Features

- A Family of 9 Devices with User Memories from 1-Kbit to 256-Kbit
- EEPROM User Memory
  - Four, Eight or Sixteen Zones
  - Self-timed Write Cycles
  - Single-Byte or Multiple-Byte Page-Write Modes
  - Programmable Access Rights for Each Zone
- 2-Kbit Configuration Memory
  - 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)
  - Encrypted Checksum
  - 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 Operation: 2.7V to 5.5V
  - Secure Nonvolatile Storage for Sensitive System or User Information
  - 2-wire Serial Interface
  - 1.0 MHz Compatibility for Fast Operation
  - Standard 8-lead Plastic Packages
  - Same Pinout as 2-wire Serial EEPROM's
- Smart Card Features
  - ISO 7816 Class A (5V) or Class B (3V) Operation
  - ISO 7816-3 Asynchronous T = 0 Protocol (Gemplus® Patent)
  - Multiple Zones, Key Sets and Passwords for Multi-application Use
  - Synchronous 2-wire Serial Interface for Faster Device Initialization
  - Programmable 8-byte Answer-To-Reset Register
  - ISO 7816-2 Compliant Modules
- High Reliability
  - Endurance: 100,000 Cycles
  - Data Retention: 10 years
  - ESD Protection: 4,000V

CryptoMemory Specification For Standard Mode of Operation

AT88SC0104C
AT88SC0204C
AT88SC0404C
AT88SC0808C
AT88SC1616C
AT88SC3216C
AT88SC6416C
AT88SC12816C
AT88SC25616C

5210A–SMIC–04/07

Table of Contents

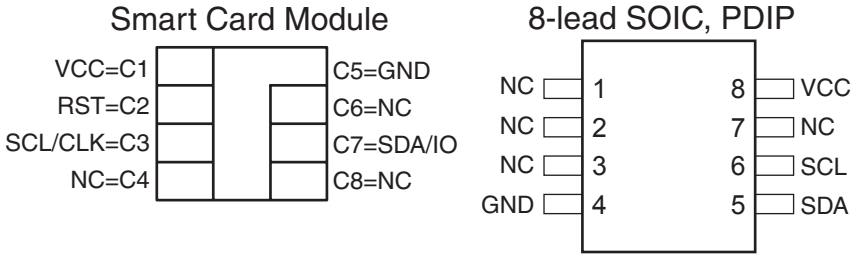
1. Pin Configuration and Package Information

1.1 Pin Configuration

Table 1-1. Package Pin Configuration

Pad	Description	ISO Module Contact	Standard Package Pin
VCC	Supply Voltage	C1	8
GND	Ground	C5	4
SCL/CLK	Serial Clock Input	C3	6
SDA/IO	Serial Data Input/Output	C7	5
RST	Reset Input	C2	NC

1.2 Package Information



2. Description

The AT88SCxxxxC is a family of 9 high-performance secure memory devices providing 1K to 256K bits of user memory with advanced built-in security and cryptographic features. The memory is divided into 4, 8 or 16 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. Cryptomemory has a configuration memory that contains registers to define the security rights for each user zone and space for passwords and secret keys used by the security logic of 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 are available for these operations.

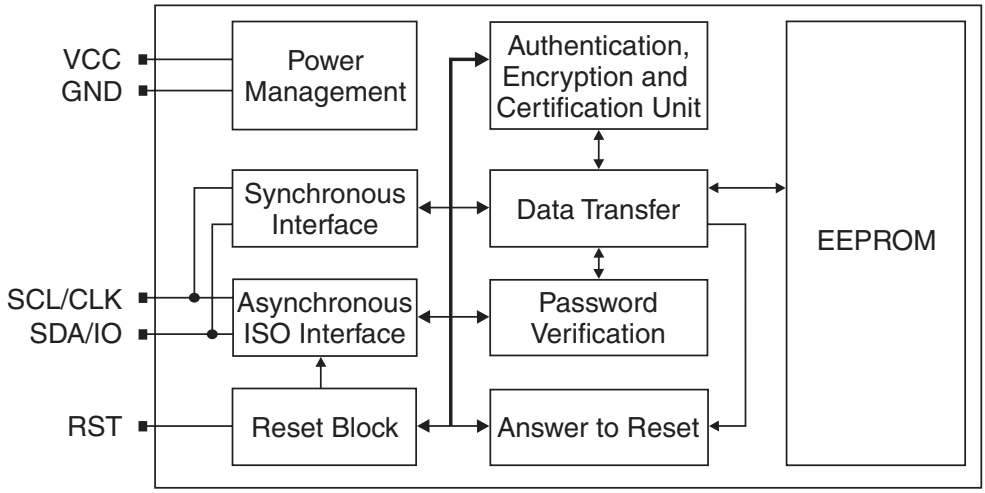
2.1 Embedded Applications

A 2-wire serial interface running at 1.0 MHz 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 pinout as 2-wire serial EEPROM's supporting only the synchronous communications protocol.

2.2 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. For devices with 32K bits of user memory and larger, communication speeds up to 153,600 baud are supported by utilizing ISO 7816-3 Protocol and Parameter Selection. All CryptoMemory devices in smart card module form will also communicate using a synchronous 2-wire serial interface.

Figure 2-1. Block Diagram



2.3 Scope and Purpose of This Document

This document covers only the Standard Mode of operation of CryptoMemory. The other modes of operation are the Authentication and Encryption Modes. This document provides all the information needed to utilize CryptoMemory in the Standard Mode. The scoping of this document allows for free distribution without formal requirements of any user agreements and serves the purpose of developing applications using only the Standard Mode of operation. Documents containing detailed description of the cryptographic technology, operation and function of the Authentication and Encryption Modes of CryptoMemory are secure and so only available under Non-Disclosure and Limited Licensing Agreements (NDA and LLA). Contact your regional Atmel sales office to obtain these secure documents.

3. Pin Description

3.1 Supply Voltage (V_{CC})

The V_{CC} input is a 2.7V to 5.5V positive voltage supplied by the host.

3.2 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.

3.3 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.

3.4 Reset (RST)

CryptoMemory provides an ISO 7816-3 compliant asynchronous answer-to-reset sequence. When the reset sequence is activated, the device will output the data programmed into the 64-bit answer-to-reset 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.

4. Detailed Description

To enable the security features of CryptoMemory, personalize the device by setting up registers and loading appropriate passwords and keys. Do this by programming the configuration memory using simple write and read commands. Gain access to the configuration memory by successfully presenting the secure code (write 7 password). After writing and verifying data in the configuration memory, blow the security fuses to lock this information in the device. For additional information on personalizing CryptoMemory, please see the examples in the protocol sections of this specification.

4.1 User Memory

The EEPROM user memory is divided into 4, 8 or 16 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 memory 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.

Figure 4-1. AT88SC0104C 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

Figure 4-2. AT88SC0204C 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

Figure 4-3. AT88SC0404C 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

Figure 4-4. AT88SC0808C 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

Figure 4-5. AT88SC1616C User Memory

ZONE		$0	$1	$2	$3	$4	$5	$6	$7
User 0	$00								
	-	128 Bytes							
	-								
	$78								
User 1	$00								
-	-								
-	-								
-	-								
User 14	$78								
User 15	$00								
	-	128 Bytes							
	-								
	$78								

Note: Page size=16 bytes

Figure 4-6. AT88SC3216C User Memory

ZONE		$0	$1	$2	$3	$4	$5	$6	$7
User 0	$00								
	-	256 Bytes							
	-								
	$F8								
User 1	$00								
-	-								
-	-								
-	-								
User 14	$F8								
User 15	$00								
	-	256 Bytes							
	-								
	$F8								

Note: Page size= 64 bytes

Figure 4-7. AT88SC6416C User Memory

ZONE		$0	$1	$2	$3	$4	$5	$6	$7
User 0	$000								
	-	512 Bytes							
	-								
	$1F8								
User 1	$000								
-	-								
-	-								
-	-								
User 14	$1F8								
User 15	$000								
	-	512 Bytes							
	-								
	$1F8								

Note: Page size= 64 bytes

Figure 4-8. AT88SC12816C User Memory

ZONE		$0	$1	$2	$3	$4	$5	$6	$7
User 0	$000								
	-	1024 Bytes							
	-								
	$3F8								
User 1	$000								
-	-								
-	-								
-	-								
User 14	$3F8								
User 15	$000								
	-	1024 Bytes							
	-								
	$3F8								

Note: Page size= 128 bytes

Figure 4-9. AT88SC25616C User Memory

ZONE		$0	$1	$2	$3	$4	$5	$6	$7
User 0	$000								
	-	2024 Bytes							
	-								
	$7F8								
User 1	$000								
-	-								
-	-								
-	-								
User 14	$7F8								
User 15	$000								
	-	2024 Bytes							
	-								
	$7F8								

Note: Page size= 128 bytes

4.1.1 Control Logic

Access to the user zones occurs only through the device's control logic. This logic is configurable through proper programming of access, passwords and keys registers of the configuration memory during device personalization. This logic also implements the cryptographic engine for performing the various higher-level security functions of the device.

4.2 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 as well as to the user zones 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 the 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 4 user zones have four sets of registers, those with 8 user zones 8 sets of registers, and those with 16 user zones 16 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.

Figure 4-10. AT88SC0104C, 0204C, 0404C Configuration Memory

<table>
<tr><th></th><th>$0</th><th>$1</th><th>$2</th><th>$3</th><th>$4</th><th>$5</th><th>$6</th><th>$7</th><th></th></tr>
<tr><td>$00</td><td colspan="8">Answer To Reset</td><td rowspan="2">Identification</td></tr>
<tr><td>$08</td><td colspan="2">Fab Code</td><td colspan="2">MTZ</td><td colspan="4">Card Manufacturer Code</td></tr>
<tr><td>$10</td><td colspan="8">Lot History Code</td><td>Read Only</td></tr>
<tr><td>$18</td><td>DCR</td><td colspan="7">Identification Number Nc</td><td rowspan="7">Access Control</td></tr>
<tr><td>$20</td><td>AR0</td><td>PR0</td><td>AR1</td><td>PR1</td><td>AR2</td><td>PR2</td><td>AR3</td><td>PR3</td></tr>
<tr><td>$28</td><td colspan="8" rowspan="3">Reserved</td></tr>
<tr><td>$30</td></tr>
<tr><td>$38</td></tr>
<tr><td>$40</td><td colspan="8" rowspan="2">Issuer Code</td></tr>
<tr><td>$48</td></tr>
<tr><td>$50</td><td colspan="8" rowspan="8">Reserved for Authentication and Encryption</td><td rowspan="8">Cryptography</td></tr>
<tr><td>$58</td></tr>
<tr><td>$60</td></tr>
<tr><td>$68</td></tr>
<tr><td>$70</td></tr>
<tr><td>$78</td></tr>
<tr><td>$80</td></tr>
<tr><td>$88</td></tr>
<tr><td>$90</td><td colspan="8" rowspan="4">Reserved for Authentication and Encryption</td><td rowspan="4">Secret</td></tr>
<tr><td>$98</td></tr>
<tr><td>$A0</td></tr>
<tr><td>$A8</td></tr>
<tr><td>$B0</td><td>PAC</td><td colspan="3">Write 0</td><td>PAC</td><td colspan="3">Read 0</td><td rowspan="10">Password</td></tr>
<tr><td>$B8</td><td>PAC</td><td colspan="3">Write 1</td><td>PAC</td><td colspan="3">Read 1</td></tr>
<tr><td>$C0</td><td>PAC</td><td colspan="3">Write 2</td><td>PAC</td><td colspan="3">Read 2</td></tr>
<tr><td>$C8</td><td colspan="7" rowspan="4">Reserved</td></tr>
<tr><td>$D0</td></tr>
<tr><td>$D8</td></tr>
<tr><td>$E0</td></tr>
<tr><td>$E8</td><td>PAC</td><td colspan="3">Write 7</td><td>PAC</td><td colspan="3">Read 7</td></tr>
<tr><td>$F0</td><td colspan="8" rowspan="2">Reserved</td><td rowspan="2">Forbidden</td></tr>
<tr><td>$F8</td></tr>
</table>

Figure 4-11. AT88SC0808C 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	Reserved for Authentication and Encryption								Cryptography
$58									
$60									
$68									
$70									
$78									
$80									
$88									
$90	Reserved for Authentication and Encryption								Secret
$98									
$A0									
$A8									
$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									

Figure 4-12. AT88SC1616C, 3216C, 6416C, 12816C, 25616C 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	AR8	PR8	AR9	PR9	AR10	PR10	AR11	PR11	
$38	AR12	PR12	AR13	PR13	AR14	PR14	AR15	PR15	
$40	Issuer Code								
$48									
$50	Reserved for Authentication and Encryption								**Cryptography**
$58									
$60									
$68									
$70									
$78									
$80									
$88									
$90	Reserved for Authentication and Encryption								**Secret**
$98									
$A0									
$A8									
$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. Communication Security Modes

Communication between the device and host operates in three basic modes: Standard, Authentication and Encryption Modes. The Standard Mode is the default mode for the device after power-up. Special procedures exist for enabling Authentication and Encryption Modes but are beyond the scope of this document. Information pertaining to use of Authentication and Encryption Modes of CryptoMemory is available from Atmel under Non-Disclosure and/or Limited Licensing Agreements (NDA and/or LLA).

Table 5-1. Communication Security Modes

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

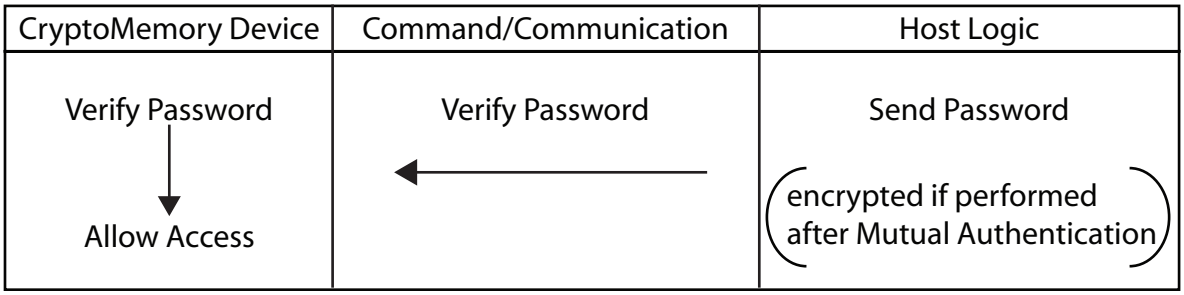
Configuration data includes the entire configuration memory except the passwords.
MAC: Message Authentication Code.

5.1 Security Operations

5.1.1 Password Verification

The use of passwords protects read and write accesses to the user zones. Any one of 8 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 5-1. Password Verification



5.1.2 Mutual Authentication

The mutual authentication mode employs cryptographic technology that allows the device to authenticate the host, and the host to authenticate the device prior to any data communication between the two. Additional information on using mutual authentication is available from Atmel under NDA and/or LLA.

5.1.3 Data Encryption

The encryption mode builds upon the mutual authentication mode such that the host and device first authenticate each other and go further to encrypt all data communications between them. Additional information on using the encryption mode is available from Atmel under NDA and/or LLA.

5.1.4 Encrypted Checksum

The encrypted checksums allows for bidirectional data validity and integrity check between the host and device. Additional information on using encrypted checksums is available from Atmel under NDA and LLA.

5.2 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.

5.2.1 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.

5.2.2 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.

5.2.3 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. Figure 5-2 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.

Figure 5-2. Write Lock example

Address	$0	$1	$2	$3	$4	$5	$6	$7
$080	110110011	xxxx xxxx locked	xxxx xxxx locked	xxxx xxxx	xxxx xxxx	xxxx xxxx locked	xxxx xxxx	xxxx xxxx

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.

5.2.4 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 memory 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 8 bytes.

Data is written first to a buffer zone in EEPROM instead of the intended destination address in the user zone or configuration memory, but with the same access conditions. If this write cycle is interrupted the original data remains in tact in the user zone or configuration memory. 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 28ms 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 14ms.

5.3 Configuration Memory Values

This section describes each individual field in the configuration memory.

5.3.1 Default Values

Atmel programs certain fields of the configuration memory 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 5-2 on page 16 summarizes device fields Atmel programs at the factory. A brief description of each field follows.

Table 5-2. Factory Programmed Fields

Device	ATR	Fab Code	Lot History Code	Write 7 Password (Secure Code)
AT88SC0104C	3B B2 11 00 10 80 00 01	10 10	Variable, locked	DD 42 97
AT88SC0204C	3B B2 11 00 10 80 00 02	20 20	Variable, locked	E5 47 47
AT88SC0404C	3B B2 11 00 10 80 00 04	40 40	Variable, locked	60 57 34
AT88SC0808C	3B B2 11 00 10 80 00 08	80 60	Variable, locked	22 E8 3F
AT88SC1616C	3B B2 11 00 10 80 00 16	16 80	Variable, locked	20 0C E0
AT88SC3216C	3B B3 11 00 00 00 00 32	32 10	Variable, locked	CB 28 50
AT88SC6416C	3B B3 11 00 00 00 00 64	64 40	Variable, locked	F7 62 0B
AT88SC12816C	3B B3 11 00 00 00 01 28	28 60	Variable, locked	22 EF 67
AT88SC25616C	3B B3 11 00 00 00 02 56	58 60	Variable, locked	17 C3 3A

5.3.2 Answer To Reset (ATR)

This is an 8 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.

5.3.3 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.

5.3.4 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.

5.3.5 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.

5.3.6 Lot History Code

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

5.3.7 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.

5.3.8 Device Configuration Register (DCR)

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

Bit 7	Bit 6	Bit 5	Bit4	Bit 3	Bit 2	Bit 1	Bit 0
SME	UCR	UAT	ETA	CS3	CS2	CS1	CS0

5.3.8.1 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”).

5.3.8.2 UCR – Unlimited Checksum Reads

UCR is applicable under authentication and encryption modes of operation.

5.3.8.3 UAT – Unlimited Authentication Trials

UAT is applicable under the authentication mode of operation.

5.3.8.4 ETA – Eight Trials Allowed

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

5.3.8.5 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.

5.3.9 Access Registers

Four, eight, or sixteen 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 5-3. Access Register

Bit 7	Bit 6	Bit 5	Bit4	Bit 3	Bit 2	Bit 1	Bit 0
PM1	PM0	AM1	AM0	ER	WLM	MDF	PGO

5.3.9.1 PM(1:0) Password Mode

Table 5-4. 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 following section). Verification of the Write password also allows modification of the read and the write passwords.

5.3.9.2 AM(1:0) – Authentication mode

The AM bits allow configuration of the authentication modes and only available under the authentication mode of operation.

5.3.9.3 ER – Encryption Required

The use of the ER bit is applicable in the encryption mode of operation.

5.3.9.4 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. Setting bit 0 to “0” locks the Write Lock Byte itself. Enabling Write Lock Mode limits write operations to one byte at a time.

5.3.9.5 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”

5.3.9.6 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”.

5.3.10 Password/Key Registers

Four, eight or sixteen 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 affect 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 5-5. Password/Key Register Definition

Bit 7	Bit 6	Bit 5	Bit4	Bit 3	Bit 2	Bit 1	Bit 0
AK1	AK0	POK1	POK0	*Res*	PW2	PW1	PW0

5.3.10.1 AK(1:0) – Authentication Key

The AK bits are applicable under the authentication mode of operation.

5.3.10.2 POK(1:0) – Program Only Key

The POK bits are applicable under the authentication mode of operation.

5.3.10.3 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.

5.3.11 Identification Number

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

5.3.12 Cryptograms

Cryptograms are applicable to authentication and encryption modes of operation.

5.3.13 Session Keys

Session keys are applicable to authentication and encryption modes of operation.

5.3.14 Secret Seeds

Secret Seeds are applicable to authentication and encryption modes of operation.

5.3.15 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.

5.3.16 Secure Code

The secure code is Write 7 Password. Properly presenting this password grants write access to the configuration memory during personalization. Atmel defines the initial values of the secure code but the customer may change these values after successful verification of Write 7 password. Table 5-2 on page 16 shows the secure codes for the various devices as they leave the Atmel factory. After blowing the PER fuse, verifying Write 7 password no longer grant write access to the configuration memory, and the configuration memory becomes read-only thereafter.

5.3.17 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.

5.3.18 Authentication Attempts Counters (AAC)

The authentication attempts counters are applicable in authentication and encryption modes of operation only.

5.4 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 4 to 7 of this byte are not used as Security Fuses and are reserved for Atmel use

.

Table 5-6. 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

The bits 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:

1. FAB – To lock the Answer To Reset and the Fab Code portions of the Configuration Memory.
2. CMA – To lock the Card Manufacturer Code of the Configuration Memory
3. PER – To lock the remainder of the Configuration Memory

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

Table 5-7 on page 21 provides a summary of access rights for all portions of the memory for each fuse condition

.

Table 5-7. Fuse Access Rights Summary

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
Crytography (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				
User Zones	*Read*	AR	AR	AR	AR
	Write				

Note: AR: Access Rights are defined by the Access Registers
PW: Password
Secure Code: Write 7 password is the Secure Code until the PER fuse is blown
Forbidden: No access is permitted

6. Protocol Selection

CryptoMemory supports two application areas with different communication protocols: a 2-wire serial communication for embedded applications and an 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.

6.0.1 Synchronous Mode for Embedded Applications

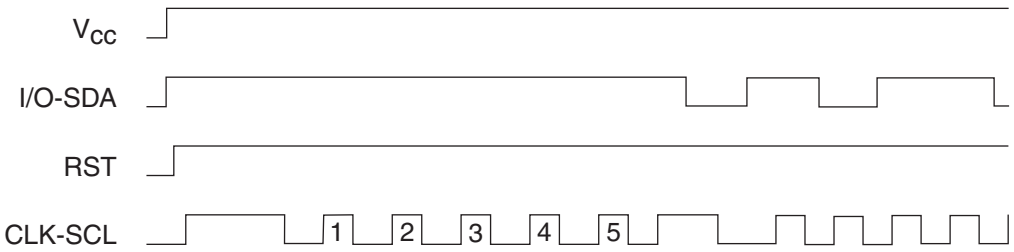
The 2-wire serial interface is used for fast and efficient communication with logic and controllers. The synchronous mode is the default after powering up V_{CC} due to the internal and/or external pull-up on RST. For embedded applications using CryptoMemory in standard plastic packages RST is not bonded out and this is the only communication protocol.

Power-up V_{CC}, RST goes high also.

After stable V_{CC}, apply 5 pulses CLK-SCL

CLK-SCL and I/O-SDA may then be driven.

Figure 6-1. Power Up Sequence for 2-Wire 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.

6.0.2 Asynchronous Mode for Smart Card Applications

The asynchronous T=0 protocol defined by ISO 7816-3 is used for compatibility with 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.

The 64-bit ATR code comes from a register that contains the characters shown in Table 6-1 on page 23 and Table 6-2 on page 23. The historical bytes (T1, T2, T3) show the density of the CryptoMemory device. This register may be modified during personalization but is locked when the PER fuse is blown. Care must be taken to respect the applicable standards defining the ATR

value if operating in asynchronous mode. The CyrptoMemory device will always output all 8 bytes in response to the asynchronous ATR command regardless of the contents of the register.

Table 6-1. ATR Codes for Lower Density CryptoMemory

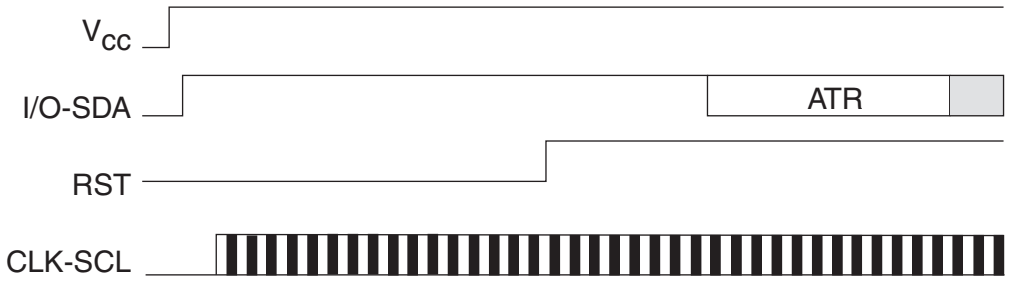
Device	TS	T0	TA(1)	TB(1)	TD(1)	TA(2)	T1	T2
AT88SC0104C	$3B	$B2	$11	$00	$10	$80	$00	$01
AT88SC0204C	$3B	$B2	$11	$00	$10	$80	$00	$02
AT88SC0404C	$3B	$B2	$11	$00	$10	$80	$00	$04
AT88SC0808C	$3B	$B2	$11	$00	$10	$80	$00	$08
AT88SC1616C	$3B	$B2	$11	$00	$10	$80	$00	$16

Table 6-2. ATR Codes for Higher Density CryptoMemory

Device	TS	T0	TA(1)	TB(1)	TD(1)	T1	T2	T3
AT88SC3216C	$3B	$B3	$11	$00	$00	$00	$00	$32
AT88SC6416C	$3B	$B3	$11	$00	$00	$00	$00	$64
AT88SC12816C	$3B	$B3	$11	$00	$00	$00	$01	$28
AT88SC25616C	$3B	$B3	$11	$00	$00	$00	$02	$56

Once the asynchronous mode has been selected, it is not possible to switch to the synchronous mode without powering off the device.

Figure 6-2. Power Up Sequence for Smart Card Mode



After a successful ATR, the Protocol and Parameter Selection (PPS) protocol defined by ISO 7816-3 may be used to negotiate the communications speed with CryptoMemory devices 32-Kbits and larger in user memory. CryptoMemory supports D values of 1,2,4,8,12 and 16 for an F value of 372. CryptoMemory also supports D values of 8 and 16 for F = 512. This allows selection of 8 communications speeds ranging from 9600 baud to 153,600 baud.

Smart card applications that support the 2-Wire protocol can also use CryptoMemory in the synchronous mode.

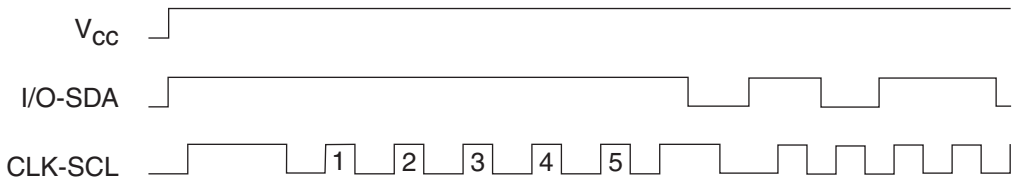
7. Synchronous Protocol

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.

7.1 Start-up Sequence

When first powering up the device, 5 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.



7.2 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 4 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.

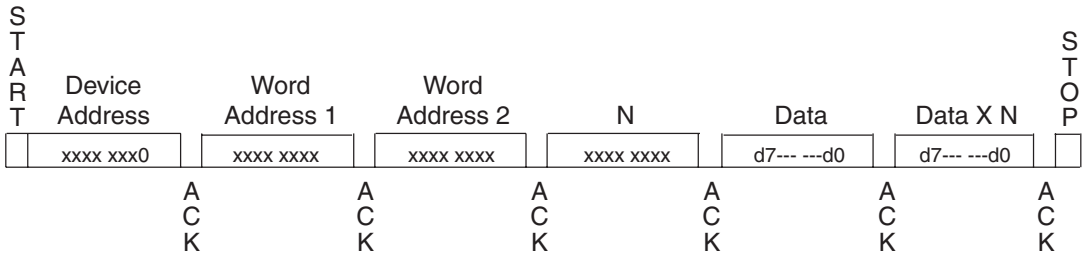
Table 7-1. CryptoMemory Synchronous Command Set

Command Description		Command	Addr 1	Addr 2	N	Data (N)
Write User Zone	Normal (AT88SC0104C-AT88SC1616C)	$B0	addr	addr	N ≤ $10	N bytes
	Normal (AT88SC3216C, AT88SC6416C)	$B0	addr	addr	N ≤ $40	N bytes
	Normal (AT88SC12816C, AT88SC25616C)	$B0	addr	addr	N ≤ $80	N bytes
	with Anti-Tearing (all devices)	$B0	addr	addr	N ≤ 08	N bytes
Read User Zone		$B2	addr	addr	N	
System Write	Write Config Zone (AT88SC0104C-AT88SC1616C)	$B4	$00	addr	N ≤ $10	N bytes
	Write Config Zone (AT88SC3216C, AT88SC6416C)	$B4	$00	addr	N ≤ $40	N bytes
	Write Config Zone (AT88SC12816C, AT88SC25616C)	$B4	$00	addr	N ≤ $80	N bytes
	Write Fuses	$B4	$01	fuse ID	$00	
	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	
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)

7.3 Command Format

Most CryptoMemory commands have the same format as a two wire interface (TWI) write command. The TWI write command is characterized by a zero in the LSB of the first byte (device address). The number of word address bytes in a TWI write command will vary depending on the size of the memory being addressed. All bytes whether part of the command or data are generated by the host and sent to the memory device that will acknowledge each byte.

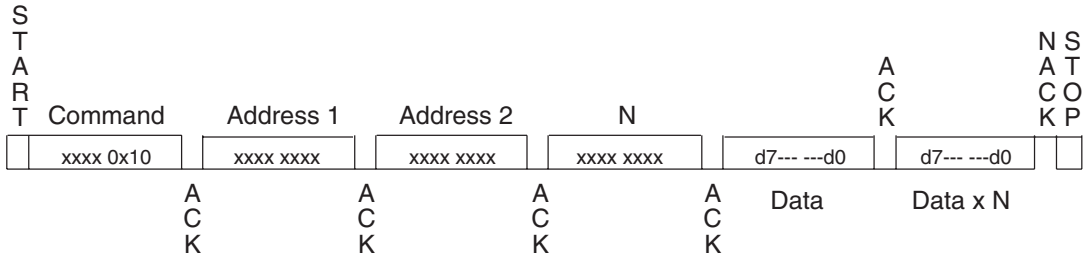
Figure 7-1. TWI Write Command:



All CryptoMemory commands will have a zero for the LSB of the first byte. All CryptoMemory commands will have 4 bytes used for defining the command and addressing the memory. All but the CryptoMemory read commands will send an additional 0 to 128 bytes of data following the 4 command bytes. These commands comply with the format of a TWI write command.

The CryptoMemory read commands (Read User Zone, System Read) do not comply with the format of a TWI write or read command. The CryptoMemory read command looks like a TWI write command (LSB of the first byte = 0) but after the 4th 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 7-2. CryptoMemory 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.

7.4 Acknowledge Polling

Each command is ended with a stop condition. Certain commands are required to be followed by an acknowledge polling sequence. Acknowledge polling consists of sending a start condition followed by the command byte and determining if the device responded 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 7-2. 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 Encrypted	$B0	addr	addr	N	Required, any CMD	20ms
		$B0	addr	addr	N	No, Send Checksum	0
	Encrypted with Anti-Tearing	$B0	addr	addr	N	No, Send Checksum	0
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
	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
Verify Password	Write Password	$BA	$0X	$00	$01	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. See Table 10-1 on page 52

7.5 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.

7.6 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.

7.6.1 Write User Zone: $B0

7.6.1.1 Functional

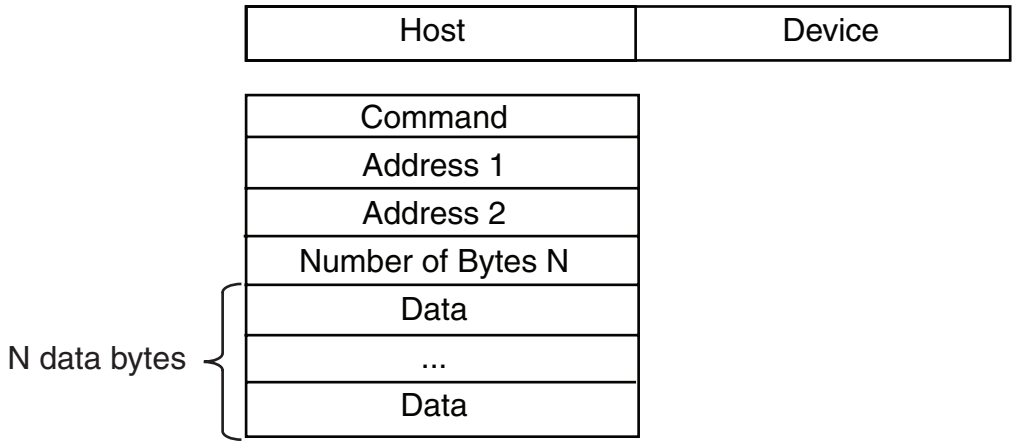


Figure 7-3. Write User Zone Command Functional Description

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 “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 as follows;

- $10 for AT88SC0104C through AT88SC1616C (EEPROM page size of 16 bytes)
- $40 for AT88SC3216C and AT88SC6416C (EEPROM page size of 64 bytes)
- $80 for AT88SC12816C and AT88SC25616C (EEPROM page size of 128 bytes)

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 writes 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.

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.

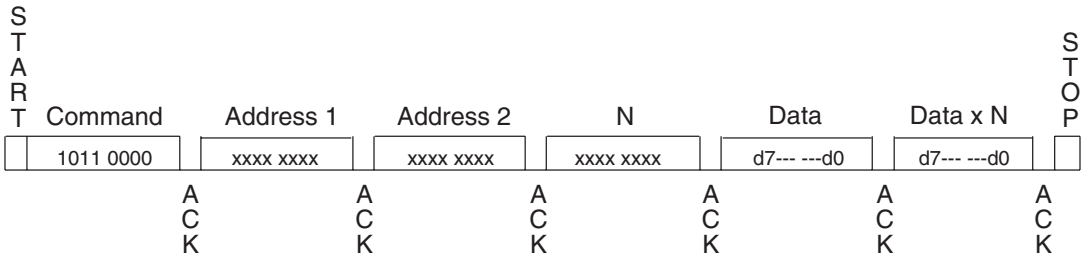


Figure 7-4. Write User Zone

7.6.2 Read User Zone: $B2

7.6.2.1 Functional

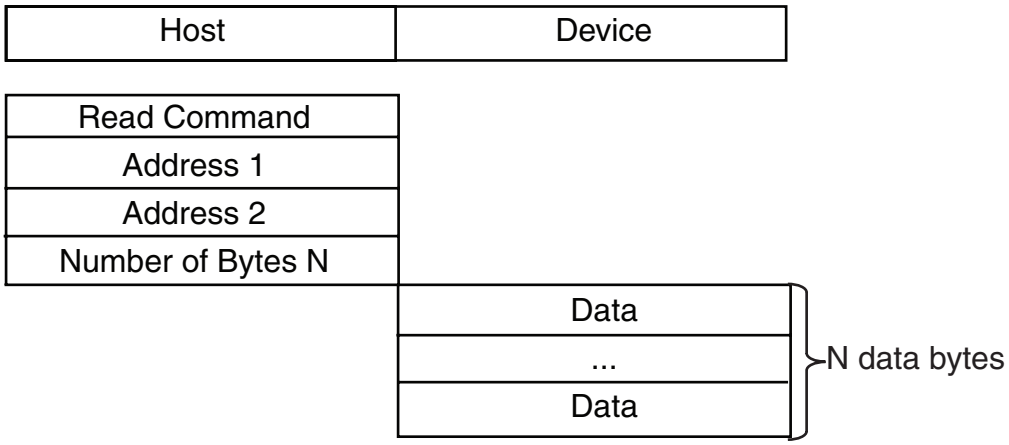


Figure 7-5. Read User Zone Command Functional Description

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 under Section 7.6.3 on page 30).

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 anytime 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.

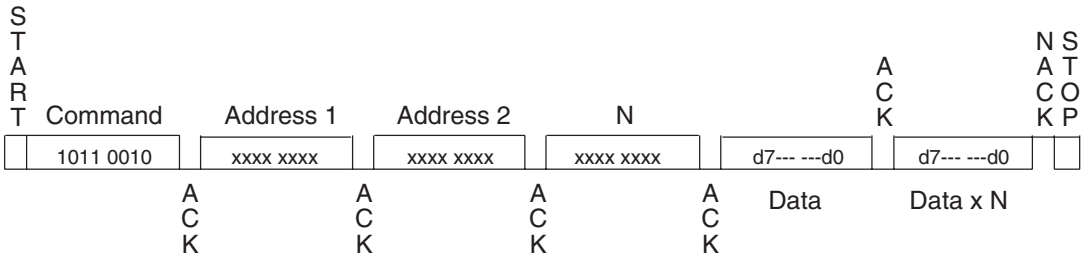


Figure 7-6. Read User Zone

7.6.3 System Write : $B4

7.6.3.1 Functional

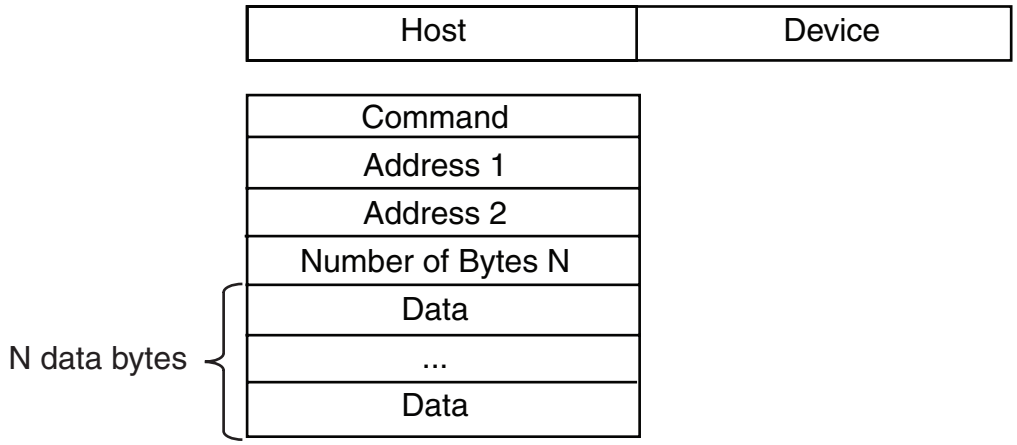


Figure 7-7. System Write Command Functional Description

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

Table 7-3. System Write Command Detail

Command Description	Command	Addr 1	Addr 2	N	Data (N)
Write Config Zone AT88SC0104C-AT88SC1616C)	$B4	$00	addr	N ≤ $10	N bytes
Write Config Zone AT88SC3216C-AT88SC6416C)	$B4	$00	addr	N ≤ $40	N bytes
Write Config Zone AT88SC12816C-AT88SC25616C)	$B4	$00	addr	N ≤ $80	N bytes
Write Fuses	$B4	$01	fuse ID	$00	
Set User Zone	$B4	$03	zone	$00	

7.6.3.2 Write Config Zone

The maximum number of bytes that may be written is as follows;

- $10 for AT88SC0104C through AT88SC1616C (EEPROM page size of 16 bytes)
- $40 for AT88SC3216C and AT88SC6416C (EEPROM page size of 64 bytes)
- $80 for AT88SC12816C and AT88SC25616C (EEPROM page size of 128 bytes)

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 memory, the host may provide an authorized starting address, but a number of bytes that causes the device to reach unauthorized address. 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.

7.6.3.3 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.

Table 7-4. Fuse Writing

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

7.6.3.4 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 7-5. 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 memory may be done with anti-tearing enabled by setting address 1 to $08 of the Write Config 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.

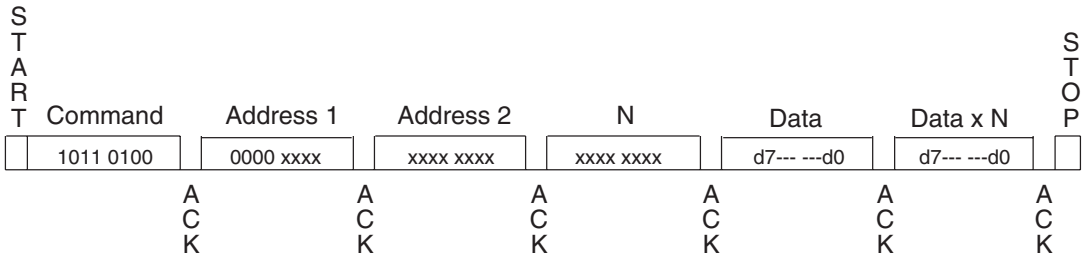


Figure 7-8. System Write

7.6.4 System Read : $B6

7.6.4.1 Functional

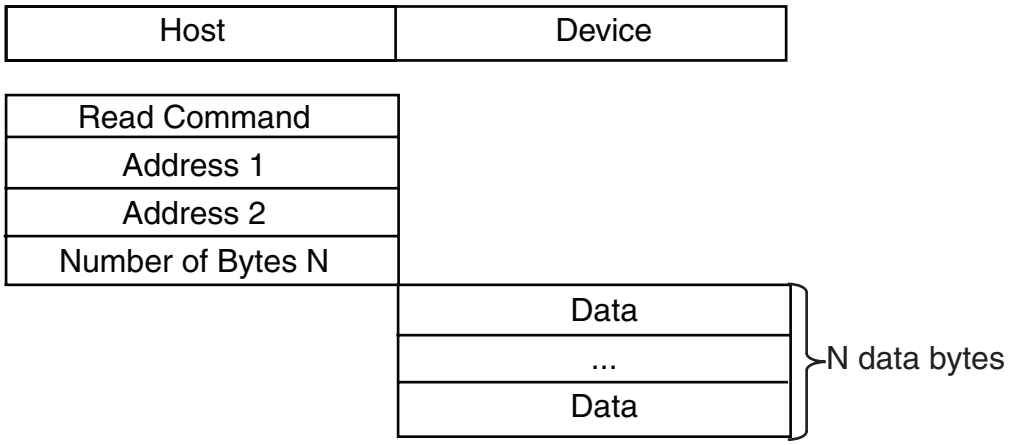


Figure 7-9. System Read Command Functional Description

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 memory, or the fuses.

Table 7-6. System Read Command Description

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

7.6.4.2 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 address. In this case the device will transmit the fuse byte (see below) in place of unauthorized bytes.

7.6.4.3 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.

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

Figure 7-10. Read Fuse Bytes

7.6.5 Verify Password : $BA

7.6.5.1 Functional

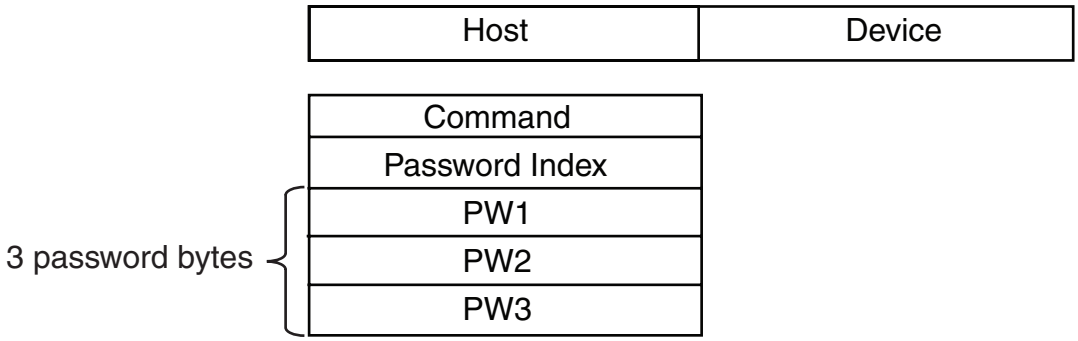


Figure 7-11. Verify Password Command Functional Description

Read password indices : $10 to $17 for passwords 0 to 7.

Write password indices : $00 to $07 for passwords 0 to 7.

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

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

r = 0: Write password,

r = 1: Read password,

p2p1p0: Password set number.

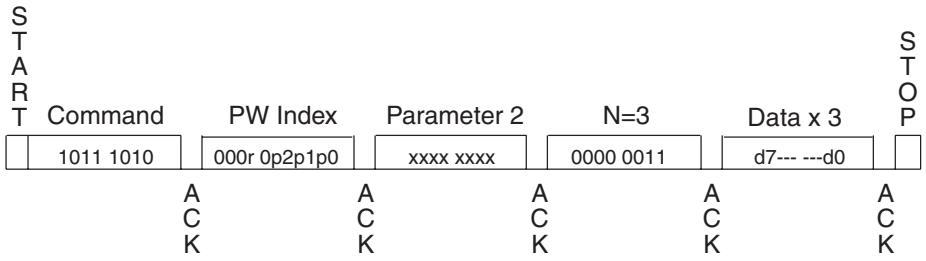


Figure 7-12. Verify Password

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 $FF.

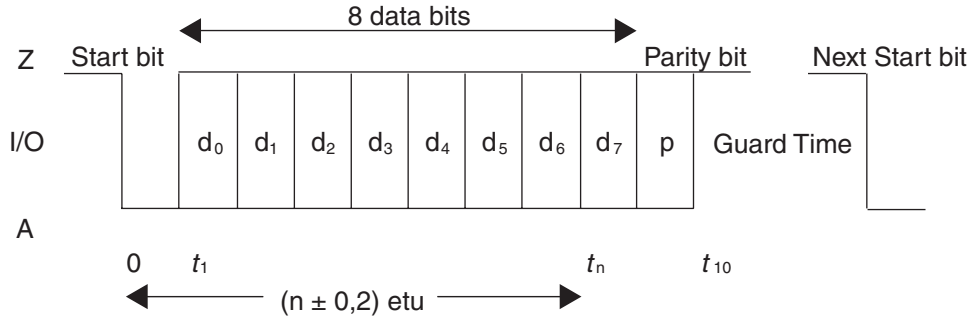
7.7 Initialization Example

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.

8. Asynchronous T=0 Protocol

8.1 Character format

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.



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.

8.2 Command format

The command sequence is as follows:

1. In compliance with ISO 7816-3, the host must send the header consisting of 5 characters: CLA, INS, P1, P2, P3.
   a. CLA refers to a class of instructions. This byte isn't tested by the device.
   b. INS is the instruction byte.
   c. P1 and P2 are reference bytes, such as a data byte address or password index.
   d. 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).

8.3 PPS Support

All CryptoMemory devices with user memory sizes 32Kbits and larger support the Protocol and Parameter Selection (PPS) protocol, section 7 of ISO 7816-3. This section only applies to these larger devices; PPS is not supported by CryptoMemory with memory sizes 16K bit or smaller.

At the end of an ATR sequence, subsequent to either a cold or a warm reset initiated by the reader, the device will be expecting either a 'Class' byte as part of a command header, or the initial character, PPSS, of a PPS request. If the device receives a byte = $FF, it will process subsequent incoming bytes as a PPS request. In all other cases, it will proceed with command processing. There are 4 bytes that comprise a PPS request or response;

- Initial Character PPSS. Always equal to $FF.
- Format Character PPS0. CryptoMemory supports two response values for PPS0, $00 and $01. See ISO 7816 for further definition of PPS0.
- Parameter Character PPS1. Encodes Fn and Dn in the same manner as TA(1) in the ATR
- Checksum PCK.

The following table shows the PPS1 values supported by CryptoMemory devices with memory sizes 32K bits and above.

Table 8-1. PPS1 Values CryptoMemory Supports

		f Max	4 MHz	5 MHz	5 MHz
		FI	0000b	0001b	1001b
DI	Di	Fi	372	372	512
0001b	1	PPS1	01	11	
		F/D	372	372	
		baud rate	9600	9600	
0010b	2	PPS1	02	12	
		F/D	186	186	
		baud rate	19200	19200	
0011b	4	PPS1	03	13	
		F/D	93	93	
		baud rate	38400	38400	
0100b	8	PPS1	04	14	94
		F/D	46.5	46.5	64
		baud rate	76800	76800	55800
0101b	16	PPS1	05	15	95
		F/D	23.25	23.25	32
		baud rate	153600	153600	111600
1000b	12	PPS1	08	18	
		F/D	31	31	
		baud rate	115200	115200	

After the ATR, the reader will have the choice of proceeding with commands using default values of F=372 and D=1 (9600 baud at 3.5712 MHz), or negotiating values Fn and Dn through a PPS exchange. Following are four examples of PPS requests and responses:

8.3.1 Example 1

We assume the CryptoMemory ATR contains the byte TA(1) = 15h, indicating that it is capable of using F=372 and D=16, leading to a baud rate of 153,600 baud at 3.5712 MHz. Assuming that this is the maximum speed supported by the device, the reader immediately attempts to set the F and D parameters leading to these values.

- PPS_request =$FF $10 $15 $FA
- PPS_response = $FF $10 $15 $FA

The newly negotiated values are effective immediately following this exchange, so that the ETU, or duration of one bit on I/O, will now be 23 clock cycles instead of 372.

8.3.2 Example 2

The reader insists on negotiating Fn and Dn equal to the default values, even though these would be used by default without the use of a PPS exchange. The two ways of doing this are by sending PPS1_request = $11 or not sending PPS1_request at all.

- PPS_request = $FF $10 $11 $FE
- PPS_response= $FF $10 $11 $FE

or

- PPS_request= $FF $00 $FF
- PPS_response = $FF $00 $FF

8.3.3 Example 3

The reader attempts to negotiate values that are not supported by the CryptoMemory device. In its response, the CryptoMemory proposes to continue with F and D, by not sending PPS1_response. Even though new Fn and Dn values aren't negotiated, this scenario is still considered a "successful" exchange according to ISO 7816.

- PPS_request= $FF $10 $45 $AA
- PPS_response= $FF $00 $FF

8.3.4 Example 4

If the reader attempts to change the protocol to any protocol other than T = 0, such as T = 1, the CryptoMemory will indicate that it only supports T = 0.

- PPS_request= $FF $01 $FE
- PPS_response= $FF $00 $FF

CryptoMemory will only operate at baud rates above the default 9600 baud through a successful PPS exchange. CryptoMemory cannot be set to higher baud rates through use of a TA(2) byte in the ATR.

8.4 Command Set

Table 8-2. CryptoMemory Asynchronous Command Set

	Command Description		CLA	INS	P1	P2	P3	Data (N)
B0	Write User Zone	Normal (0104C-1616C)	$00	$B0	addr	addr	N ≤ $10	N bytes
		Normal (3216C, 6416C)	$00	$B0	addr	addr	N ≤ $40	N bytes
		Normal (12816C, 25616C)	$00	$B0	addr	addr	N ≤ $80	N bytes
		with Anti-Tearing (all dvcs)	$00	$B0	addr	addr	N ≤ $08	N bytes
B2	Read User Zone		$00	$B2	addr	addr	N	
B4	System Write	Write Config Zone (Devices 0104C-1616C)	$00	$B4	$00	addr	N ≤ $10	N bytes
		Write Config Zone (Devices 3216C, 6416C)	$00	$B4	$00	addr	N ≤ $40	N bytes
		Write Config Zone (Devices 12816C, 25616C)	$00	$B4	$00	addr	N ≤ $80	N bytes
		Write Fuses	$00	$B4	$01	fuse ID	$00	
		Set User Zone	$00	$B4	$03	zone	$00	
		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	
B6	System Read	Read Config Zone	$00	$B6	$00	addr	N	
		Read Fuse Byte	$00	$B6	$01	$00	$01	
BA	Verify Password	Write Password	$00	$BA	$0X	$00	$03	3 byte password X=password set (0-7)
		Read Password	$00	$BA	$1X	$00	$03	3 byte password X=password set (0-7)

8.4.1 Status Words

Table 8-3. Asychronous Mode Return Status Definitions

SW1 SW2	Meaning
$67 $00	The length is incorrect
$69 $00	The command is unauthorized
$6B $00	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 procedure bytes 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.

8.4.2 Example : Write EEPROM command

The following illustrates the data exchanges that occur during a write operation of 4 bytes : $04, $09, $19, $97 to addresses $02, $03, $04, $05 in the current user zone.

	Host	Device	Val	Note
Start	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	4 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
Finish		SW2	$00	

8.5 Command Descriptions

8.5.1 Write User Zone: $B0

8.5.1.1 Functional

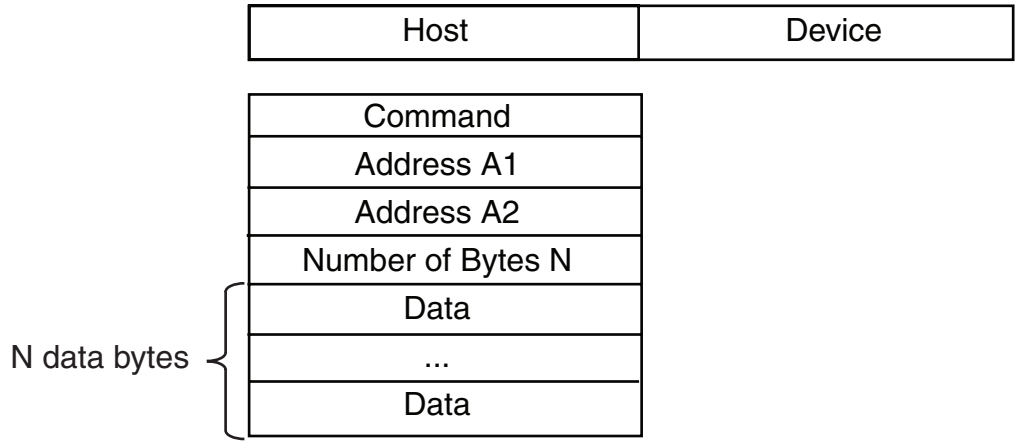


Figure 8-1. Write User Zone Command Functional Description

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, (see Section 7.6.3 on page 30).

The maximum number of bytes that may be written is as follows;

- $10 for AT88SC0104C through AT88SC1616C (EEPROM page size of 16 bytes)
- $40 for AT88SC3216C and AT88SC6416C (EEPROM page size of 64 bytes)
- $80 for AT88SC12816C and AT88SC25616C (EEPROM page size of 128 bytes)

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 with anti-tearing command (00 B4 0B zz 00), all subsequent writes to the user zone will be in anti-tearing mode.

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.

User Write					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

Figure 8-2. Write User Zone

8.5.2 Read User Zone: $B2

8.5.2.1 Functional

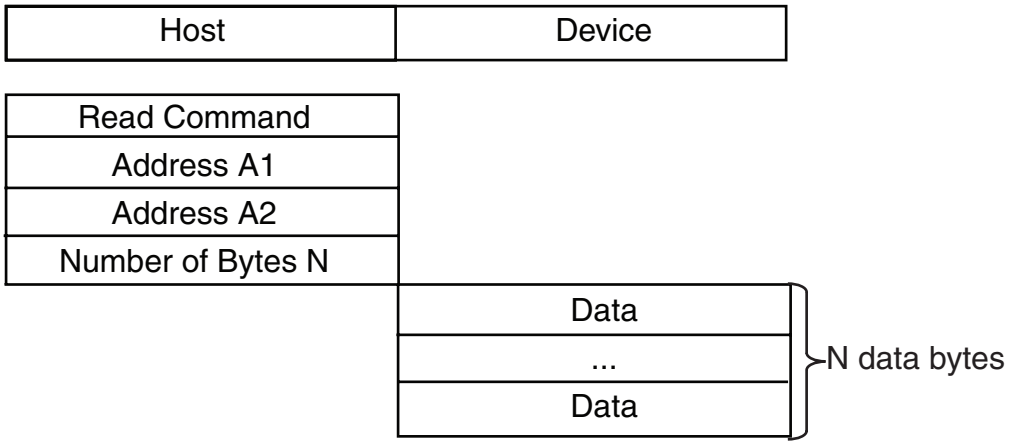


Figure 8-3. Read User Zone Command Functional Description

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 under Section 8.5.3.4 on page 43). 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.

User Read					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

Figure 8-4. Read User Zone

8.5.3 System WRITE: $B4

8.5.3.1 Functional

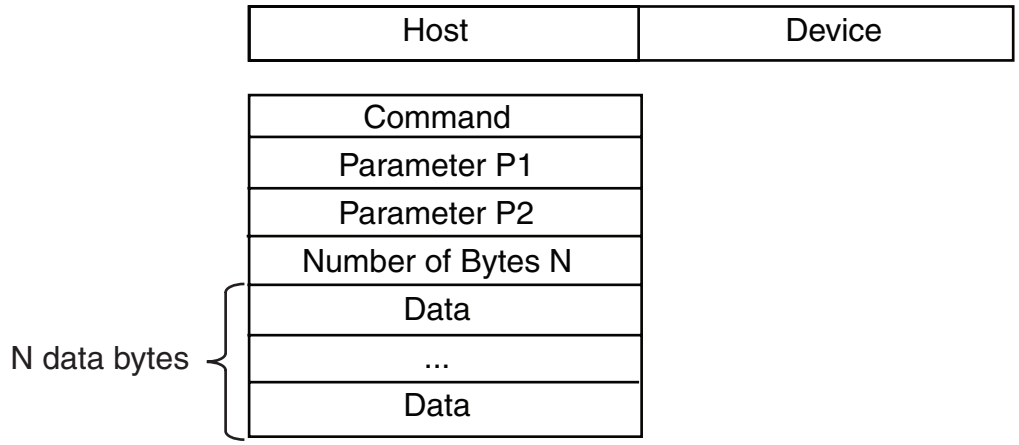


Figure 8-5. System WRITE Command Functional Description

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 or set the user zone.

Table 8-4. System WRITE Command Detail

Command	CLA	INS	P1	P2	P3	Data(N)
Write Config Zone (Devices 0104C-1616C)	$00	$B4	$00	addr	N ≤$10	N bytes
Write Config Zone (Devices 3216C-6416C)	$00	$B4	$00	addr	N ≤$40	N bytes
Write Config Zone (Devices 12816C-25616C)	$00	$B4	$00	addr	N ≤$80	N bytes
Write Fuses	$00	$B4	$01	fuse ID	$00	
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 memory 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 8-5. Anti-Tearing

Command	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	

8.5.3.2 Write Config Zone

The maximum number of bytes that may be written is as follows:

- $10 for AT88SC0104C through AT88SC1616C (EEPROM page size of 16 bytes)
- $40 for AT88SC3216C and AT88SC6416C (EEPROM page size of 64 bytes)
- $80 for AT88SC12816C and AT88SC25616C (EEPROM page size of 128 bytes)

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 memory, the host may provide an authorized starting address, but a number of bytes that causes the device to reach unauthorized address. 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.

8.5.3.3 Write Fuses

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’.

Table 8-6. Fuse Writing

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

8.5.3.4 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.

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

Figure 8-6. System WRITE

8.5.4 System READ: $B6

8.5.4.1 Functional

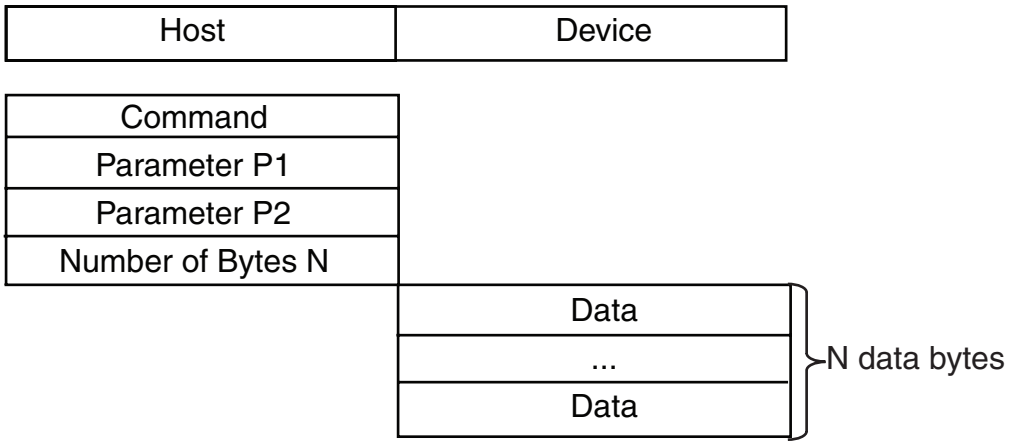


Figure 8-7. System READ Command Functional Description

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, or the fuses.

Table 8-7. System READ Command Detail

Command	CLA	INS	P1	P2	P3
Read Config Zone	$00	$B6	$00	addr	N
Read Fuse Byte	$00	$B6	$01	$00	$01

8.5.4.2 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 memory, the host may provide an authorized starting address, but a number of bytes N that causes the device to reach unauthorized address. 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 were not valid.

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

Figure 8-8. System READ

8.5.4.3 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.

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

Figure 8-9. Fuse Byte Description

8.5.5 Verify Password: $BA

8.5.5.1 Functional

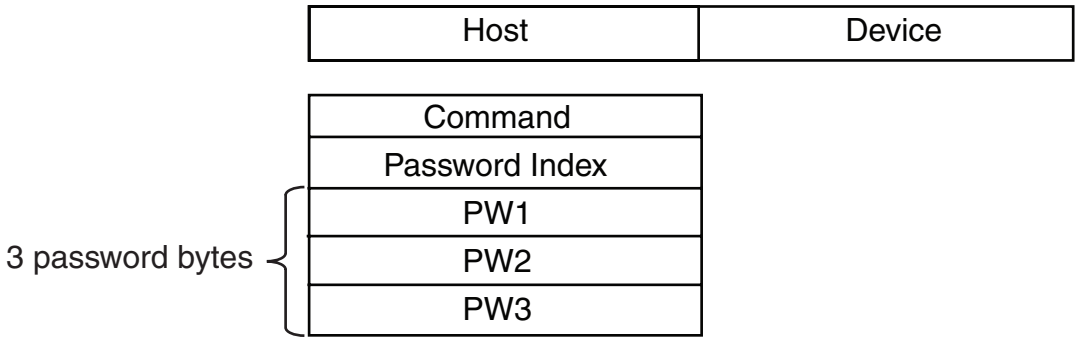


Figure 8-10. Verify Password Command Functional Description

Read password indices : $10 to $17 for passwords 0 to 7.

Write password indices : $00 to $07 for passwords 0 to 7.

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

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

r = 0: Write password,

r = 1: Read password,

p2p1p0: Password set number.

Verify Password					**Data Sent**		
CLA	INS : Command	P1	P2	P3	PW1	PW2	PW3
**	$BA	000r $0p_2p_1p_0$	**	$03	d_7--- ---d_0	d_{15}--- ---d_8	d_{23}--- ---d_{16}

Figure 8-11. Verify Password

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 decrements the associated attempts counter before verifying the password, to prevent attacks. If the password is correct, the device memorizes this success, clears the pasword attempts counter and returns $90 $00. If the password is wrong, the device simply returns $69 $00 after decrementing the attempts count. The Write 7 password is also known as the Secure Code and must be properly presented before access to the configuration memory is granted when personalizing the device

9. Initialization Example

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 Configuration Memory

Before any data can be written to the configuration memory, 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 memory. Use the Read Config Zone command to read back the security code at address $E9 for verification that the configuration memory has been unlocked.

9.3 Write Data to 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 memory 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 AT88SC0104C 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. Zone Configuration Example

User Zone	Data	Security Requirements	Access Register	Password/Key Register
0	Zone 0 Data	None	$FF	$FF
1	Zone 1 Data	Read/Write Password (Set 1)	$7F	$F9

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 (*).

```
*AT88SC0104C 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

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

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

*WRITE PASSWORDS IN CONFIGURATION MEMORY
*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 MEMORY 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
Power_off
```

10. Absolute Maximum Ratings

Stresses beyond those listed under ‘Absolute Maximum Ratings’ may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of this specification is not implied. Exposure to absolute maximum rating conditions for extended periods of time may affect device reliability.

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

10.1 DC and AC Characteristics

DC Characteristics

Applicable over recommended operating range from V_{CC} = +2.7 to 5.5V

T_{AC} = -40° to +85° C (unless otherwise noted)

Symbol	Parameter	Test Condition	Min	Typ	Max	Units
V_{CC}	Supply Voltage		2.7		5.5	V
I_{CC}	Supply Current (V_{CC} = 5.5V)	Async READ at 3.57MHz			5	mA
I_{CC}	Supply Current (V_{CC} = 5.5V)	Async WRITE at 3.57MHz			5	mA
I_{CC}	Supply Current (V_{CC} = 5.5V)	Synch READ at 1MHz			5	mA
I_{CC}	Supply Current (V_{CC} = 5.5V)	Synch WRITE at 1MHz			5	mA
I_{SB}	Standby Current (V_{CC}= 5.5V)	$V_{IN} = V_{CC}$ or GND			100	µA
V_{IL}	SDA/IO Input Low Voltage(1)		0		V_{CC} x 0.2	V
V_{IL}	Clock Input Low Voltage(1)		0		V_{CC} x 0.2	V
V_{IL}	RST Input Low Voltage(1)		0		V_{CC} x 0.2	V
V_{IH}	SDA/IO Input High Voltage(1)		V_{CC} x 0.7		V_{CC}	V
V_{IH}	SCL/CLK Input High Voltage(1)		V_{CC} x 0.7		V_{CC}	V
V_{IH}	RST Input High Voltage(1)		V_{CC} x 0.7		V_{CC}	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 Current	V_{CC} x 0.7 < V_{IH} < V_{CC}			150	µA
V_{OH}	SDA/IO Output High Voltage	20K ohm 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

Note: 1. V_{IL} min and V_{IH} max are reference only and are not tested

Table 10-1.

AC Characteristics Applicable over recommended operating range from V_{CC} = +2.7 to 5.5V T_{AC} = -40° to +85° C (unless otherwise noted)				
Symbol	**Parameter**	**Min**	**Max**	**Units**
f_{CLK}	Async Clock Frequency (V_{CC} Range: +4.5 - 5.5V)	1	5	MHz
f_{CLK}	Async Clock Frequency (V_{CC} Range: +2.7 - 3.3V)	1	4	MHz
f_{CLK}	Synchronous 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		35	ns
$t_{HD.STA}$	Start Hold Time	200		ns
$t_{SU.STA}$	Start Set-up Time	200		ns
$t_{HU.DAT}$	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 (at 25° C)		5	ms
t_{WR}	Write Cycle Time		7	ms

10.2 Timing Diagrams for Synchronous Communications

Figure 10-1. Bus Timing:
SCL: Serial Clock, SDA: Serial Data I/O

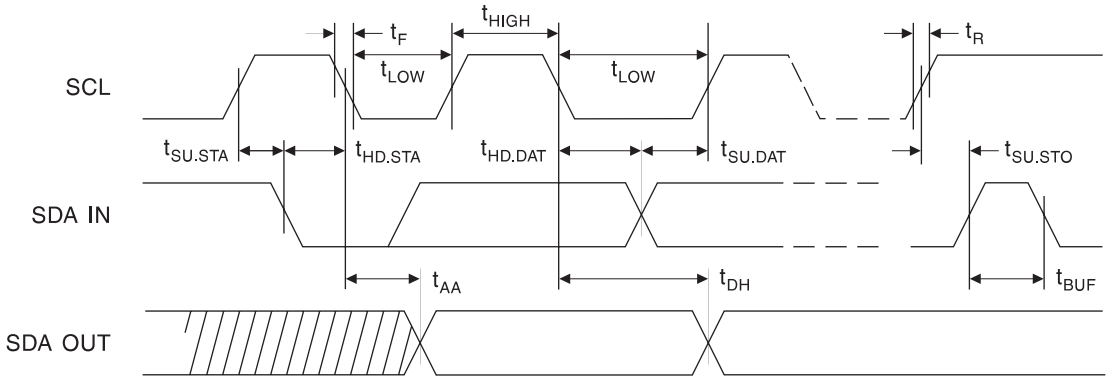
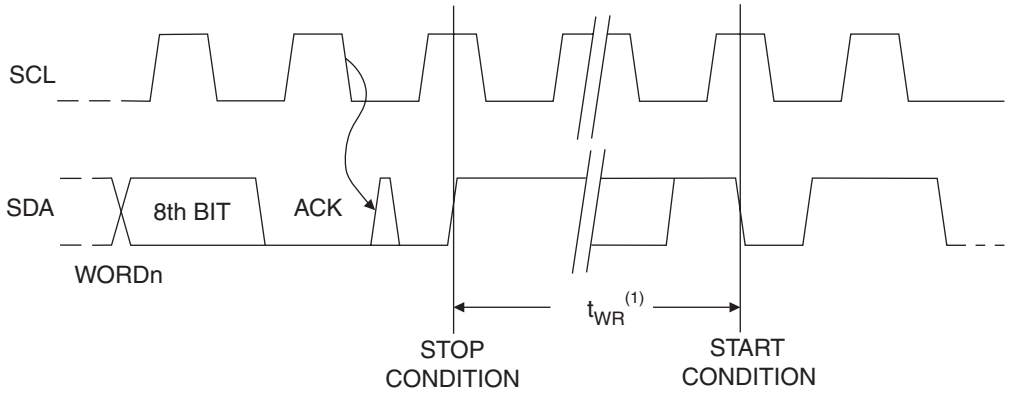


Figure 10-2. Write Cycle Timing:
SCL: Serial Clock, SDA: Serial Data I/O



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 10-3. Data Validity

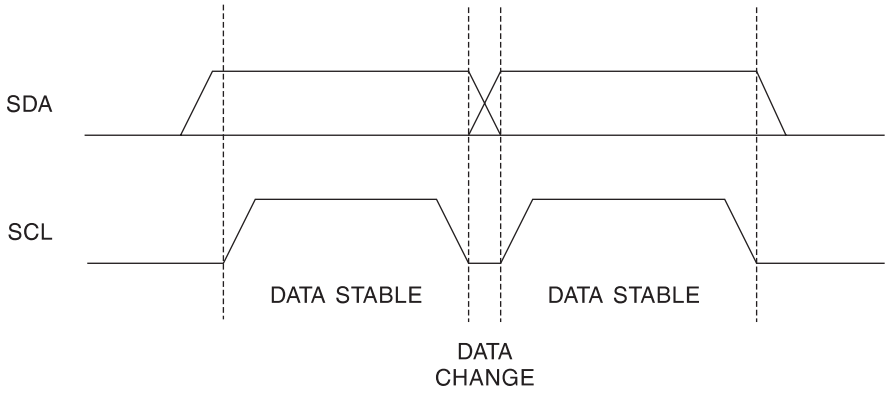


Figure 10-4. Start and Stop Definition

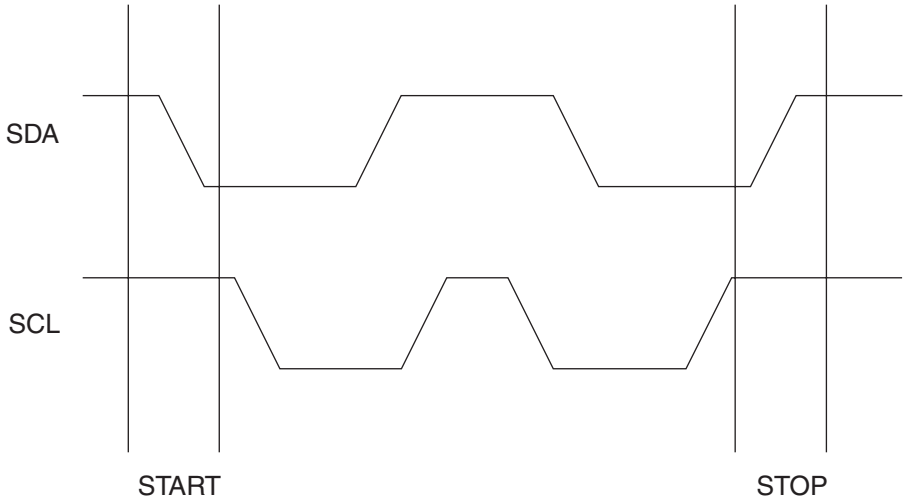
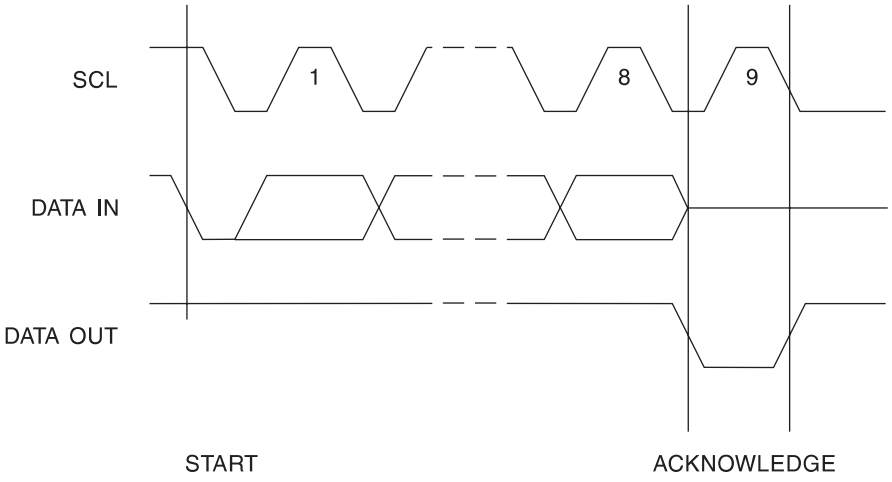


Figure 10-5. Output Acknowledge



11. DC Tamper Detection Limits

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

11.1 High Voltage and Low Voltage Limit

If V_{CC} is taken below or above these voltage limits the device will enter a reset sequence once V_{CC} is retuned to normal levels and before the device operation can begin again.

11.2 Minimum Clock Pulse

In synchronous operation if the clock pulse width falls below the limit of this circuit the device will enter a reset sequence.

11.3 Maximum Clock Frequency

In asynchronous operation if the clock frequency exceeds the limit of this circuit the device will enter a reset sequence.

11.4 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.

11.5 Noise Suppression

Pulses of short duration on SCL/CLK, SDA/IO and RST are ignored if they fall below the threshold of this circuit. The pulses are filtered out and the device does not enter the reset sequence.

Tamper Detection
Applicable over recommended operating range from T_{AC} = -40° to +85° C (unles otherwise noted)

Symbol	Parameter	Test Condition	Min	Typ	Max	Units
V_{cc}	High Voltage Limit		6.0		6.5	V
V_{cc}	Low Voltage Limit		2.0		2.4	V
t_{CLK}	Minimum CLK pulse width	Synchronous Operation	200		280	nS
f_{CLK}	Minimum CLK frequency	Asynchronous Operation	12		14	MHz
t_{POR}	POR Delay		10		70	uS
t_{SUP}	Min. SCL, SDA, RST pulse		50		200	uS

Atmel Corporation

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

Regional Headquarters

Europe
Atmel Sarl
Route des Arsenaux 41
Case Postale 80
CH-1705 Fribourg
Switzerland
Tel: (41) 26-426-5555
Fax: (41) 26-426-5500

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

Japan
9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
Japan
Tel: (81) 3-3523-3551
Fax: (81) 3-3523-7581

Atmel Operations

Memory
2325 Orchard Parkway
San Jose, CA 95131, USA
Tel: 1(408) 441-0311
Fax: 1(408) 436-4314

Microcontrollers
2325 Orchard Parkway
San Jose, CA 95131, USA
Tel: 1(408) 441-0311
Fax: 1(408) 436-4314

La Chantrerie
BP 70602
44306 Nantes Cedex 3, France
Tel: (33) 2-40-18-18-18
Fax: (33) 2-40-18-19-60

ASIC/ASSP/Smart Cards
Zone Industrielle
13106 Rousset Cedex, France
Tel: (33) 4-42-53-60-00
Fax: (33) 4-42-53-60-01

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906, USA
Tel: 1(719) 576-3300
Fax: 1(719) 540-1759

Scottish Enterprise Technology Park
Maxwell Building
East Kilbride G75 0QR, Scotland
Tel: (44) 1355-803-000
Fax: (44) 1355-242-743

RF/Automotive
Theresienstrasse 2
Postfach 3535
74025 Heilbronn, Germany
Tel: (49) 71-31-67-0
Fax: (49) 71-31-67-2340

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906, USA
Tel: 1(719) 576-3300
Fax: 1(719) 540-1759

Biometrics
Avenue de Rochepleine
BP 123
38521 Saint-Egreve Cedex, France
Tel: (33) 4-76-58-47-50
Fax: (33) 4-76-58-47-60

Literature Requests
www.atmel.com/literature