Chipsmall Limited consists of a professional team with an average of over 10 year of expertise in the distribution of electronic components. Based in Hongkong, we have already established firm and mutual-benefit business relationships with customers from,Europe,America and south Asia,supplying obsolete and hard-to-find components to meet their specific needs.

With the principle of “Quality Parts,Customers Priority,Honest Operation,and Considerate Service”,our business mainly focus on the distribution of electronic components. Line cards we deal with include Microchip,ALPS,ROHM,Xilinx,Pulse,ON,Everlight and Freescale. Main products comprise IC,Modules,Potentiometer,IC Socket,Relay,Connector.Our parts cover such applications as commercial,industrial, and automotives areas.

We are looking forward to setting up business relationship with you and hope to provide you with the best service and solution. Let us make a better world for our industry!

Contact us

Tel: +86-755-8981 8866 Fax: +86-755-8427 6832
Email & Skype: info@chipsmall.com Web: www.chipsmall.com
Address: A1208, Overseas Decoration Building, #122 Zhenhua RD., Futian, Shenzhen, China

Atmel AT88SC118

CryptoCompanion Chip for CryptoRF and CryptoMemory Products

DATASHEET

Features

- Atmel® CryptoCompanion™ Chip 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

1. Product Overview

The Atmel AT88SC118 is designed as the mate to the CryptoRF (CRF) and CryptoMemory (CM) chips, collectively referred to in the remainder of this document as CRF. Within the operation descriptions, the AT88SC118 CryptoCompanion chip is sometimes referred to as CMC or CryptoMemory Companion chip.

The AT88SC118 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 AT88SC118 does not ever generate a SHA-1 digest of datasets larger than a single round.

1.1 General Operation

The CRF chip 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 AT88SC118 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 chip 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 AT88SC118 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 chip. 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 AT88SC118 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 CMC challenge, and the CMC 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 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 AT88SC118.
- 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 CryptoCompanion Security

The following is a partial list of the security features on this chip.

- Strong internal EEPROM encryption scheme.
- Dynamically encrypted internal SRAM data.
- Programmable power-up penalty.
- Escalating attack penalty.
- Authentication timeouts.
- Anti-tearing counters.
- Anti-tearing RNG Seed.
- Secure Personalization.
- Command usage limitations to prevent exhaustive attacks.
- Uniquely encrypted F Secrets inside chip.
- High security internal clocking scheme.
- Over and under voltage detection tampers.
- Internal data integrity validation.
- Active shield over security sensitive blocks

1.4 Package, Pinout, and I/O

1.4.1 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. 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 chip.

1.4.2 Package

The AT88SC118 is packaged in an 8-lead SOIC package. The pinout is as follows:

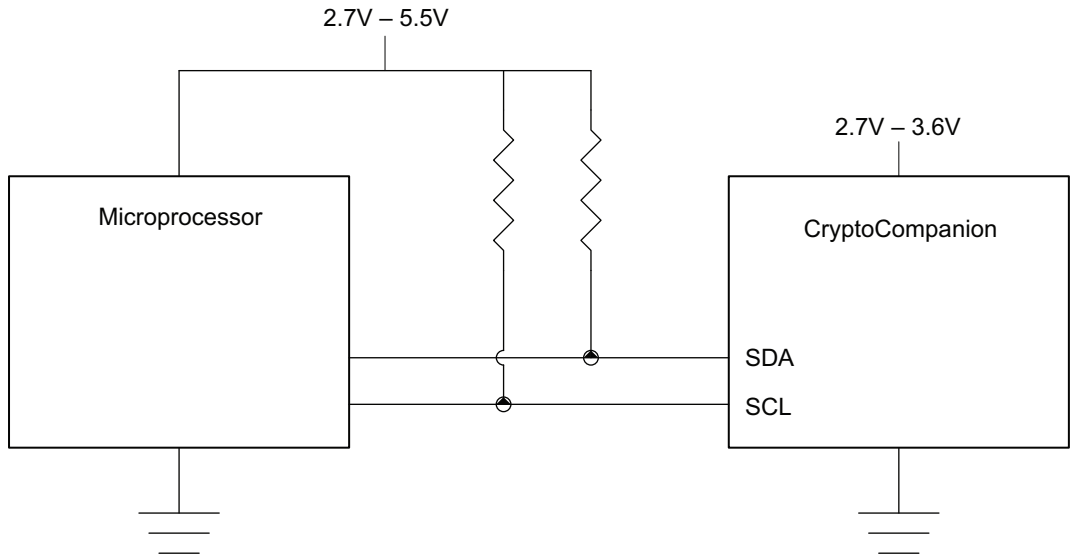
Table 1-2. 8-lead SOIC package pinout

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.

1.4.3 Connection Diagram

Figure 1-1. Connection Diagram



1.4.4 Environmental

The AT88SC118 is guaranteed to operate over the industrial temperature range of -40°C to 85°C. ESD is rated at 2KV, Human Body Model.

1.4.5 TWI Input/Output Operation

The AT88SC118 communicates to the system using a 2-Wire Interface (TWI), which is similar to SMBus™. The chip 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 chips. 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 chip), and then process the outputs of the AT88SC118 (which may include sending some of the outputs to the CRF chip).

The AT88SC118 cannot directly communicate with CRF or CM chips. Both CRF/CM and the AT88SC118 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.

Table 1-3. AT88SC118 Communications Packets Naming Conventions.

AT88SC118 Name	TWI Name	Description
Device Address	Device Name	This byte selects a particular chip on the 2-Wire bus. Bit 1 of this byte on the AT88SC118 selects between accesses to: If 1 = Command/Data or If 0 = The Status Register. Bit 0 of this byte is the standard 2-wire R/W pin. If 1 = The bytes following the device address travel from the slave to the master (Read). If 0 = These bytes flow to the slave (Write).
Cmd	Word Address	If the device address specified a command input (TWI Write), then this byte specifies the command to be executed by the AT88SC118. This byte doesn't exist on Read operations.
Size	$Data_N$	The total number of bytes to follow this byte may be zero in the case that there are no operand bytes. This byte doesn't exist on status read operations.
Data	$Data_{N+1}$, …	Operand input or output bytes as specified in the command descriptions in Section 3., "Command Descriptions"

If the upper six bits of the device address byte sent over the TWI match the upper six bits of the Dev field in the EEPROM, then the AT88SC118 may respond to this transmission; otherwise, it will NACK this byte. Dev is set to a value of 0xC0 on shipment from Atmel.

In general, the AT88SC118 will fail to ACK (NACK) the device address byte if bit 1 of the device address is zero (command/data transfer) and the AT88SC118 is busy.

The AT88SC118 is designed in such a way that the TWI Size field should be consistent with the count values specified in the command parameter descriptions from Section 3., "Command Descriptions". If the TWI Size field is inconsistent with the command parameter count value, the AT88SC118 will respond in different ways depending on the specific command. Some of these responses may include security penalties, other error indications, or some input bytes may be silently ignored.

1.4.5.1 Command Input

Table 1-4. Command Input Byte Sequence

Byte	Direction	Name	Description
0	To Slave	Device Address	This byte selects a particular chip on the 2-Wire bus. Bit 1 should be zero to indicate a command transfer to the AT88SC118. Bit 0 should be zero to indicate the data bytes travel from the master to the slave (TWI Write).
1	To Slave	Cmd	The ordinal of the command to be executed by the AT88SC118, from Table 1-5.
2	To Slave	Size	The total number of bytes to follow this byte may be zero in the case that there are no operand bytes.
3, …	To Slave	Data	Operand bytes as specified in Section 3., “Command Descriptions”.

If the command ordinal is legal, the AT88SC118 will ACK the command input and start processing. It takes a variable amount of time to process the command, up to 20ms depending on the number of EEPROM pages to be written. If an illegal command ordinal (≥0x15) is sent to the chip, it will lock up for a “security delay”, then resume normal operation. See Section 1.6.4, “Security Delay”.

Values in the Cmd byte are chosen from the table below:

Table 1-5. Cmd Byte Values

Command	Value
VerifyFlash	0x01
Startup	0x02
ChallengeResponse	0x03
Auth_1	0x04
Auth_2	0x05
EncryptPassword	0x06
Encryption_1	0x07
Encryption_2	0x08
GrindBytes	0x09
GetRandom	0x0A
IncrementCounter	0x0B
ReadCounter	0x0C
WriteMemory	0x0D
WriteMemoryEncrypted	0x0E
WriteMemoryAuthorized	0x0F
ReadMemory	0x10
ReadMemoryDigest	0x11
ReadManufacturingID	0x12
Lock	0x13
Clear	0x14
Crunch	0x15

1.4.5.2 Command Output

The command output can be extracted from the AT88SC118 using the following byte sequence.

Table 1-6. Command Output Byte Sequence

Byte	Direction	Name	Description
0	To Slave	Device Address	This byte selects a particular chip on the 2-Wire bus. Bit 1 should be zero to indicate that this is a command output. Bit 0 should be one to indicate that the data will travel from the slave to the master.
1	To Master	Size	The total number of bytes to follow this byte may be zero in the case that there are no output bytes.
2, …	To Master	Data	Output bytes as specified in Section 3., “Command Descriptions”.

Command output bytes can be repeatedly read from the AT88SC118 as they remain valid until a new command is sent to the AT88SC118. Until <size> bytes of the new command have been sent, DataAvailable will remain set, and that number of bytes can be read from the SRAM output buffer, though the new input bytes will overwrite the old output bytes.

Some commands do not have any data output, for instance ‘Clear’. On completion of these commands, the DataAvailable bit will be cleared, and the system can read just the size byte, which will have a value of zero.

1.4.5.3 Status

This register can be read to determine the current status or the error information using the following byte stream. This sequence can be run at any time, regardless of whether or not the AT88SC118 is busy or locked.

Table 1-7. Byte Stream Sequence

Byte	Direction	Name	Description
0	To Slave	Device Address	This byte selects a particular chip on the 2-Wire bus. Bit 1 should be one to select the status register. Bit 0 is the standard 2-Wire R/W pin and should be one (data bytes travel from the slave to the master).
1	To Master	Status	Returns the current value of the status register.

The status register value is described in the following table:

Table 1-8. Status Register Value

Byte	Name	Description
0	Data Available	The AT88SC118 has completed processing of the command, and data is available in the output buffer. A successfully completed command that does not have any output will *not* set this bit.
1	Busy	The AT88SC118 is processing a command and is unable to accept more input or provide output, or it is in some sort of security penalty period.
2	StartupDone	The ChallengeResponse command has successfully run this power cycle. Once set, this bit will remain set until the next reset or power cycle.
3 – 4	Reserved	Will always be zero.
5 – 7	Error	An error occurred during prior input or command processing. The value of these three bits denotes the particular condition that occurred.

The eight error codes are used as follows:

Table 1-9. Error Codes

Name	Value	Description
OK	0	Enabled, no error.
RstLocked	1	The AT88SC118 is disabled until the next power cycle or reset assertion. Whenever the error bits are in this state, the Busy bit in the status register will also be asserted.
BadCmd	2	The formatting of the command was invalid, or one of the operands had an unacceptable value.
TimeDelay	3	The AT88SC118 is disabled up for a certain period of time and will respond to commands after this delay has elapsed. This delay may be a Power Delay (Section 1.6.2, “Reset Protection and Power Delay”) or Security Delay (Section 1.6.3, “Reset Locking”). Whenever the error bits are in this state, the Busy bit in the status register will also be asserted.
AuthFail	4	Either authentication must be completed prior to the execution of this command or there was a problem during the execution of the auth commands themselves.
—	5	
¾	6	
¾	7	

The system must poll this register (using TWI reads) after sending a command to the chip before attempting to read the result.

This register cannot be written, attempts to do so will result in a NACK.

1.4.6 Byte Order

The AT88SC118 uses a big-endian byte order for all large integers (addresses, counters) which means that the most significant byte appears first on the bus. Within this document, that byte is shown on the left side of the page. Arrays (F values, cryptograms, passwords, digests) appear in index order, byte 0 first (or on the left of the page).

The 2-Wire protocol specifies that the most significant bit within a byte appears first on the bus and it appears on the left side of the page.

1.5 Memory Architecture

The 4Kb (512 byte) EEPROM within the AT88SC118 is organized into a number of sections, each of which have different access restrictions.

1.5.1 Memory Locking

On shipment from Atmel, certain locations are preloaded by Atmel, per Section 1.5.13, “Memory Initialization Values”. All other data locations are unknown. The system manufacturer should load all areas important for proper system operation with the desired initial values.

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 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 1-10. 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.

1.5.2 Secure Personalization

Customers desiring to write secrets into the AT88SC118 during personalization without exposing these secrets to attackers should purchase the version of the chip in which Lock[1:0] is 10.

In these parts, Atmel will write a transport key into the EncKey location within EEPROM during wafer probe. Once the AT88SC118 leaves the Atmel factory, the EncKey location cannot be written under any circumstances.

When the part is unlocked and therefore in the personalization phase, the WriteMemoryEncrypted command permits the incoming data to be encrypted using EncKey as the encryption key. Data can also be written unencrypted if desired. Verification of the EEPROM contents must use the ReadMemoryDigest command as ReadMemory is prohibited in these parts as shipped. Once locked, the WriteMemoryEncrypted and ReadMemoryDigest commands are prohibited — WriteMemory and ReadMemory are then enabled over a restricted address space.

The value written into EncKey will be the first 16 bytes of the SHA-1 digest of the concatenation of the 15 byte ManufacturingID with a 16 byte secret provided to Atmel by the system manufacturer. The upper six bits of the Lock byte will contain a secret tag assigned by Atmel to differentiate between various secrets that may have been used to generate EncKey. This tag will be erased when the AT88SC118 is locked, leaving the Lock byte with the value 0xFF.

1.5.3 ManufacturingID (MfrID)

These 15 bytes contain unique wafer manufacturing information. This data can be used as the AT88SC118 serial number if desired and can also be used by Atmel to track production of the part. It is written by Atmel at wafer test and cannot be modified by the customer, regardless of whether or not the part has been locked.

The ManufacturingID value can only be obtained by executing the ReadManufacturingID command.

Note: If Lock[1:0] is '10', then the contents of the second 32 byte block which includes this value can be accessed with ReadMemoryDigest. ReadMemory can never be used to access the first 48 bytes of memory (SHA Constant, EncKey, MfrID, and Lock).

1.5.4 Passwords

P0 – P15. These are the passwords used to enable reading and/or writing of various zones in CRF. For example, CP0 is the configuration byte for P0, and determines the particular attributes which govern the use of P0. The password configuration bytes are organized as below:

Table 1-11. Password Configuration Bits.

Bit	Name	Description
0	Encrypt	If 1 = EncryptPassword will return this password value in the clear. In this situation, the password offers little security value but may be useful for mapping.
1	Connect	If 1 = Then obey the "F number" restrictions below. If 0 = Ignore "F Number".
2 – 3	Reserved	Must be zero.
4 – 7	F Number	The secret to which this password is connected. Unless the current authentication session has been computed using this secret this password cannot be read in either clear or encrypted mode.

Once the AT88SC118 is locked, these elements (P0 – P15 and CP0 – CP15) can never be read directly, nor can they be written.

1.5.5 Nonvolatile Counters

The AT88SC118 implements four counters that can each increment to a maximum value of 6.4 million. They cannot be reset, nor can they be decremented. Their current state can be read using the ReadCounter command and they are incremented with the IncrementCounter command. It is recommended that the IncrementCounter command not be issued after the counter has reached a value of 6.4 million. Access to these two commands does not require authorization to have completed.

The above constraints only apply to a locked CMC. In an unlocked AT88SC118, the contents of the EEPROM locations that hold the current state of the various counters can be freely read and/or written using ReadMemory (ReadMemoryDigest) or WriteMemory (WriteMemoryEncrypted).

They should be initialized to a count of zero before the AT88SC118 is locked, by writing the following values into all four of the 16 byte counter areas:

0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0x00 0x00 0x00 0x00 0xFF 0x00 0x00 0x00" at addresses "x0, x1, …

Atmel recommends that all counters be properly initialized even if the application does not utilize all of them.

1.5.6 RNGSeed

This location within the EEPROM is initialized during Atmel manufacturing with a 16 byte random number obtained from an external high quality hardware random number generator. It is used as part of the input to the random number generation capability within the AT88SC118. It may be read and/or written when the part is unlocked.

Caution: Atmel does not recommend that it be written to a fixed value.

1.5.7 Read-Only Memory

When the part is locked, the memory in this area can be read but never written except as described in the next paragraph. After the system has properly responded to the startup challenge, there are no restrictions on the reading of this memory. This memory section starts at address 0x110 and extends to 0x100 | RW-Bound – 1.

RW-Bound must be at least 0x10 and less than 0xF8 or F-Bound, whichever is smaller.

1.5.8 Read/Write Memory

The memory in this area has general Read/Write permissions, similar to a standard Serial EEPROM. After the system has properly responded to the startup challenge, there are no restrictions on the access to this memory.

The first byte in this section is at address 0x100 | RW-Bound. If RW-Bound is less than 0x10, the results will be unpredictable.

1.5.9 Secrets

F0 – F15. These secrets are used to generate the G_C value for the particular CM/CRF chip based on the F1 algorithm, SHA-1. Up to 16 F values that can be supported by the AT88SC118.

The low byte of the memory address of the first should be written into F-Bound. The three least significant bits of F-bound are ignored. The first F value is always F0, independent of F-Bound. If F-bound is < RW-Bound or if F-Bound is < 0x80, the results will be unpredictable.

Example: If F-Bound is 0xD0, the first F value is F0 at memory address 0x1D0. The last F value is F5 at address 0x1F8.

Example: If 0xFF is written into F-Bound, CMC will use only a single secret, named F0, which will be located at address 0x1F8 (since the low three bits of F-bound are ignored).

These elements can never be read directly, nor can they be written after the part has been locked.

1.5.10 CF0 – CF15

This location within the EEPROM is initialized during Atmel manufacturing with a 16 byte random number obtained from an external high quality hardware random number generator. It is used internally within the AT88SC118. It may be read and/or written when the part is unlocked.

Caution: Atmel does not recommend that it be written to a fixed value.

1.5.11 Restricted Bytes

These locations within the EEPROM are initialized during Atmel manufacturing with a four byte random number obtained from an external high quality hardware random number generator. It is used internally within the AT88SC118. It cannot be read and/or written when the part is unlocked or locked. When reading from these locations, the result will be 0xFF for these four bytes.

1.5.12 Memory Map

Figure 1-2. Memory Map

Most Significant Address Bits	Least Significant Address Bits 0	1	2	3	4	5	6	7
0x000	SHA Constant							
0x008								
0x010	EncKey							
0x018								
0x020	ManufacturingID							
0x028								Lock
0x030	P0			CP0	P1			CP1
0x038	P2			CP2	P3			CP3
0x040	P4			CP4	P5			CP5
0x048	P6			CP6	P7			CP7
0x050	P8			CP8	P9			CP9
0x058	P10			CP10	P11			CP11
0x060	P12			CP12	P13			CP13
0x068	P14			CP14	P15			CP15
0x070	Counter0							
0x078								
0x080	Counter1							
0x088								
0x090	Counter2							
0x098								
0x0A0	Counter3							
0x0A8								
0x0B0	SystemSecret							
0x0B8								
0x0C0	CmcSecret							
0x0C8								
0x0D0	RNGSeed							
0x0D8								
0x0E0	FlashDigest							
0x0E8								
0x0F0					RstProt	RW-Bound	F-Bound	Dev
0x0F8	CF0	CF1	CF2	CF3	CF4	CF5	CF6	CF7
0x100	CF8	CF9	CF10	CF11	CF12	CF13	CF14	CF15
0x108	Mode	PwrDelay	spare	spare	Restricted	Restricted	Restricted	Restricted
0x110	Read-Only Memory							
…								
0x178	Read/Write Memory							
0x180	F0							
0x188	F1							
0x190	F2							
0x198	F3							
0x1A0	F4							
0x1A8	F5							
0x1B0	F6							
0x1B8	F7							
0x1C0	F8							
0x1C8	F9							
0x1D0	F10							
0x1D8	F11							
0x1E0	F12							
0x1E8	F13							
0x1F0	F14							
0x1F8	F15							

1.5.13 Memory Initialization Values

Upon shipment from the Atmel factory, the following locations will have predefined values. The contents of all other locations are not guaranteed by Atmel.

Table 1-12. Predefined Initial Memory Values

Name	Initial Value
SHA Constant	Defined by FIPS PUB 180-1.This is written at the Atmel factory and cannot subsequently be changed.
EncKey	Customer Specific, Contact Atmel. See Section 1.5.2, “Secure Personalization”.
ManufacturingID	A unique value for all AT88SC118 chips. See Section 1.5.3, “ManufacturingID (MfrID)”.
Lock	xxxx_xx10 or xxxx_xx00, per Section 1.5.1, “Memory Locking” and Section 1.5.2, “Secure Personalization”. Consult Atmel for ordering information.
RNGSeed	Random values for each AT88SC118. See Section 1.5.6, “RNGSeed”.
Dev	TWI bus address, shipped as 0xC0. See Section 1.5.4, “Passwords”.
CF0 – CF15	Random values for each AT88SC118. See Section 1.5.10, “CF0 – CF15 ”.

Certain values within the AT88SC118 memory array *must* be properly programmed prior to locking of the memory. Failure to properly initialize these locations will result in unpredictable and/or unsecure operation of the part.

Table 1-13. Customer Defined Memory Values

Name	Initial Value
SystemSecret, CmcSecret	These values are used to perform a mutual authentication between the AT88SC118 and the system processor. See Section 3.2, “Startup Command” and Section 3.3, “ChallengeResponse Command”.
RW_Bound	The boundary between ReadOnly and ReadWrite memory. See Section 1.5.7, “Read-Only Memory” and Section 1.5.8, “Read/Write Memory”.
F_Bound	Controls the number of F secrets in the array. See Section 1.5.9, “Secrets” for value limitations.
Mode	The lower two bits control the way in which VerifyFlash is run, see Section 3.1, “VerifyFlash Command”. The upper five bits *must* be zero for proper operation; other values may result in security or functional issues.
FlashDigest	If Mode.Bit[1:0] is set to zero, then this must be set to the proper value per the descriptions in the VerifyFlash command, see Section 3.1, “VerifyFlash Command”.

1.6 Security Features

1.6.1 Environmental Detectors

The AT88SC118 contains an over and under voltage detector for V_{CC} and includes a POR detector to prevent any unknown startup states. If this detector is triggered, the AT88SC118 will be held in reset until the condition is cleared.

The operating clock is internally generated independent of SDA and SCL and glitches on those pins are filtered out. The AT88SC118 includes a metal obfuscation pattern over the memory block.

1.6.2 Reset Protection and Power Delay

There is a Reset Protection Register in EEPROM (RstProt) that normally has a value of one before power is applied. On reset, the AT88SC118 writes this register in the EEPROM to a value of zero, and starts a counter. That counter counts 1MHz clocks up to a total delay interval of approximately 67 seconds, and at that time, the AT88SC118 writes the protection register to a value of one. If a command is in progress when this time interval is reached, the register will be updated at the completion of the command. After this write, the reset protection circuit goes idle until the next reset.

If at the time of reset or power-up, the Protection Register already has a value of zero, then the AT88SC118 goes into a Power Delay state for the same amount of time during which it will neither accept nor acknowledge any command. At the end of the time interval, it will reset the register to a value of one and resume normal operation. A power-up or pin reset during the Power Delay interval will restart the delay counter and start a new interval during which commands will be ignored.

The AT88SC118 is designed to permit the system to execute the reset operation (and operate for at least 67 seconds) a minimum of one million times. If the part is continuously reset every 67 seconds, this limit will be reached in about two years.

The Power Delay of 67 seconds is the maximum delay that the AT88SC118 can support. The actual delay is derived from the contents PwrDelay byte within the EEPROM, according to the following table. The measured delay will vary by up to +/- 25% over manufacturing and operating conditions.

Table 1-14. Reset Protection and Power Delay

PwrDelay	Nominal Delay Interval
0x00	262ms
0x01	524ms
0x02	785ms
0x04	1.3s
0x08	2.4s
Other	Unpredictable

PwrDelay	Nominal Delay Interval
0x10	4.5s
0x20	8.7s
0x40	17s
0x80	34s
0xFF	67s

Note: 1. Short power delay times may decrease the overall security of the system.

The reset protection circuit and associated power delay operates regardless of whether the AT88SC118 is locked or unlocked.

Failure to meet Power-Up and Power-Down conditions listed in Table 1-1, for the V_{CC} and GND pins may result in invoking a reset protection state, causing a Power Delay interval.

1.6.3 Reset Locking

Certain conditions cause the AT88SC118 to lock up until the Reset pin is asserted or the power is cycled. Depending on the time interval from the last power-up, this action may or may not cause a delay to be enforced. During this time, the Status Register will show the RstLocked error state and the Busy pin will be asserted.

- Some command other than VerifyFlash is attempted before Startup/ChallengeResponse has been run or some command other than ChallengeResponse follows Startup.
- ChallengeResponse is run but the preceding command is not Startup.
- VerifyFlash fails for any reason other than that it has been disabled.
- ChallengeResponse fails for any reason.
- Second attempt to run VerifyFlash in a single power cycle.

1.6.4 Security Delay

When certain operations do not complete successfully, the AT88SC118 will enter a temporary security delay for a period of time during which no commands will be honored by the AT88SC118. During this time, the system may read the Status Register which will contain the TimeDelay error code and busy bit set.

The following conditions cause the AT88SC118 to enter a security delay when it is locked. Unlocked AT88SC118 chips never enter the security delay sequence.

- A second attempt to run Startup after the first has completed within the same power or reset cycle.
- Some command other than Auth_2 follows Auth_1.
- The values sent to the AT88SC118 for Auth_2 do not match those computed internally (authentication failed).
- The values sent to the AT88SC118 for Encryption_2 do not match those computed internally (encryption key verification failed).
- An illegal command ordinal is sent to the AT88SC118.

The first time one of these conditions is detected after a power cycle or reset event, the AT88SC118 will delay ~260ms. After each subsequent failure condition is detected, the AT88SC118 will delay for an interval twice the length of the previous delay.

Once this doubling reaches a delay equal to or greater than PwrDelay, all subsequent failure conditions will trigger a lockout interval equal to PwrDelay. The maximum Security Delay is 32s, regardless of the value of PwrDelay.

1.6.5 Command Sequencing

Depending on whether the AT88SC118 is locked or not, some commands must be executed in a certain order, this section outlines those restrictions.

1.6.5.1 When AT88SC118 is Unlocked

When the AT88SC118 is unlocked, there is no security delay, and there is no requirement that Startup/Challenge be executed prior to any other command. This strategy may facilitate quicker initialization.

Note: The Power Delay continues to be active when unlocked and authentication must still be run for those commands that require it (EncryptPassword, Encryption_1&2, GrindBytes).

When the AT88SC118 is unlocked, the following commands are enabled:

- Read Memory can be run only if the least significant two bits of the lock byte in EEPROM are both zero. All locations from 0x30 onwards can be read.
- ReadMemoryDigest can be run on all locations within the EEPROM if Lock[1:0] has a value of 0x10.
- WriteMemory can be run over all locations from 0x30 onwards.
- WriteMemoryEncrypted can only be run if Lock[1:0] has a value of 0x10.
- The Lock command can be run to exit the unlocked state.

1.6.5.2 When AT88SC118 is Locked

When the AT88SC118 is locked, the security delays from Section 1.6.3, “Reset Locking” apply.

The first command run after power-up or a reset must be either VerifyFlash or Startup. If the first command is Startup, then VerifyFlash cannot be run until the next power cycle. If the first command is VerifyFlash, then the next command must be Startup. After Startup, the next command must always be Challenge Response.

No other command can be run until ChallengeResponse has successfully completed. Any attempt to run another command prior to ChallengeResponse or a failure of the ChallengeResponse command will cause the AT88SC118 to lock up until the next power cycle or reset assertion.

A complete and successful authentication sequence (Auth_1 and Auth_2) must be run prior to those commands that require it:

- EncryptPassword
- Encryption_1
- Encryption_2
- GrindBytes.

Failure to run the authentication sequence will result in an error code in the Status Register but no delay.

When the AT88SC118 is locked, the following commands are disabled:

- WriteMemoryEncrypted
- ReadMemoryDigest
- Lock.

WriteMemory is available only for Read/Write memory (the region between RWBound and F-Bound). ReadMemory is only available for ReadOnly + ReadWrite memory (the region between address 0x110 and F-Bound). Any attempt to violate these restrictions will result in a BadCmd error message but no penalty.

2. CMC ↔ CRF Authentication

The AT88SC118 supports the mutual authentication sequence of the CRF chip in a manner such that the shared secrets are not ever exposed on theAT88SC118 or CRF busses. This section describes that mutual authentication sequence. To be consistent with the parameter names in the command descriptions, the AT88SC118 is referred to by its alternate name of CMC.

2.1 Nomenclature

Table 2-1. Nomenclature

Symbol	Description
X_i	The subscript ‘i’ indicates a key index in the CRF memory array. CRF contains four sets of key values. Only those from a single set can be used in a successful authentication sequence.
Y^A, Y^E	The superscripts ‘A’ and ‘E’ indicate the two possible phases of the crypto setup for CRF: • ‘A’ indicates the authentication phase which prefaces all cryptographic communication with CRF. • ‘E’ indicates the optional encryption phase.
C	The initial cryptogram state from CRF to CMC. It is the state generated as a result of a previous authentication or encryption sequence and is unique.
CH, C_i	These values are the challenge and response during the mutual authentication and encryption sequences: • CH^A is the authentication challenge to CRF from CMC. • C_i^A is the authentication response from CRF to CMC. • C^A is the copy of this computed within CMC. • CH^E is the encryption challenge to CRF from CMC. • C_i^E is the encryption response from CRF to CMC. • C^E is the copy of this computed within CMC.
F2	This is the Atmel proprietary algorithm implemented within CMC and CRF. [A, B, C] = F2(X, Y, Z) indicates that X, Y, and Z are inputs to the F2 algorithm, and that execution of the algorithm on these inputs yields the set of outputs A, B, and C.
G, G_i	The secret stored in CRF or computed on CMC from ID and Fn.
ID	This is the unique serial or identification number for CRF which is obtained from the Nc register within the CRF EEPROM.
K_{ID}	This is a constant generated by the external system in a manner of its choosing. It should typically be a function of the ID number and an external secret, but may also include other information about the item to which CRF is attached, the system configuration or other values held external to CMC. CMC treats K_{ID} as a constant and does not interpret its value.
Q	These are random values created in the RNG of CMC which are used as part of the authentication and encryption sequences.
S^A, S^{iA}	These are the encryption keys generated as part of the authentication sequence: • – S^A is generated by CMC. • S_i^A is independently generated by CRF. Their value should be identical. The S keys generated by the encryption sequence are ignored.

2.2 Authentication and Encryption Sequence

Table 2-2. Authentication and Encryption Sequence

	CMC Command	CMC Computation	Dir.	CRF Computation	CRF Command
A.			←	ID, C	Read Config
B.	Auth_1	$G = F1(F_n, K_{ID}, ID)$ $Q^A = RNG$ $[CH^A, C^A, S^A] = F2(G, C, Q^A)$ CH^A, Q^A	→		
C.			←	$[CH, C_i^A, S_i^A] = F2(G_i, C_i, Q^A)$ $CH^A =? CH$ C_i^A	Verify Crypto
D.	Auth_2	$C_i^A =? C^A$			
E.	Encrypt_1	$Q^E = RNG$ $[CH^E, C^E, S^E] = F2(S^A, C^A, Q^E)$ CH^E, Q^E	→		
F.			←	$[CH, C_i^E, S_i^E] = F2(S_i^A, C_i^A, Q^E)$ $CH^E =? CH$ C_i^E	Verify Crypto
G.	Encrypt_2	$C_i^E =? C^E$			

3. Command Descriptions

3.1 VerifyFlash Command

System sends information to the AT88SC118 which would typically be based on the state of an external nonvolatile (e.g. Flash) program store. If the input digest indicates a problem, the AT88SC118 will set up the Status Register to indicate a RstLocked error code but will accept no commands until the next reset or power cycle. This command can be run once only per reset.

- **If Mode.Bit [1:0] == 00**
  This command simply verifies that the incoming digest matches that stored in memory. This is useful if the external ASIC has hardware that can verify the boot code, in which case that hardware would respond to the return code of this command. VerifyFlash *must* run before startup.
- **If Mode.Bit [1:0] == 01**
  This command implements a simple signature mechanism for an externally loaded module. In this case the FlashDigest stored in EEPROM is a secret also known by the entity that generates legal download images. The system sends both the download digest and the signature to the AT88SC118; the AT88SC118 generates a comparison signature using its stored value and verifies that they are the same. This mode is useful if the external system has some confidence in the boot code, but does not have sufficient space to implement a full public key signature verification module. VerifyFlash *must* run before startup.
- **If Mode.Bit [1:0] == 11**
  This command is disabled.
- **Mode.Bit [1:0] == 10**
  This command should not be used.
- **VerifyFlash**
  It will return OK without any computation or comparison being performed.

Table 3-1. Inputs

Name	Size	Description
Digest	20	Digest of external memory.
Signature	20	SHA-1(Digest, FlashDigest), ignored if Mode.Bit [1:0] = 00.

Table 3-2. Outputs

Name	Size	Description

3.2 Startup Command

The AT88SC118 resets all internal state, generates a 20 byte random number, and sends to system as challenge start. To permit the system processor to mutually authenticate the AT88SC118, it will also compute a response to a challenge from the system.

CmcResponse = SHA-1(CmcChallenge, CmcSecret).

This command can be run only once per reset or power cycle.

Table 3-3. Inputs

Name	Size	Description
CmcChallenge	20	Authentication challenge to the AT88SC118 from system processor.

Table 3-4. Outputs

Name	Size	Description
SysChallenge	20	Authentication challenge to system processor from RNG.
CmcResponse	20	Challenge response to CmcChallenge.

3.3 ChallengeResponse Command

System sends 20 byte challenge response to the AT88SC118. The AT88SC118 computes SHA1 (SysChallenge, SystemSecret) and compares with response. If incorrect, the AT88SC118 locks up until the next time the Reset pin is asserted or power is removed.

The prior command must have been Startup, or the AT88SC118 will enter the RstLocked state.

Table 3-5. Inputs

Name	Size	Description
SysResponse	20	Calculated response from system.

Table 3-6. Outputs

Name	Size	Description

3.4 Auth_1 Command

Loads into the AT88SC118 the accessible information about the CRF for which authentication is to be computed and builds the values needed for the CRF chip to perform its authentication sequence. This step computes the values of C^A and S^A. These values are retained in volatile registers within the AT88SC118 (named C and S) for use during Auth_2 and Encrypt_1. See Section 2.2, “Authentication and Encryption Sequence” or more details on the authentication algorithm.

Execution of this command automatically resets any previous state including C and S registers and causes a reset of the crypto engine state.

After execution of Auth_1, the next command must be Auth_2. If it is not, the AT88SC118 locks up for some time. See Section 1.6.3, “Reset Locking”.

Table 3-7. Inputs

Name	Size	Description
C	8	Initial cryptogram seed from CRF.
K_{ID}	16	Constant value to be included in G calculation.
ID	8	Serial number from which G is calculated. Referred to as Nc in CRF documentation.
Selector	1	Selects one of the F values from the EEPROM to be used for authentication.

Table 3-8. Outputs

Name	Size	Description
Q^A	8	Random number input to authentication sequence.
CH^A	8	Authentication challenge from Cmc to CRF.

3.5 Auth_2 Command

Receives the output of the CRF authentication command and verifies that the CRF chip has knowledge of G. See Section 2.2, “Authentication and Encryption Sequence” for more details on the authentication algorithm.

If the incoming Ci^A value is incorrect, the AT88SC118 locks up for some time. See Section 1.6.3, “Reset Locking”.

The authentication times out when a delay of one second expire; at this point one must re-authenticate.

Table 3-9. Inputs

Name	Size	Description
Ci^A	8	Authentication response from CRF to the AT88SC118, second half of mutual authentication.

Table 3-10. Outputs

Name	Size	Description

3.6 EncryptPassword Command

Compute an encrypted password to be sent to the CRF, using the current state of the crypto engine. This can be run at any time after the authentication sequence has completed. This command is optional.

Table 3-11. Inputs

Name	Size	Description
Selector	1	Which password to use.

Table 3-12. Outputs

Name	Size	Description
EncPwd	3	Encrypted password to be sent to CRF.

3.7 Encryption_1 Command

Similar to Auth_1, this sequence generates an intermediate value used for subsequent encryption of data to/from CRF. This pass through the crypto engine is similar to the computation done during authentication with the exceptions that G is replaced by S, the input C is replaced with the AT88SC118 register C, and Q^E is newly generated by the RNG on the AT88SC118. See Section 2.2, “Authentication and Encryption Sequence” for more details on the encryption algorithm.

A valid authentication sequence must be run before these commands which will have set up the C and S registers. This command (and its mate, Encryption_2) can be run multiple times per authentication sequence, but running it more than once will cause the AT88SC118 to be out of synchronization with CRF until the next Auth_1/Auth_2 sequence is run.

After execution of Encryption_1, the next command must be Encryption_2. If not, the AT88SC118 will lock up for a security delay.

Table 3-13. Inputs

Name	Size	Description

Table 3-14. Outputs

Name	Size	Description
Q^E	8	Random number for encryption sequence.
CH^E	8	Encryption challenge from AT88SC118 to CRF.

3.8 Encryption_2 Command

Similar to Auth_2, this sequence takes the encryption response from CRF and compares it the value computed at the end of Encryption_1.

This command can only be run after the execution of Encryption_1. If the incoming Ci^E value is incorrect, the AT88SC118 locks up for a security delay (see Section 1.6.3, “Reset Locking”) and sets the error code in the status register to AuthFail.

Table 3-15. Inputs

Name	Size	Description
Ci^E	8	Authentication response from CRF to the AT88SC118.

Table 3-16. Outputs

Name	Size	Description

3.9 GrindBytes Command

Passes a variable number of bytes through the crypto engine on the AT88SC118 and sends the output of the crypto engine back to the system. This command is used to keep the AT88SC118 in sync with the crypto engine on the CRF chip, to decrypt encrypted data read from CRF, to encrypt data to be written to CRF, and to generate or verify a checksum.

The AT88SC118 does not interpret these bytes, merely passes them through the crypto engine.

GrindBytes cannot be run prior to the successful execution of the Auth_2 nor after the execution of the Clear command.

There is a limit of 4096 for maximum number of GrindBytes that can be run per Authentication.

Table 3-17. Inputs

Name	Size	Description
Size	1	One less than the number of bytes to be sent through crypto engine. If this byte is 0 grind 1 byte, If 0x13 grind 20 bytes. If ≥ 0x14, return BadCmd.
Data	¾	Crypto engine input bytes, maximum 20.

Table 3-18. Outputs

Name	Size	Description
Data	¾	Crypto engine output bytes, maximum 20.

3.10 GetRandom Command

The AT88SC118 generates a 20 byte random number using its internal high quality random number generator and outputs this value. There is no restriction on the system as to where these random numbers may be used — their cryptographic quality makes them suitable for any operation on the system in addition to the CRF operations.

When the AT88SC118 is unlocked, the random numbers generated will follow a predictable pattern based on the state of the RNGSeed EEPROM value and the number of power cycles since this seed has been written. This mechanism facilitates testing.

Table 3-19. Inputs

Name	Size	Description

Table 3-20. Outputs

Name	Size	Description
Data	20	Random bytes from the RNG.

3.11 IncrementCounter Command

Increment the value of the specified counter by one.

Table 3-21. Inputs

Name	Size	Description
Counter	1	Counter index to be incremented, must be from 0 – 3. The upper four bits of this parameter are ignored.

Table 3-22. Outputs

Name	Size	Description

3.12 ReadCounter Command

Returns the 32 bit current state of the specified counter. There are no read restrictions on the counters.

Table 3-23. Inputs

Name	Size	Description
Counter	1	Counter index to be read, must be from 0 – 3. The upper four bits of this parameter are ignored.

Table 3-24. Outputs

Name	Size	Description
Value	4	Current value of counter.

3.13 WriteMemory Command

Writes the contents of the specified address and those following it up to the end of the Read/Write memory space. Prior to locking, any byte after the lock byte can be written with this command. After the AT88SC118 has been locked, only the Read/Write space can be written with this command.

The input data must always be 16 bytes long, though fewer bytes may be written into the EEPROM. While the AT88SC118 ignores these pad bytes, Atmel recommends that they always be 0xFF.

Table 3-25. Inputs

Name	Size	Description
Address	2	Address in EEPROM of the first byte of data to be written. The most significant seven bits are ignored.
Count	1	If zero, write 1 byte… if 0x0F, write 16 bytes. The upper four bits are ignored.
Data	16	Clear text bytes; padded to 16 bytes total.

Table 3-26. Outputs

Name	Size	Description