol	Parameter	Min	Max	Units
f_{CLK}	Clock Frequency	0	1	MHz
	Clock Duty cycle	40	60	%
t_R	Rise Time - SDA, RST		1	uS
t_F	Fall Time - SDA, RST		1	uS
t_R	Rise Time - SCL		9% x period	uS
t_F	Fall Time - SCL		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		5	mS

3. Transport Key

Certain operational modes of CryptoCompanion chip require knowledge of a key for proper custom configuration. When applicable, Atmel shall program customer provided key values at the factory for production orders. For generic and sample orders, this key, available as a transport key, shall be

```
0x17 0x44 0x1A 0x48 0xDA 0xDB 0x23 0xFB 0x70 0xCC 0xB8 0x43 0x09 0x20 0x59 0xEB
```

4. Ordering Codes

Table 4.

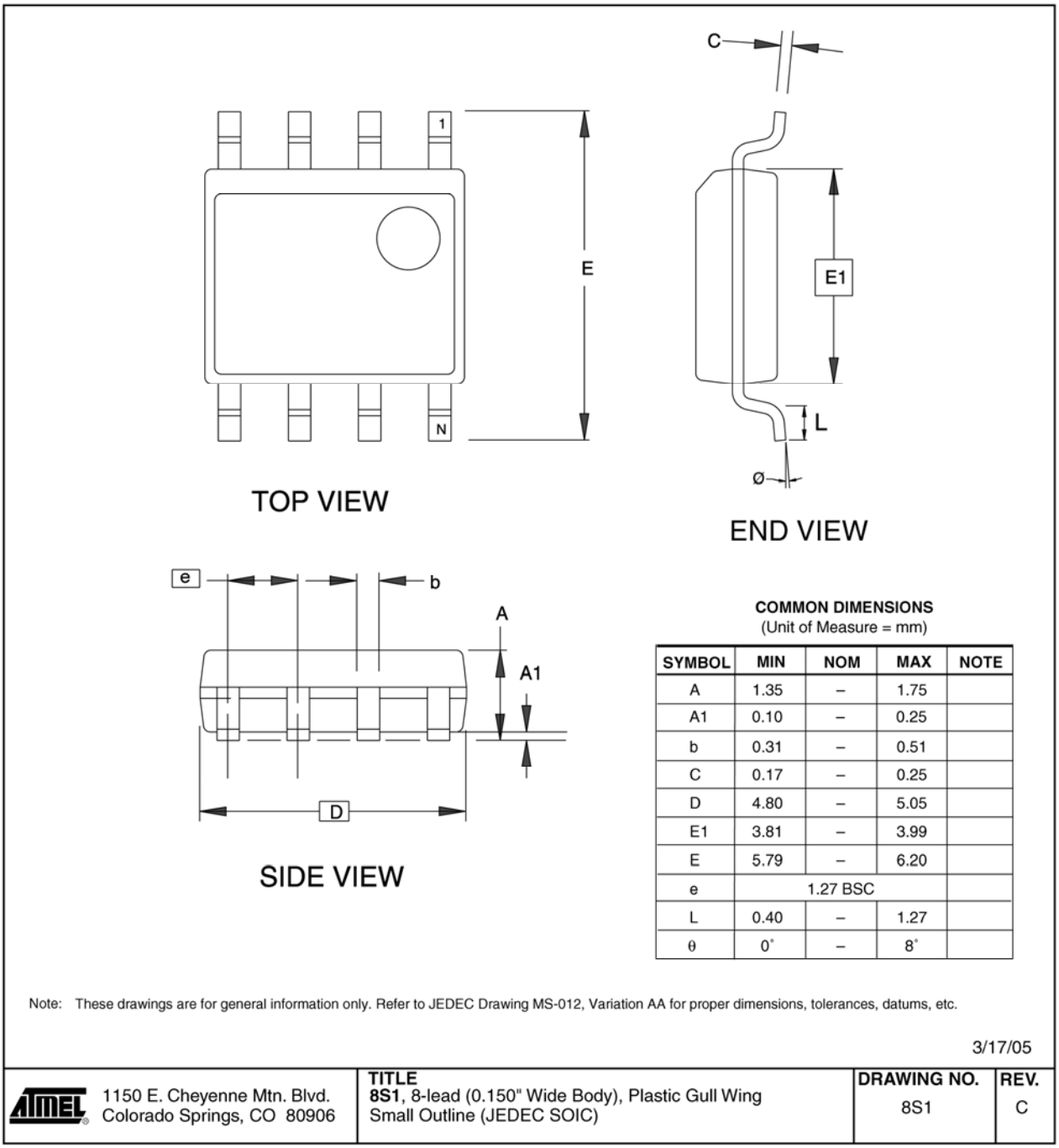
Ordering Code	Package	Voltage Range	Temperature Range
AT88SC016-SX	8S1	2.7V – 3.6V	Lead Free/Halogen Free, Commercial (0°C – 70°C)

Table 5.

Package Type	Description
8S1	8-lead, 0.150” Wide, Plastic Gull Wing Small Outline Package (JEDEC SOIC)

5. Package Drawing

Figure 1. 8S1 – SOIC



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.

3/17/05

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

6. Revision History

Doc. Rev.	Date	Comments
A	2-20-08	Initial document released

Headquarters

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

International

Atmel Asia
Room 1219
Chinachem Golden Plaza
77 Mody Road Tsimshatsui
East Kowloon
Hong Kong
Tel: (852) 2721-9778
Fax: (852) 2722-1369

Atmel Europe
Le Krebs
8, Rue Jean-Pierre Timbaud
BP 309
78054 Saint-Quentin-en-
Yvelines Cedex
France
Tel: (33) 1-30-60-70-00
Fax: (33) 1-30-60-71-11

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

Product Contact

Web Site
www.atmel.com

Technical Support
CryptoMemory@atmel.com
CryptoRF@atmel.com

Sales Contact
www.atmel.com/contacts

Literature Requests
www.atmel.com/literature