Atmel AT88SC118

CryptoCompanion Device for CryptoRF and CryptoMemory Products

SUMMARY DATASHEET

Features

- Atmel® CryptoCompanion™ Device to Atmel CryptoRF® and Atmel 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
  - 6.4 million maximum counts per counter
- Application features
  - Low voltage supply: 2.7V – 3.6V
  - 2-Wire Serial Interface (TWI, 5V compatible)
  - Standard 8-lead SOIC plastic package, green compliant (exceeds RoHS)
- High reliability
  - Endurance: 100,000 cycles
  - Data retention: 10 years
  - ESD protection: 3,000V min. HBM

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

1. Product Overview

The CryptoCcompanion is designed as the mate to the CryptoRF (CRF) and CryptoMemory (CM) devices, collectively referred to in the remainder of this document as CRF.

The 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, and c in that order and then pad them to a block size of 64 bytes before computing the digest. The CryptoCompanion does not ever generate a SHA-1 digest of datasets larger than a single round.

1.1 General Operation

The CRF device contains secrets that must be known or derived by a Host system in order to establish a trusted link between the two and permit communications to happen. The CryptoCompanion stores these secrets in an obscured way in nonvolatile memory and contains all the circuitry necessary to perform the authentication, password, and encryption/decryption functions 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 device has a serial or identification number (ID) and authentication secret G_i stored in EEPROM. ID is freely readable; G_i can never be read and is unique for all tags.
- The CryptoCompanion contains an EEPROM that contains a set of common secrets (F_n). The AT88SC118 combines F_n with ID and K_{ID} to compute a value of G that is expected to match that in the CRF device. Specifically, G = SHA-1(F_n, ID, K_{ID}).
- G is further diversified by the inclusion of a number (K_{ID}) generated by the Host 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 the AT88SC118. This permits scenarios that offer varying degrees of additional security.
- The CryptoCompanion includes a general purpose cryptographic quality Random Number Generator which is used to seed a mutual authentication process between the AT88SC118 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 device 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 and 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 the CryptoCompanion.
- Global secrets are protected using strong security, standard algorithm (SHA-1).
- Implements a crunching algorithm to prevent micro-controller based CRF replicas.
- 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, and fast time to market.

1.3 Package, Pinout, and I/O

1.3.1 Pinout

All pins not otherwise specified are considered Test pins and should be grounded on the board.

Table 1-1. Pin Descriptions

Pin	Description
V_{CC} and GND	**Power Supply and Ground.** Power supply is 2.7 – 3.6V and the supply current is less than 5mA. The CryptoCompanion will be available to accept commands 60ms after the later of V_{CC} 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, V_{CC} must exhibit a monotonic ramp at a minimum rate of 50mV/ms until V_{CC} has crossed the 2.7V level. During power-down, V_{CC} must exhibit a monotonic ramp at a minimum rate of 50mV/ms once it has dropped below the 2.5V boundary. CryptoCompanion does not support hot swapping or hot plugging. V_{CC} 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 1mF and 0.01mF. The capacitors should be manufactured using X5R or X7R dielectric material. These capacitors should be connected to the AT88SC118 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 V_{CC} pin. **Caution:** Failure to follow these recommendations may result in improper operation.
SDA	2-Wire Interface Data pin and 5V compatible. Data setup time = 0.1µs minimum and data hold time = 0 µs minimum.The system board must include an external pull-up resistor.
SCL	2-Wire Interface Clock pin and 5V compatible. Maximum SCL rate is 400KHz, min. T_{LOW} = 1.2µs, min. T_{HIGH} = 0.6µs. The system board must include an external pull-up resistor.
RST	**Reset**. This active low input will reset all states within the AT88SC118. It is honored regardless of the state of PowerDown.
PDN	**PowerDown.** 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 10µA. There is a 50ms delay between this pin falling and the first transition on SDA or SCL that will be accepted by the device.

1.3.2 Package

The CryptoCompanion is packaged in an 8-lead SOIC package. The pinout is as follows:

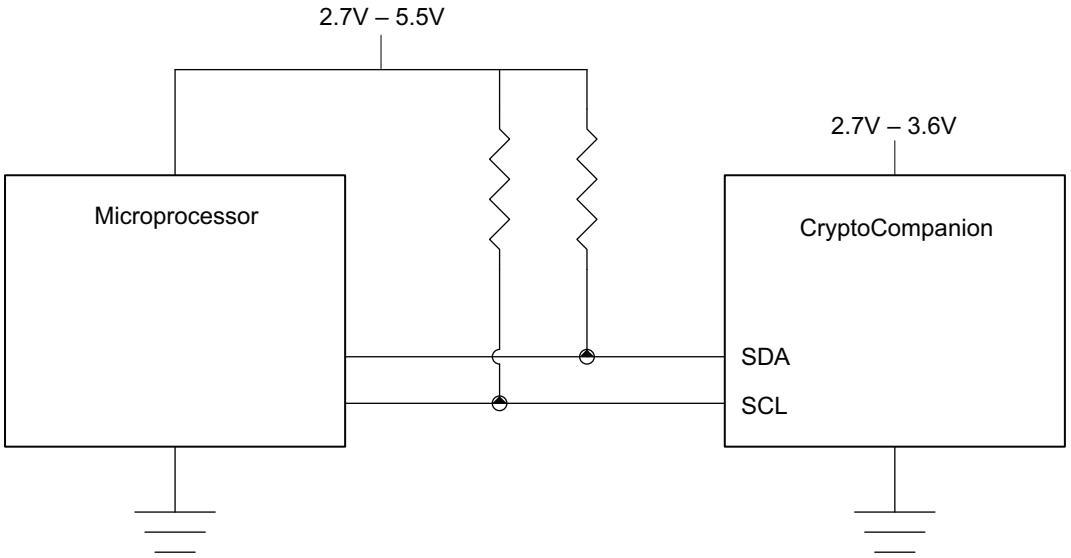
Table 1-2. 8-lead SOIC package pinout

Pin Number	Pin Name
1	PDN
2	RST
3 and 7	NC
4	GND
5	SDA
6	SCL
8	V_{CC}

Note: Pins 3 and 7 are not internally connected and should be connected to ground on the PC board.

1.3.3 Connection Diagram

Figure 1-1. Connection Diagram



1.3.4 TWI Input/Output Operation

The CryptoCcompanion communicates to the system using a 2-Wire Interface (TWI), which is similar to SMBus™. The device operates as a slave and does not support clock stretching. This 2-Wire protocol is identical to that supported by the Atmel AT24C16B Serial EEPROM devices. Refer to the datasheet on the Atmel website for detailed timing and protocol information.

The system processor is expected to properly format commands for the AT88SC118 (which may include information from the CRF device), and then process the outputs of the AT88SC118 (which may include sending some of the outputs to the CRF device).

The CryptoCompanion cannot directly communicate with CRF devices. Both CRF and the 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 devices are on the same bus.

1.4 Memory Locking

When this initialization is complete, the Lock command should be executed which limits access to the memory per the restrictions listed later in this section. The system can determine the current lock value by using the ReadManufacturingID command to read out the ManufacturingID value (MfrID) and the lock byte.

The table below describes the encoding of the least significant two bits of the Lock byte. On shipment from Atmel, Lock[1:0] will have a value of either 10 or 00, depending on the part number ordered. An Atmel AT88SC118 in either of these two states is considered unlocked. It is not possible to change from one of these unlocked states to the other.

After the Lock command has been executed, the Lock byte will have the value 0xFF. Subsequent changes to the Lock byte are impossible.

Table 1-3. Memory Locking

LockBit 1	LockBit 0 (LSB)	Meaning
1	1	Locked. ReadMemory and WriteMemory enabled, subject to the restrictions in this section. WriteMemoryEncrypted and ReadMemoryDigest disabled.
1	0	Unlocked/Confidential. ReadMemoryDigest, WriteMemory, and WriteMemoryEncrypted enabled. ReadMemory disabled.
0	0	Unlocked. ReadMemory and WriteMemory enabled. WriteMemoryEncrypted and ReadMemoryDigest disabled.

2. AC and DC Characteristics

Table 2-1. DC Characteristics[1]

Applicable over recommended operating range from V_{CC} = +2.7 to 3.6 V, T_{AC} = -40° C to 85° C (unless otherwise noted).

Symbol	Parameter	Test Condition	Min	Typ	Max	Units
V_{CC}	Supply Voltage		2.7		3.6	V
I_{CC}	Supply Current	400kHz			5	mA
I_{SB}	Standby Current	$V_{IN} = V_{CC}$ or GND			15	µA
V_{IL}	SDA Input Low Voltage		-0.3		V_{CC} x 0.3	V
V_{IL}	CLK Input Low Voltage		-0.3		V_{CC} x 0.3	V
V_{IL}	RST Input Low Voltage		-0.3		V_{CC} x 0.3	V
V_{IL}	PDN Input Low Voltage		-0.3		V_{CC} x 0.3	V
V_{IH}	SDA Input High Voltage		V_{CC} x 0.7		5.25	V
V_{IH}	SCL Input High Voltage		V_{CC} x 0.7		5.25	V
V_{IH}	RST Input High Voltage		V_{CC} x 0.7		5.25	V
V_{IH}	PDN Input High Voltage		V_{CC} x 0.7		5.25	V
I_{IL}	SDA Input Low Current	$0 < V_{IL} < V_{CC}$ x 0.15	-10		10	µA
I_{IL}	SCL Input Low Current	$0 < V_{IL} < V_{CC}$ x 0.15	-10		10	µA
I_{IL}	RST Input Low Current	$0 < V_{IL} < V_{CC}$ x 0.15	-10		10	µA
I_{IL}	PDN Input Low Current	$0 < V_{IL} < V_{CC}$ x 0.15	-10		10	µA
I_{IH}	SDA Input High Current	V_{CC} x 0.7 < V_{IH} < V_{CC}	-10		10	µA
I_{IH}	SCL Input High Current	V_{CC} x 0.7 < V_{IH} < V_{CC}	-10		10	µA
I_{IH}	RST Input High Current	V_{CC} x 0.7 < V_{IH} < V_{CC}	-10		10	µA
I_{IH}	PDN Input High Current	V_{CC} x 0.7 < V_{IH} < V_{CC}	-10		10	µA
V_{OH}	SDA Output High Voltage	20k Ohm External Pull-up			V_{CC} x 0.8	V
V_{OL}	SDA Output Low Voltage	I_{OL} = 1mA, Vcc=2.7V			0.4	V

Note: 1. Typical values at 25°C. Maximum values are characterized values and not test limits in production.

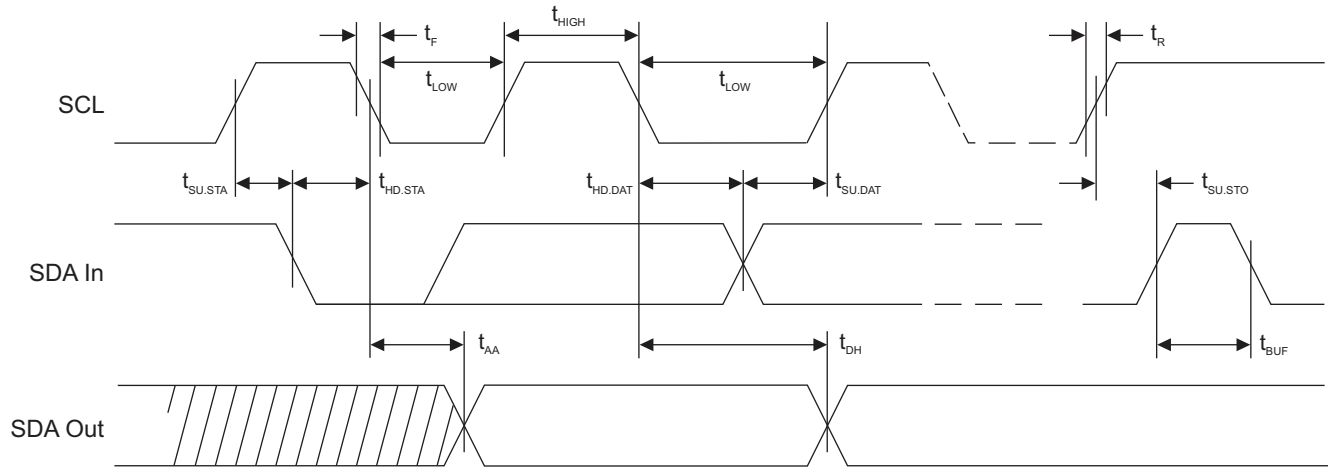
Table 2-2. AC Characteristics[1]

Applicable over recommended operating range from V_{CC} = +2.7 to 3.6 V, T_{AC} = -40° C to 85° C, CL = 30pF (unless otherwise noted).

Symbol	Parameter	Min	Max	Units
f_{CLK}	Clock Frequency	0	400	kHz
	Clock Duty Cycle[2]	40	60	%
t_R	Rise Time: SDA, RST, PDN[2]		300	nS
t_F	Fall Time: SDA, RST, PDN[2]		300	nS
t_R	Rise Time: SCL[2]		300	nS
t_F	Fall Time: SCL[2]		300	nS
t_{AA}	Clock Low to Data Out Valid		900	nS
$t_{HD.STA}$	Start Hold Time	600		nS
$t_{SU.STA}$	Start Set-up Time	600		nS
$t_{HD.DAT}$	Data In Hold Time	100		nS
$t_{SU.DAT}$	Data In Set-up Time	100		nS
$t_{SU.STO}$	Stop Set-up Time	600		nS
t_{DH}	Data Out Hold Time	50	900	nS

Notes: 1. Typical values at 25°C. Maximum values are characterized values and not test limits in production.
2. This parameter is not tested. Values are based on characterization and/or simulation data.

Figure 2-1. SCL: Serial Clock, SDA: Serial Data I/O



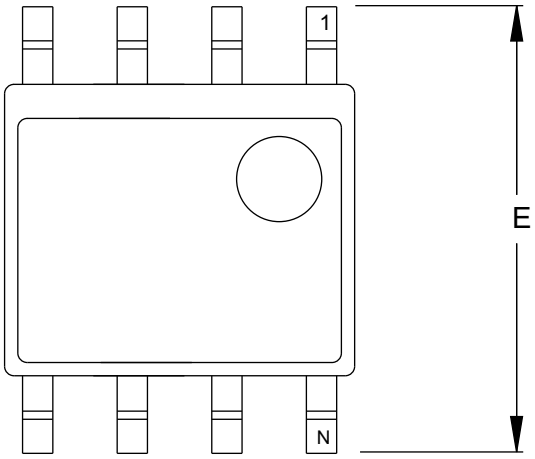
3. Ordering Codes

Ordering Code		Memory Locking	Package	Voltage Range	Temperature Range
AT88SC118-SH-CM	Bulk	00 (Unlocked)	8S1	2.7V – 3.6V	Green Compliant (exceeds RoHS) Industrial (-40°C to 85°C)
AT88SC118-SH-CM-T	Tape and Reel				
AT88SC118-SH-CN	Bulk	10 (Unlocked/Confidential)			
AT88SC118-SH-CN-T	Tape and Reel				

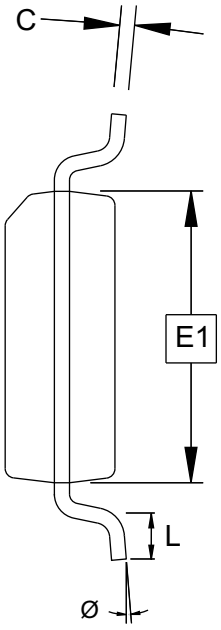
Package	Description
8S1	8-lead, 0.150" Wide, Plastic Gull Wing Small Outline (JEDEC SOIC)

4. Package Drawing

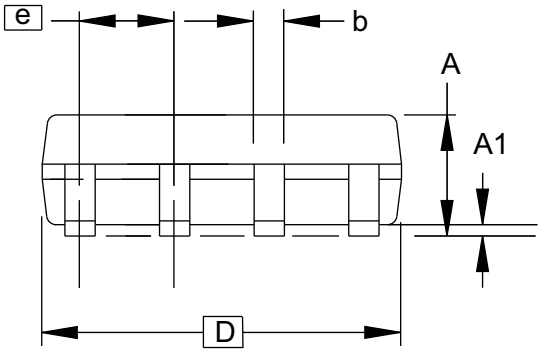
4.1 8S1 — 8-lead JEDEC SOIC



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

5. Revision History

Doc. Rev.	Date	Comments
8858AS	04/2013	Initial 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**

© 2013 Atmel Corporation. All rights reserved. / Rev.: Atmel-8858AS-CryptoComp-AT88SC118-Datasheet-Summary_042013

Atmel®, Atmel logo and combinations thereof, Enabling Unlimited Possibilities®, CryptoAuthentication™, CryptoCompanion™, CryptoRF®, CryptoMemory®, and others are registered trademarks or trademarks of Atmel Corporation or its subsidiaries. Other terms and product names may be trademarks of others.

DISCLAIMER: The information in this document is provided in connection with Atmel products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Atmel products. EXCEPT AS SET FORTH IN THE ATMEL TERMS AND CONDITIONS OF SALES LOCATED ON THE ATMEL WEBSITE, ATMEL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ATMEL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS AND PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ATMEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Atmel makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and products descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Unless specifically provided otherwise, Atmel products are not suitable for, and shall not be used in, automotive applications. Atmel products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.

SAFETY-CRITICAL, MILITARY, AND AUTOMOTIVE APPLICATIONS DISCLAIMER: Atmel products are not designed for and will not be used in connection with any applications where the failure of such products would reasonably be expected to result in significant personal injury or death (“Safety-Critical Applications”) without an Atmel officer's specific written consent. Safety-Critical Applications include, without limitation, life support devices and systems, equipment or systems for the operation of nuclear facilities and weapons systems. Atmel products are not designed nor intended for use in military or aerospace applications or environments unless specifically designated by Atmel as military-grade. Atmel products are not designed nor intended for use in automotive applications unless specifically designated by Atmel as automotive-grade.