AT88SC0104CA, AT88SC0404CA
AT88SC0204CA, AT88SC0808CA

Atmel CryptoMemory Specification Datasheet

Features

- One of a family of devices with user memories from 1Kbit to 8Kbit
- EEPROM user memory
  - Four or eight zones
  - Self-timed write cycles
  - Single-byte or multiple-byte page-write modes
  - Programmable access rights for each zone
- 2Kbit configuration zone
  - 37-byte OTP area for user-defined codes
  - 160-byte area for user-defined keys and passwords
- High security features
  - 64-bit mutual authentication protocol (under license of ELVA)
  - Cryptographic Message Authentication Codes (MAC)
  - Stream encryption
  - Four key sets for authentication and encryption
  - Eight sets of two 24-bit passwords
  - Anti-tearing function
  - Voltage and frequency monitor
- Embedded application features
  - Low voltage supply: 2.7V to 3.6V
  - Secure nonvolatile storage for sensitive system or user information
  - Two-wire serial interface (TWI, 5V compatible)
  - 1.0MHz compatibility for fast operation
  - Standard 8-lead plastic packages, green compliant (exceeds RoHS)
  - Same pinout as two-wire Serial EEPROMs
- Smart card features
  - ISO 7816 Class B (3V) operation
  - ISO 7816-3 asynchronous T = 0 protocol (Gemplus® patent)
  - Multiple zones, key sets and passwords for multi-application use
  - Synchronous two-wire serial interface for faster device initialization
  - Programmable 8-byte Answer-To-Reset (ATR) register
  - ISO 7816-2 compliant moduls
- High Reliability
  - Endurance: 100,000 cycles
  - Data retention: 10 years
  - ESD protection: 2,000V

Table of Contents

1. Pin Configuration and Package Information 4
   - 1.1 Pin Configuration 4
   - 1.2 Package Information 4
2. Description 5
   - 2.1 Atmel AT88SCxxxxC Family of Products Differences 5
   - 2.2 Embedded Applications 5
   - 2.3 Smart Card Applications 5
   - 2.4 Scope 5
3. Block Diagram 6
4. Pin Description 7
   - 4.1 Supply Voltage (V_{CC}) 7
   - 4.2 Clock (SCL/CLK) 7
   - 4.3 Serial Data (SDA/IO) 7
   - 4.4 Reset (RST) 7
5. Configuration and User Zone Description 8
   - 5.1 Detailed Description 8
   - 5.2 Control Logic 8
   - 5.3 Configuration Memory 8
   - 5.4 User Memory 11
6. Communication Security Modes 14
   - 6.1 Security Operations 14
   - 6.2 Data Protection Features 17
   - 6.3 Configuration Memory Values 18
   - 6.4 Security Fuses 22
7. Protocol Selection 24
   - 7.1 Synchronous Mode for Embedded Applications 24
   - 7.2 Asynchronous Mode for Smart Card Applications 25
8. Synchronous Protocol 26
   - 8.1 Start-up Sequence 26
   - 8.2 Command Set 27
   - 8.3 Command Format 28
   - 8.4 Acknowledge Polling 29
   - 8.5 Device Addressing 30
   - 8.6 TWI Command Descriptions 30
   - 8.7 Write User Zone: $B0 31
   - 8.8 Random Read: $B1 32
   - 8.9 Read User Zone: $B2 33
   - 8.10 System Write: $B4 34
   - 8.11 System Read: $B6 36
   - 8.12 Verify Crypto: $B8 38
   - 8.13 Verify Password: $BA 40
9. Initialization Example 41
   - 9.1 Write Data to User Zones 41
   - 9.2 Unlock the Configuration Memory 41
   - 9.3 Write Data to the Configuration Memory 41
   - 9.4 Set Security Fuses 41

10. Asynchronous T=0 Protocol 44
10.1 Character Format 44
10.2 Command format 44
10.3 Command Set 45
10.4 T=0 Command Descriptions 47
10.5 Write User Zone: $B0 47
10.6 Read User Zone: $B2 48
10.7 System WRITE: $B4 49
10.8 System READ: $B6 51
10.9 Verify CRYPTO: $B8 53
10.10 Verify Password: $BA 55
11. Initialization Example 56
11.1 Write Data to User Zones 56
11.2 Unlock the Configuration Memory 56
11.3 Write Data to the Configuration Memory 56
11.4 Set Security Fuses 56
12. Absolute Maximum Ratings* 59
12.1 DC and AC Characteristics 59
12.2 Timing Diagrams for Synchronous Communications 60
13. POR and Tamper Conditions 62
13.1 Power On Reset (POR) Delay 62
13.2 Tamper Detection 62
14. Ordering Information 63
Appendix A. Errata 64
A.1 Send Checksum Command in TWI Mode 64
Appendix B. Revision History 65

1. Pin Configuration and Package Information

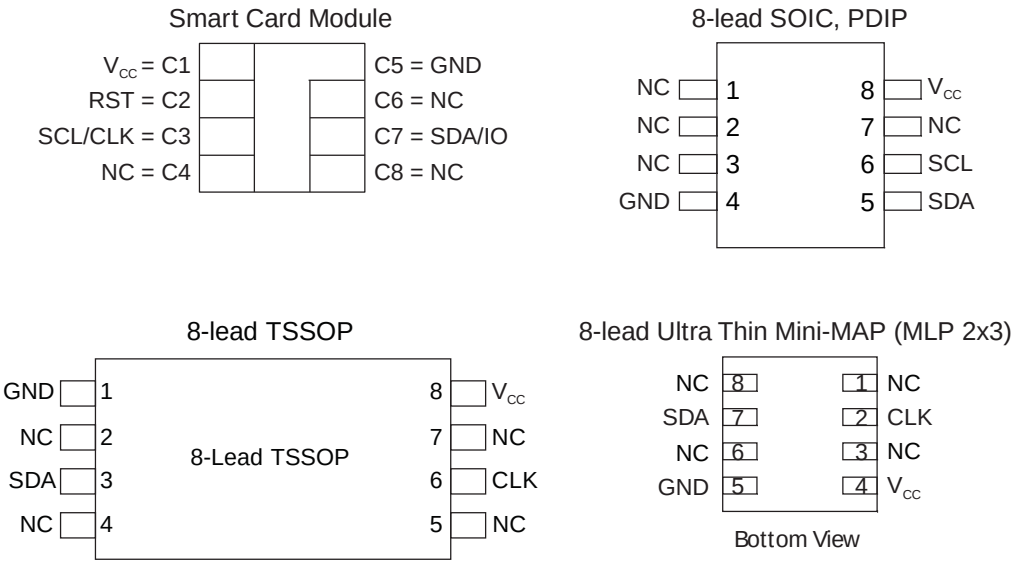
1.1 Pin Configuration

Table 1-1. Package Pin Configuration

Pad	Description	ISO Module Contact	Standard Package Pin	TSSOP	Mini-Map
V_{CC}	Supply Voltage	C1	8	8	4
GND	Ground	C5	4	1	5
SCL/CLK	Serial Clock Input	C3	6	6	2
SDA/IO	Serial Data Input/Output	C7	5	3	7
RST	Reset Input	C2	NC	NC	NC

1.2 Package Information

Figure 1-1. Atmel CryptoMemory Packages



2. Description

The Atmel® AT88SCxxxxCA is a family of four high-performance secure memory devices providing 1K to 8K bits of user memory with advanced built-in security and cryptographic features. The memory is divided into four or eight user zones each of which may be individually set with different security access rights or used together to provide space for one or multiple data files. A configuration zone contains registers to define the security rights for each user zone and space for passwords and secret keys used by the security logic of Atmel CryptoMemory®.

Through dynamic, symmetric-mutual authentication, data encryption, and the use of encrypted checksums, CryptoMemory provides a secure place for storage of sensitive information within a system. With its tamper protection circuits, this information remains safe even under attack.

CryptoMemory also provides high security, low cost and ease of implementation of host-client type systems without the need for a microprocessor operating system. The embedded cryptographic engine provides for a dynamic, symmetric-mutual authentication between the device and host, as well as performs stream encryption for all data and passwords exchanged between the device and host. Up to four unique key sets may be used for these operations.

2.1 Atmel AT88SCxxxxC Family of Products Differences

The key differentiating feature of the AT88SCxxxxCA family of memory devices from AT88SCxxxxC family is support for hardware implementation of the TWI read command. Support for this TWI hardware command allows for faster application development and also permits greater device versatility. In addition, AT88SCxxxxCA offers a random read command, whereby given a starting address, the user can clock unlimited number of bytes from the device up to the memory capacity. Last but not least, the AT88SCxxxxCA family of devices specifically targets low voltage and low power applications.

2.2 Embedded Applications

A two-wire serial interface running at 1.0MHz is used for fast and efficient communications with up to 15 devices that may be individually addressed. CryptoMemory is available in industry standard 8-lead packages with the same familiar pin layout as two-wire Serial EEPROMs supporting only the synchronous communications protocol.

Note: TSSOP pinout not the same

2.3 Smart Card Applications

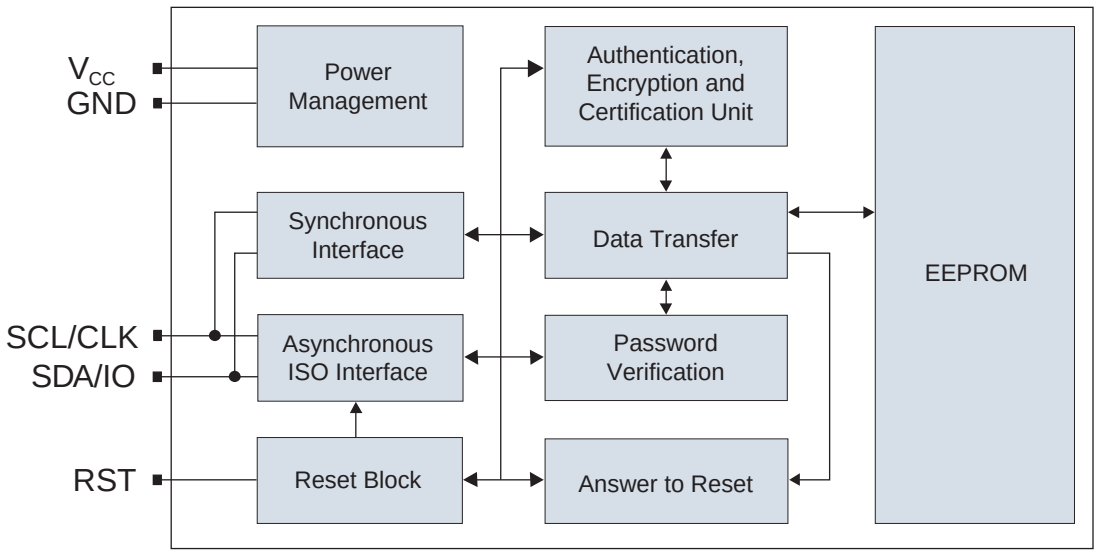
CryptoMemory offers the ability to communicate with virtually any smart card reader using the asynchronous T=0 protocol defined in ISO 7816-3. All CryptoMemory devices in smart card module form will also communicate using a synchronous two-wire serial interface.

2.4 Scope

This CryptoMemory specification document includes all specifications for the standard, authentication, and encryption modes of CryptoMemory operation.

3. Block Diagram

Figure 3-1. Block Diagram



4. Pin Description

4.1 Supply Voltage (V_{CC})

The V_{CC} input is a 2.7V to 3.6V positive voltage supplied by the host.

4.2 Clock (SCL/CLK)

In the asynchronous T=0 protocol, the SCL/CLK input is used to provide the device with a carrier frequency *f*. The nominal length of one bit emitted on I/O is defined as an "elementary time unit" (etu) and is equal to 372/ *f*. When the synchronous protocol is used, the SCL/CLK input is used to clock data in on the positive clock edge and clock data out on the negative clock edge.

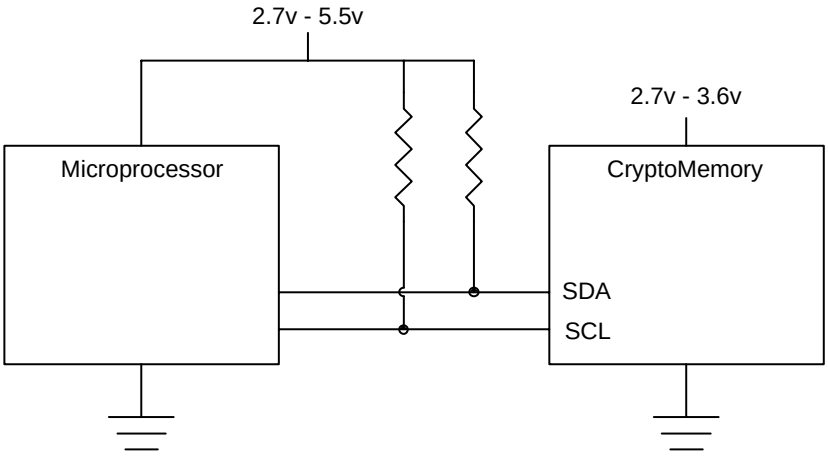
4.3 Serial Data (SDA/IO)

The SDA pin is bi-directional for serial data transfer. This pin is open-drain driven and may be wired with any number of other open drain or open collector devices. An external pull up resistor should be connected between SDA and V_{CC}, a nominal value of 4.7K ohm may be used. The value of this resistor and the system capacitance loading the SDA bus will determine the rise time of SDA. This rise time will determine the maximum frequency during read operations. Low value pull up resistors will allow higher frequency operations while drawing higher average power supply current.

4.4 Reset (RST)

CryptoMemory provides an ISO 7816-3 compliant asynchronous Answer-To-Reset (ATR) sequence. When the reset sequence is activated, the device will output the data programmed into the 64-bit ATR register. When RST is low, all internal logic, access rights and write cycles are in reset, except the asynchronous mode activation flag. A weak internal pull-up on the RST input pad allows the device to be used in synchronous mode without bonding RST. For synchronous only smart card applications an external pull-up on RST is recommended to ensure synchronous operation under any system timings or conditions. CryptoMemory does not support a synchronous answer to reset sequence. The RST input is not available in the plastic package options for CryptoMemory.

Figure 4-1. Connection Diagram



Note: While the Atmel CryptoMemory AT88SCXXXXCA is a low voltage device (2.7V to 3.6V) its I/O buffers are designed for standard high voltage applications (2.7V to 5.5V)

5. Configuration and User Zone Description

5.1 Detailed Description

To enable the security features of CryptoMemory, personalize the device by setting up registers and loading appropriate passwords and keys. This is accomplished though programming the configuration zone of CryptoMemory using simple write and read commands. To gain access to the configuration zone, the secure code (Write 7 password) must be successfully presented. After writing and verifying data in the configuration zone, the security fuses must be blown to lock this information in the device. For additional information on personalizing CryptoMemory, please see the examples in the protocol sections of this specification.

5.2 Control Logic

Access to the user zones occurs only through the control logic built into the device. This logic is configurable through access registers, key registers and keys programmed into the configuration memory during device personalization. Also implemented in the control logic is a cryptographic engine for performing the various higher-level security functions of the device.

5.3 Configuration Memory

The configuration memory consists of 2048 bits of EEPROM memory used for storing passwords, keys, codes, and defining security levels to be used for each user zone. The control logic defines access rights to the configuration memory and the user may not alter these rights. The access rights include the ability to program certain portions of the configuration memory and then lock the data written through use of security fuses. The configuration memory for each CryptoMemory device is identical with the exception of the number of access registers and password/key registers available. Devices with four user zones have four sets of registers, and those with eight user zones, eight sets of registers. Unused memory space in the register region becomes reserved to ensure other components of the configuration memory remain at the same address location regardless of the number of user zones in a device.

Table 5-1. Atmel AT88SC0104CA/0204CA/0404CA Configuration Memory

	$0	$1	$2	$3	$4	$5	$6	$7	
$00	Answer to Reset								Identification
$08	Fab Code		MTZ		Card Manufacturer Code				
$10	Lot History Code								Read Only
$18	DCR	Identification Number Nc							Access Control
$20	AR0	PR0	AR1	PR1	AR2	PR2	AR3	PR3	
$28	Reserved								
$30									
$38									
$40	Issuer Code								
$48									
$50	AAC0	Cryptogram C_0							Cryptography
$58	Session Encryption Key S_0								
$60	AAC1	Cryptogram C_1							
$68	Session Encryption Key S_1								
$70	AAC2	Cryptogram C_2							
$78	Session Encryption Key S_2								
$80	AAC3	Cryptogram C_3							
$88	Session Encryption Key S_3								
$90	Secret Seed G_0								Secret
$98	Secret Seed G_1								
$A0	Secret Seed G_2								
$A8	Secret Seed G_3								
$B0	PAC	Write 0			PAC	Read 0			Password
$B8	PAC	Write 1			PAC	Read 1			
$C0	PAC	Write 2			PAC	Read 2			
$C8	PAC	Write 3			PAC	Read 3			
$D0	PAC	Write 4			PAC	Read 4			
$D8	PAC	Write 5			PAC	Read 5			
$E0	PAC	Write 6			PAC	Read 6			
$E8	PAC	Write 7			PAC	Read 7			
$F0	Reserved								Forbidden
$F8									

Table 5-2. Atmel AT88SC0808CA Configuration Memory

	$0	$1	$2	$3	$4	$5	$6	$7	
$00	Answer to Reset								Identification
$08	Fab Code		MTZ		Card Manufacturer Code				
$10	Lot History Code								Read Only
$18	DCR	Identification Number Nc							Access Control
$20	AR0	PR0	AR1	PR1	AR2	PR2	AR3	PR3	
$28	AR4	PR4	AR5	PR5	AR6	PR6	AR7	PR7	
$30	Reserved								
$38									
$40	Issuer Code								
$48									
$50	AAC0	Cryptogram C_0							Cryptography
$58	Session Encryption Key S_0								
$60	AAC1	Cryptogram C_1							
$68	Session Encryption Key S_1								
$70	AAC2	Cryptogram C_2							
$78	Session Encryption Key S_2								
$80	AAC3	Cryptogram C_3							
$88	Session Encryption Key S_3								
$90	Secret Seed G_0								Secret
$98	Secret Seed G_1								
$A0	Secret Seed G_2								
$A8	Secret Seed G_3								
$B0	PAC	Write 0			PAC	Read 0			Password
$B8	PAC	Write 1			PAC	Read 1			
$C0	PAC	Write 2			PAC	Read 2			
$C8	PAC	Write 3			PAC	Read 3			
$D0	PAC	Write 4			PAC	Read 4			
$D8	PAC	Write 5			PAC	Read 5			
$E0	PAC	Write 6			PAC	Read 6			
$E8	PAC	Write 7			PAC	Read 7			
$F0	Reserved								Forbidden
$F8									

5.4 User Memory

The EEPROM user memory is divided into four (AT88SC0104CA/0204CA/0404CA) or eight (AT88SC0808CA) user zones. Multiple zones allow for the storage of different data types or files in different zones. Access to user zones is possible only after meeting security requirements. The customer defines these security requirements in the configuration zone during device personalization. When the same security requirements define access to multiple zones, the zones effectively serve as one large storage area albeit with the requirement to select each zone prior to access. User zone access is personalized by customer via the access registers.

Table 5-3. Atmel AT88SC0104CA User Memory

Zone		$0	$1	$2	$3	$4	$5	$6	$7
User 0	$00								
	–	32 bytes							
	–								
	$18								
User 1	$00								
	–	32 bytes							
	–								
User 2	$00								
	–	32 bytes							
	–								
	$18								
User 3	$00								
	–	32 bytes							
	–								
	$18								

Note: Page size = 16 bytes

Table 5-4. Atmel AT88SC0204CA User Memory

Zone		$0	$1	$2	$3	$4	$5	$6	$7
User 0	$00								
	–	64 bytes							
	–								
	$38								
User 1	$00								
	–	64 bytes							
	–								
	$38								
User 2	$00								
	–	64 bytes							
	–								
	$38								
User 3	$00								
	–	64 bytes							
	–								
	$38								

Note: Page size = 16 bytes

Table 5-5. Atmel AT88SC0404CA User Memory

Zone		$0	$1	$2	$3	$4	$5	$6	$7
User 0	$00								
	–	128 bytes							
	–								
	$78								
User 1	$00								
	–	128 bytes							
	–								
	$78								
User 2	$00								
	–	128 bytes							
	–								
	$78								
User 3	$00								
	–	128 bytes							
	–								
	$78								

Note: Page size = 16 bytes

Table 5-6. Atmel AT88SC0808CA User Memory

Zone		$0	$1	$2	$3	$4	$5	$6	$7
User 0	$00								
	–	128 bytes							
	–								
	$78								
User 1	$00								
–	–								
–									
–	–								
User 6	$78								
User 7	$00								
	–	128 bytes							
	–								
	$78								

Note: Page size = 16 bytes

6. Communication Security Modes

Communication between the device and host operates in three basic modes. Standard mode is the default mode for the device after power-up. Authentication mode is activated by a successful authentication sequence. Encryption mode is activated by a successful encryption activation following a successful authentication. Data transferred to and from the device is handled per the following table.

Table 6-1. Communication Security Modes

Mode	Configuration Data	User Data	Passwords	Data Integrity Check
Standard/Password	clear	clear	clear	MDC
Authentication	clear	clear	encrypted	MAC
Encryption	clear	encrypted	encrypted	MAC

Note: 1. Configuration data includes the entire configuration memory except the passwords

- MDC: Modification Detection Code
- MAC: Message Authentication Code

6.1 Security Operations

6.1.1 Password Verification

The use of passwords protects read and write accesses to the user zones. Any one of eight password sets is available for assignment to any user zone through configuration of access registers. CryptoMemory provides separate 24-bit passwords for read and write operations. Read passwords grant only read accesses to zones under password protection, while write passwords grant both read and write accesses. Successful presentation of any password renders the verify password command active until the presentation of another password or device reset. Only one password may be active at a time. Presenting incorrect passwords decrements the value of the corresponding password attempts counter (PAC). Decrementing the PAC to $00 permanently disables the corresponding password and permanently renders the corresponding user zone(s) under protection inaccessible. Operation in authentication or encryption modes requires encryption of passwords for all password transactions.

Figure 6-1. Password Verification

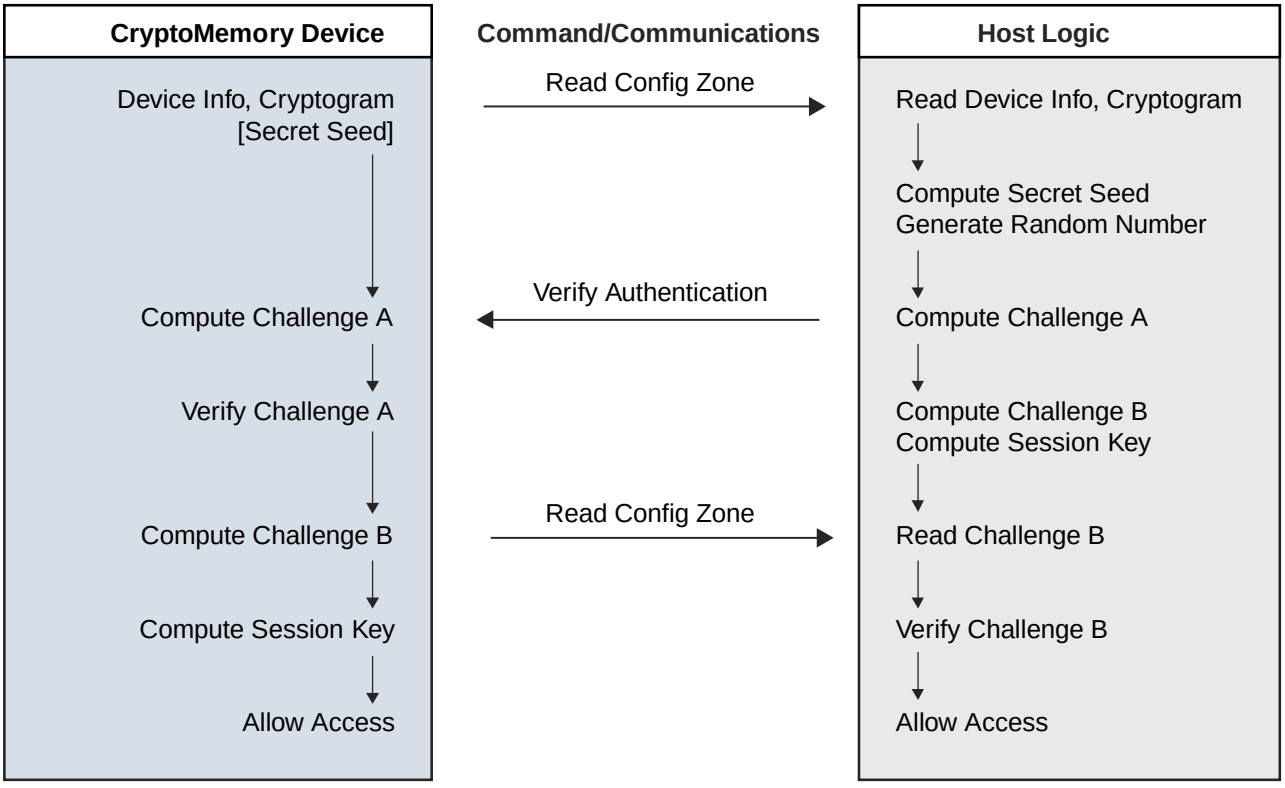


6.1.2 Authentication Protocol

The use of a mutual authentication protocol further protects access to user zones. Any one of four key sets is available for assignment to any user zone through configuration of access registers. Each key set consists of a secret seed, a cryptogram, and a session encryption key. A verify crypto command exists to allow the use of any one of the key sets to enter authentication mode. Each successful entry into authentication mode renders the mode active for the current key set until the next call to the verify crypto command or device reset. Only one key set may be active at anytime. Unsuccessful calls of the verify crypto command exits authentication mode and decrements the value of the authentication attempts counter (AAC) register. Decrementing AAC to $00 permanently disables the corresponding key set and permanently renders the corresponding user zone(s) under protection inaccessible.

Entry into authentication mode is a process through which the host and CryptoMemory device mutually authenticate one another. First, the host generates a 64-bit random number, reads a current cryptogram and identification information from the device, and uses this information in conjunction with the corresponding secret seed to generate a 64-bit challenge for the device. The host also generates a new cryptogram and session encryption key in the process. The host then sends the challenge and random number to the device by calling the verify crypto command. The device utilizes the random number from the host to generate its own challenge, new cryptogram and session encryption key. It then compares the challenge to the one from the host. If the challenges match, then the device declares the host authentic, overwrites its corresponding current cryptogram and session encryption key with the new ones. To complete the mutual authentication, the host reads the new cryptogram from the device and compares it with its new cryptogram. The new cryptogram from the device serves as a challenge to the host. If the cryptograms match then the device is authentic. Only an authentic pair of host and device can generate the same challenges and cryptograms. Activating mutual authentication requires the use of the verify authentication variant of the verify crypto command (see Section 8.2, Command Set and Section 10.3, Command Set).

Figure 6-2. The Mutual Authentication Process

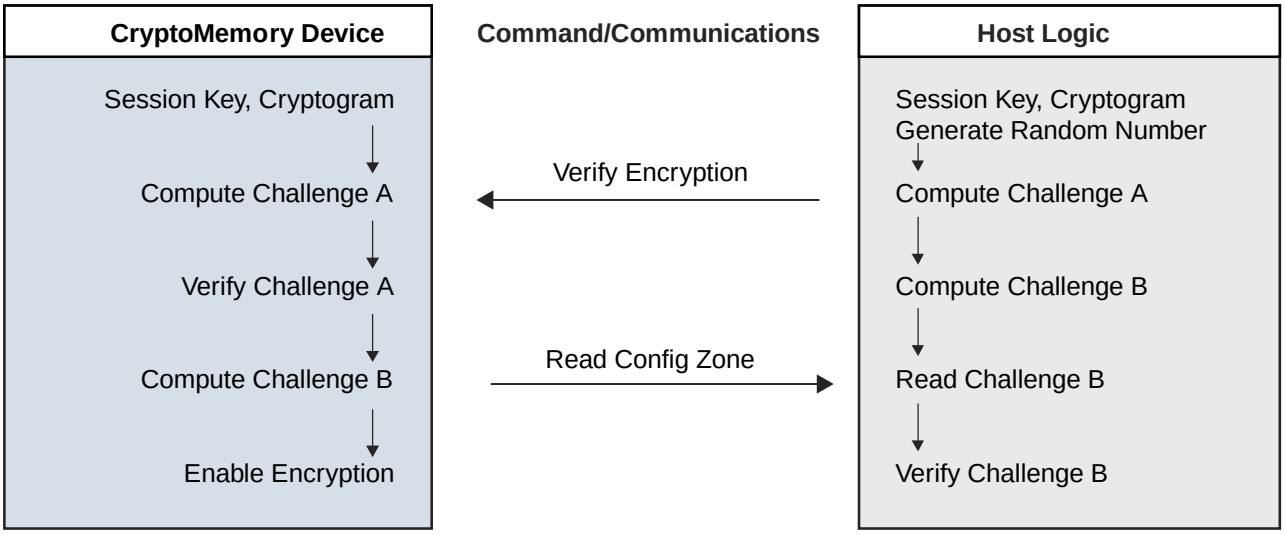


6.1.3 Data Encryption

CryptoMemory allows the use of encryption between a host system and the CryptoMemory device to protect the confidentiality of data during read-write accesses and verify password operations. To enable encryption, the host must generate a challenge using the session encryption key generated from the authentication activation step. The host then needs to call the verify crypto command again with the device still in active authentication mode. The session encryption key must belong to the active authentication key set. The host may enable encryption at any time after which data content of communication between host and device user zones becomes encrypted. If a user zone configuration in the access register requires encryption, however, then the host must enter encryption mode and must encrypt all data content to and from the zone in the remainder of the active encryption session in order to communicate with the zone. CryptoMemory does not encrypt system zone data except for password and password attempt counters. Passwords and password attempt counters require encryption during active authentication or encryption modes.

Each successful entry into encryption mode renders the mode active for the current key set until the next call to the verify crypto command or device reset. Only one key set may be active at anytime. Unsuccessful calls of the verify crypto command exits both encryption and authentication modes and decrements the value of the authentication attempts counter (AAC) register. Decrementing AAC to $00 permanently disables the corresponding key set and permanently renders the corresponding user zone(s) under protection inaccessible. Activating encryption is similar in process to activating authentication with the exception that the session encryption key replaces the secret seed. The process uses the verify encryption variant of the verify crypto command (see Section 8.2, Command Set and Section 10.3, Command Set)

Figure 6-3. Encryption Activation Process from Active Authentication Mode



6.1.4 Encrypted Checksum (Message Authentication Code, MAC)

CryptoMemory implements a data validity check function in the form of an encrypted checksum. This checksum provides a bi-directional data integrity check and data origin authentication capability in the form of a Message Authentication Code (MAC): only the host/device that carried out a valid authentication is capable of computing a valid MAC. When writing data to the CryptoMemory device in authentication or encryption communication modes, the host must send a valid checksum immediately following the write command. If the checksum is invalid, the device rejects the write command and resets the device security privileges. The host must reinitiate entry into authentication and, if applicable, encryption modes to continue. The use of checksum is optional when reading data. Calls to the read checksum command resets device security so its use is recommended only at the completion of all data read operations from the device.

6.2 Data Protection Features

Security operations control access to data stored in CryptoMemory. After gaining access, additional options exist to protect data in the user memory.

6.2.1 Modify Forbidden

The Modify Forbidden option renders the user zone read-only by restricting all write operations to it. It is recommended to program all required data in the user zone prior to enabling this option. Modify forbidden is available for any user zone and is selectable by configuring appropriate access registers.

6.2.2 Program Only

The program only option constrains data bit modification to programming from logic “1” to logic “0” only. Data bits may never change from logic “0” to logic “1”. Program only is available for any user zone and is selectable by configuring appropriate access registers.

6.2.3 Write Lock

The write lock option provides ability to render individual bytes within a user zone read-only by restricting all write operations to it. It operates on 8-byte page level whereby the lowest addressed byte of the page serves as the write access control byte for that page. Table 6-2 shows the use of write lock for data at addresses $080 - $087. The byte at $080 controls write access to bytes from $080 to $087.

Table 6-2. Write Lock example

Address	$0	$1	$2	$3	$4	$5	$6	$7
$080	11011001	xxxx xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx
		locked	locked			locked		

The write lock option also applies to the access control byte for each page by writing its least significant (rightmost) bit to logic “0”. Moreover, only logic modifications from logic “1” to logic “0” of the access control byte are permissible. Write lock is available for any user zone and is selectable by configuring appropriate access registers. Furthermore, configuring a user zone with the write lock option restricts writing to that zone to a byte at a time. Attempts to write several bytes within a command; results in writing only the first byte.

6.2.4 Anti-tearing (Power Loss Protection)

In the event of a power loss during a write cycle, the integrity of the device's stored data may be recovered. This function is optional, and the host may choose to activate the anti-tearing function for any write to a user zone or configuration zone by use of the appropriate B4 system write command. When anti-tearing is active, write commands will take longer to execute since more write cycles are required. Additionally, the data written is limited to eight bytes.

Data is written first to a buffer zone in EEPROM instead of the intended destination address in the user zone or configuration zone, but with the same access conditions. If this write cycle is interrupted the original data remains intact in the user zone or configuration zone. The data is then written in the required memory location. If this second write cycle is interrupted the device will automatically recover the data from the system buffer zone at the next power-up and write it to the intended destination address.

In two-wire mode, the host is required to perform ack polling for 36ms after write commands when anti-tearing is active. At power-up five clock cycles are required to check the anti-tearing flags. In the event that the device needs to carry out the data recovery process the host is required to perform ack polling for 18ms.

6.3 Configuration Memory Values

This section describes each individual field in the configuration memory.

6.3.1 Default Values

Atmel programs certain fields of the system zone at the factory. The customer may elect to change the content of all of these fields except for the lot history code field, which is permanently locked. Atmel programs the remainder of the fields, including all of the configuration memory and user zones to ones prior to releasing the device from the factory. Table 6-3, “Factory Programmed Fields,” summarizes device fields Atmel programs at the factory. A brief description of each field follows.

Table 6-3. Factory Programmed Fields

Device	ATR	Fab Code	Lot History code	Write 7 Password (Secure Code)
AT88SC0104CA	3B B2 11 00 10 80 00 01	10 10	Variable, locked	DD 42 97
AT88SC0204CA	3B B2 11 00 10 80 00 02	20 20	Variable, locked	E5 47 47
AT88SC0404CA	3B B2 11 00 10 80 00 04	40 40	Variable, locked	60 57 34
AT88SC0808CA	3B B2 11 00 10 80 00 08	80 60	Variable, locked	22 E8 3F

6.3.2 Answer To Reset (ATR)

This is an eight byte wide register with content that Atmel defines. This register is read/write accessible prior to blowing the FAB fuse, but becomes read-only after blowing the fuse.

6.3.3 Fab Code

This field is a 16-bit wide register with content that Atmel defines. This field is read/write accessible prior to blowing the FAB fuse, but becomes read-only after blowing the fuse.

6.3.4 Memory Test Zone (MTZ)

This field is a 16-bit wide register with open read/write access privileges at all times for testing basic communication to the device. This field is free of all security constraints at all times.

6.3.5 Card Manufacturer Code

This field is a 32-bit wide register with read/write access privileges for the customer to define its content. The content of this field becomes read-only after blowing the PER fuse.

6.3.6 Lot History Code

This field is a 64-bit wide register with content that Atmel defines. This field is read-only.

6.3.7 Issuer Code

This field is a 128-bit wide register with read/write access privileges for customer to define its content. The content of this field becomes read-only after blowing the PER fuse.

6.3.8 Device Configuration Register (DCR)

This 8-bit register allows selection of the following device configuration options (active low). The values programmed have an immediate effect on the logic of the device. The default value is “1” for each bit.

Table 6-4. Device Configuration Register (DCR)

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
SME	UCR	UAT	ETA	CS3	CS2	CS1	CS0

6.3.8.1 SME – Supervisor Mode Enable

Asserting this bit (SME = “0”) enables supervisor mode for Write 7 password such that verifying Write 7 password grants read and write accesses to all password sets and PACs. Verifying Write 7 password does not grant access to other passwords when this bit is not asserted (SME = “1”).

6.3.8.2 UCR – Unlimited Checksum Reads

Asserting this bit (UCR = “0”) allows unlimited number of checksum reads without requiring a new authentication. Not asserting this bit (UCR = “1”) limits the read of checksum to one attempt after which the device resets the crypto algorithm after executing the read checksum command.

6.3.8.3 UAT – Unlimited Authentication Trials

Asserting this bit (UAT = “0”) disables the Authentication Attempts Counter (AAC) thus allowing unlimited authentication attempts. The AAC decrements after each unsuccessful attempt but the internal logic ignores it value. Asserting this bit also prevents reset of the crypto algorithm after reading the MAC in encryption mode. The UAT bit does not affect the password attempts counter.

6.3.8.4 ETA – Eight Trials Allowed

Asserting this bit (ETA = “0”) extends the trials limit to 8 incorrect attempts to authenticate or verify a password. The counter (AAC or PAC) will decrement ($FF, $FE, $FC, $F8, $F0, $E0, $C0, $80, $00) with each incorrect attempt. Disabling this bit (ETA = “1”) limits authentication and password verification trials to only four incorrect attempts ($FF, $EE, $CC, $88, $00).

6.3.8.5 CS0 – CS3: Programmable Chip Select (Only Relevant in Synchronous Protocol)

The four most significant bits (b4 – b7) of every command comprise the chip select address. All CryptoMemory devices will respond to the default chip select address of $B (1011). Each device also responds to a second chip select address programmed into CS0-CS3 of the device configuration register. By programming each device to a unique chip select address, it is possible to connect up to 15 devices on the same serial data bus and communicate individually to each. Global communications to all devices sharing the bus is accomplished using the default chip select address $B.

6.3.9 Access Registers

Four (AT88SC0104CA/0204CA/0404CA) or eight (AT88SC0808CA) 8-bit access registers allow personalization of the device. Each access register works in conjunction with a password/key register to define the security settings for each individual zone of the user memory. Values in the access registers take immediate effect after programming. The default value for each bit is “1”.

Table 6-5. Access Register

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
PM1	PM0	AM1	AM0	ER	WLM	MDF	PGO

6.3.9.1 PM(1:0) Password Mode

Table 6-6. Password Mode

PM0	PM1	Access
1	1	No password required
1	0	Write password required
0	*	Read and write passwords required

When PM = “11”, the user zone under protection requires no password. When PM = “10”, the zone requires write password verification for writing and reading is free. When PM = “01” or “00”, reading requires the read password verification and writing requires write password verification. However, proper verification of the write password also grants read access. The password set required is specified by PW(3:0) in the corresponding passwords/keys register (see Section 6.3.10, Password/Key Registers). Verification of the write password also allows modification of the read and the write passwords.

6.3.9.2 AM(1:0) – Authentication mode

Table 6-7. Authentication Mode

AM1	AM0	Access
1	1	No authentication required
1	0	Authentication for write
0	1	Normal authentication mode
0	0	Dual access mode

When AM = “11”, the user zone under protection requires no authentication. When AM = “10”, the zone requires authentication only for write accesses and read accesses are free. When AM = “01”, the zone requires authentication for both write and read accesses. In both of these configurations, the Authentication Key (AK) in the corresponding passwords/keys register specifies the required secret seed and corresponding cryptogram, and when applicable the session encryption key (see the following Section 6.3.10).

Finally, when AM = “00”, the dual access mode is active in which authentication using the Program Only Key (POK) gives a right to read and program the zone (i.e. write '0's only), while authentication using the AK gives full read and write access to the zone. In this way, a token application may be implemented, whereby regular hosts with knowledge of POK may decrement the stored value, and only master hosts with knowledge of AK may reset the token to its full value. Please see the following Section 6.3.10on the passwords/keys register for further definition of POK and AK.

Notes:
1. When AM = "00", the POK bits in the corresponding password/key register are ignored
2. When AM = ‘00’ and PGO = ‘0’; bits in the zone may not be written to ‘1’ even when using the AK
3. Requiring authentication automatically requires the use of secure checksums for write operations (See Section 6.1.4, Encrypted Checksum (Message Authentication Code, MAC)

6.3.9.3 ER – Encryption Required

When ER = "0", the host is required to activate the encryption mode in order to read/write the corresponding user zone. No data read from or written to the zone may be transmitted in the clear. If ER = "1", the host may activate the encryption mode, but isn't specifically required to do so by the device.

6.3.9.4 WLM – Write Lock Mode

Asserting this bit (WLM = “0”) divides the user zone into 8-byte pages. The first byte of each page becomes the write lock byte and defines the locked/unlocked status for each byte in the page. Write access is forbidden to a byte if its associated bit in the write lock byte is set to “0”. Bit 7 controls byte 7; bit 6 controls byte 6, etc. By setting bit 0 to “0” locks the write lock byte itself. Enabling write lock mode limits write operations to one byte at a time.

6.3.9.5 MDF – Modify Forbidden

Asserting this bit (MDF = “0”) renders the user zone read-only at all times. The user zone must, therefore, be programmed before setting this bit to “0”

6.3.9.6 PGO – Program Only

Asserting this bit (PGO = “0”) allows changing of data within the user zone under protection from “1” to “0” and never from “0” to “1”.

6.3.10 Password/Key Registers

Four (AT88SC0104CA/0204CA/0404CA) or eight (AT88SC0808CA) 8-bit password/key registers receive definition during device personalization. Each password/key register works in conjunction with a corresponding access register to define the security settings of each zone. The values programmed have an immediate effect on the logic of the device. The default value is “1” for each bit. Bit 3 is reserved and should be left as value “1.”

Table 6-8. Password/Key Register Bit Map

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
AK1	AK0	POK1	POK0	Res	PW2	PW1	PW0

6.3.10.1 AK(1:0) – Authentication Key

These bits define which of the four secret seeds G_0-G_3 must be used in an authentication to allow access to the user zone if authentication is selected in the corresponding access register. Each access register may point to a unique authentication secret, or access registers for multiple zones may point to the same authentication secret. In this case authentication with a single secret seed will open several zones.

6.3.10.2 POK(1:0) – Program Only Key

When the user zone has the dual access mode selected (AM = "00"), these bits define which of the four secret seeds G_0-G_3 must be used in an authentication to allow read and program (i.e. write '0's only) access to the user zone.

6.3.10.3 PW(2:0) – Password Set

These bits define which of the eight password sets must be presented to allow access to the user zone when the password mode is selected.

6.3.11 Identification Number

A 56-bit number the customer defines during personalization. It is recommended that a unique identification number be assigned to each device.

6.3.12 Cryptograms (C_0 – C_3)

Each of these fields contains a 56-bit cryptogram for use during authentication. The internal logic modifies the cryptogram each time it successfully verifies the authentication. The customer may program an initial value for the cryptogram during personalization. It is recommended that the initial values be random numbers.

6.3.13 Session Keys (S_0 – S_3)

Each of these fields contains a 64-bit session key for use during encryption. The internal logic modifies the session key each time it successfully processes authentication or encryption verification. The session keys do not require initial values and does programming initial values are not necessary.

6.3.14 Secret Seeds (G_0-G_3)

Each of these fields contains a 64-bit secret seed that is used in conjunction with the corresponding cryptogram and session key during the authentication and encryption sequences. The customer programs the secret seeds during device personalization.

6.3.15 Password Sets

The password fields contain eight sets of two 24-bit passwords for read and write operations. The customer defines the values of these passwords during personalization. Successfully verifying the write password allows modification of the read and the write passwords of the same set.

6.3.16 Secure Code

The secure code is the Write 7 password. Properly presenting this password grants write access to the configuration memory during personalization. Atmel defines the initial value of the secure code but the customer may change these values after successful presentation during a verify password operation for Write 7 password. Table 6-3, Factory Programmed Fields shows the secure codes for various devices when they leave the Atmel factory. After blowing the PER fuse, verifying Write 7 password no longer grants write access to the configuration memory, and the configuration memory becomes read-only thereafter.

6.3.17 Password Attempts Counters (PAC)

Each of the sixteen PAC fields contains an 8-bit attempts counter for the verify password process. Each PAC corresponds to a password. The attempts counter limits the number of incorrect consecutive presentations of the corresponding password to four, after which it locks the password from future use. The PAC will decrement ($FF, $EE, $CC, $88, $00) with each incorrect attempt to present the password. The PAC permanently locks the corresponding password once its value reaches $00. Prior to reaching $00, any correct presentation of the password resets the PAC value to $FF.

6.3.18 Authentication Attempts Counters (AAC)

Each of the four AAC fields contains an 8-bit attempt counter for the authentication process. Each AAC field corresponds to each authentication key set. The attempts counter limits the number of incorrect consecutive attempts to authenticate to for, after which it locks the authentication key set from future use. The AAC will decrement ($FF, $EE, $CC, $88, $00) with each incorrect attempt to authenticate. The AAC permanently locks the corresponding key set once its value reaches $00. Prior to reaching $00, any correct attempt to authenticate resets the AAC value to $FF.

6.4 Security Fuses

CryptoMemory uses four fuses. The status of these fuses is given in a ‘fuse byte.’ A value of ‘0’ indicates that the fuse has been blown. Bits four to seven of this byte are not used as security fuses and are reserved for Atmel use.

Table 6-9. Device Fuses

F_7	F_6	F_5	F_4	F_3	F_2	F_1	F_0
resv	resv	resv	resv	SEC	PER	CMA	FAB

SEC, PER, CMA, and FAB are non-volatile fuses blown at the end of various steps in the manufacturing and personalization process. Once blown, these fuses can never be reset. Atmel blows the SEC fuse to lock the lot history code before the device leaves the factory. Blowing the remainder of the fuses must follow the sequence:

- **FAB** To lock the ATR and the fab code portions of the configuration memory
- **CMA** To lock the card manufacturer code of the configuration memory
- **PER** To lock the remainder of the configuration memory

Any attempt to blow a fuse out of sequence will be unsuccessful.

Table 6-10 provides a summary of access rights for all portions of the memory for each fuse condition.

Table 6-10. Configuration Memory Access Control by Security Fuses

Zone	Operation	Fuse			
		SEC = 0	FAB = 0	CMA = 0	PER = 0
Identification (Except MTZ and CMC)	Read	Free	Free	Free	Free
	Write	Secure Code	Forbidden	Forbidden	Forbidden
Memory Test Zone (MTZ)	Read	Free	Free	Free	Free
	Write				
Card Manufacturer Code (CMC)	Read	Free	Free	Free	Free
	Write	Secure Code	Secure Code	Forbidden	Forbidden
Read Only (Lot History Code)	Read	Free	Free	Free	Free
	Write	Forbidden	Forbidden	Forbidden	Forbidden
Access Control	Read	Free	Free	Free	Free
	Write	Secure Code	Secure Code	Secure Code	Forbidden
Cryptography (Except Encryption Keys S)	Read	Free	Free	Free	Free
	Write	Secure Code	Secure Code	Secure Code	Forbidden
Encryption Keys (S)	Read	Secure Code	Secure Code	Secure Code	Forbidden
	Write				
Secret	Read	Secure Code	Secure Code	Secure Code	Forbidden
	Write				
Passwords	Read	Secure Code	Secure Code	Secure Code	Write PW
	Write				
Password Attempts Counters (PAC)	Read	Free	Free	Free	Free
	Write	Secure Code	Secure Code	Secure Code	Write PW
Forbidden	Read	Forbidden	Forbidden	Forbidden	Forbidden
	Write				

Note: Secure code: Write 7 password is the secure code until the PER fuse is blown

7. Protocol Selection

CryptoMemory supports two application areas with different communication protocols:

- Two-wire serial communication for embedded applications
- ISO 7816 asynchronous T=0 smart card interface

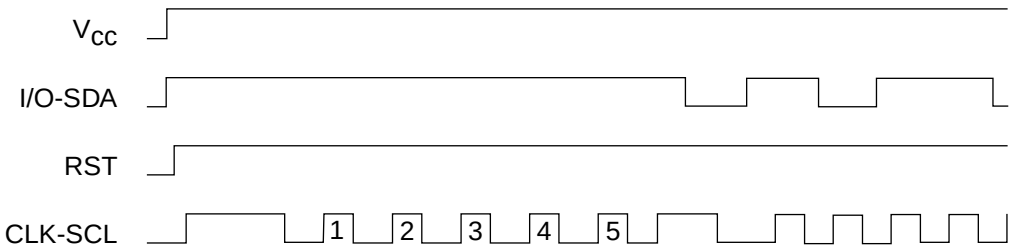
The power-up sequence of CryptoMemory determines what mode it shall operate in. A brief description of each of these modes follows.

7.1 Synchronous Mode for Embedded Applications

The two-wire serial interface is used for fast and efficient communication with logic and controllers. The synchronous mode is the default after powering up V_{CC} due to the internal and/or external pull-up on RST. For embedded applications using CryptoMemory in standard plastic packages RST is not bonded out and this is the only communication protocol.

- Power-up V_{CC}, RST goes high also
- After stable V_{CC}, apply five pulses CLK-SCL
- CLK-SCL and I/O-SDA may then be driven

Figure 7-1. Asynchronous Mode



The asynchronous mode is selected when RST is low on a rising edge of CLK. Once the asynchronous mode has been selected, it is not possible to return to the synchronous mode other than by powering the device off and on again.

7.2 Asynchronous Mode for Smart Card Applications

The asynchronous T=0 protocol defined by ISO 7816-3 is used for compatibility with the industry standard smart card readers. Selecting this mode requires the following power-up sequence, which complies with ISO 7816-3 for a cold reset in smart card applications.

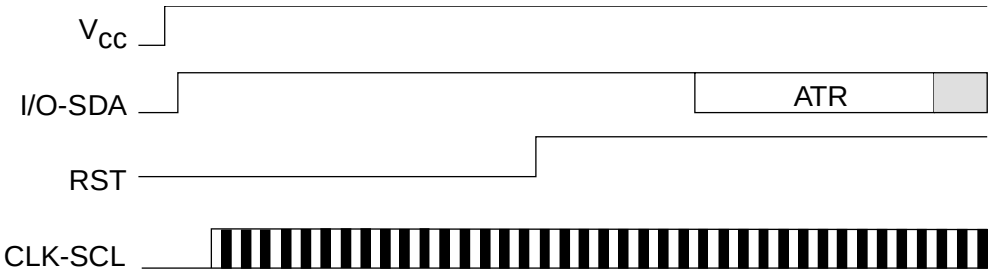
- Power up V_{CC}; RST, IO-SDA and CLK-SCL are low
- Set I/O-SDA in receive mode
- Provide a clock signal to CLK-SCL
- RST goes high after 400 clock cycles

The device will respond with a 64-bit ATR code, including historical bytes to indicate the memory density within the CryptoMemory family. Once the asynchronous mode has been selected, it is not possible to switch to the synchronous mode without powering off the device.

Table 7-1. ATR Codes for Lower Density CryptoMemory

Atmel Device	TS	T0	TA(1)	TB(1)	TD(1)	TA(2)	T1	T2
AT88SC0104CA	$3B	$B2	$11	$00	$10	$80	$00	$01
AT88SC0204CA	$3B	$B2	$11	$00	$10	$80	$00	$02
AT88SC0404CA	$3B	$B2	$11	$00	$10	$80	$00	$04
AT88SC0808CA	$3B	$B2	$11	$00	$10	$80	$00	$08

Figure 7-2. Power Up Sequence for Smart Card Mode



Smart card applications that support the two-wire protocol can also use CryptoMemory in the synchronous mode.

8. Synchronous Protocol

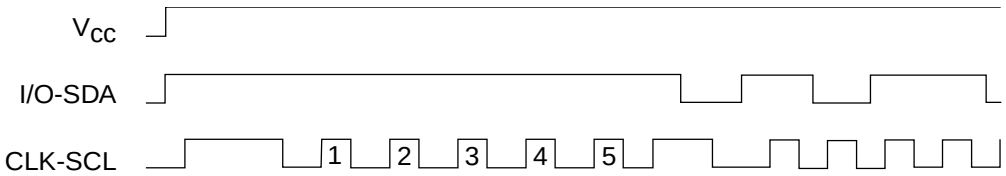
Communication with the CryptoMemory using the synchronous protocol is very similar to communication with AT24Cxxx Serial EEPROM devices using a two-wire protocol (TWI). Basic command structure and timing are the same. However, a significant difference exists when reading the CryptoMemory device that will be described below.

8.1 Start-up Sequence

When first powering up the device, five pulses are required on CLK-SCL for reading of internal registers. This may be accomplished by sending one full command byte to the device. The device will not respond but will then be ready to respond to the next correct command sequence.

- Power-up V_{CC}
- External pull-up resistor pulls I/O-SDA high with V_{CC}
- After stable V_{CC}, 5 pulses are applied to CLK-SCL
- CLK-SCL and I/O-SDA may be driven

Figure 8-1. Start-up Sequence



8.2 Command Set

The command set of CryptoMemory is expanded compared to a Serial EEPROM as the functionality of CryptoMemory exceeds that of a simple memory device. Each instruction sent to the CryptoMemory must have four bytes, Command, Address 1, Address 2, and N. The last byte, N, defines the number of any additional data bytes to be sent or received from the CryptoMemory device. In addition, the random read command is available. It is the only one byte command but must be preceded by an aborted write command in order to set up the read address.

Table 8-1. Atmel CryptoMemory Synchronous Command Set

Command Description		Command	Addr 1	Addr 2	N	Data (N)
Write User Zone	Normal (AT88SC0104CA-AT88SC0808CA)	$B0	addr	addr	N ≤ $10	N bytes
	with Anti-tearing (all devices)	$B0	addr	addr	N ≤ $08	N bytes
Read Read	Random Read	$B1	Details on command usage below			
Read User Zone	Normal Read	$B2	addr	addr	N	N bytes
System Write	Write Config Zone (AT88SC0104CA-AT88SC0808CA)	$B4	$00	addr	N ≤ $10	N bytes
	Write Fuses	$B4	$01	fuse ID	$00	
	Send Checksum	$B4	$02	$00	$02	2 bytes
	Set User Zone	$B4	$03	zone	$00	
	Write Config Zone with Anti-tearing	$B4	$08	addr	N ≤ $08	N bytes
	Set User Zone with Anti-tearing	$B4	$0B	zone	$00	
System Read	Read Conifg Zone	$B6	$00	addr	N	
	Read Fuse Byte	$B6	$01	$00	$01	
	Read Checksum	$B6	$02	$00	$02	
Verify Crypto	Verify Authentication	$B8	$0X	$00	$10	8 random bytes + 8 challenge bytes X= key set (0-3)
	Verify Encryption	$B8	$1X	$00	$10	8 random bytes + 8 challenge bytes X= key set (0-3)
Verify Password	Write Password	$BA	$0X	$00	$03	3 byte password X=password set (0-7)
	Read Password	$BA	$1X	$00	$03	3 byte password X=password set (0-7)

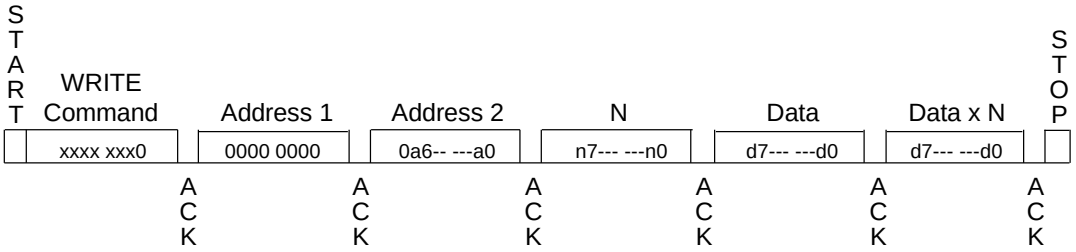
8.3 Command Format

Most CryptoMemory commands have the same format as a two wire interface (TWI) write command characterized by a zero in the LSB of the first byte (device address). The only exception is the random read command that has a one in the LSB of the device address byte.

8.3.1 Write Command Format

The host generates all command and data bytes within a write transaction and sends these to the device. The device acknowledges each byte.

Figure 8-2. CryptoMemory Write Command



The number of bytes CryptoMemory can write within each call of a write command is constrained by the physical page size of the EEPROM memory. The maximum number of bytes to write for each call to the write command is $10. All CryptoMemory write commands comply with the format for the TWI write command.

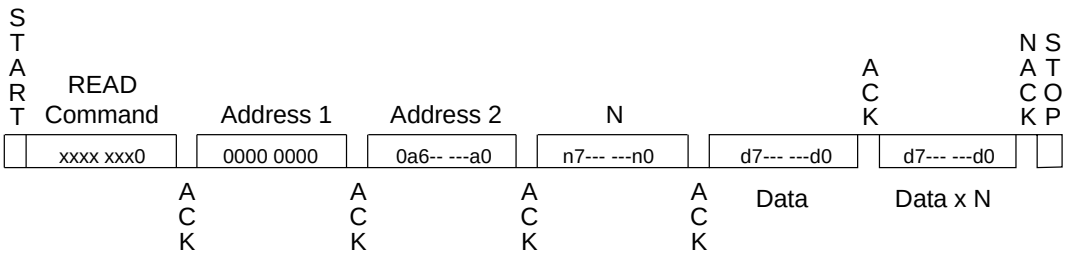
8.3.2 Read Command Format

The CryptoMemory read commands (read user zone, system read and random read) do not comply with the format of the TWI read command. The CryptoMemory read user zone and system read commands closely resemble the TWI write command format by having a zero in the LSB in the device address byte. The random read command closely resembles the format for the TWI read command but requires additional steps to specify the read address.

8.3.2.1 Normal Read: $B2 or $B6 (Read User Zone or System Read)

The CryptoMemory normal read command looks like a TWI write command (LSB of the fist byte = 0) but after the fourth byte of the command the CryptoMemory device will begin to send data back on the bus. The number of bytes sent by CryptoMemory will be equal to the value of N.

Figure 8-3. CryptoMemory Normal Read Command

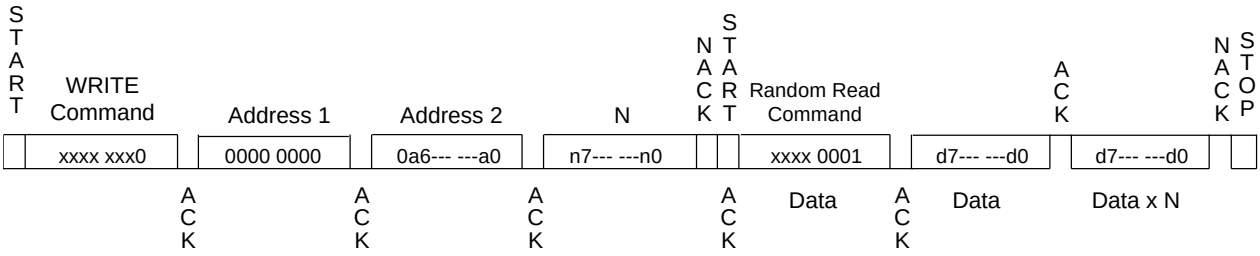


The response of CryptoMemory will cause contention with the host on a standard TWI bus. Typically CryptoMemory cannot be used on a standard TWI bus but requires a modified TWI protocol to account for the unique read command format.

8.3.2.2 Random Read: $B1

The random read command provides the host ability to sequentially clock data from the device starting from a specified address. The host needs to issue a “dummy” write operation in order to specify the start address for the random read. The host does this by clocking in the four bytes of the write command and then follows them with a start condition instead of a data byte. At this point, the device’s internal logic is pointing to the address from the aborted write operation. The host may then issue the random read command byte ($B1) to which the device will respond with the EEPROM byte at the current address location and then increment the internal address by one. The device will continue to sequentially send out bytes as long as the host keeps acknowledging each byte with an ACK. Address “roll over” is from the last byte of the current zone to the first byte of that zone. The host terminates random read by issuing a NACK signal instead of an ACK.

Figure 8-4. Random Read Command



CryptoMemory will NACK the N parameter of the dummy write operation if the write were issued to an illegal write location. The NACK response, however, does not affect the loading of the read address. The random read command works for both configuration and user memory. It is important to implement the CryptoMemory read commands as specified; otherwise CryptoMemory responses will cause contention on the bus with a host using standard TWI protocol.

8.4 Acknowledge Polling

A stop condition ends each command. Certain commands require an acknowledge polling sequence. Acknowledge polling consists of sending a start condition followed by the command byte and determining if the device responds with an ACK. If the device is not ready for the command it will not acknowledge and the sequence must be repeated (start condition, command byte, check for ACK). The ACK indicates the operation has completed but gives no indication of the success or failure of the command.

- **Read Commands:** No ACK polling required
- **Write Commands:** ACK polling required except encrypted write commands. Any command may be used
- **Set commands:** No ACK polling required
- **Verify commands:** ACK polling required with B2 or B6 commands only

The following table lists the specific requirements for ACK polling and the maximum expected delay before the device will ACK indicating readiness for the next command.

Table 8-2. Minimum Delay for ACK Polling for each Command

Command Description		Command	Addr 1	Addr 2	N	ACK Polling CMD	Delay
Write User Zone	Normal	$B0	addr	addr	N	Required, any CMD	5ms
	Normal with Anti-tearing	$B0	addr	addr	N	Required, any CMD	20ms
	Encrypted	$B0	addr	addr	N	No, Send Checksum	0
	Encrypted with Anti-tearing	$B0	addr	addr	N	No, Send Checksum	0
Random Read		$B1	N/A	N/A	N/A	Not Required	
Read User Zone		$B2	addr	addr	N	Not Required	0
System Write	Write Config Zone	$B4	$00	addr	N	Required, any CMD	5ms
	Write Fuses	$B4	$01	fuse ID	$00	Required, any CMD	5ms
	Send Checksum	$B4	$02	$00	$02	Required, any CMD	5ms
	Send Checksum with Anti-tearing	$B4	$02	$00	$02	Required, any CMD	20ms
	Set User Zone	$B4	$03	zone	$00	Not Required	0
	Write Config Zone with Anti-tearing	$B4	$08	addr	N	Required, any CMD	20ms
	Set User Zone with Anti-tearing	$B4	$0B	zone	$00	Not Required	0
System Read	Read Config Zone	$B6	$00	addr	N	Not Required	0
	Read Fuse Byte	$B6	$01	$00	$01	Not Required	0
	Read Checksum	$B6	$02	$00	$02	Note Required	0
Verify Crypto	Verify Authentication	$B8	$0X	$00	$10	Required; B2 or B6 only	10ms
	Verify Encryption	$B8	$1X	$00	$10	Required; B2 or B6 only	10ms
Verify Password	Write Password	$BA	$0X	$00	$03	Required; B2 or B6 only	10ms
	Read Password	$BA	$1X	$00	$03	Required; B2 or B6 only	10ms

Note: Delays are based on operation at 25° C

8.5 Device Addressing

The first nibble of the command byte corresponds to the device address. All CryptoMemory devices will respond to the device address $B. A specific device may be set to respond to another value ($0 to $F) in addition to $B by setting this value in the second nibble of the Device Configuration Register (DCR) in the configuration memory. The DCR is set to $FF at the Atmel factory and thus will respond to device address $B and $F unless the DCR is modified. For a device to respond only to $B the DCR should be set to $B also.

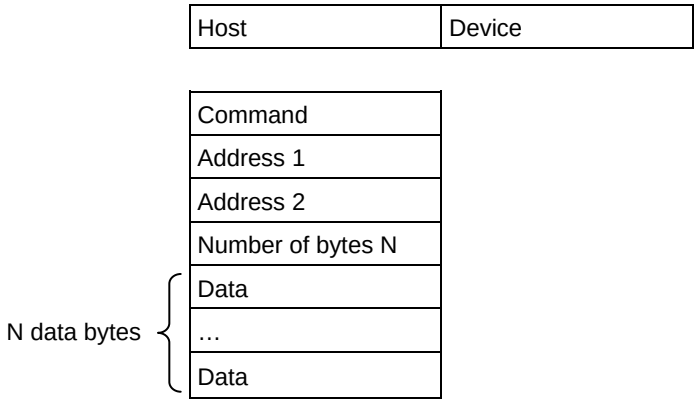
8.6 TWI Command Descriptions

In the following section operations are described in two parts: the instruction is described first from a functional point of view (parameters and data exchanged), after which they are detailed for the synchronous two-wire protocol. In these diagrams, values are shown in binary format with bits to the left transmitted first, i.e. bytes are transmitted most significant bit first.

8.7 Write User Zone: $B0

8.7.1 Functional

Figure 8-5. Write User Zone Command Functional Description

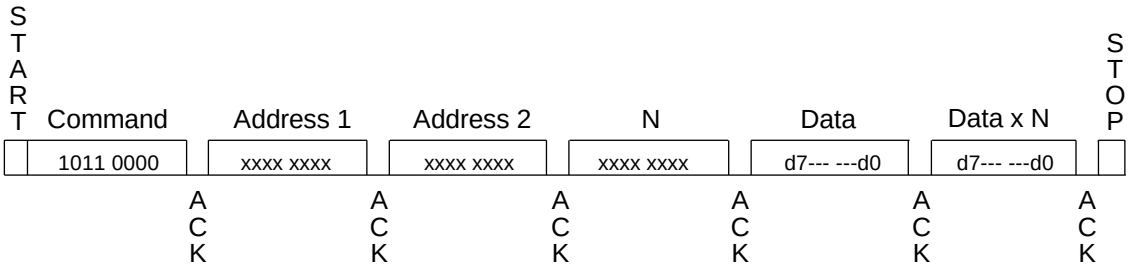


The write user zone command $B0 allows writing of data in the device's currently selected user zone (the procedure for selecting a user zone is described below, see Section 8.10 System Write: $B4).

The data byte address to be written is defined by Address 1 and Address 2 in the command. The value N defines how many bytes are to be written. The maximum number of bytes that may be written is $10 corresponding to the EEPROM page size. In anti-tearing mode the maximum value for N is $08 for all devices. A write in anti-tearing mode is activated with the set user zone with anti-tearing command; all subsequent write operations to the user zone will be in anti-tearing mode. A write may be started in the middle of an EEPROM page but should not extend past the end of the page.

When a write user zone command is sent in authentication mode or encryption mode the data is saved in a buffer until a cryptographic checksum is received. The host must send the checksum it has computed immediately after the write user zone command. If the checksum is valid, CryptoMemory writes the data; if the checksum is incorrect, the data is discarded and the cryptographic engine is reset. If the host is not allowed to write in the zone, the device will not acknowledge the N byte. After this command the host must perform ACK polling.

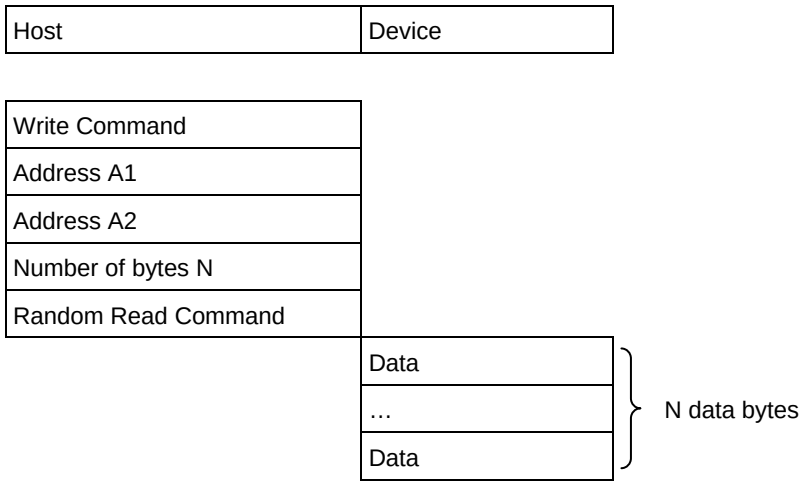
Figure 8-6. Write User Zone Command Structure



8.8 Random Read: $B1

8.8.1 Functional

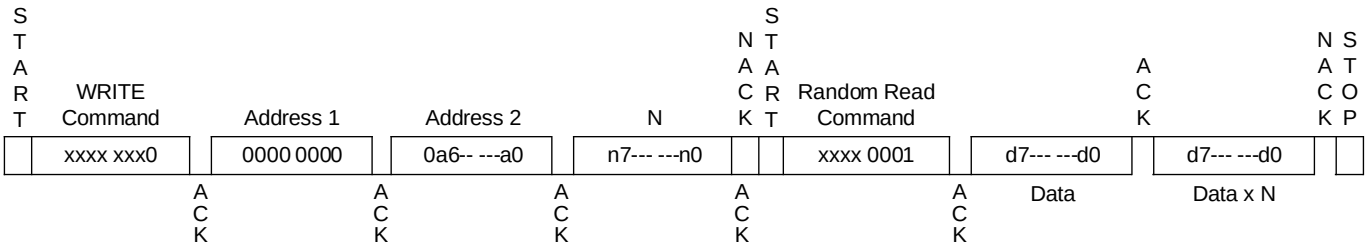
Figure 8-7. Random Read Sequence Description



The Random Read command $B1 allows reading of data from the devices configuration memory or currently selected user zone (The Section 8.10 System Write: $B4 describes how to select a user zone).

The random read command provides the host ability to sequentially clock data from the device starting from a specified address. The host needs to first specify the start address to read from in the memory by executing a “dummy” operation. The host does this by clocking in the four bytes of the write command and then follows them with a start condition instead of a data byte. At this point, the device’s internal logic is pointing to the address from the aborted write operation. The host may then issue the random read command byte ($B1) to which the device will respond with the EEPROM byte at the current address location and then increment the internal address by one. The device will continue to sequentially send out bytes as long as the host keeps acknowledging each byte with an ACK. During this operation the address will “roll over” from the last byte of the current zone to the first byte of the same zone. The host terminates random read by issuing a NACK signal instead of an ACK.

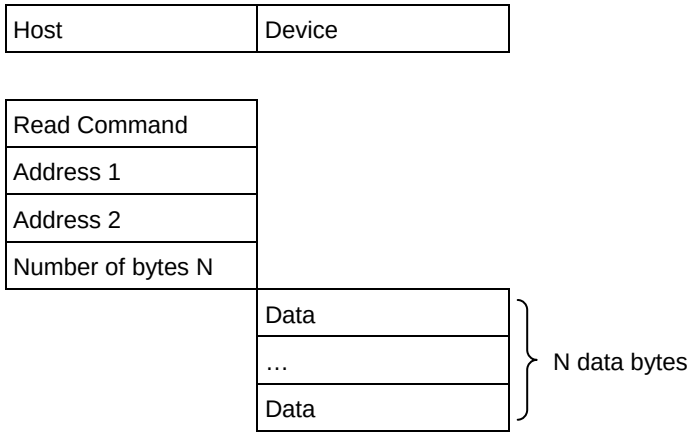
Figure 8-8. Random Read Command Structure



8.9 Read User Zone: $B2

8.9.1 Functional

Figure 8-9. Read User Zone Command Functional Description

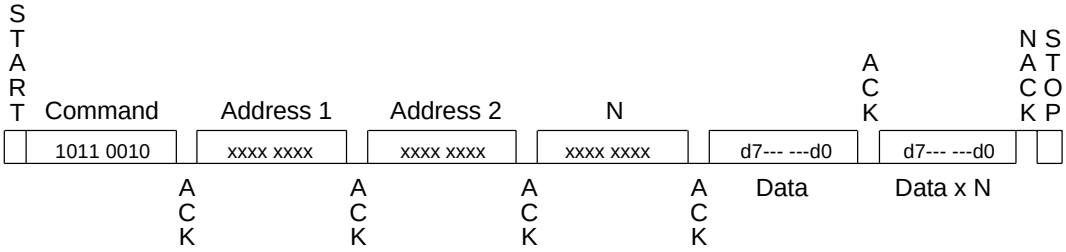


The read user zone command $B2 allows reading of data from the device's currently selected user zone (the procedure for selecting a user zone is described in Section 8.10, System Write: $B4).

The data byte address to be read is defined by Address 1 and Address 2 in the command and is internally incremented following the transmission of each data byte. The value N defines how many bytes CryptoMemory will read, a value of zero will result in 256 bytes read. The host however, may cease clocking the device and end the transmission with a NACK and stop at any time prior to receiving all N bytes. During a read operation the address will "roll over" from the last byte of the current zone, to the first byte of the same zone.

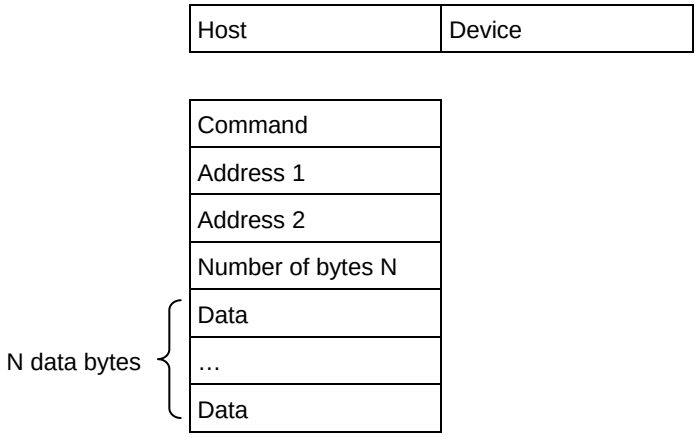
If the host is not allowed to read the zone, the device will not acknowledge the N byte.

Figure 8-10. Read User Zone Command Structure



8.10 System Write: $B4

Figure 8-11. System Write Command Functional Description



The system write command allows writing of configuration data to the device. Depending on the value of the Address 1 parameter, the host may write data in the configuration zone, program the fuses, or set the user zone.

Table 8-3. System Write Command Detail

Command Description	Command	Addr 1	Addr 2	N	Data (N)
Write Config Zone	$B4	$00	addr	N ≤ $10	N bytes
Write Fuses	$B4	$01	fuse ID	$00	
Send Checksum	$B4	$02	$00	$02	2 bytes
Set User Zone	$B4	$03	zone	$00	

8.10.1.1. Write Config Zone

The maximum number of bytes that may be written is $10 and this corresponds to the EEPROM page size. In anti-tearing mode the maximum value for N is $08 for all devices. A write may be started in the middle of an EEPROM page but should not extend past the end of the page. If the address provided is an unauthorized address, the device will not write the requested data. Since access rights vary throughout the configuration zone, the host may provide an authorized starting address, but a number of bytes that causes the device to reach unauthorized data. In this case, the device will prevent the internal write cycle and no bytes will be written in the EEPROM. After this command the host must perform ACK polling.

8.10.1.2 Write Fuses

The fuses may only be "programmed", that is written from '1' to '0'. The write fuses operation is allowed only after successfully presenting the secure code (Write 7 password). The fuses must be blown sequentially: FAB must be blown first, CMA may be blown only if FAB is ‘0’, and PER only if CMA is ‘0’. After this command the host must perform ACK polling. The SEC fuse is blown at the Atmel factory to protect lot history information.

Table 8-4. Fuse Identification

Fuse	Fuse ID
SEC	$07
FAB	$06
CMA	$04
PER	$00

8.10.1.3 Send Checksum

To write data to user zones that require authentication or encryption for write access (ER = “0”, AM[1:0] = “00”, “01”, or “10” in the access register), the host should first carry out the write command $B0. At this point the memory is unchanged and the device is waiting for the host to provide a valid checksum before initiating the write cycle. The host immediately sends the checksum it has computed using the system write command with P1 = $02. Only if the checksum is valid will the device initiate the write cycle. Furthermore, if the device receives an incorrect checksum, it will clear the authentication privilege. After this command the host must perform ACK polling.

8.10.1.4 Set User Zone

Before reading and writing data in the user zones, the host must select a zone with this command. At this time the host chooses whether anti-tearing should be active for this zone.

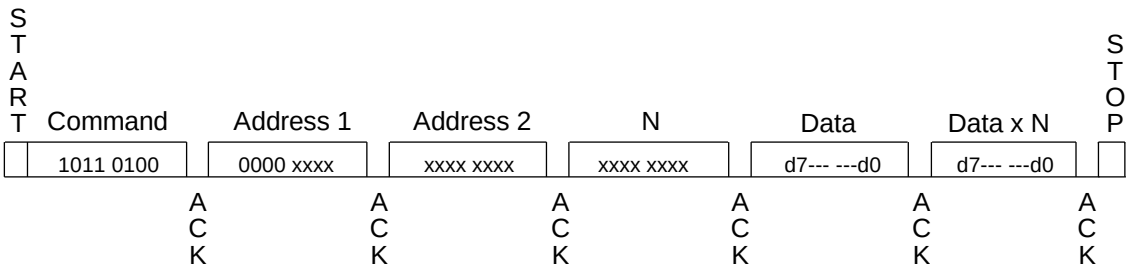
Table 8-5. Anti-tearing

Command Description	Command	Addr 1	Addr 2	N	Data (N)
Write Config Zone with Anti-tearing	$B4	$08	addr	N ≤ $08	N bytes
Set User Zone with Anti-tearing	$B4	$0B	zone	$00	

Data written to the configuration zone may be done with anti-tearing enabled by setting Address 1 to $08 of the write configuration zone command.

To enable anti-tearing for writes to a user zone, a set user zone command is executed with Address 1 set to $0B. All subsequent write user zone commands will be executed with anti-tearing enabled until the next set user zone command. Anti-tearing should be turned off if not required, as it would otherwise cause more write cycles than necessary

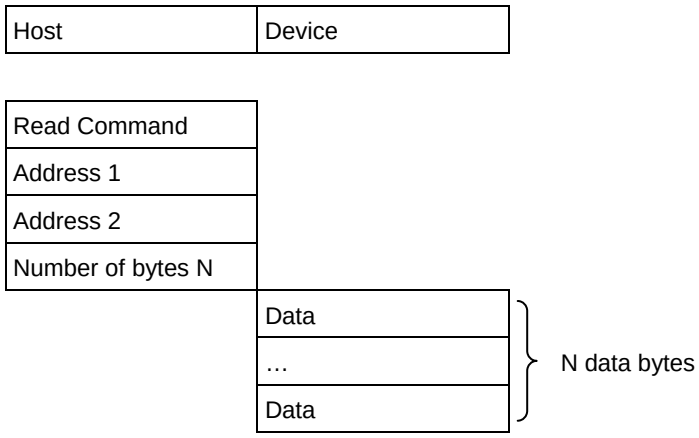
Figure 8-12. System Write Command Detail



8.11 System Read: $B6

8.11.1 Functional

Figure 8-13. System Read Command Functional Description



The system read command allows reading of system data from the device. Depending on the value of Address 1, the host may read the data in the configuration zone, or the fuses.

Table 8-6. Zone Configuration Example

Command Description	Command	Addr 1	Addr 2	N
Read Config Zone	$B6	$00	addr	N
Read Fuse Byte	$B6	$01	$00	$01
Read Checksum	$B6	$02	$00	$02

8.11.2 Read Config Zone

The data byte address to be read is defined by Address 2 in the command and is internally incremented following the transmission of each data byte. The value N defines how many bytes CryptoMemory will read, a value of zero will result in 256 bytes read. If the address provided is an unauthorized address, the device will not ACK the N byte and will not return any data. Since access rights vary throughout the configuration zone, the host may provide an authorized starting address and a number of bytes N that causes the device to reach unauthorized data. In this case the device will transmit the fuse byte (see below) in place of unauthorized bytes.

8.11.3 Read Fuse Byte

Fuse data is returned in the form of a single byte. Bits zero to three represent the fuse states; a value of ‘0’ indicates the fuse has been blown. Bits four to seven are not used as security fuses and are reserved by Atmel.

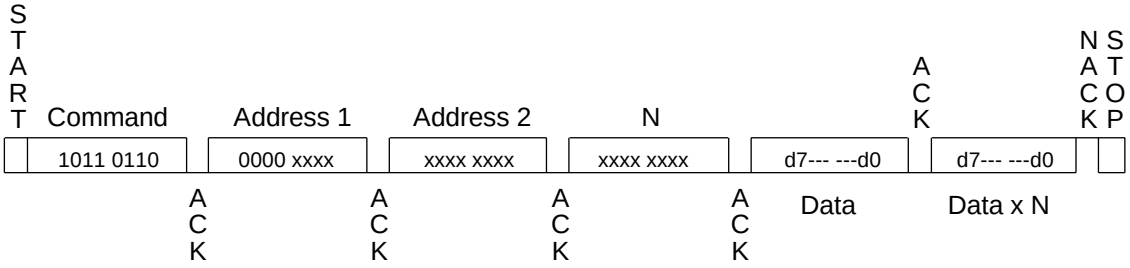
Table 8-7. Fuse Byte Definition

F_7	F_6	F_5	F_4	F_3	F_2	F_1	F_0
resv	resv	resv	resv	SEC	PER	CMA	FAB

8.11.3.1 Read Checksum

The checksum consists of two bytes, and the read checksum command must be sent with parameter N = 2.

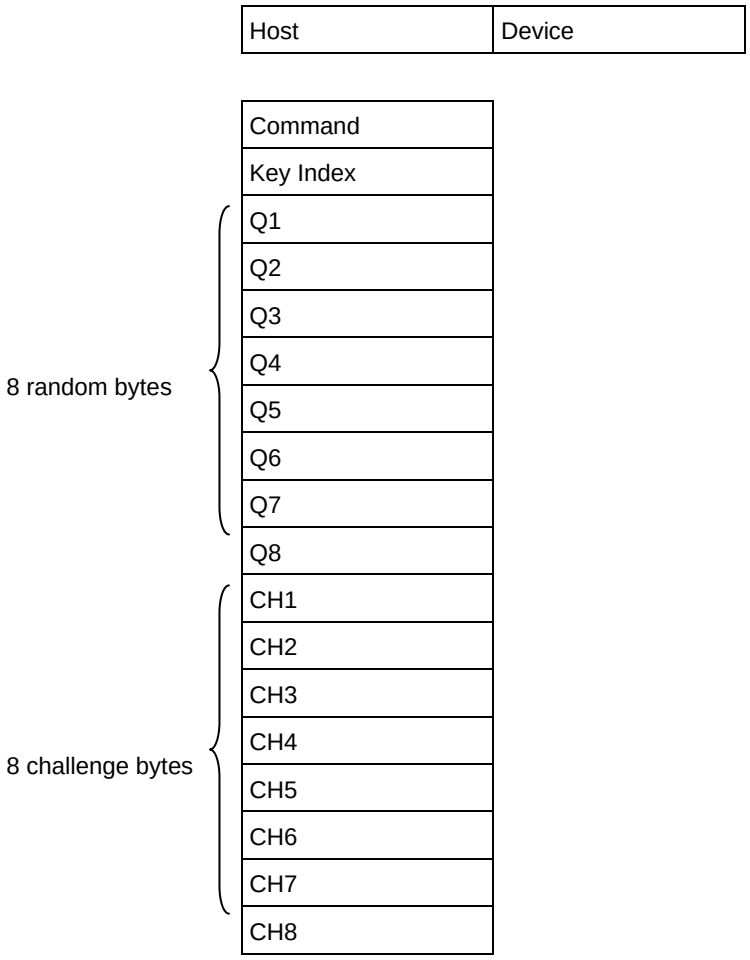
Figure 8-14. System Read



8.12 Verify Crypto: $B8

8.12.1 Functional

Figure 8-15. Verify Crypto Command Functional Description



When the device receives the verify crypto command, it computes a challenge based on the received random number, Q, the internally stored associated cryptogram, C_i, and secret seed, G_i (or session encryption key, S_i). The device also decrements the associated attempts counter. It then compares the computed challenge with the challenge sent by the host. If the challenges match, the device computes and writes a new C_i and S_i. The device utilizes the success or failure information of the authentication process and updates the attempts counter accordingly.

Key index:

b0000_00nn : Secret Seed G_0-G_3

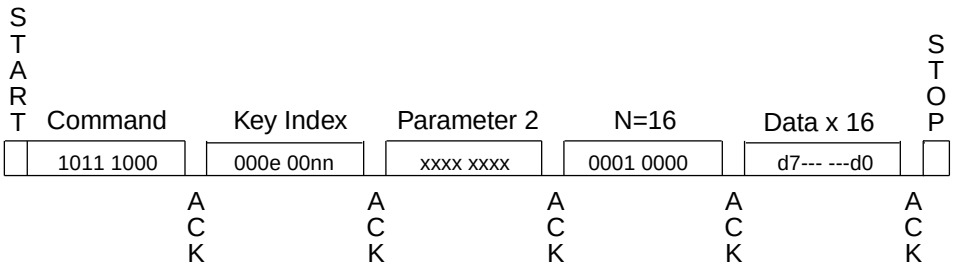
b0001_00nn : Session Encryption Key S_0-S_3

Data :

Q : Host random number, 8 bytes

CH : Host challenge, 8 bytes

Figure 8-16. Verify Crypto

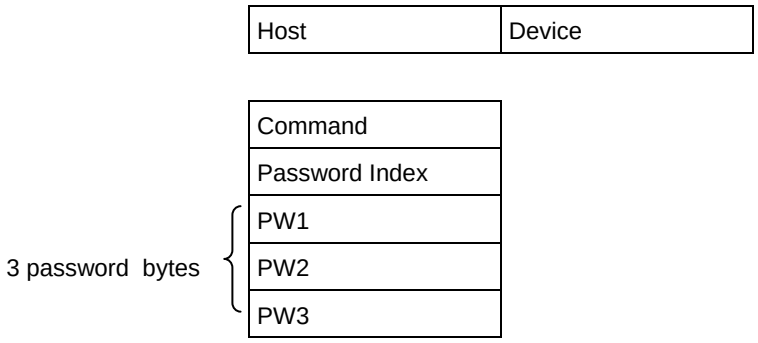


Once the sequence has been carried out, the device requires the host to perform an ACK polling with either the read user zone $B2 command or system read $B6 command. To verify whether the authentication succeeded, the host could either read the associated attempts counter to confirm the value is $FF, or read the post authentication cryptogram from the device and compare with the cryptogram generated when the host computed the challenge bytes.

8.13 Verify Password: $BA

8.13.1 Functional

Figure 8-17. Verify Password Command Functional Description



Read password indices: $10 to $17 for passwords 0, 1, 2, and 7.

Write password indices: $00 to $07 for passwords 0, 1, 2, and 7.

Secure code index: $07 (equivalent to Write Password 7).

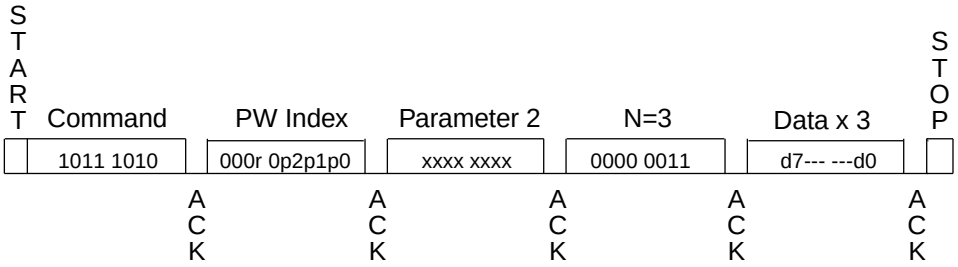
Four password index bits "r" and "ppp" indicate the password to compare:

r = 0 : Write password,

r = 1 : Read password,

$p_2p_1p_0$: Password set number

Figure 8-18. Verify Password



Once the sequence has been carried out, the device requires the host to perform an ACK polling sequence with the system read command $B6. In order to know whether the inserted password was correct, the host can read the corresponding attempts counter and verify the value is zero.

9. Initialization Example

The first step in initializing CryptoMemory is to determine what data is to be stored in the device and what the security settings need to be to protect this data. Once defined, determine the proper settings for CryptoMemory registers and select values for passwords. To initialize the CryptoMemory device, the following sequence is recommended to take place in a secure location to protect sensitive data and passwords that may be loaded into the device.

9.1 Write Data to User Zones

In the default configuration from Atmel, all user zones have free access rights. Writing initial data into the user zones should be done before setting security configurations. Use the set user zone command and write user zone command to write initial data into the user zones. The read user zone command may be used to verify the data written.

9.2 Unlock the Configuration Memory

Before any data can be written to the configuration zone, it must be unlocked by presenting the correct security code (Write 7 password). Use the verify password command with the proper secure code supplied by Atmel to unlock the configuration zone. Use the read config zone command to read back the security code at address $E9 for verification that the configuration zone has been unlocked.

9.3 Write Data to the Configuration Memory

Writing this data is accomplished by performing the write config zone command at the appropriate address location. The read config zone command may be used to verify the data written. As soon as values are written to the registers, keys, and passwords, they become effective in determining the security of the user zones.

9.4 Set Security Fuses

Once all data is written and verified into user zones and the configuration zone the security fuses should be set before the device is released from the secure location used for device initialization. There are three fuses, FAB, CMA and PER that must be set. These three fuses must be set in the order listed (FAB, then CMA, then PER). The write fuse command is used to set each of the three fuses individually. The read fuse command may be used to check the status of all three fuses. Once all fuses have been set the read fuse command should return a value of zero for the second nibble of the fuse byte.

The AT88SC0104CA is used for this example. A small pattern is written into the first two user zones. Security for each of these two user zones and the associated register values are shown in the table below. Simple values for passwords are used.

Table 9-1. CryptoMemory Asynchronous Command Set

User Zone	Data	Security Requirements	Access Register	Password/Key Register
0	Zone 0	None	$FF	$FF
1	Zone 1	Read/Write Password (Set 1)	$7F	$F9
2	Zone 2	Read/Write Authentication (Set 2)	$DF	$BF
3	Zone 3	Read/Write Password (Set 1), Read/Write Authentication (Set 2) with encryption required	$57	$B9

The following shows the two-wire commands sent to the CryptoMemory device for the purpose of initializing the device. The flow is consistent with the steps described above; comments have been added as indicated with an asterisk (*).

*Atmel AT88SC0104CA Initialization Example

```
*WRITE DATA TO USER ZONES
*Set User Zone 0
B4 03 00 00

*Write data = Zone 0 Data
B0 00 00 0B 5A 6F 6E 65 20 30 20 44 61 74 61

*Set User Zone 1
B4 03 01 00

*Write data = Zone 1 Data
B0 00 00 0B 5A 6F 6E 65 20 31 20 44 61 74 61

*Set User Zone 2
B4 03 02 00

*Write data = Zone 2 Data
B0 00 00 0B 5A 6F 6E 65 20 32 20 44 61 74 61

*Set User Zone 3
B4 03 03 00

*Write data = Zone 3 Data
B0 00 00 0B 5A 6F 6E 65 20 33 20 44 61 74 61

*UNLOCK CONFIGURATION ZONE
BA 07 00 03 DD 42 97

*WRITE CODES IN CONFIGURATION ZONE
*Write Card Mfg Code = P001
B4 00 0B 04 50 30 30 31

*Write Identification Number = 00000000012345
B4 00 19 07 00 00 00 00 01 23 45

*Write Issuer Code = STATION 035
B4 00 40 10 53 54 41 54 49 4F 4E 20 30 33 35 00 00 00 00 00

*WRITE REGISTERS IN CONFIGURATION ZONE
*Write Registers AR1/PR1 = 7F F9
B4 00 22 02 7F F9 DF BF 57 B9

*WRITE KEYS IN CONFIGURATION MEMORY
*Write Ci for set 2 = 22222222222222
B4 00 71 07 22 22 22 22 22 22 22

*Write Gc for set 2 = 5B4F9AE4B5098BE7
B4 00 A0 08 5B 4F 9A E4 B5 09 8B E7
*WRITE PASSWORDS IN CONFIGURATION MEMORY

*WRITE PASSWORDS IN CONFIGURATION ZONE
*Write Passwords, read 7 = 10 00 01, write 7 = 11 00 11
B4 00 B9 07 11 00 11 FF 10 00 01

*READ ENTIRE CONFIGURATION ZONE TO VERIFY
B6 00 00 F0
```

```
*Device Response:
3B B2 11 00 10 80 00 01 10 10 FF 50 30 30 31 FF
8C AD A8 10 0A AB FF FF FB 00 00 00 00 01 23 45
FF FF 7F F9 FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
53 54 41 54 49 4F 4E 20 30 33 35 00 00 00 00 00
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF 11 00 11 FF 10 00 01
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

*SET SECURITY FUSES
*Set FAB Fuse
B4 01 06 00

*Set CMA Fuse
B4 01 04 00

*Set PER Fuse
B4 01 00 00

*Read Fuse Byte = X0
B6 01 00 01

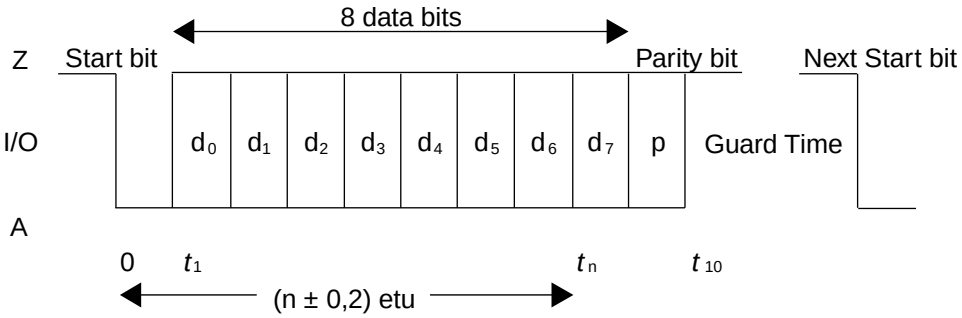
*Device Response:
00
90 00
```

10. Asynchronous T=0 Protocol

10.1 Character Format

The CryptoMemory complies with the asynchronous T=0 protocol defined in ISO 7816-3. The character format is shown in the following figure. Note that the byte is transmitted with the least significant bit first.

Figure 10-1. Character Format



Even parity is used: the parity bit is such that the overall sum of bits in the data byte and the parity bit is an even number. If a transmission error is detected, the receiving device indicates this by applying a low level on the I/O channel during the guard time. This tells the transmitting device to retransmit the byte.

10.2 Command format

The command sequence is as follows:

1. In compliance with ISO 7816-3, the host must send the header consisting of five characters: CLA, INS, P1, P2, P3
   - CLA refers to a class of instructions. This byte isn't tested by the device
   - INS is the instruction byte
   - P1 and P2 are reference bytes, such as a data byte address or password index
   - P3 is the number of data bytes transferred during the command. For outgoing transfers (e.g. read commands), P3 = 0 means that 256 data bytes will be emitted by the card. For incoming commands, P3 = 0 means that no data bytes will be transferred
2. The device replies with a "procedure byte" normally equal to the INS code received. If a problem occurred, then the device will respond with a status word pair SW1-SW2, indicating the end of the command
3. Data transfer (P3 bytes)
4. A final SW1-SW2 sequence gives the status of the device after completion of the command. A normal completion is indicated by SW1-SW2 = $90-$00

Note: For all bytes transmitted by the device or by the host, including header, procedure, status and data bytes, if a parity error is detected, the receiver requests that byte to be sent again (see character format)

10.3 Command Set

Table 10-1. CryptoMemory Asynchronous Command Set

	Command Description		CLA	INS	P1	P2	P3	Data (N)
B0	**Write User Zone**	Normal	$00	$B0	addr	addr	N ≤ $10	N bytes
		with Anti-tearing	$00	$B0	addr	addr	N ≤ $08	N bytes
B2	**Read User Zone**	Read User Zone	$00	$B2	addr	addr	N	
B4	**System Write**	Write Config Zone	$00	$B4	$00	addr	N ≤ $10	N bytes
		Write Fuses	$00	$B4	$01	fuse ID	$00	
		Send Checksum	$00	$B4	$02	$00	$02	2 bytes
		Set User Zone	$00	$B4	$03	zone	$00	
		Write Config Aone w/a-t	$00	$B4	$08	addr	N ≤ $08	N bytes
		Set User Zone w/a-t	$00	$B4	$0B	zone	$00	
B6	**System Read**	Read Config Zone	$00	$B6	$00	addr	N	
		Read Fuse Byte	$00	$B6	$01	$00	$01	
		Read Checksum	$00	$B6	$02	$00	$02	
B8	**Verify Crypto**	Verify Authentication	$00	$B8	$0X	$00	$10	8 random bytes + 8 challenge bytes X=key set (0-3)
		Verify Encryption	$00	$B8	$1X	$00	$10	8 random bytes + 8 challenge bytes X=key set (0-3)
BA	**Verify Password**	Write Password	$00	$BA	$0X	$00	$03	3 byte password X=password set (0, 1,2 or 7)
		Read Password	$00	$BA	$1X	$00	$03	3 byte password X=password set (0, 1,2 or 7)

10.3.1 Status Words

Table 10-2. Asynchronous Mode Return Status Words Definitions

SW1 SW2	Meaning
$62 $00	The memory is unchanged (waiting for checksum)
$67 $00	The length is incorrect
$69 $00	The command is unauthorized
$6B $00	The address is incorrect
$6D $00	The instruction code is invalid
$90 $00	The command was successfully executed

These status words indicate the state of the device at the end of the command. In normal conditions, the device sends the INS byte as the procedure byte, and $90 $00 as the final *status word*. In certain conditions described below, the device may interrupt the command by returning a status word in place of INS as the procedure byte.

$67 $00 is returned as a procedure byte when the number of data bytes to be transferred is incorrect.

$69 $00 is returned after read/write commands as procedure bytes if the host is not allowed to read/write at the address provided. It is also returned after password commands if the maximum number of attempts has been exceeded. The device will return $69 $00 as a final status word in place of $90 $00, if the password presentation failed.

$6B $00 is returned as procedure bytes if the address is incorrect.

$6D $00 is returned as procedure bytes if the INS code received is not supported.

10.3.2 Example: Write EEPROM command

The following illustrates the data exchanges that occur during a write operation of four bytes: $04, $09, $19, and $97 to addresses $02, $03, $04, and $05 in the current user zone.

Start

Host	Device	Val	Note
CLA		**	Class (ignored by CryptoMemory)
INS		$B0	Write instruction
P1		**	Address byte A1 (ignored by 0104C - 1616C)
P2		$02	Address byte A2 = $02
P3		$04	Four data bytes
	INS	$B0	Device responds with INS code
Data		$04	Byte to be written at start address $02
Data		$09	Byte to be written at address $03
Data		$19	Byte to be written at address $04
Data		$97	Byte to be written at address $05
	Write Cycle		~5ms
	SW1	90	Write operation successful
	SW2	$00	

Finish

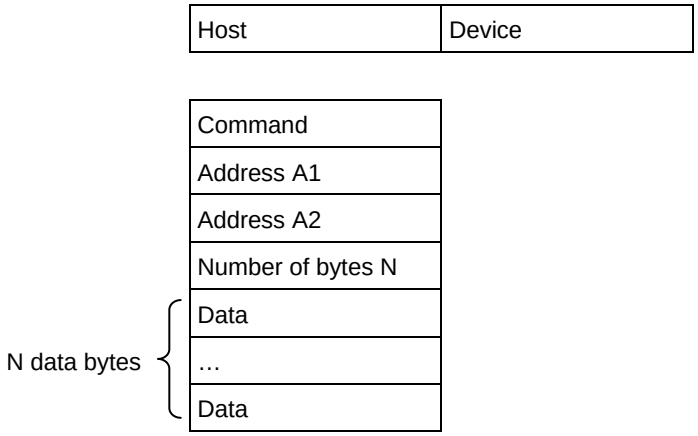
10.4 T=0 Command Descriptions

The command set of CryptoMemory is expanded compared to a Serial EEPROM as the functionality of CryptoMemory exceeds that of a simple memory device. Each instruction sent to the CryptoMemory must have four bytes: Command, Address 1, Address 2, and N. The last byte, N, defines the number of any additional data bytes to be sent or received from the CryptoMemory device.

10.5 Write User Zone: $B0

10.5.1 Functional

Figure 10-2. Write User Zone Command Functional Description



The write user zone command $B0 allows writing of data into the device's currently selected user zone (the procedure for selecting a user zone is described below.

The maximum numbers of bytes that may be written in a single write operation is $10 and corresponds to the EEPROM page size. Each data byte within a page must only be loaded once. In anti-tearing mode the maximum value for N is $08 for all devices. A write in anti-tearing mode is activated with the set user zone command with the anti-tearing option (00 B4 0B zz 00); all subsequent writes to the user zone will be in anti-tearing mode.

"When a write user zone command is sent in authentication mode or encryption mode the data is saved in a buffer until a cryptographic checksum is received. The host must send the checksum it has computed immediately after the write user zone command. If the checksum is valid, CryptoMemory writes the data; if the checksum is incorrect the data is discarded and the cryptographic engine is reset."

If the host is not allowed to write in the zone, the device will return the "Command Unauthorized" code ($69 $00) after it has received the P3 byte.

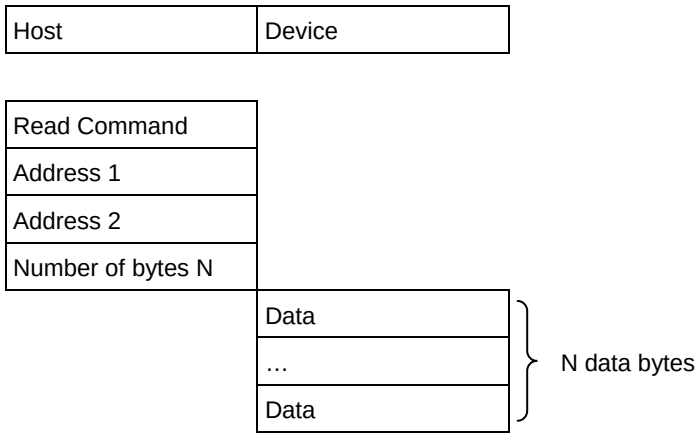
Table 10-3. Write User Zone Command Structure

Command Header					Data Sent		
CLA	INS : Command	P1 : Address 1	P2 : Address 2	P3 : N	Data(1)	...	Data(N)
**	$B0	0000 0000	$0a_6$-- ---a_0	$000n_4$ --- n_0	d_7--- ---d_0	...	d_7--- ---d_0

10.6 Read User Zone: $B2

10.6.1 Functional

Figure 10-3. Read User Zone Command Functional Description



The read user zone command $B2 allows reading of data from the device's currently selected user zone (the procedure for selecting a user zone is described below). The byte address is internally incremented following the transmission of each data byte. During a read operation the address will "roll over" from the last byte of the current zone, to the first byte of the same zone.

If the host is not allowed to read the zone, the device will return the "Command Unauthorized" code ($69 $00) after it has received the header.

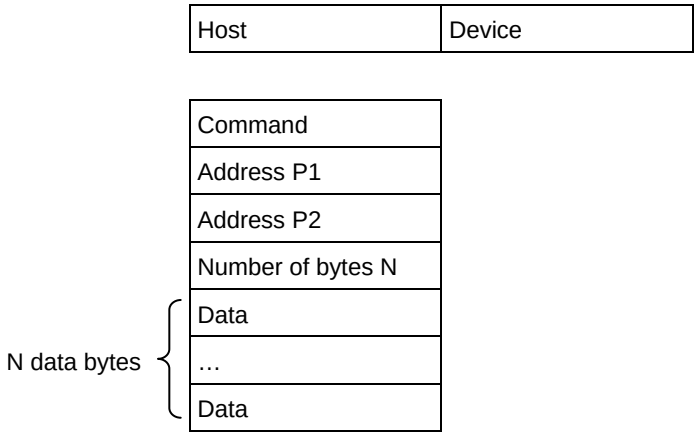
Table 10-4. Read User Zone Command Structure

Command Header					Data Returned		
CLA	INS : Command	P1 : Address 1	P2 : Address 2	P3 : N	Data(1)	...	Data(N)
**	$B2	0000 0000	$0a_6$-- ---a_0	n_7 --- n_0	d_7--- ---d_0	...	d_7--- ---d_0

10.7 System WRITE: $B4

10.7.1 Functional

Figure 10-4. System Write Command Functional Description



The system write command allows writing of system data to the device. Depending on the value of the P1 parameter, the host may write data in the configuration memory, program the fuses, send a checksum or set the user zone.

Table 10-5. System Write Command Detail

Command	CLA	INS	P1	P2	P3	Data(N)
Write Config Zone	$00	$B4	$00	addr	N ≤ $10	N bytes
Write Fuses	$00	$B4	$01	fuse ID	$00	
Send Checksum	$00	$B4	$02	$00	$02	2 bytes
Set User Zone	$00	$B4	$03	zone	$00	

The anti-tearing function is controlled by P1: the host may choose to write in the configuration zone with anti-tearing enabled by setting P1 = $08 instead of $00. Similarly, the host may choose to activate anti-tearing for a user zone by carrying out the *Set* user zone command with P1 = $0B instead of $03. All subsequent write user zone commands are then carried out with anti-tearing enabled until the next set user zone command. Anti-tearing should be turned off if not required, as it would otherwise cause more write cycles than necessary.

Table 10-6. Anti-tearing

Command Description	CLA	INS	P1	P2	P3	Data(N)
Write Config Zone w/ a-t	$00	$B4	$08	addr	N ≤ $08	N bytes
Set User Zone w/ a-t	$00	$B4	$0B	zone	$00	

10.7.2 Write Config Zone

The maximum number of bytes to write for each call of the write command is $16 and corresponds to the EEPROM page size. Each data byte within a page must only be loaded once. In anti-tearing mode the maximum value for N is $08 for all devices.

If the address provided at P2 is an unauthorized address, the device will return the "Command Unauthorized" code ($69 $00) after it has received the header. Since access rights vary throughout the configuration zone, the host may provide an authorized starting address, but a number of bytes that causes the device to reach unauthorized data. In this case, the device will prevent the internal write cycle and no bytes will be written in the EEPROM. At the end of the command the "Command Unauthorized" code ($69 $00) will be returned instead of $90 $00 to indicate that no write cycle occurred.

10.7.3 Write Fuses

Table 10-7. Fuse Bytes

Fuse	Fuse ID
SEC	$07
FAB	$06
CMA	$04
PER	$00

The fuses may only be "programmed", that is written from '1' to '0'. The write fuses operation is only allowed after successfully presenting the secure code (Write 7 password). The fuses must be blown sequentially: FAB must be blown first, CMA may be blown only if FAB is ‘0’, and PER only if CMA is ‘0’. The SEC fuse is blown at the Atmel factory to protect lot history information.

10.7.4 Send Checksum

To write data to user zones that require authentication or encryption for write access (ER = “0”, AM [1:0] = “00”, “01”, or “10” in the access register), the host should first carry out the write command $B0, after which the device will return a special status word: $62 $00. At this point the memory is unchanged and the device is waiting for the host to provide a valid checksum before initiating the write cycle. The host immediately sends the checksum it has computed using the system write command with P1 = $02. Only if the checksum is valid will the device initiate the write cycle. Furthermore, if the device receives an incorrect checksum, it will clear the authentication privilege. After this command the host must perform ACK polling.

10.7.5 Set User Zone

Before reading and writing data in the user zones, the host should select a zone with this command. At this time the host may choose whether anti-tearing should be active for this zone.

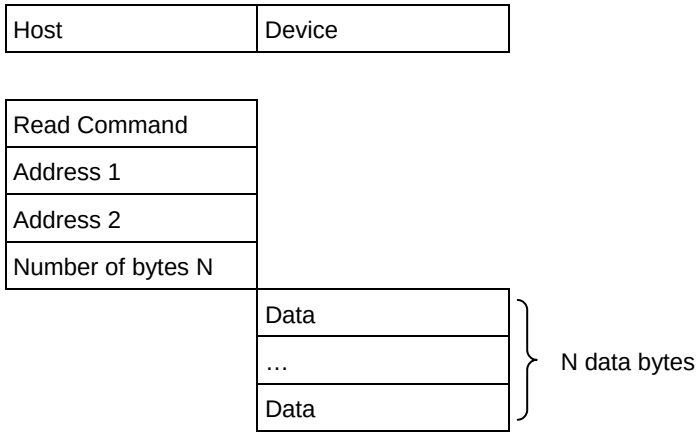
Table 10-8. System Write Command Structure

Command Header					Data Sent		
CLA	INS : Command	P1	P2	P3	Data(1)	...	Data(N)
**	$B4	p_7 --- p_0	p_7 --- p_0	n_7 --- n_0	d_7--- ---d_0	...	d_7--- ---d_0

10.8 System READ: $B6

10.8.1 Functional

Figure 10-5. System READ Command Functional Description



The System Read command allows reading of the system data from the device. Depending on the value of the P1 parameter, the host may read the data in the configuration memory, the fuses, or a checksum.

Table 10-9. System READ Command Detail

Command	CLA	INS	P1	P2	P3	Data (N)
Read Config Zone	$00	$B6	$00	addr	N	
Read Fuse Byte	$00	$B6	$01	$00	$01	
Read Checksum	$00	$B6	$02	$00	$02	

10.8.2 Read Config Zone

To read 256 bytes, the host should set N = $00. This is true for any outgoing command, and is defined by ISO 7816-3. If the address provided at P2 is an unauthorized address, the device will return the "Command Unauthorized" code ($69 $00) after it has received the header. Since access rights vary throughout the configuration zone, the host may provide an authorized starting address, but a number of bytes N that causes the device to reach unauthorized data. In this case, the device will transmit the authorized bytes, but unauthorized bytes will be replaced by the "fuse byte" (see below). At the end of this command the "Command Unauthorized" code ($69 $00) will be returned instead of $90 $00 to indicate that some of the bytes returned are not valid

10.8.3 Read Fuse Byte

Fuse data is returned in the form of a single byte. Bits 0 to 3 represent the fuse states; a value of ‘0’ indicates the fuse has been blown. Bits 4 to 7 are not used as security fuses and are reserved by Atmel.

Table 10-10. Fuse Byte Definition

F_7	F_6	F_5	F_4	F_3	F_2	F_1	F_0
resv	resv	resv	resv	SEC	PER	CMA	FAB

10.8.4 System Read Command Structure

Table 10-11. System Read

Command Header					Data Returned		
CLA	INS : Command	P1	P2	P3	Data(1)	...	Data(N)
**	$B6	p_7 --- p_0	p_7 --- p_0	n_7 --- n_0	d_7--- ---d_0	...	d_7--- ---d_0

10.8.5 Read Checksum

The checksum consists of two bytes, and the read checksum command must be sent with parameter P3 = 2.

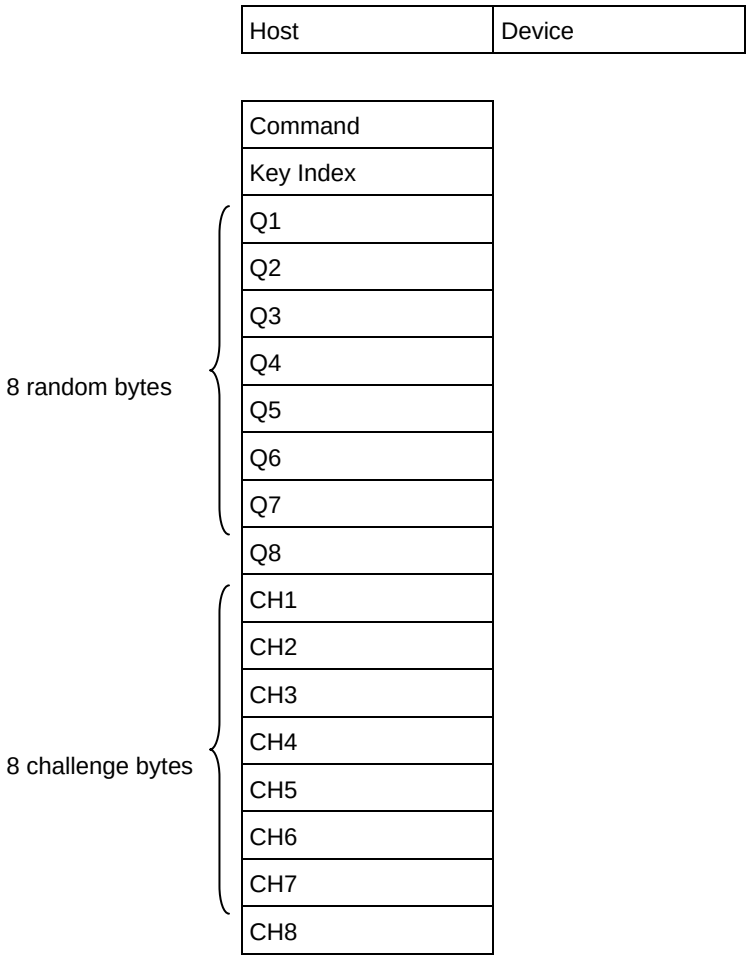
Table 10-12. System READ

System Read					Data Returned		
CLA	INS : Command	P1	P2	P3	Data(1)	...	Data(N)
**	$B6	p_7 --- p_0	p_7 --- p_0	n_7 --- n_0	d_7--- ---d_0	...	d_7--- ---d_0

10.9 Verify CRYPTO: $B8

10.9.1 Functional

Figure 10-6. Verify Crypto Command Functional Description



When the device receives the verify crypto command, it computes a challenge based on the received random number, Q, the internally stored associated cryptogram, C_i, and secret seed, G_i (or session encryption key, S_i). The device also increments the associated attempts counter. It then compares the computed challenge with the challenge sent by the host. If the challenges match, the device computes and writes a new C_i and S_i. The device utilizes the success or failure information of the authentication process and updates the authentication attempts counter accordingly.

Key index:

b0000_00nn : Secret Seed G_0-G_3

b0001_00nn : Session Encryption Key S_0-S_3

Data :

Q : Host random number, 8 bytes

CH : Host challenge, 8 bytes

Table 10-13. Verify Crypto

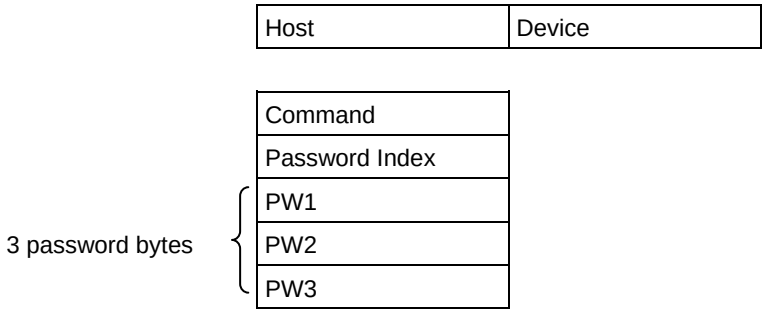
Verify Crypto					Data Sent			
CLA	INS : Command	P1	P2	P3	Q1	Q8	CH1	CH8
**	$B8	000e 00nn	**	$10	d_7--- ---d_0	d_{63}--- ---d_{56}	d_7--- ---d_0	d_{63}--- ---d_{56}

The device increments the associated attempts counter each time prior to verifying the challenge, to prevent attacks. If the authentication succeeds, the device memorizes this success, clears the attempts counter and returns $90 $00. If the authentication fails, the device simply returns $69 $00. If the maximum number of trials has been exceeded, the device will return $69 $00 instead of the INS code, after receiving the header, to indicate the command is unauthorized.

10.10 Verify Password: $BA

10.10.1 Functional

Figure 10-7. Verify Password Command Functional Description



Read password indices: $10 to $17 for passwords 0, 1, 2, and 7.

Write password indices: $00 to $07 for passwords 0, 1, 2, and 7.

Secure code index: $07 (equivalent to Write Password 7).

Four password index bits "r" and "ppp" indicate the password to compare:

r = 0: Write password,

r = 1: Read password,

$p_2p_1p_0$: Password set number

Table 10-14. Verify Password Command Structure

Command Structure					Data Sent		
CLA	INS : Command	P1	P2	P3	PW1	PW2	PW3
**	$BA	000r $0p_2p_1p_0$	**	$30	d_7--- ---d_0	d_{15}--- ---d_8	d_{23}--- ---d_{16}

If the maximum number of trials has been exceeded, the device will return $69 $00 instead of the INS code, after receiving the header, to indicate the command is unauthorized. The device increments the associated attempts count before verifying the password, to prevent attacks. If the password is correct, the device memorizes this success, clears the attempts count and returns $90 $00. If the password is wrong, the device simply returns $69 $00 after incrementing the attempts count. The Write 7 password is also known as the secure code and must be properly presented before access to the configuration zone is granted when personalizing the device.

11. Initialization Example

The first step in initializing CryptoMemory is to determine what data is to be stored in the device and what the security settings need to be to protect this data. Once defined, determine the proper settings for CryptoMemory registers and select values for passwords. To initialize the CryptoMemory device, the following sequence is recommended to take place in a secure location to protect sensitive data and passwords that may be loaded into the device.

11.1 Write Data to User Zones

In the default configuration from Atmel, all user zones have free access rights. Writing initial data into the user zones should be done before setting security configurations. Use the set user zone command and write user zone command to write initial data into the user zones. The read user zone command may be used to verify the data written.

11.2 Unlock the Configuration Memory

Before any data can be written to the configuration zone, it must be unlocked by presenting the correct security code (Write 7 Password). Use the verify password command with the proper secure code supplied by Atmel to unlock the configuration zone. Use the read config zone command to read back the security code at address $E9 for verification that the configuration zone has been unlocked.

11.3 Write Data to the Configuration Memory

Writing this data is accomplished by performing the write config zone command at the appropriate address location. The read config zone command may be used to verify the data written. As soon as values are written to the registers, keys, and passwords, they become effective in determining the security of the user zones.

11.4 Set Security Fuses

Once all data is written and verified into user zones and the configuration zone the security fuses should be set before the device is released from the secure location used for device initialization. There are three fuses, FAB, CMA, and PER that must be set. These three fuses must be set in the order listed (FAB, then CMA, then PER). The write fuse command is used to set each of the three fuses individually. The read fuse command may be used to check the status of all three fuses. Once all fuses have been set the read fuse command should return a value of zero for the second nibble of the fuse byte.

The AT88SC0104CA is used for this example. A small pattern is written into the first two user zones. Security for each of these two user zones and the associated register values are shown in the table below. Simple values for passwords are used.

Table 11-1. Zone Configuration Example

User Zone	Data	Security Requirements	Access Register	Password/Key Register
0	Zone 0	None	$FF	$FF
1	Zone 1	Read/Write Password (Set 1)	$7F	$F9
2	Zone 2	Read/Write Authentication (Set 2)	$DF	$BF
3	Zone 3	Read/Write Password (Set 1), Read/Write Authentication (Set 1) with Encryption Required	$57	$B9

The following shows the TPDU commands sent to the CryptoMemory device for the purpose of initializing the device. The flow is consistent with the steps described above; comments have been added as indicated with an asterisk (*).

*Atmel AT88SC0104CA Initialization Example

```
*WRITE DATA TO USER ZONES
*Set User Zone 0
00 B4 03 00 00

*Write data = Zone 0 Data
00 B0 00 00 0B 5A 6F 6E 65 20 30 20 44 61 74 61

*Set User Zone 1
00 B4 03 01 00

*Write data = Zone 1 Data
00 B0 00 00 0B 5A 6F 6E 65 20 31 20 44 61 74 61

*Set User Zone 2
B4 03 02 00

*Write data = Zone 2 Data
B0 00 00 0B 5A 6F 6E 65 20 32 20 44 61 74 61

*Set User Zone 3
B4 03 03 00

*Write data = Zone 3 Data
B0 00 00 0B 5A 6F 6E 65 20 33 20 44 61 74 61

*UNLOCK CONFIGURATION ZONE
00 BA 07 00 03 DD 42 97

*WRITE CODES IN CONFIGURATION ZONE
*Write Card Mfg Code = P001
00 B4 00 0B 04 50 30 30 31

*Write Identification Number = 00000000012345
00 B4 00 19 07 00 00 00 00 01 23 45

*Write Issuer Code = STATION 035
00 B4 00 40 10 53 54 41 54 49 4F 4E 20 30 33 35 00 00 00 00 00

*WRITE REGISTERS IN CONFIGURATION ZONE
*Write Registers AR1/PR1 = 7F F9
00 B4 00 22 02 7F F9 DF BF 57 B9

*WRITE KEYS IN CONFIGURATION MEMORY
*Write Ci for set 2 = 22222222222222
B4 00 71 07 22 22 22 22 22 22 22

*Write Gc for set 2 = 5B4F9AE4B5098BE7
B4 00 A0 08 5B 4F 9A E4 B5 09 8B E7
*WRITE PASSWORDS IN CONFIGURATION MEMORY

*WRITE PASSWORDS IN CONFIGURATION ZONE
*Write Passwords, read 7 = 10 00 01, write 7 = 11 00 11
00 B4 00 B9 07 11 00 11 FF 10 00 01

*READ ENTIRE CONFIGURATION ZONE TO VERIFY
00 B6 00 00 F0
```

```
*Device Response:
3B B2 11 00 10 80 00 01 10 10 FF 50 30 30 31 FF
8C AD A8 10 0A AB FF FF FB 00 00 00 00 01 23 45
FF FF 7F F9 FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
53 54 41 54 49 4F 4E 20 30 33 35 00 00 00 00 00
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF 11 00 11 FF 10 00 01
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

*SET SECURITY FUSES
*Set FAB Fuse
00 B4 01 06 00

*Set CMA Fuse
00 B4 01 04 00

*Set PER Fuse
00 B4 01 00 00

*Read Fuse Byte = X0
00 B6 01 00 01

*Device Response:
00
90 00
```

12. Absolute Maximum Ratings*

Operating temperature	−40°C to +85°C
Storage temperature	−65°C to + 150°C
Voltage on any pin with respect to ground	− 0.7 to V_{CC} +0.7V
Maximum operating voltage	6.0V
DC output current	5.0mA

*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 condition beyond those indicated in the operational sections of this specification is not implied. Exposure to absolute maximum rating conditions for extended periods of time may affect device reliability.

12.1 DC and AC Characteristics

Table 12-1. DC Characteristics

Symbol	Parameter	Test Condition	Min	Typ	Max	Units
V_{CC}	Supply Voltage		2.7		3.6	V
I_{CC}	Supply Current (V_{CC} = 3.3V)	Async Read at 3.57MHz			5	mA
I_{CC}	Supply Current (V_{CC} = 3.3V)	Async Write at 3.57MHz			5	mA
I_{CC}	Supply Current (V_{CC} = 3.3V)	Synch Read at 1MHz			5	mA
I_{CC}	Supply Current (V_{CC} = 3.3V)	Synch Write at 1MHz			5	mA
I_{SB}	Standby Current (V_{CC} = 3.3V)	V_{IN} = V_{CC} or GND			100	µA
V_{IL}	SDA/IO 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}(3)	SDA/IO Input High Voltage		V_{CC} x 0.7		5.5	V
V_{IH}(3)	SCL/CLK Input High Voltage		V_{CC} x 0.7		5.5	V
V_{IH}(3)	RST Input High Voltage		V_{CC} x 0.7		5.5	V
I_{IL}	SDA/IO Input Low Current	0 < V_{IL} < V_{CC} x 0.15			15	µA
I_{IL}	SCL/CLK Input Low Current	0 < V_{IL} < V_{CC} x 0.15			15	µA
I_{IL}	RST Input Low Current	0 < V_{IL} < V_{CC} x 0.15			50	µA
I_{IH}	SDA/IO Input High Current	V_{CC} x 0.7 < V_{IH} < V_{CC}			20	µA
I_{IH}	SCL/CLK Input High Current	V_{CC} x 0.7 < V_{IH} < V_{CC}			100	µA
I_{IH}	RST Input High Voltage	V_{CC} x 0.7 < V_{IH} < V_{CC}			150	µA
V_{OH}	SDA/IO Output High Voltage	20K Ω external pull-up	V_{CC} x 0.7		V_{CC}	V
V_{OL}	SDA/IO Output Low Voltage	I_{OL} = 1mA	0		V_{CC} x 0.15	V
I_{OH}	SDA/IO Output High Current	V_{OH}			20	µA
I_{OL}	SDA/IO Output High Current	V_{OL}			10	µA

Notes:
1. Applicable over recommended operating voltage range from V_{CC} = 2.7V to 3.6V
2. T_{AC} = -40°C to +85°C (unless otherwise noted)
3. To prevent latch up conditions from occurring during power up of the AT88SCXXXXCA, V_{CC} must be turned on before applying V_{IH}. For powering down, V_{IH} must be removed before turning V_{CC} off

Table 12-2. AC Characteristics

Symbol	Parameter	Min	Max	Units
f_{CLK}	Async Clock Frequency	1	4	MHZ
f_{CLK}	Synch Clock Frequency	0	1	MHZ
	Clock Duty cycle	40	60	%
t_R	Rise Time - SDA/IO, RST		1	µS
t_F	Fall Time - SDA/IO, RST		1	µS
t_R	Rise Time – SCL/CLK		9% x period	µS
t_F	Fall Time – SCL/CLK		9% x period	µS
t_{AA}	Clock Low to Data Out Valid		250	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

Notes: 1. Applicable over recommended operating range from V_{CC} = 2.7V to 3.6V
2. T_{AC} = -40°C to +85°C, CL = 30pF (unless otherwise noted)

12.2 Timing Diagrams for Synchronous Communications

Figure 12-1. Bus Timing

SCL: Serial Clock, SDA: Serial Data I/O

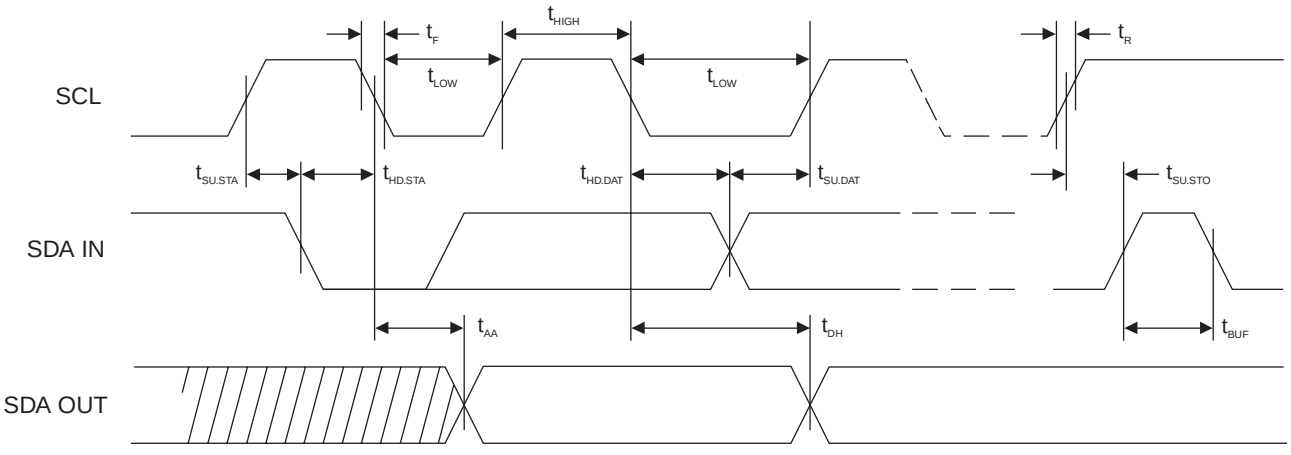
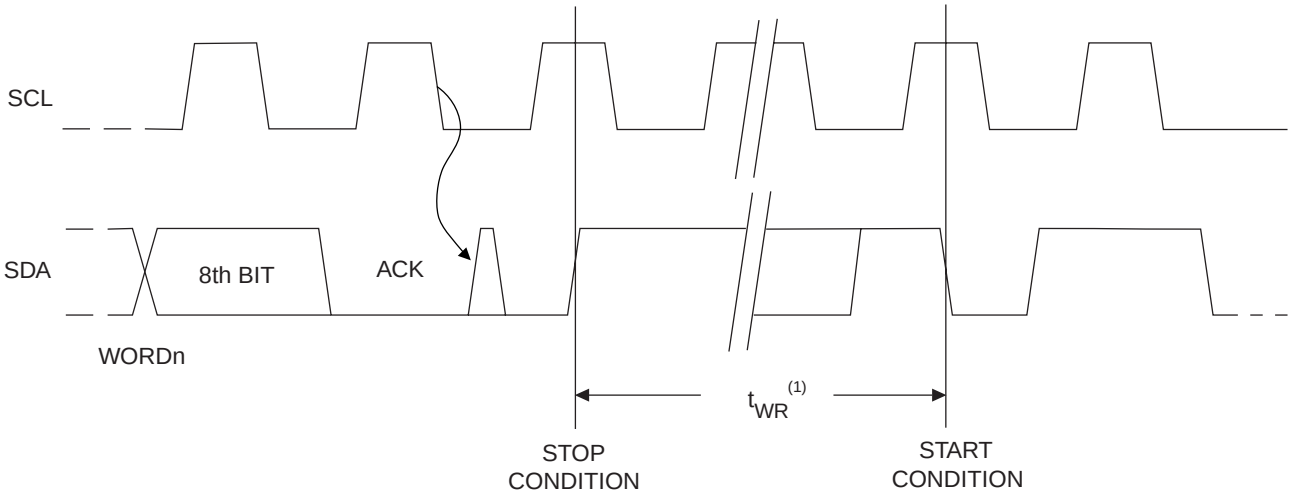


Figure 12-2. Write Cycle Timing

SCL: Serial Clock, SDA: Serial Data I/O



Note: The write cycle time t_{WR} is the time from a valid stop condition of a write sequence to the end of the internal clear/write cycle

Figure 12-3. Data Validity

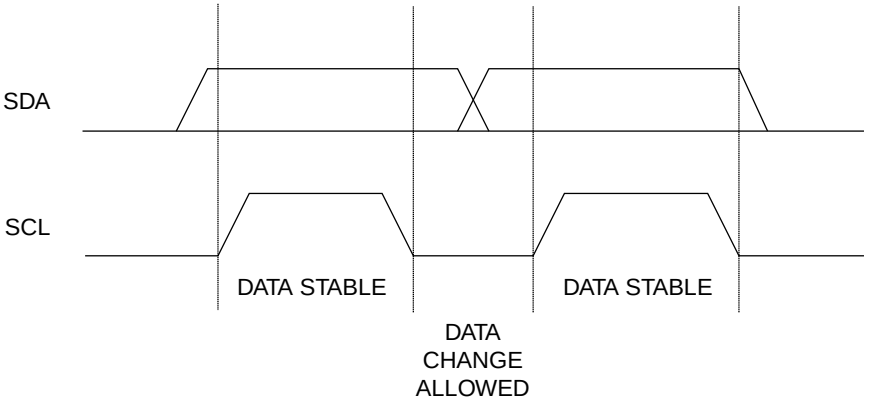


Figure 12-4. Start and Stop Definition

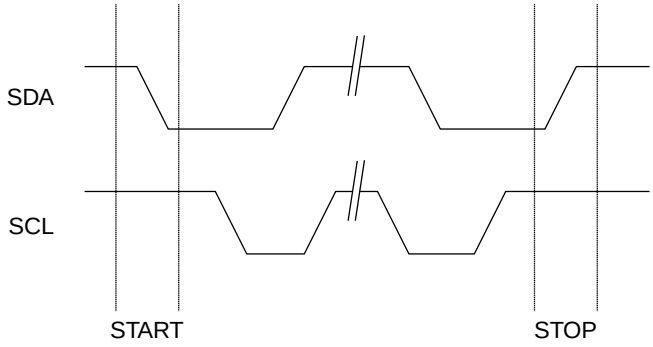
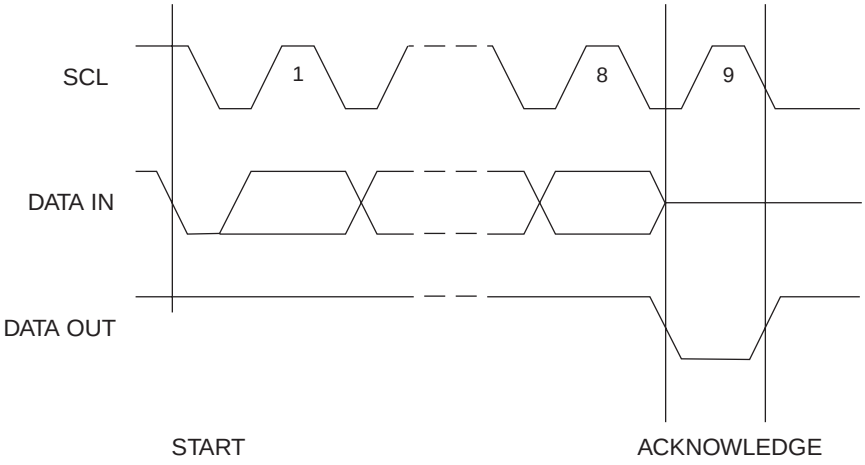


Figure 12-5. Output Acknowledge



13. POR and Tamper Conditions

The CryptoMemory device family incorporates several tamper detection circuits to prohibit operation outside the limits of reliable circuit operation.

13.1 Power On Reset (POR) Delay

Anytime the device is reset either on initial power up or by a tamper detection circuit, there is a time delay from when normal conditions are restored to when the device may be operated. During this reset sequence all security flags within the device are reset to their initial values..

13.2 Tamper Detection

CryptoMemory contains tamper detection sensors to detect operation outside of specified limits. These sensors monitor the internal supply voltage and clock frequency. An additional sensor detects high intensity light attacks. The die is disabled and will not function when tampering is detected.

14. Ordering Information

Atmel Ordering Code	Package	Voltage Range	Temperature Range
AT88SCxxxxCA-MJ	M2 – J Module - ISO	2.7V–5.5V	Commercial (0°C–70°C)
AT88SCxxxxCA-MP	M2 – P Module - ISO		
AT88SCxxxxCA-MJTG	M2 – J Module - TWI		
AT88SCxxxxCA-MPTG	M2 – P Module – TWI		
AT88SCxxxxCA-PU	8P3	2.7V–5.5V	Green compliant (exceeds RoHS) / Industrial (−40°C–85°C)
AT88SCxxxxCA-SH	8S1		
AT88SCxxxxCA-TH	8X	2.7V–5.5V	Industrial (−40°C–85°C)
AT88SCxxxxCA-Y6H-T	8MA2		
AT88SCxxxxCA-WI	7 mil wafer		

Note: Ordering Codes are valid for all devices covered by this datasheet. (See P.1 for a complete list)

Package Type[1] [2]	Description
M2 – J Module : ISO or TWI	M2 ISO 7816 smart card module
M2 – P Module : ISO or TWI	M2 ISO 7816 smart card module with Atmel® logo
8P3	8-lead, 0.300” wide, Plastic Dual Inline (PDIP)
8S1	8-lead, 0.150” wide, Plastic Gull Wing Small Outline (JEDEC SOIC)
8X	8-lead, 4.4mm body, Plastic Thin Shrink Small Outline (TSSOP)
8MA2	8-lead, 2.0x3.0mm, 0.50mm pitch, Ultra Thin Mini-Map, Dual No Lead (DFN), (MLP 2x3)

Note:
1. Formal drawings may be obtained from an Atmel sales office
2. Both the J and P module packages are used for either ISO (T=0 / 2-wire mode) or TWI (2-wire mode only)

Appendix A. Errata

A.1 Send Checksum Command in TWI Mode

"When a write user zone command is sent in authentication mode or encryption mode the data is saved in a buffer until a cryptographic checksum is received. The host must send the checksum it has computed immediately after the write user zone command. If the checksum is valid, CryptoMemory writes the data; if the checksum is incorrect the data is discarded and the cryptographic engine is reset.

If there is any activity on the TWI bus between the write user zone command and the send checksum command the EEPROM write may be aborted and the data in the user zone will be unchanged."

Appendix B. Revision History

Doc. Rev.	Date	Comments
8664E	12/2011	Update template Add ordering information
8664D	06/2011	Table 8-1, Atmel CryptoMemory Synchronous Command Set Correct value in “Verify Password, Addr 1, from $0X to $1X
8664C	01/2010	Convert to MS Word
8664B	08/2009	Update document
8664A	05/2009	Initial document release



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

Atmel Asia Limited
Unit 01-5 & 16, 19F
BEA Tower, Millennium City 5
418 Kwun Tong Road
Kwun Tong, Kowloon
HONG KONG
Tel: (+852) 2245-6100
Fax: (+852) 2722-1369

Atmel Munich GmbH
Business Campus
Parkring 4
D-85748 Garching b. Munich
GERMANY
Tel: (+49) 89-31970-0
Fax: (+49) 89-3194621

Atmel Japan G.K.
16F Shin-Osaki Kangyo Building
1-6-4 Osaki
Shinagawa-ku, Tokyo 141-0032
JAPAN
Tel: (+81)(3) 6417-0300
Fax: (+81)(3) 6417-0370

© 2011 Atmel Corporation. All rights reserved. / Rev.: **8664E–CRYPTO–12/11**

Atmel®, logo and combinations thereof, 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.