

CryptoMemory® Devices

AT88SC0104C,	AT88SC0204C,	AT88SC0404C
AT88SC0808C,	AT88SC1616C,	AT88SC3216C
AT88SC6416C,	AT88SC12816C,	AT88SC25616C

Features

- A Family of Nine Devices with User Memories from 1-Kbit to 256-Kbit
- EEPROM User Memory
 - 4, 8, or 16 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
 - 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
 - Two-Wire serial interface
 - 1 MHz compatibility for fast operation
 - Standard 8-lead plastic packages
 - Same pinout as Two-Wire serial EEPROMs
- Smart Card Features
 - ISO 7816 Class A (5V) or Class B (3V) operation

- Synchronous Two-Wire serial interface for faster device initialization*
- ISO 7816-3 asynchronous T = 0 protocol*
- Multiple zones, key sets and passwords for multi-application use
- Programmable 8-byte Answer-To-Reset (ATR) Register
- ISO 7816-2 compliant modules
- High Reliability
 - Endurance: 100,000 cycles
 - Data retention: 10 years
 - ESD Protection: 4,000V

Note: * Modules available with either Two-Wire or T = 0 modes.

Table of Contents

CryptoMemory® Devices.....	1
Features.....	1
1. Pin Configuration and Package Information.....	6
1.1. Pin Configuration.....	6
1.2. Package Information.....	6
2. Description.....	7
2.1. Embedded Applications.....	7
2.2. Smart Card Applications.....	7
2.3. Scope and Purpose of This Document.....	7
3. Pin Description.....	9
3.1. Supply Voltage (V_{CC}).....	9
3.2. Clock (SCL/CLK).....	9
3.3. Serial Data (SDA/IO).....	9
3.4. Reset (RST).....	9
4. Detailed Description.....	10
4.1. User Memory.....	10
4.2. Control Logic.....	14
4.3. Configuration Memory.....	14
5. Communication Security Modes.....	18
5.1. Security Operations.....	18
5.1.1. Password Verification.....	18
5.1.2. Mutual Authentication.....	18
5.1.3. Data Encryption.....	19
5.1.4. Encrypted Checksum.....	20
5.2. Data Protection Features.....	20
5.2.1. Modify Forbidden.....	21
5.2.2. Program Only.....	21
5.2.3. Write Lock.....	21
5.2.4. Anti-tearing (Power Loss Protection).....	21
5.3. Configuration Memory Values.....	21
5.3.1. Default Values.....	21
5.3.2. Answer-to-Reset (ATR).....	22
5.3.3. FAB Code.....	22
5.3.4. Memory Test Zone (MTZ).....	22
5.3.5. Card Manufacturer Code.....	22
5.3.6. Lot History Code.....	22
5.3.7. Issuer Code.....	22
5.3.8. Device Configuration Register (DCR).....	22
5.3.9. Access Registers.....	23
5.3.10. Password/Key Registers.....	24
5.3.11. Identification Number.....	25

5.3.12.	Cryptograms ($C_0 - C_3$).....	25
5.3.13.	Session Keys ($S_0 - S_3$).....	25
5.3.14.	Secret Seeds ($G_0 - G_3$).....	25
5.3.15.	Password Sets.....	25
5.3.16.	Secure Code.....	25
5.3.17.	Password Attempts Counters (PAC).....	26
5.3.18.	Authentication Attempts Counters (AAC).....	26
5.4.	Security Fuses.....	26
6.	Protocol Selection.....	28
6.1.	Synchronous Mode for Embedded Applications.....	28
6.2.	Asynchronous Mode for Smart Card Applications.....	28
7.	Synchronous Protocol.....	30
7.1.	Start-up Sequence.....	30
7.2.	Command Set.....	30
7.3.	Command Format.....	31
7.4.	Acknowledge Polling.....	32
7.5.	Device Addressing.....	33
7.6.	Command Descriptions.....	33
7.6.1.	Write User Zone: \$B0.....	34
7.6.2.	Read User Zone: \$B2.....	35
7.6.3.	System WRITE: \$B4.....	36
7.6.4.	System Read: \$B6.....	38
7.6.5.	Verify Crypto: \$B8.....	39
7.6.6.	Verify Password: \$BA.....	40
8.	Synchronous Initialization Example.....	42
8.1.	Write Data to User Zones.....	42
8.2.	Unlock the Configuration Memory.....	42
8.3.	Write Data to the Configuration Memory.....	42
8.4.	Set Security Fuses.....	42
9.	Asynchronous T=0 Protocol.....	45
9.1.	Character Format.....	45
9.2.	Command format.....	45
9.3.	PPS Support.....	45
9.4.	Command Set.....	48
9.4.1.	Status Words.....	49
9.4.2.	Example: Write EEPROM Command.....	50
9.4.3.	Write User Zone: \$B0.....	50
9.4.4.	Read User Zone: \$B2.....	51
9.4.5.	System Write: \$B4.....	52
9.4.6.	Send Checksum.....	53
9.4.7.	System READ: \$B6.....	54
9.4.8.	Verify Crypto: \$B8.....	55
9.4.9.	Verify Password: \$BA.....	56
10.	Asynchronous Initialization Example.....	58
10.1.	Write Data to User Zones.....	58

10.2. Unlock the Configuration Memory.....	58
10.3. Write Data to the Configuration Memory.....	58
10.4. Set Security Fuses.....	58
11. Absolute Maximum Ratings*.....	61
11.1. DC and AC Characteristics.....	61
11.2. Timing Diagrams for Synchronous Communications.....	62
12. DC Tamper Detection Limits.....	65
12.1. High Voltage and Low Voltage Limits.....	65
12.2. Minimum Clock Pulse.....	65
12.3. Maximum Clock Frequency.....	65
12.4. Power-On Reset (POR) Delay.....	65
12.5. Noise Suppression.....	65
13. Ordering Information.....	66
14. Package Marking Information.....	67
14.1. Package Drawings.....	68
14.1.1. 8-Lead SOIC.....	68
15. Revision History.....	71
Microchip Information.....	72
Trademarks.....	72
Legal Notice.....	72
Microchip Devices Code Protection Feature.....	72
Product Page Links.....	73

1. Pin Configuration and Package Information

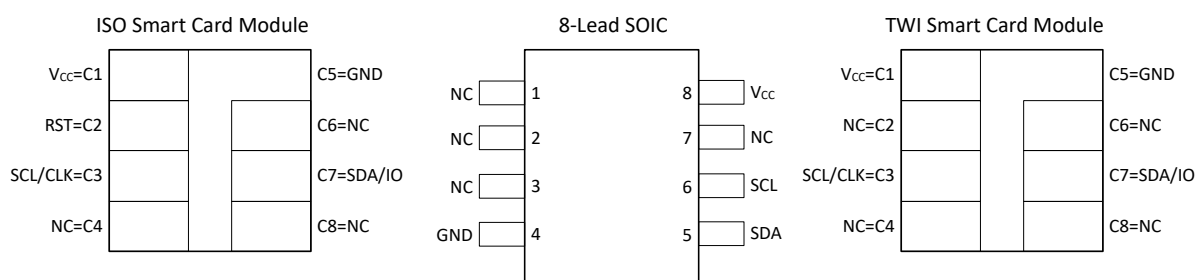
1.1. Pin Configuration

Table 1-1. Package Pin Assignments

Pad	Description	ISO Module	TWI Module	SOIC
V _{CC}	Supply Voltage	C1	C1	8
GND	Ground	C5	C5	4
SCL/CLK	Serial Clock Input	C3	C3	6
SDA/IO	Serial Data Input/Output	C7	C7	5
RST	Reset Input	C2	NC	NC

1.2. Package Information

Figure 1-1. CryptoMemory[®] Packages



2. Description

The Microchip AT88SCxxxxC is a family of nine high-performance secure memory devices, providing 1 Kbit to 256 Kbits 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 effectively provide space for one or multiple data files. A configuration zone contains registers to define the security rights for each user zone, as well as space for passwords and secret keys used by the security logic of Microchip 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 enables dynamic, symmetric-mutual authentication between the device and host, and also 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 Two-Wire serial interface running at 1 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 Two-Wire Serial EEPROMs 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 32 Kbits of user memory or more, communication speeds of 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 Two-Wire serial interface.

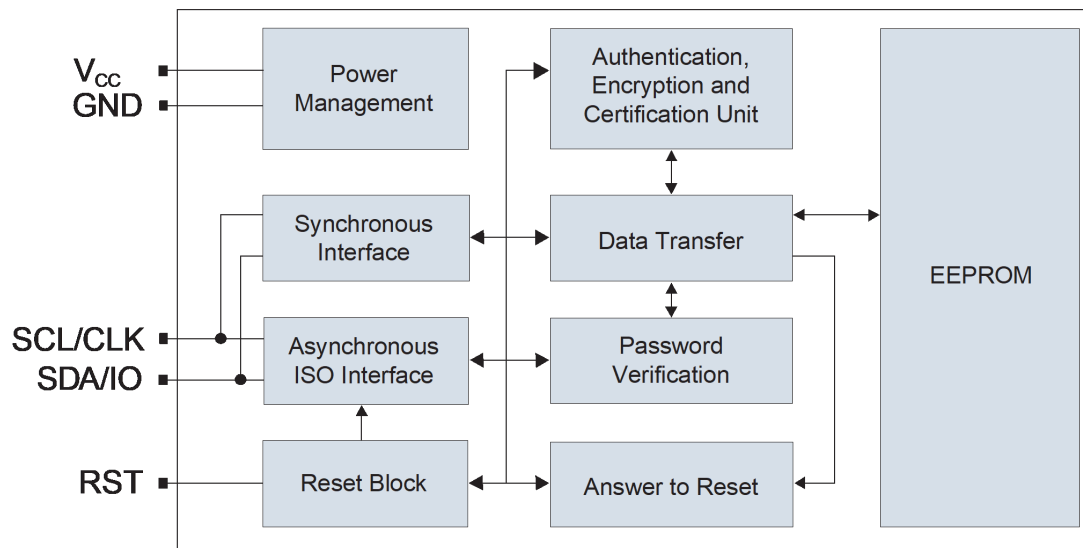
2.3. Scope and Purpose of This Document

This document covers all three major operational modes of CryptoMemory®:

- Standard mode
- Authentication mode
- Encryption mode

It provides all the information necessary to take full advantage of the security capabilities of CryptoMemory. It is designed for use in conjunction with functional cryptographic libraries or companion hardware from Microchip; therefore, it requires cryptographic library and/or companion hardware documentation to complement its use. Contact your regional Microchip sales office for information on the most current versions of functional libraries and available cryptographic companion hardware.

Figure 2-1. Block Diagram



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 bidirectional 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 must be connected between SDA and V_{CC} , a nominal value of 4.7K Ω 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 (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 ATR 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. This is accomplished through programming the Configuration zone 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 initialization examples in [8. Synchronous Initialization Example](#) and [10. Asynchronous Initialization Example](#).

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 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. The following nine tables present the memory maps of the user zones for each device density.

Table 4-1. AT88SC0104C User Memory

Memory Size = 1 Kb, User Zones = 4, Page Size = 16 bytes

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

Table 4-2. AT88SC0204C User Memory

Memory Size = 2 Kb, User Zones = 4, Page Size = 16 bytes

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								

Table 4-3. AT88SC0404C User Memory

Memory Size = 4 Kb, User Zones = 4, Page Size = 16 bytes

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								

Table 4-4. AT88SC0808C User Memory

Memory Size = 8 Kb, User Zones = 8, Page Size = 16 bytes

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

Table 4-5. AT88SC1616C User Memory

Memory Size = 16 Kb, User Zones = 16, Page Size = 16 bytes

Zone		\$0	\$1	\$2	\$3	\$4	\$5	\$6	\$7
User 0	\$00								
	–	128 bytes							
	–								
	\$78								
User 1	\$00								
	–								
	–								
	–								
User 14	\$00								
	–								
	–								
	\$78								
User 15	\$00								
	–	128 bytes							
	–								
	\$78								

Table 4-6. AT88SC3216C User Memory

Memory Size = 32 Kb, User Zones = 16, Page Size = 64 bytes

Zone		\$0	\$1	\$2	\$3	\$4	\$5	\$6	\$7
User 0	\$00								
	—	256 bytes							
	—								
	\$F8								
User 1	\$00								
	—								
	—								
	—								
User 14	\$00								
	—								
	—								
	\$F8								
User 15	\$00								
	—	256 bytes							
	—								
	\$F8								

Table 4-7. AT88SC6416C User Memory

Memory Size = 64 Kb, User Zones = 16, Page Size = 64 bytes

Zone		\$0	\$1	\$2	\$3	\$4	\$5	\$6	\$7
User 0	\$000								
	—	512 bytes							
	—								
	\$1F8								
User 1	\$000								
	—								
	—								
	—								
User 14	\$000								
	—								
	—								
	\$1F8								
User 15	\$000								
	—	512 bytes							
	—								
	\$1F8								

Table 4-8. AT88SC12816C User Memory

Memory Size = 128 Kb, User Zones = 16, Page Size = 128 bytes

Zone		\$0	\$1	\$2	\$3	\$4	\$5	\$6	\$7
User 0	\$000								
	–	1024 bytes							
	–								
	\$3F8								
User 1	\$000								
	–								
	–								
	–								
User 14	\$000								
	–								
	–								
	\$3F8								
User 15	\$000								
	–	1024 bytes							
	–								
	\$3F8								

Table 4-9. AT88SC25616C User Memory

Memory Size = 256 Kb, User Zones = 16, Page Size = 128 bytes

Zone		\$0	\$1	\$2	\$3	\$4	\$5	\$6	\$7
User 0	\$000								
	–	2048 bytes							
	–								
	\$7F8								
User 1	\$000								
	–								
	–								
	–								
User 14	\$000								
	–								
	–								
	\$7F8								
User 15	\$000								
	–	2048 bytes							
	–								
	\$7F8								

4.2. Control Logic

Access to the user zones occurs only through the device's control logic. 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.

4.3. 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 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 four user zones have four sets of registers; those with eight user zones have eight sets of registers; and those with 16 user zones have 16 sets of registers. Unused memory space in the register region becomes reserved to ensure that other components of the configuration memory remain at the same address location regardless of the number of user zones in a device.

Table 4-10. AT88SC0104C/0204C/0404C 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								Secret
\$90	Secret Seed G ₀								
\$98	Secret Seed G ₁								
\$A0	Secret Seed G ₂								
\$A8	Secret Seed G ₃								Password
\$B0	PAC	Write 0			PAC	Read 0			
\$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			Forbidden
\$F0	Reserved								
\$F8									

Table 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	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								Secret
\$90	Secret Seed G ₀								
\$98	Secret Seed G ₁								
\$A0	Secret Seed G ₂								
\$A8	Secret Seed G ₃								Password
\$B0	PAC	Write 0			PAC	Read 0			
\$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			Forbidden
\$F0	Reserved								
\$F8									

Table 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	AAC0	Cryptogram C ₀							
\$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. Communication Security Modes

Communication between the device and host operates in three basic modes.

- Standard mode — Default mode for the device after power-up
- Authentication mode — Activated by a successful authentication sequence
- Encryption mode — Activated by a successful encryption activation following a successful authentication

Data transferred to and from the device is handled per the following table.

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

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

- MAC: Message Authentication Code

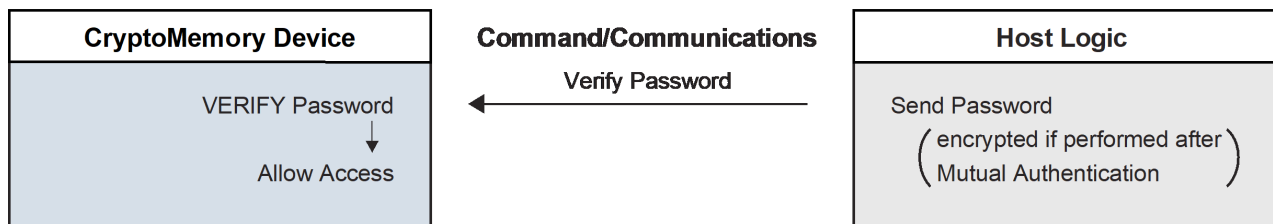
5.1. Security Operations

5.1.1. Password Verification

The use of passwords protects read and write access to the user zones. Any one of eight password sets is available for assignment to any user zone through configuration of the access registers.

CryptoMemory® provides separate 24-bit passwords for read and write operations. Read passwords grant only read access to zones under password protection, while write passwords grant both read and write access. 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



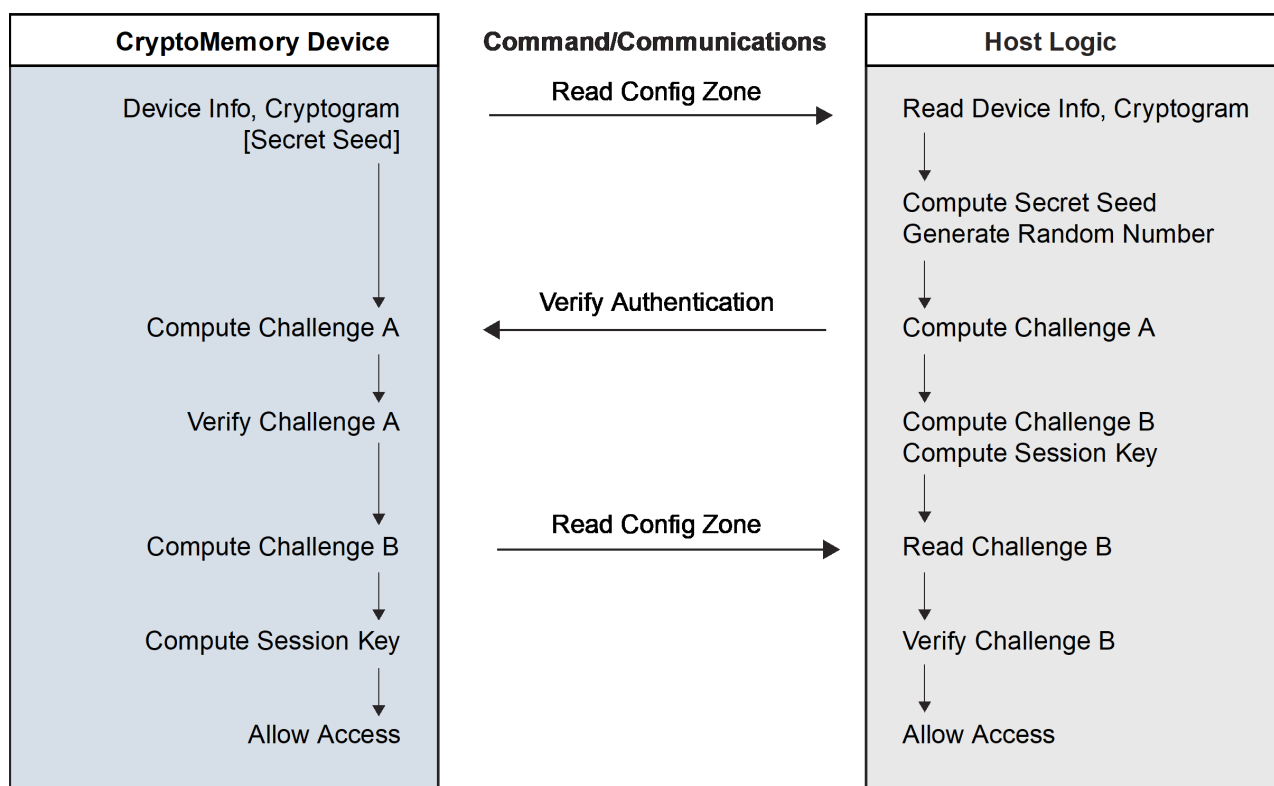
5.1.2. Mutual Authentication

The 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 until the next call to the Verify Crypto command or device reset. Only one key set may be active at any time. Unsuccessful calls of the Verify Crypto command will exit Authentication mode and will decrement 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 the current cryptogram, 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 and 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 newly calculated 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. Mutual authentication requires the use of the verify authentication variant of the Verify Crypto command (see [Table 7-1](#), or [Table 9-2](#)).

Figure 5-2. The Mutual Authentication Process



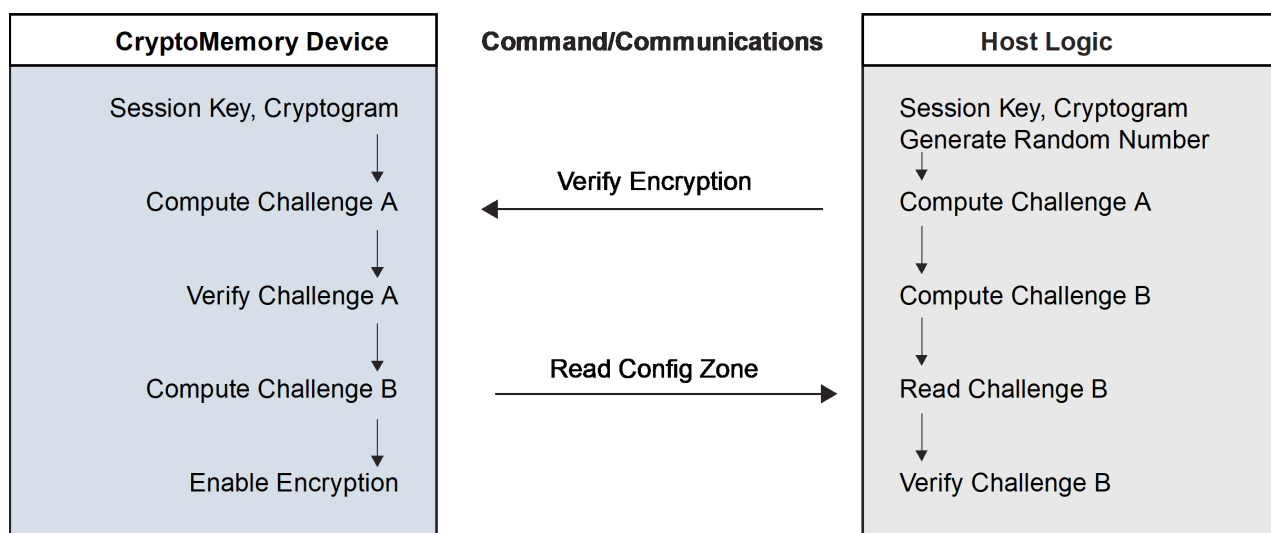
5.1.3. Data Encryption

CryptoMemory[®] allows the use of encryption between a host system and the CryptoMemory device to protect the confidentiality of data during read-write access and password verification operations. To enable encryption, the host must issue the Verify Crypto command with a valid session encryption key while the device is 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 all data exchanged between the host and the device's user zones will be encrypted. If a user

zone configuration in the access register requires encryption, the host must enter Encryption mode and must encrypt all data transmitted to and from the zone for the duration of the active encryption session. Note that CryptoMemory does not encrypt system zone data except for passwords and password attempt counters. These elements 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 a device reset. Only one key set may be active at any time. Unsuccessful calls to the Verify Crypto command exit both Encryption and Authentication modes, and decrement the value of the Authentication Attempts Counter (AAC) register. Decrementing the 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 [Table 7-1](#), or [Table 9-2](#)).

Figure 5-3. Encryption Activation Process from Active Authentication Mode



5.1.4. Encrypted Checksum

CryptoMemory[®] implements a data validity check function in the form of an encrypted checksum. This checksum provides bidirectional data integrity checking and data origin authentication in the form of a Message Authentication Code (MAC). Only the host or 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. Invoking the Read Checksum command resets the device's security settings; therefore, it is recommended to use this command only after all data read operations from the device have been completed.

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 the ability to render individual bytes within a user zone read-only by restricting all write operations to it. It operates at the 8-byte page level whereby the lowest addressed byte of the page serves as the write access control byte for that page. Table 5-2 shows the use of Write Lock for data at addresses \$080 to \$087. The byte at \$080 controls write access to bytes from \$080 to \$087.

Table 5-2. 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.

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 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 are limited to eight bytes.

Data are 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 remain intact in the User zone or Configuration zone. The data are 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 18 ms after each write command when anti-tearing is active. At power-up, five clock cycles are required to check the anti-tearing flags. In the event the device needs to carry out the data recovery process the host is required to perform ACK polling for 14 ms.

5.3. Configuration Memory Values

This section describes each field in the configuration memory.

5.3.1. Default Values

Microchip programs certain fields of the configuration memory at the factory. The customer may elect to change the contents of all of these fields except for the lot history code field, which is

permanently locked. Microchip programs the remainder of the fields, including all configuration memory and user zones, to ones prior to releasing the device from the factory. [Table 5-3](#) summarizes the device fields Microchip programs at the factory. A brief description of each field follows.

Table 5-3. 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 defined by Microchip. This register is read/write accessible prior to blowing the FAB fuse, but becomes read-only after the fuse is blown.

5.3.3. FAB Code

This field is a 16-bit-wide register with content defined by Microchip. It is read/write accessible prior to blowing the FAB fuse, but becomes read-only after the fuse is blown.

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 with 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, allowing the customer to define its content. The content of this field becomes read-only after the PER fuse is blown.

5.3.6. Lot History Code

This field is a 64-bit-wide register with content defined by Microchip. This field is read-only.

5.3.7. Issuer Code

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

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 effect on the device's logic. The default value for each bit is one.

Table 5-4. 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

5.3.8.1. SME (Supervisor Mode Enable)

Asserting this bit (SME = 0) enables Supervisor mode for the Write 7 password, such that verifying the Write 7 password grants read and write access to all password sets and PACs. Verifying the 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)

Asserting this bit (UCR = 0) allows an unlimited number of checksum reads without requiring new authentication. Not asserting this bit (UCR = 1) limits the reading of the checksum to one attempt, after which the device resets the crypto algorithm after executing the Read Checksum command.

5.3.8.3. 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 its value. Asserting this bit also prevents the reset of the crypto algorithm after reading the MAC in Encryption mode. The UAT bit does not affect the Password Attempts Counter.

5.3.8.4. ETA (Eight Trials Allowed)

Asserting this bit (ETA = 0) extends the trials limit to eight 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).

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 with a unique Chip Select address, it is possible to connect up to 15 devices on the same serial data bus and communicate with each individually. Global communication 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 one.

Table 5-5. 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

5.3.9.1. PM(1:0) Password Mode

Table 5-6. 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 following section).

Verification of the write password also allows modification of the read and write passwords for each password set.

5.3.9.2. AM(1:0) Authentication Mode

Table 5-7. 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 access, and read access is free. When AM = 01, the zone requires authentication for both write and read access. 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 section [6. Protocol Selection](#)).

Finally, when AM = 00, Dual Access mode is active, in which authentication using the Program Only Key (POK) grants the right to read and program the zone (i.e., write zeros only), while authentication using the AK grants 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 the AK may reset the token to its full value. See section [6. Protocol Selection](#) on 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 one, even when using the AK.
3. Requiring authentication automatically requires the use of secure checksums for write operations (See [“5.1.4. Encrypted Checksum”](#)).

5.3.9.3. ER (Encryption Required)

When ER = 0, the host is required to activate Encryption mode to enable read/write access to 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 Encryption mode, but isn't specifically required to do so by the device.

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 zero. Bit 7 controls byte 7; bit 6 controls byte 6, and so on. Setting bit 0 to zero 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. Therefore, the user zone must 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 one to zero, but never from zero to one.

5.3.10. Password/Key Registers

Four, eight or sixteen 8-bit password/key registers receive their definitions 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 for each bit is one. Bit 3 is reserved and must be left set to one.

Table 5-8. Password/Key Register Definition

Bit 7	Bit 6	Bit 5	Bit 4	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

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.

5.3.10.2. 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 zeros only) access to the user zone.

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 defined by the customer during personalization. It is recommended that a unique identification number be assigned to each device.

5.3.12. 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.

5.3.13. 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 programming initial values is not necessary.

5.3.14. 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.

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 both the read and write passwords of the same set.

5.3.16. Secure Code

The secure code is the Write 7 password. Properly presenting this password grants write access to the configuration memory during personalization. Microchip defines the initial value of the secure code, but the customer may change this value after successful presentation during a verify

password operation for the Write 7 password. [Table 5-3](#) shows the secure codes for various devices when they leave the Microchip factory. After blowing the PER fuse, verifying the Write 7 password no longer grants 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 consecutive incorrect 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)

Each of the four AAC fields contains an 8-bit attempts counter for the authentication process. Each AAC field corresponds to an authentication key set. The attempts counter limits the number of consecutive incorrect attempts to authenticate to four, 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.

5.4. Security Fuses

CryptoMemory[®] uses four fuses. The status of these fuses is given in a 'fuse byte.' A value of zero indicates that the fuse has been blown. Bits 4 to 7 of this byte are not used as security fuses and are reserved for Microchip use.

Table 5-9. Device Fuses

F7	F6	F5	F4	F3	F2	F1	F0
Resv	Resv	Resv	Resv	SEC	PER	CMA	FAB

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

1. **FAB:** To lock the ATR 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 5-10](#) provides a summary of access rights for all portions of the memory for each fuse condition.

Table 5-10. 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
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				
User Zones	Read	AR	AR	AR	AR
	Write				

Notes:

1. AR: Access rights are defined by the access registers.
2. PW: Password.
3. Secure Code: The Write 7 password is the secure code until the PER fuse is blown.
4. Forbidden: No access is permitted.

6. 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

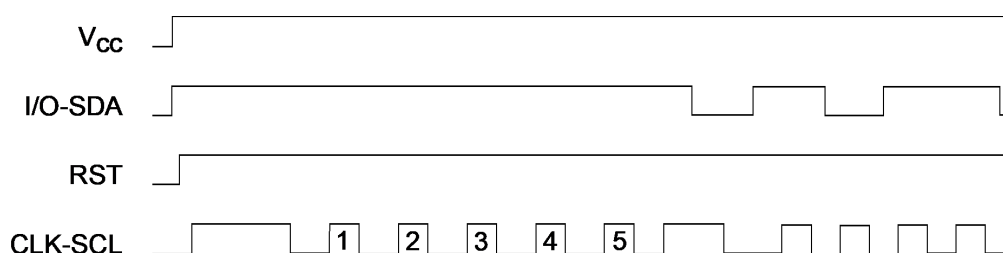
The power-up sequence of CryptoMemory determines its operating mode. A brief description of each mode follows.

6.1. Synchronous Mode for Embedded Applications

The Two-Wire serial interface is used for fast and efficient communication with logic and controllers. 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 available.

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

Figure 6-1. Asynchronous Mode



Asynchronous mode is selected when RST is low on a rising edge of CLK. Once Asynchronous mode has been selected, it is not possible to return to Synchronous mode except by powering the device off and on again.

6.2. 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 to 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](#) and [Table 6-2](#). The historical bytes (T1, T2, T3) indicate 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 when operating in Asynchronous mode. The CryptoMemory device will always output all 8 bytes in response to the asynchronous ATR command, regardless of the contents of the register.

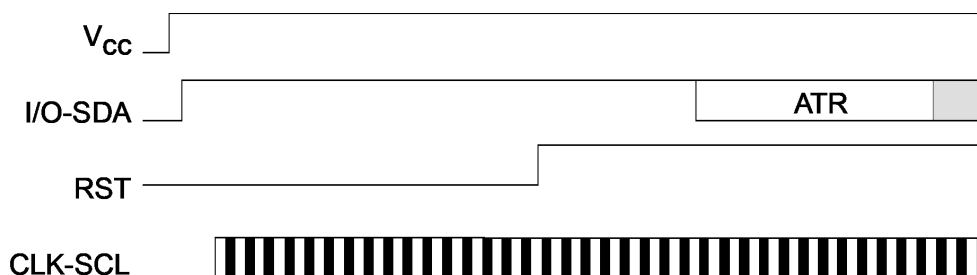
Table 6-1. ATR Codes for Lower Density CryptoMemory®

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 Asynchronous mode has been selected, it is not possible to switch to 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 Kb and larger in user memory. CryptoMemory supports D values of 1, 2, 4, 8, 12, and 16 for an F value of 372. It also supports D values of 8 and 16 for F = 512. This allows selection of eight communication speeds ranging from 9,600 baud to 153,600 baud.

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

7. Synchronous Protocol

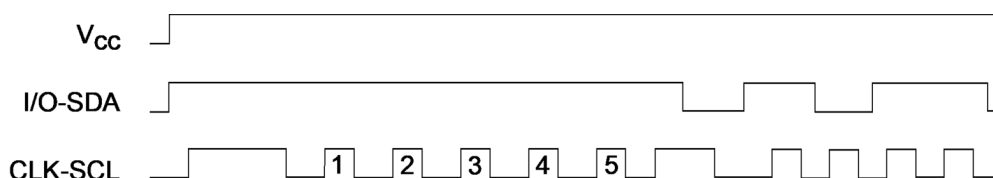
Communication with the CryptoMemory[®] using the synchronous protocol is very similar to communication with AT24Cxxx Serial EEPROM devices using a Two-Wire protocol (TWI). The basic command structure and timing are the same; however, a significant difference exists when reading the CryptoMemory device, which is described below.

7.1. Start-up Sequence

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

- Power-up V_{CC} .
- An external pull-up resistor pulls I/O-SDA high with V_{CC} .
- After V_{CC} is stable, five pulses are applied to CLK-SCL.
- CLK-SCL and I/O-SDA may then be driven.

Figure 7-1. Start-up Sequence



7.2. Command Set

The command set of CryptoMemory[®] is expanded compared to that of a Serial EEPROM, as the functionality of CryptoMemory exceeds that of a simple memory device. Each instruction sent to the CryptoMemory must contain four bytes:

- Command
- Address 1
- Address 2
- N

The value of N in the final instruction byte defines the number of additional data bytes to be sent or received from the CryptoMemory device.

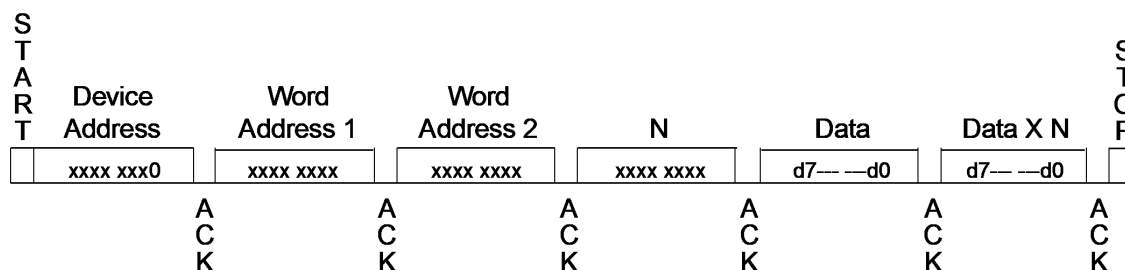
Table 7-1. CryptoMemory[®] Synchronous Command Set

Command Description		Command	ADDR 1	ADDR 2	N	Data(N)
Write User Zone	Normal (AT88SC0104C-AT88SC1616C)	\$B0	ADDR	ADDR	$N \leq 10$	N bytes
	Normal (AT88SC3216C, AT88SC6416C)	\$B0	ADDR	ADDR	$N \leq 40$	N bytes
	Normal (AT88SC12816C, AT88SC25616C)	\$B0	ADDR	ADDR	$N \leq 80$	N bytes
	With Anti-Tearing (All Devices)	\$B0	ADDR	ADDR	$N \leq 08$	N bytes
Read User Zone		\$B2	ADDR	ADDR	N	
System Write	Write Config Zone (AT88SC0104C-AT88SC1616C)	\$B4	\$00	ADDR	$N \leq 10$	N bytes
	Write Config Zone (AT88SC3216C, AT88SC6416C)	\$B4	\$00	ADDR	$N \leq 40$	N bytes
	Write Config Zone (AT88SC12816C, AT88SC25616C)	\$B4	\$00	ADDR	$N \leq 80$	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	$N \leq 08$	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)

7.3. 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 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, which will acknowledge each byte.

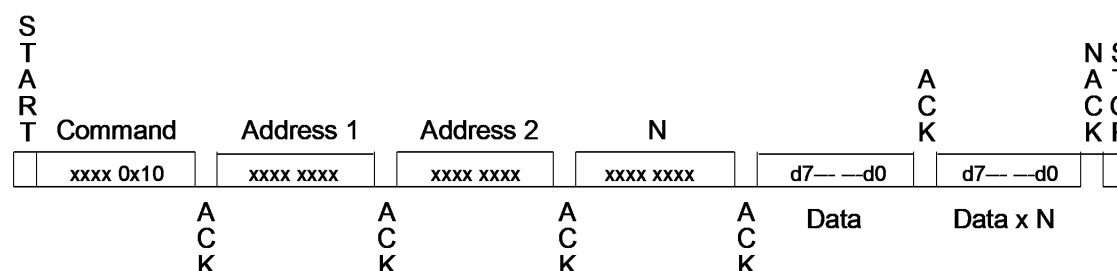
Figure 7-2. TWI Write Command



All CryptoMemory commands have a zero in the LSB of the first byte. All CryptoMemory commands use four bytes to define the command and address the memory. All CryptoMemory commands, except for the read commands, send an additional 0 to 128 bytes of data following the four 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 resembles a TWI write command (LSB of the first byte = 0), but after the fourth byte of the command, the CryptoMemory device begins to send data back on the bus. The number of bytes sent by CryptoMemory will be equal to the value of N.

Figure 7-3. CryptoMemory[®] Read Command



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

7.4. 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 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 that 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 for 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	5 ms
	Normal with Anti-Tearing	\$B0	addr	addr	N	Required, any CMD	20 ms
	Encrypted	\$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	addr	addr	N	Required, any CMD	5 ms
	Write Fuses	\$B4	\$00	fuse ID	\$00	Required, any CMD	5 ms
	Send Checksum	\$B4	\$01	\$00	\$02	Required, any CMD	5 ms
	Send Checksum with Anti-Tearing	\$B4	\$02	\$00	\$02	Required, any CMD	20 ms
	Set User Zone	\$B4	\$03	zone	\$00	Not Required	0
	Write Config Zone with Anti-Tearing	\$B4	\$08	addr	N	Required, any CMD	20 ms
	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 Crypto	Verify Authentication	\$B8	\$0X	\$00	\$10	Required; B2 or B6 only	10 ms
	Verify Encryption	\$B8	\$1X	\$00	\$10	Required; B2 or B6 only	10 ms
Verify Password	Write Password	\$BA	\$0X	\$00	\$01	Required; B2 or B6 only	10 ms
	Read Password	\$BA	\$1X	\$00	\$03	Required; B2 or B6 only	10 ms

Note: Delays are based on operation at 25°C.

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 Microchip 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 must be set to \$B as well.

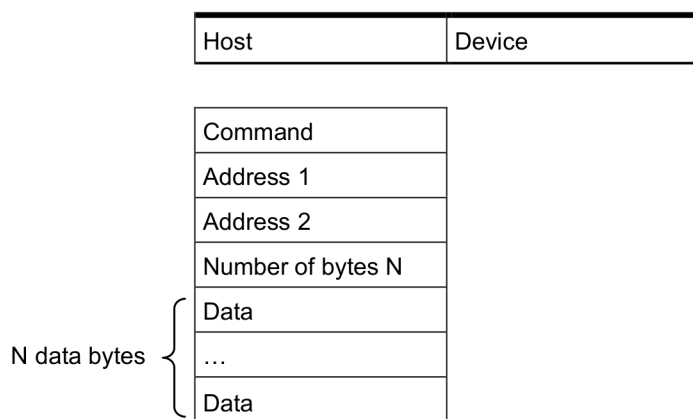
7.6. Command Descriptions

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

7.6.1. Write User Zone: \$B0

7.6.1.1. Functional

Figure 7-4. Write User Zone Command Functional Description



The Write User Zone command \$B0 allows writing of data to the device's currently selected user zone (the procedure for selecting a user zone is described in section 7.6.3. [System WRITE: \\$B4](#)).

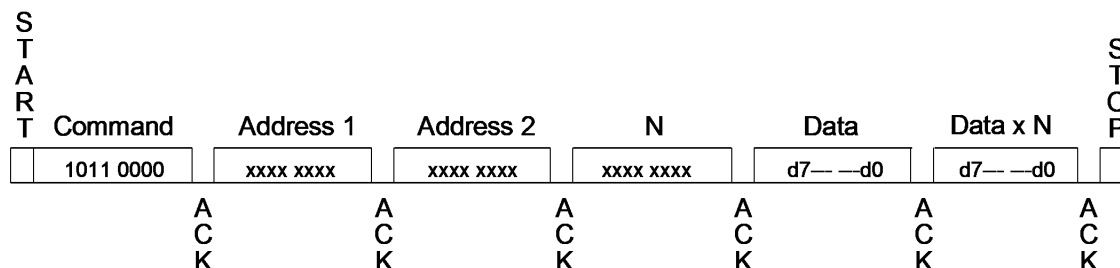
The data byte address to be written is defined by Address 1 and Address 2 in the command. The value N defines how many bytes to write. The maximum number of bytes that may be written is as follows:

- \$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 must 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 unless operating in Encrypted mode; in that case, this command must be followed by the send Checksum command.

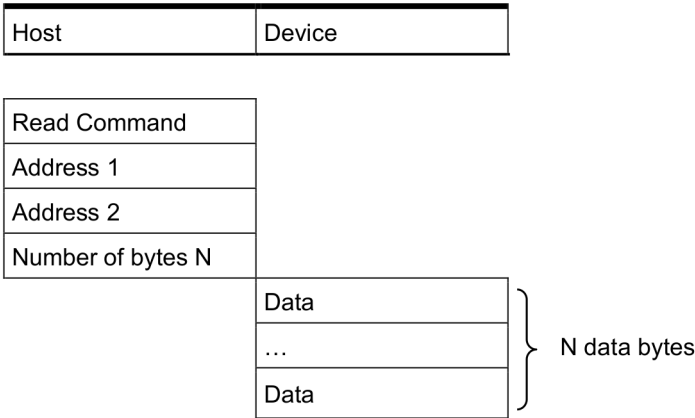
Figure 7-5. Write User Zone



7.6.2. Read User Zone: \$B2

7.6.2.1. Functional

Figure 7-6. Read User Zone Command Functional Description

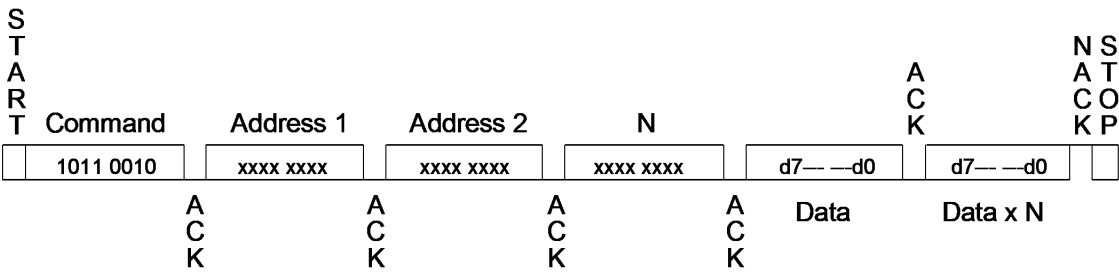


The Read User Zone command \$B2 allows reading of data from the device's currently selected user zone (the procedure for selecting a user zone is described in section 7.6.3. [System WRITE: \\$B4](#)).

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 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.

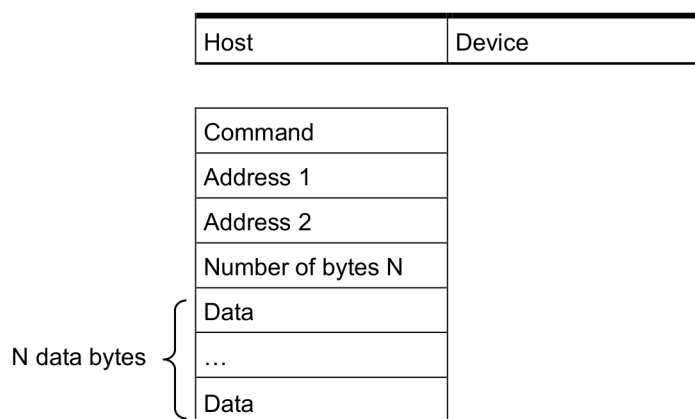
Figure 7-7. Read User Zone



7.6.3. System WRITE: \$B4

7.6.3.1. Functional

Figure 7-8. System Write Command Functional Description



The System Write command allows writing of system data to the device. Depending on the value of the Address 1 parameter, the host may write data to 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	$N \leq \$10$	N bytes
Write Config Zone AT88SC3216C-AT88SC6416C	\$B4	\$00	ADDR	$N \leq \$40$	N bytes
Write Config Zone AT88SC12816C-AT88SC25616C	\$B4	\$00	ADDR	$N \leq \$80$	N bytes
Write Fuses	\$B4	\$01	Fuse ID	\$00	
Send Checksum	\$B4	\$02	\$00	\$02	2 bytes
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 must 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 specify 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.

7.6.3.3. Write Fuses

The fuses may only be “programmed,” that is, written from one to zero. 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 zero, and PER only if CMA is zero. 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. Send Checksum

To write data to user zones that require authentication for write access (AM [1:0] = 00 or 10 in the access register), the host must 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 sends the checksum it has computed using the System Write command with Address 1 = \$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.

7.6.3.5. Set User Zone

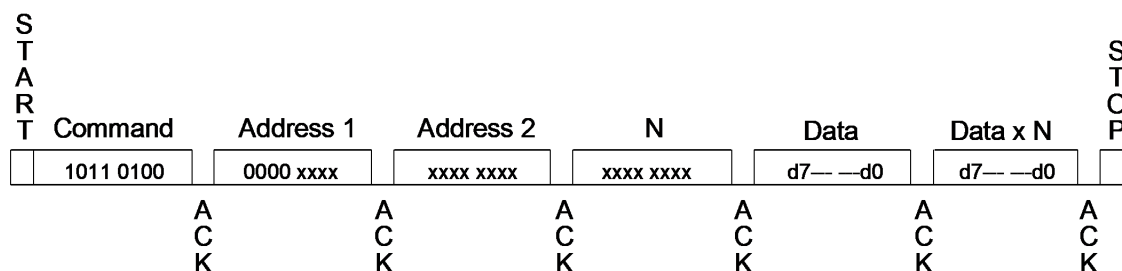
Before reading and writing data in the user zones, the host must select a zone with this command. At this time, the host chooses whether anti-tearing will be active for this zone.

Table 7-5. Anti-Tearing

Command Description	Command	Addr 1	Addr 2	N	Data(N)
Write Config Zone with Anti-Tearing	\$B4	\$08	ADDR	$N \leq \$08$	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 Configuration zone command.

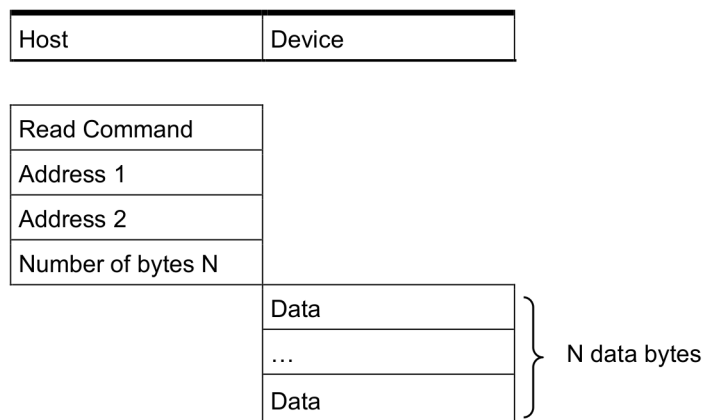
To enable anti-tearing for writes to a user zone, a Set User Zone command is executed with Address 1 set to \$0B. All subsequent Write User Zone commands will be executed with anti-tearing enabled until the next Set User Zone command. Anti-tearing must be turned off if not required, as it would otherwise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

Figure 7-9. System Write

7.6.4. System Read: \$B6

7.6.4.1. Functional

Figure 7-10. 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 data from the configuration memory, the fuses or a checksum.

Table 7-6. System Read Command Detail

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

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 unauthorized, the device will not ACK the N-byte and will not return any data. Since access rights vary throughout the configuration memory, 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.

7.6.4.3. Read Fuse Byte

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

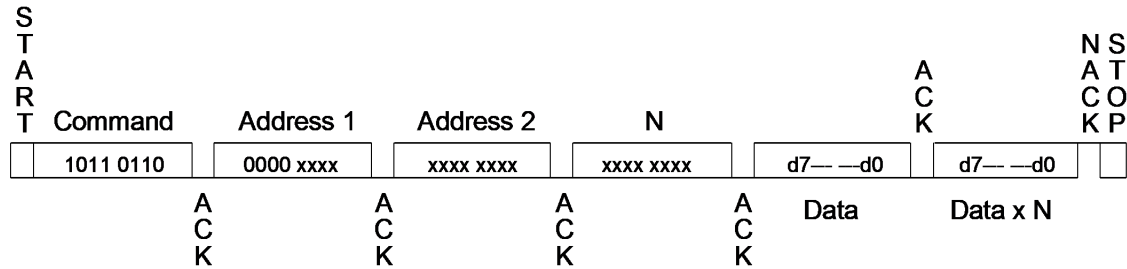
Table 7-7. Fuse Byte Definition

F ₇	F ₆	F ₅	F ₄	F ₃	F ₂	F ₁	F ₀
resv	resv	resv	resv	SEC	PER	CMA	FAB

7.6.4.4. Read Checksum

The checksum consists of two bytes, and the Read Checksum command must be sent with parameter N set to 2.

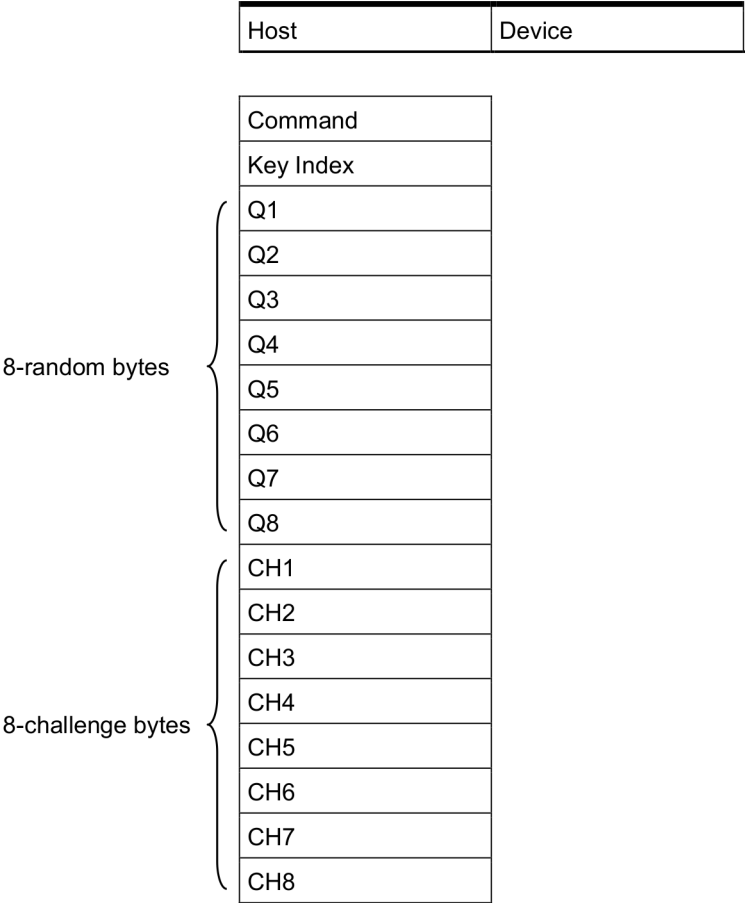
Figure 7-11. System Read



7.6.5. Verify Crypto: \$B8

7.6.5.1. Functional

Figure 7-12. 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 the 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.

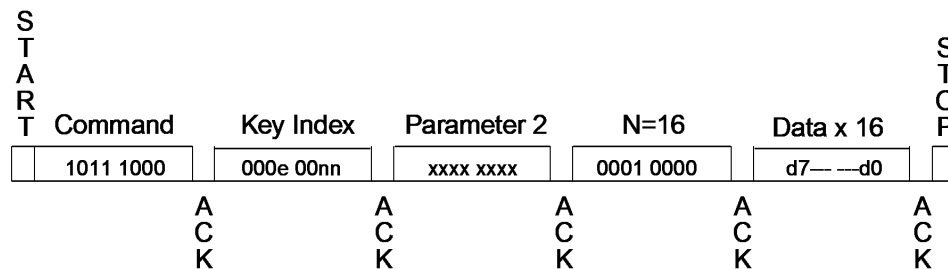
Key index:

- 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 7-13. Verify Crypto

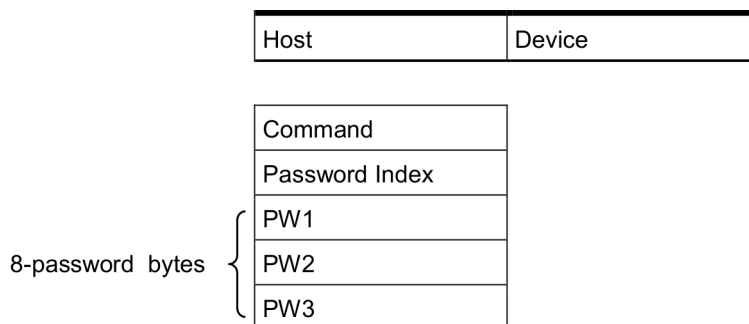


Once the sequence has been carried out, the device requires the host to perform an ACK polling with either the Read User Zone \$B2 command or System Read \$B6 command. To verify whether the authentication succeeded, the host can either read the associated attempts counter to confirm the value is \$FF, or read the post-authentication cryptogram from the device and compare it with the cryptogram generated when the host computed the challenge bytes.

7.6.6. Verify Password: \$BA

7.6.6.1. Functional

Figure 7-14. Verify Password Command Functional Description



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

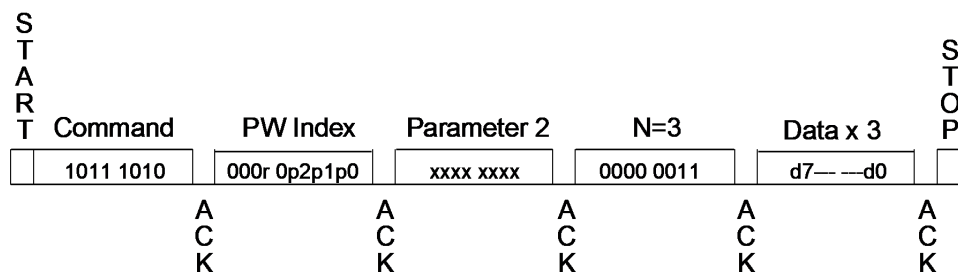
Write password indices: \$00 to \$07 for passwords 0 to 7.

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 7-15. 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. To determine whether the inserted password was correct, the host can read the corresponding password attempts counter and verify that the value is \$FF.

8. Synchronous Initialization Example

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

8.1. Write Data to User Zones

In the default configuration from Microchip, all user zones have free access rights. Writing initial data into the user zones must 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.

8.2. Unlock the 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 Microchip to unlock the configuration memory. Use the Read Config Zone command to read back the security code at address \$E9 to verify that the configuration memory has been unlocked.

8.3. 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.

8.4. Set Security Fuses

Once all data have been written and verified in the user zones and the configuration memory, the security fuses must 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 in the specified order: first FAB, followed by CMA, and then PER. Each fuse is set individually using the Write Fuse command. The status of all three fuses can be verified using the Read Fuse command. Once all fuses have been set, the Read Fuse command will 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 each of the four user zones. The security for each of the four user zones and the associated register values are shown in the table below. Simple values for codes, keys, and passwords are used.

Table 8-1. Example Zones Configuration

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 section 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 (*).

***AT88SC0104C 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 MEMORY
BA 07 00 03 DD 42 97

*WRITE CODES IN CONFIGURATION MEMORY
*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 MEMORY
*Write Registers AR1/PR1 = 7F F9, AR2/PR2 = DF BF, AR3/PR3 = 57 B9
B4 00 22 06 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, read 7 = 10 00 01, write 7 = 11 00 11
B4 00 22 06 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
B4 00 B9 07 11 00 11 FF 10 00 01

*READ ENTIRE CONFIGURATION MEMORY 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 DF BF 57 B9 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 22 22 22 22 22 22 22 22 FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
5B 4F 9A E4 B5 09 8B E7 D8 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

```

```
*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:
```

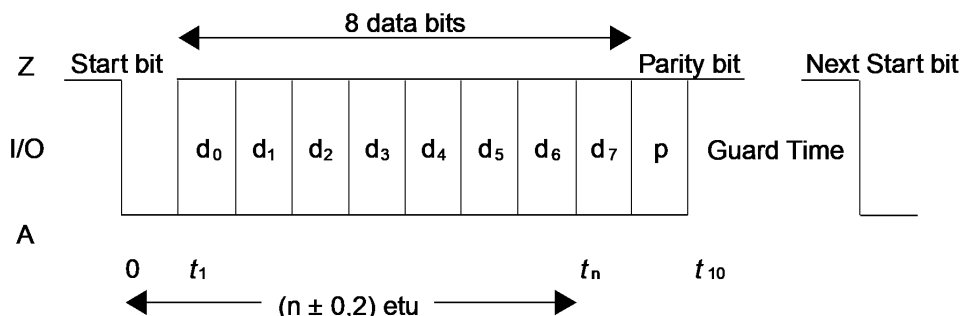
```
00
```

9. Asynchronous T=0 Protocol

9.1. 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.

Figure 9-1. Character Format



Note: The byte is transmitted with the least significant bit first

Even parity is used: the parity bit is set so that the overall sum of the 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 instructs the transmitting device to retransmit the byte.

9.2. Command format

The command sequence is as follows:

- In compliance with ISO 7816-3, the host must send a header consisting of five characters: CLA, INS, P1, P2 and P3
 - CLA refers to a class of instructions. This byte is not 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.
- The device replies with a "procedure byte," normally equal to the INS code received. If a problem occurs, the device will respond with a status word pair, SW1-SW2, indicating the end of the command.
- Data transfer (P3 bytes).
- A final SW1-SW2 sequence gives the status of the device after completion of the command. 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 be sent again (see character format).

9.3. PPS Support

All CryptoMemory[®] devices with user memory size 32Kb and larger support the Protocol and Parameter Selection (PPS) protocol, Section 7 of ISO 7816-3. This section only applies to these larger devices; CryptoMemory devices with memory sizes 16-Kbit or smaller do not support PPS.

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 four 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 32Kb and above.

Table 9-1. PPS1 Values Supported by Microchip CryptoMemory[®]

DI	DI	f Max	4MHz	5MHz	5MHz
		FI	0000b	0001b	1001b
		FI	372	372	372
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. The following are four examples of PPS requests and responses:

Example: We assume 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 that results in the specified baud rate.

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

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

Example: The reader insists on negotiating Fn and Dn equal to the default values, even though these would be used by default without a PPS exchange. There are two ways to do this: by sending PPS1_request = \$11 or by 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

Example: The reader attempts to negotiate values that are not supported by the CryptoMemory device. In its response, the CryptoMemory proposes to continue with the existing F and D values 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

Example: 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 the use of a TA(2) byte in the ATR.

9.4. Command Set

Table 9-2. CryptoMemory[®] Asynchronous Command Set

	Command Description		CLA	INS	P1	P2	P3	Data(N)
B0	Write User Zone	Normal (0104C-1616C)	\$00	\$B0	ADDR	ADDR	$N \leq \$10$	N bytes
		Normal (3216C, 6416C)	\$00	\$B0	ADDR	ADDR	$N \leq \$40$	N bytes
		Normal (12816C, 25616C)	\$00	\$B0	ADDR	ADDR	$N \leq \$80$	N bytes
		With Anti-Tearing (all devices)	\$00	\$B0	ADDR	ADDR	$N \leq \$08$	N bytes
B2	Read User Zone		\$00	\$B2	ADDR	ADDR	N	
B4	System Write	Write Config Zone (Devices 0104C-1616C)	\$00	\$B4	\$00	ADDR	$N \leq \$10$	N bytes
		Write Config Zone (Devices 3216C, 6416C)	\$00	\$B4	\$00	ADDR	$N \leq \$40$	N bytes
		Write Config Zone (Devices 12816C, 25616C)	\$00	\$B4	\$00	ADDR	$N \leq \$80$	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 Zone w/a-t	\$00	\$B4	\$08	ADDR	$N \leq \$08$	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 (0-7)
		Read Password	\$00	\$BA	\$1X	\$00	\$03	3-byte password X = password set (0-7)

9.4.1. Status Words

Table 9-3. CryptoMemory[®] Asynchronous Mode Status Words

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. Under 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.

- The Status Word \$62 \$00 is returned after a write command when the device is waiting for the host to send a secure checksum before initiating the write cycle. This will happen only in Authentication mode and Encryption mode.
- The Status Word \$67 \$00 is returned in place of the procedure byte when the number of data bytes to be transferred is incorrect.
- The Status Word \$69 \$00 is returned in place of the procedure byte after read/write commands if the host is not allowed to read or write at the address provided. It is also returned after a password command 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, authentication or encryption activation failed due to invalid data, or if any incoming command failed due to a bad checksum (MAC).
- The Status Word \$6B \$00 is returned in place of the procedure byte if the address is incorrect.
- The Status Word \$6D \$00 is returned in place of the procedure byte if the INS code received is not supported.

9.4.2. Example: Write EEPROM Command

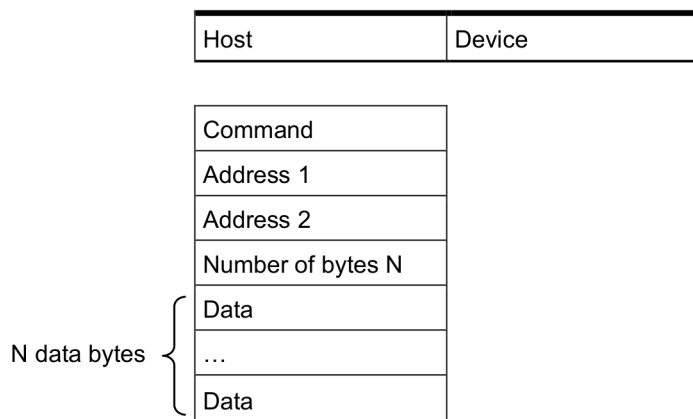
The following illustrates the data exchanges that occur during a write operation of four bytes—\$04, \$09, \$19 and \$97—to addresses \$02, \$03, \$04, \$05 in the current user zone.

Steps	Host	Device	Val	Note
Start	CLA		**	Class (ignored by CryptoMemory [®])
Step 2	INS		\$B0	Write Instruction
Step 3	P1		**	Address byte A1 (ignored by 0104C - 1616C)
Step 4	P2		\$02	Address byte A2 = \$02
Step 5	P3		\$04	Four data bytes
Step 6		INS	\$B0	Device responds with INS code
Step 7	Data		\$04	Byte to be written at start address \$02
Step 8	Data		\$09	Byte to be written at address \$03
Step 9	Data		\$19	Byte to be written at address \$04
Step 10	Data		\$97	Byte to be written at address \$05
Step 11		Write Cycle		~5 ms
Step 12		SW1	90	Write operation successful
Finish		SW2	\$00	

9.4.3. Write User Zone: \$B0

9.4.3.1. Functional

Figure 9-2. Write User Zone Command Functional Description



The Write User Zone command \$B0 allows data to be written into the device's currently selected user zone (the procedure for selecting a user zone is described in section 9.4.5. [System Write: \\$B4](#)).

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 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.

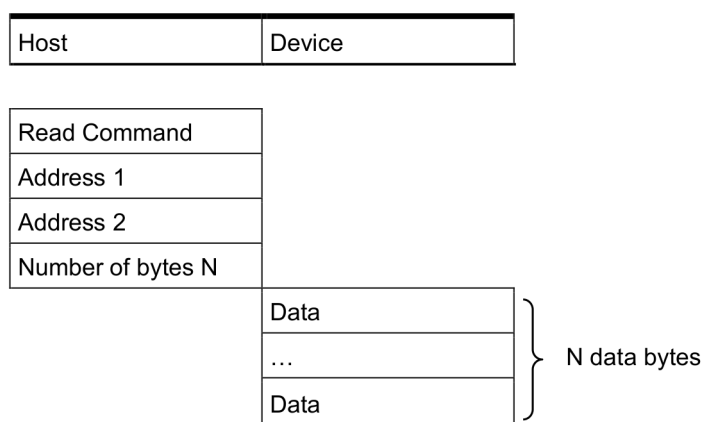
Table 9-4. Write User Zone

Write User Zone Command					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

9.4.4. Read User Zone: \$B2

9.4.4.1. Functional

Figure 9-3. Read User Zone Command Functional Description



The Read User Zone command \$B2 allows data to be read from the device's currently selected user zone (the procedure for selecting a user zone is described in section 9.4.5. [System Write: \\$B4](#)). 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.

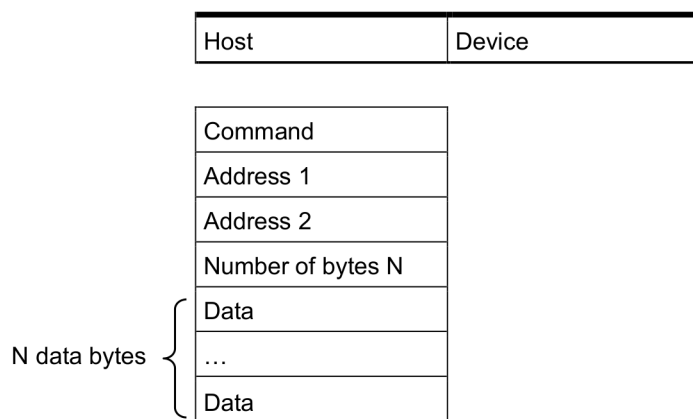
Table 9-5. Read User Zone

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

9.4.5. System Write: \$B4

9.4.5.1. Functional

Figure 9-4. System Write Command Functional Description



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

Table 9-6. System Write Command Detail

Command	CLA	INS	P1	P2	P3	Data(N)
Write Config Zone (Devices 0104C-1616C)	\$00	\$B4	\$00	ADDR	$N \leq \$10$	N bytes
Write Config Zone (Devices 3216C-6416C)	\$00	\$B4	\$00	ADDR	$N \leq \$40$	N bytes
Write Config Zone (Devices 12816C-25616C)	\$00	\$B4	\$00	ADDR	$N \leq \$80$	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 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 must be turned off if not required, as it would otherwise cause more write cycles than necessary.

Table 9-7. Anti-Tearing

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

9.4.5.2. 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 unauthorized, 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 specify a number of bytes that causes the device to reach an unauthorized address. In this case, the device will prevent the internal write cycle, and no bytes will be written to 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.

9.4.5.3. Write Fuses

The fuses may only be programmed, that is written from one to zero. The write fuses operation is allowed only after successfully presenting the secure code (Write 7 password). The fuses must be blown sequentially:

1. FAB must be blown first.
2. CMA may be blown only if FAB is zero.
3. PER may be blown only if CMA is zero.

Table 9-8. Fuse Writing

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

9.4.6. Send Checksum

To write data to user zones that require authentication for write access (AM [1:0] = 01 or 00 in the access register), the host must first carry out the write user zone command \$B0, after which the device will return a special status word: \$62 \$00. This indicates that the memory is unchanged and the device is waiting for the host to provide a valid checksum before initiating the write cycle. The host sends the checksum it has computed using the System Write command opcode \$B4 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.

9.4.6.1. Set User Zone

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

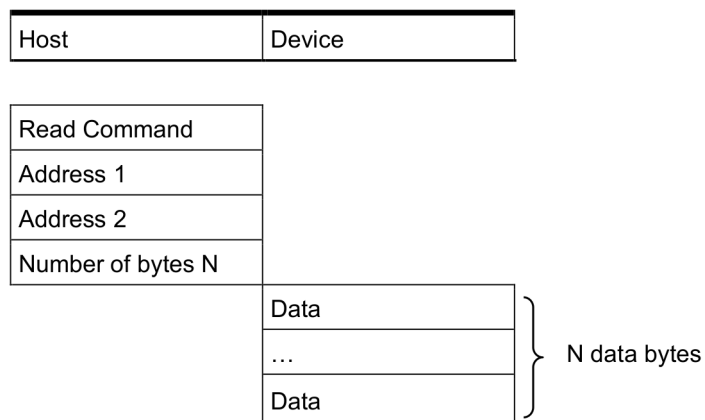
Table 9-9. System Write

User Read					Data Returned		
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

9.4.7. System READ: \$B6

9.4.7.1. Functional

Figure 9-5. System READ Command Functional Description



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

Table 9-10. 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
Read Checksum	\$00	\$B6	\$02	\$00	\$02

9.4.7.2. Read Config Zone

To read 256 bytes, the host must set N = \$00. This is true for any outgoing command and is defined by ISO 7816-3. If the address provided at P2 is unauthorized, 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 specify a number of bytes, N, that causes the device to reach an 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 are not valid.

9.4.7.3. Read Fuse Byte

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

Table 9-11. 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

9.4.7.4. Read Checksum

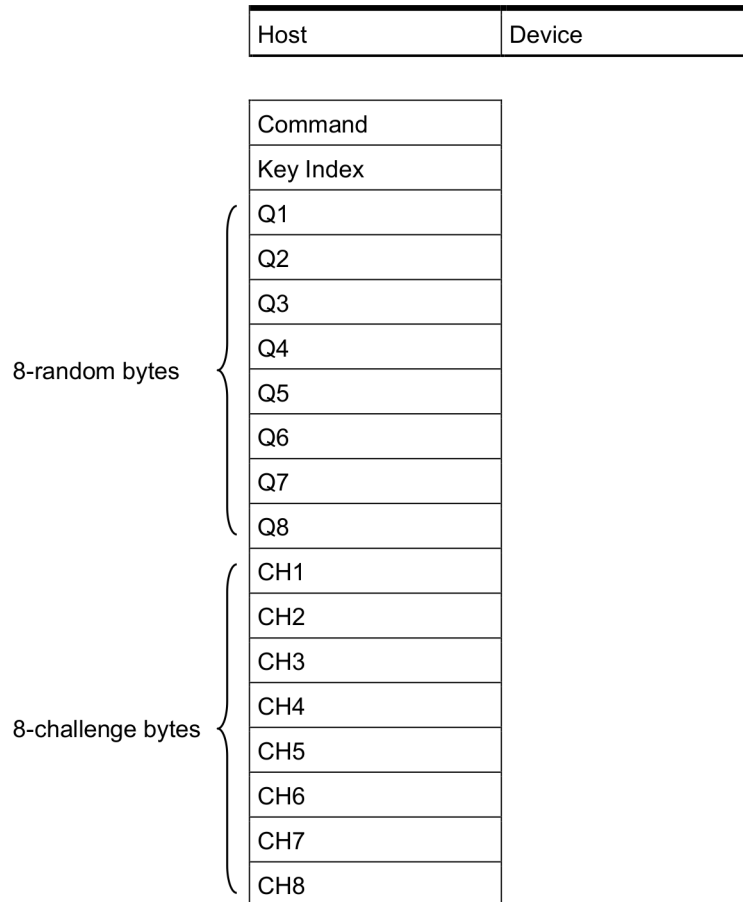
The checksum consists of two bytes, and the Read Checksum command must be sent with parameter P3 = 2.

Table 9-12. 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

9.4.8. Verify Crypto: \$B8

9.4.8.1. Functional

Figure 9-6. 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 G₀-G₃
- b0001_00nn : Session Encryption Key S₀-S₃

Data :

- Q : Host random number, 8 bytes

- CH : Host challenge, 8 bytes

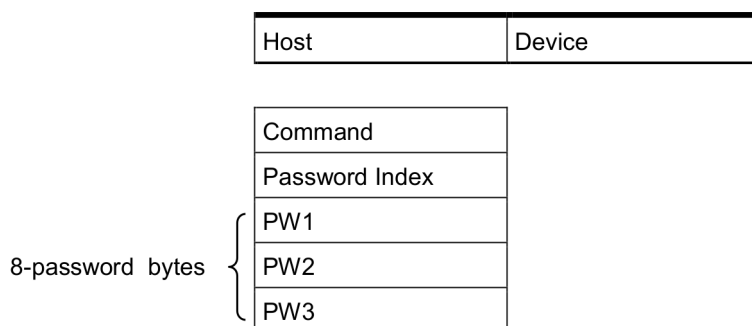
Table 9-13. Verify Crypto

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

To prevent replay attacks, the device increments the Associated Attempts Counter before each verification challenge. 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 that the command is unauthorized.

9.4.9. Verify Password: \$BA

9.4.9.1. Functional

Figure 9-7. Verify 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

Table 9-14. Verify Password

Verify Password					Data Sent		
CLA	INS : Command	P1	P2	P3	PW1	PW2	PW3
**	\$BA	000r 0p ₂ p ₁ p 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 that the command is unauthorized. To prevent replay attacks, the device decrements the Associated Attempts Counter before verifying the password. If the password is correct, the device memorizes this success, clears the attempts counter and returns \$90 \$00. If the password is incorrect, the device simply returns \$69 \$00 after decrementing the attempts counter. The Write 7 password is also known as the secure code and

must be properly presented before write access to the configuration memory is granted when personalizing the device.

10. Asynchronous Initialization Example

The first step in initializing CryptoMemory[®] is to determine what data are to be stored in the device and what security settings are needed 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.

10.1. Write Data to User Zones

In the default configuration from Microchip, all user zones have free access rights. Writing initial data into the user zones must 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.

10.2. Unlock the 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 Microchip to unlock the configuration memory. Use the Read Config Zone command to read back the security code at address \$E9 to verify that the configuration memory has been unlocked.

10.3. 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.

10.4. Set Security Fuses

Once all data have been written and verified in the user zones and the configuration memory, the security fuses must 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 in the specified order: first, FAB, followed by CMA, and then PER. Each fuse is set individually using the Write Fuse command. The status of all three fuses can be verified using the Read Fuse command. Once all fuses have been set, the Read Fuse command will 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 four user zones. Security for each of these four user zones and the associated register values are shown in the table below. Simple values for passwords are used.

Table 10-1. 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 2) 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 (*).

***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

*Set User Zone 2
00 B4 03 02 00

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

*Set User Zone 3
00 B4 03 03 00

*Write data = Zone 3 Data
00 B0 00 00 0B 5A 6F 6E 65 20 33 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, AR2/PR2 = DF BF, AR3/PR3 = 57 B9
00 B4 00 22 06 7F F9 DF BF 57 B9

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

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

*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 DF BF 57 B9 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 22 22 22 22 22 22 22 FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
5B 4F 9A E4 B5 09 8B E7 D8 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

*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
```

11. 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	6V
DC output current	5 mA

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 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.

11.1. DC and AC Characteristics

Table 11-1. DC Characteristics

Applicable over the recommended operating range from $V_{CC} = +2.7V$ to $5.5V$, $T_{AC} = -40^{\circ}C$ to $+85^{\circ}C$ (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 3.57 MHz			5	mA
I_{CC}	Supply Current ($V_{CC} = 5.5V$)	Async Write at 3.57 MHz			5	mA
I_{CC}	Supply Current ($V_{CC} = 5.5V$)	Synch Read at 1 MHz			5	mA
I_{CC}	Supply Current ($V_{CC} = 5.5V$)	Synch Write at 1 MHz			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		$V_{CC} \times 0.2$	V
V_{IL}	Clock Input Low Voltage ⁽¹⁾		0		$V_{CC} \times 0.2$	V
V_{IL}	RST Input Low Voltage ⁽¹⁾		0		$V_{CC} \times 0.2$	V
V_{IH}	SDA/IO Input High Voltage ⁽¹⁾		$V_{CC} \times 0.7$		V_{CC}	V
V_{IH}	SCL/CLK Input High Voltage ⁽¹⁾		$V_{CC} \times 0.7$		V_{CC}	V
V_{IH}	RST Input High Voltage ⁽¹⁾		$V_{CC} \times 0.7$		V_{CC}	V
I_{IL}	SDA/IO Input Low Current	$0 < V_{IL} < V_{CC} \times 0.15$			15	μA
I_{IL}	SCL/CLK Input Low Current	$0 < V_{IL} < V_{CC} \times 0.15$			15	μA
I_{IL}	RST Input Low Current	$0 < V_{IL} < V_{CC} \times 0.15$			50	μA
I_{IH}	SDA/IO Input High Current	$V_{CC} \times 0.7 < V_{IH} < V_{CC}$			20	μA
I_{IH}	SCL/CLK Input High Current	$V_{CC} \times 0.7 < V_{IH} < V_{CC}$			100	μA
I_{IH}	RST Input High Voltage	$V_{CC} \times 0.7 < V_{IH} < V_{CC}$			150	μA
V_{OH}	SDA/IO Output High Voltage	20K ohm external pull-up	$V_{CC} \times 0.7$		V_{CC}	V
V_{OL}	SDA/IO Output Low Voltage	$I_{OL} = 1\text{ mA}$	0		$V_{CC} \times 0.15$	V
I_{OH}	SDA/IO Output High Current	V_{OH}			20	μA

Note:

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

Table 11-2. AC Characteristics

Applicable over the recommended operating range from $V_{CC} = +2.7V$ to $5.5V$, $T_{AC} = -40^{\circ}C$ to $+85^{\circ}C$ (*unless otherwise noted*).

Symbol	Parameter	Min.	Max.	Units
f _{CLK}	Async Clock Frequency (V _{CC} range: +4.5V to 5.5V)	1	5	MHz
f _{CLK}	Async Clock Frequency (V _{CC} range: +2.7V to 3.3V)	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		35	µs
t _{HD.STA}	Start Hold Time	200		ns
t _{SU.STA}	Start Setup Time	200		ns
t _{HD.DAT}	Data In Hold Time	10		ns
t _{SU.DAT}	Data In Setup Time	100		ns
t _{SU.STO}	Stop Setup 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

11.2. Timing Diagrams for Synchronous Communications

Figure 11-1. Bus Timing

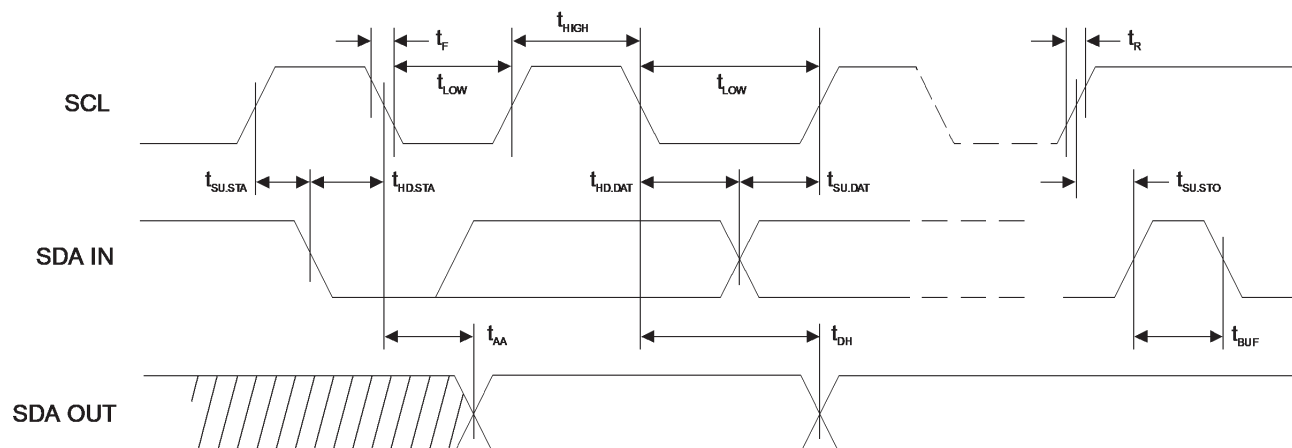
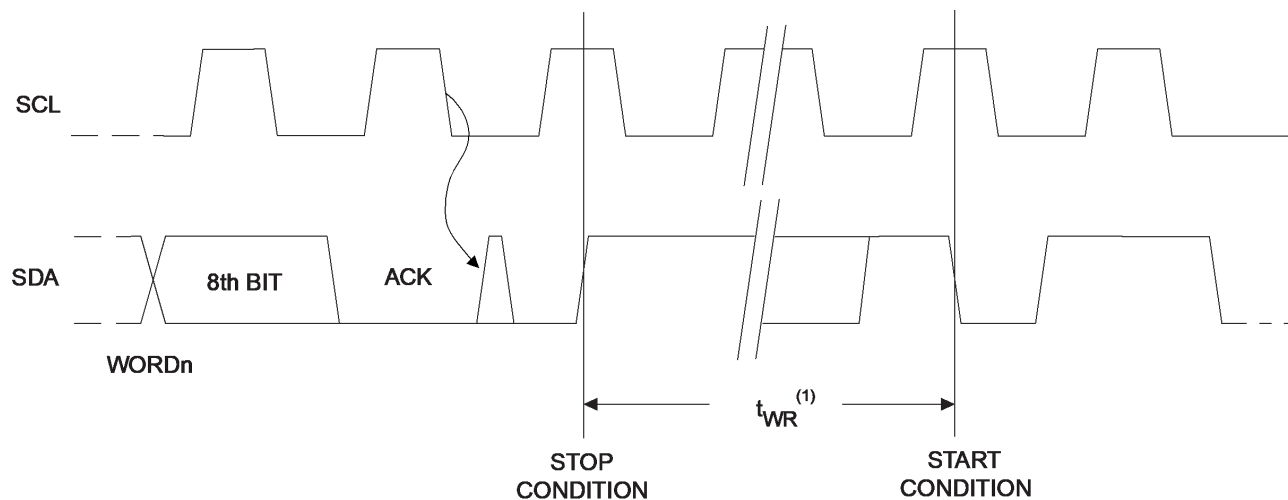


Figure 11-2. Write Cycle Timing



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 11-3. Data Validity

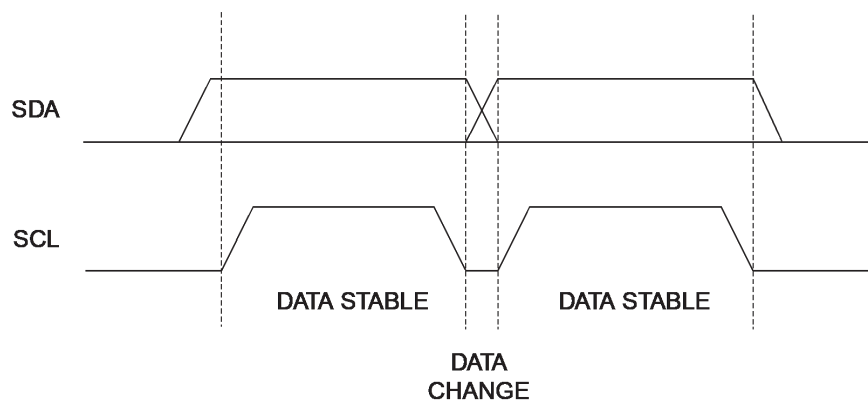


Figure 11-4. Start and Stop Definition

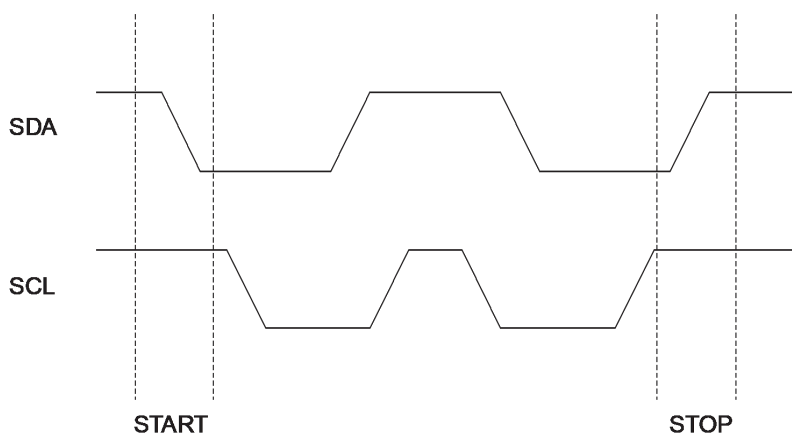
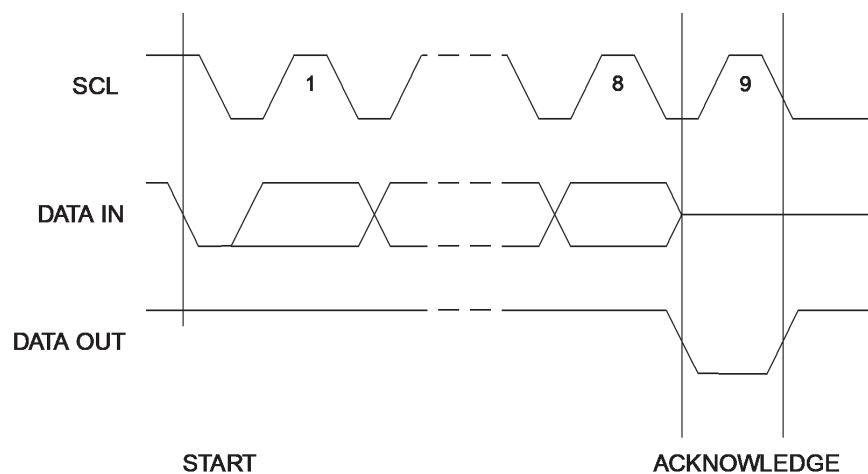


Figure 11-5. Output Acknowledge

12. DC Tamper Detection Limits

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

12.1. High Voltage and Low Voltage Limits

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

12.2. 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.

12.3. Maximum Clock Frequency

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

12.4. Power-On Reset (POR) Delay

Any time 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.

12.5. Noise Suppression

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

Table 12-1. Tamper Detection

Applicable over the recommended operating range from $T_{AC} = -40^{\circ}\text{C}$ to $+85^{\circ}\text{C}$ (unless 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	μs
t_{SUP}	Min. SCL, SDA, RST Pulse		50		200	ns

13. Ordering Information

Microchip Ordering Code	Package	Delivery Information		Voltage Range	Temperature Range
		Form	Quantity		
AT88SCxxxxC-MJ	M2 – J Module - ISO	Tape and Reel	—	2.7V to 5.5V	Commercial Temperature (0°C to 70°C)
AT88SCxxxxC-MJTG	M2 – J Module - TWI				
AT88SC3216C-SU	8S1	Bulk (Tubes)	100 per Tube	2.7V to 5.5V	Green Compliant (Exceeds RoHS) Industrial Temperature (-40°C to 85°C)
AT88SC3216C-SU-T		Tape and Reel	4,000 per Reel		
AT88SC6416C-SU		Bulk (Tubes)	100 per Tube		
AT88SC6416C-SU-T		Tape and Reel	4,000 per Reel		
AT88SC12816C-SU		Bulk (Tubes)	100 per Tube		
AT88SC12816C-SU-T		Tape and Reel	4,000 per Reel		
AT88SC25616C-SU		Bulk (Tubes)	100 per Tube		
AT88SC25616C-SU-T		Tape and Reel	4,000 per Reel		
AT88SC0104C-SH		Bulk (Tubes)	100 per Tube		
AT88SC0104C-SH-T		Tape and Reel	4,000 per Reel		
AT88SC0204C-SH		Bulk (Tubes)	100 per Tube		
AT88SC0204C-SH-T		Tape and Reel	4,000 per Reel		
AT88SC0404C-SH		Bulk (Tubes)	100 per Tube		
AT88SC0404C-SH-T		Tape and Reel	4,000 per Reel		
AT88SC0808C-SH		Bulk (Tubes)	100 per Tube		
AT88SC0808C-SH-T		Tape and Reel	4,000 per Reel		
AT88SC1616C-SH		Bulk (Tubes)	100 per Tube		
AT88SC1616C-SH-T		Tape and Reel	4,000 per Reel		
AT88SCxxxxC-WI	7 mil wafer	—	—		Industrial Temperature (-40°C to 85°C)

Note: Ordering codes are valid for all devices covered by this data sheet (see p.1 for a complete list).

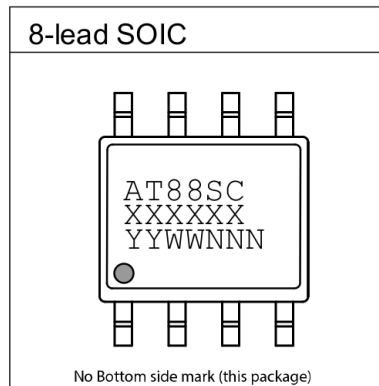
Package Type ^{(1) (2) (3)}	Description
M2 – J Module : ISO or TWI	M2 ISO 7816 Smart Card Module
8S1	8-lead, 0.150" wide, Plastic Gull Wing Small Outline (JEDEC SOIC)

Notes:

- Formal drawings may be obtained from a Microchip sales office.
- The MJ module ISO package style can operate in either T=0 mode (asynchronous protocol) or TWI mode (synchronous protocol). The mode of operation will be determined by the power-up sequence as specified in section 6. [Protocol Selection](#).
- The 8S1 and MJTG package can only be used with TWI mode.

14. Package Marking Information

Figure 14-1. AT88SCxxxxC Part Marking



Note 1: ● designates pin 1

Note 2: Package drawings are not to scale

Date Codes		
YY = Year ⁽¹⁾	WW = Work Week of Assembly ⁽¹⁾	Line 2 = XXXXXX
24: 2024	01: Week 1	8SC0104C = 0104C
25: 2025	02: Week 2	88SC0204C = 0204C
26: 2026	...	88SC0404C = 0404C
27: 2027	52: Week 52	88SC0808C = 0808C
Device Prefix	Trace Code	88SC1616C = 1616C
AT	Assigned Trace Code includes YYWW and three digits NNN ⁽²⁾	88SC3216C = 3216C
		88SC6416C = 6416C
		88SC12816C = 12816C
		88SC25616C = 25616C

Notes:

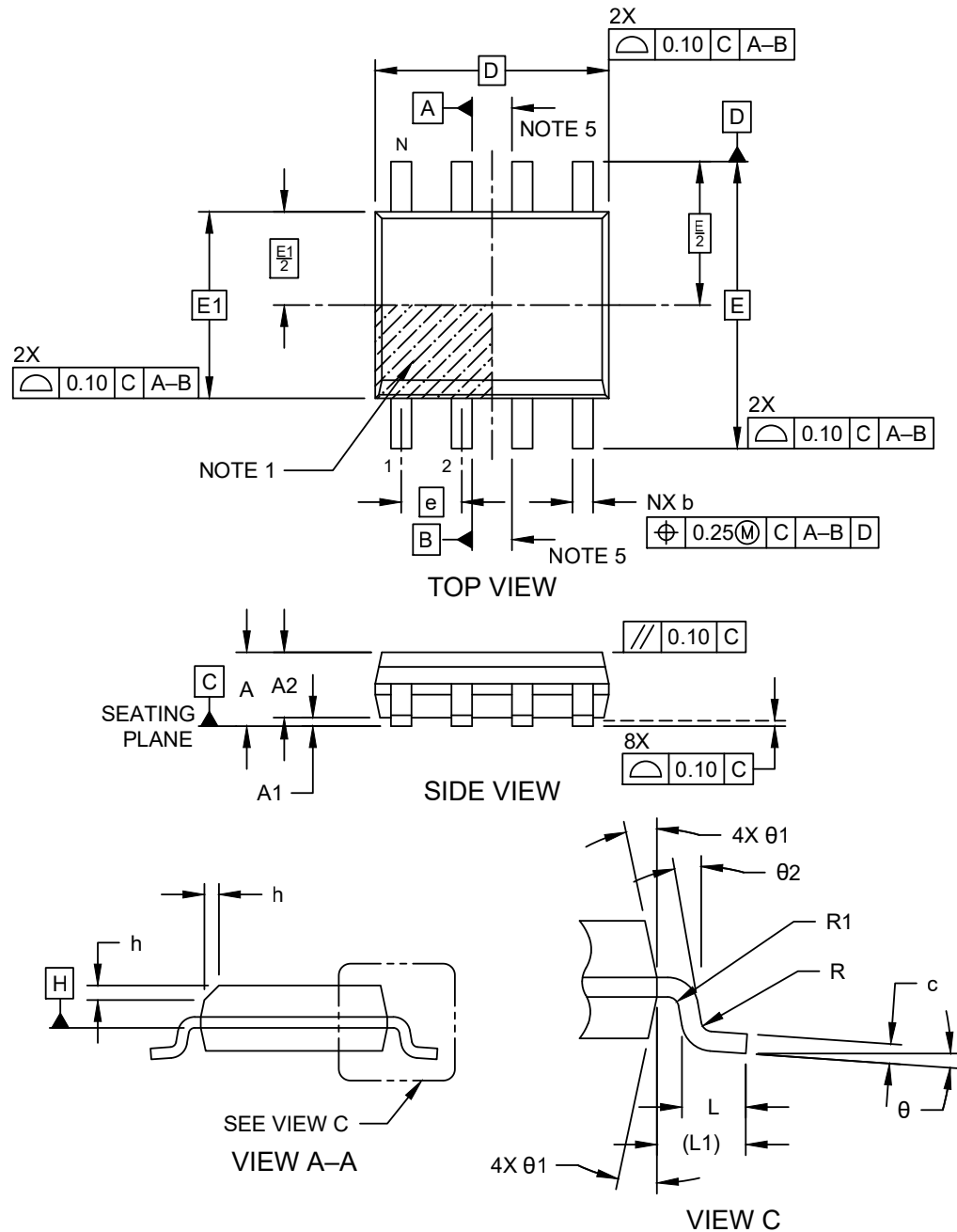
- YY corresponds to calendar year; WW corresponds to calendar year work week.
- NNN is a lot #.

14.1. Package Drawings

14.1.1. 8-Lead SOIC

8-Lead Plastic Small Outline (3BX) - Narrow, 3.90 mm (.150 In.) Body [SOIC]

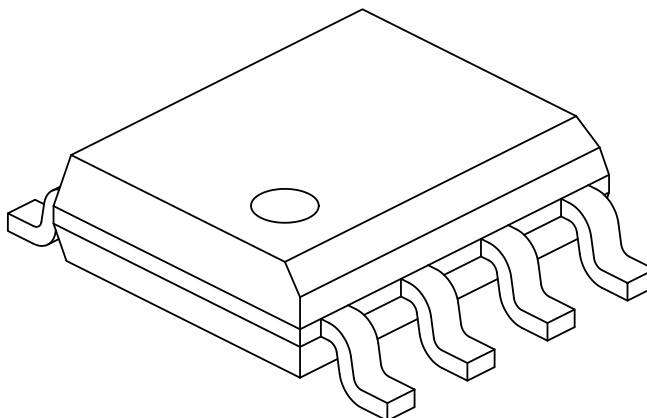
Note: For the most current package drawings, please see the Microchip Packaging Specification located at <http://www.microchip.com/packaging>



Microchip Technology Drawing No. C04-00057-3BX Rev L Sheet 1 of 2

8-Lead Plastic Small Outline (3BX) - Narrow, 3.90 mm (.150 In.) Body [SOIC]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at <http://www.microchip.com/packages>



Dimension Limits	Units	MILLIMETERS		
		MIN	NOM	MAX
Number of Pins	N	8		
Pitch	e	1.27 BSC		
Overall Height	A	–	–	1.75
Molded Package Thickness	A2	1.25	–	–
Standoff §	A1	0.10	–	0.25
Overall Width	E	6.00 BSC		
Molded Package Width	E1	3.90 BSC		
Overall Length	D	4.90 BSC		
Chamfer (Optional)	h	0.25	–	0.50
Foot Length	L	0.40	–	1.27
Footprint	L1	1.04 REF		
Lead Thickness	c	0.17	–	0.25
Lead Width	b	0.31	–	0.51
Lead Bend Radius	R	0.07	–	–
Lead Bend Radius	R1	0.07	–	–
Foot Angle	θ	0°	–	8°
Mold Draft Angle	θ1	5°	–	15°
Lead Angle	θ2	0°	–	–

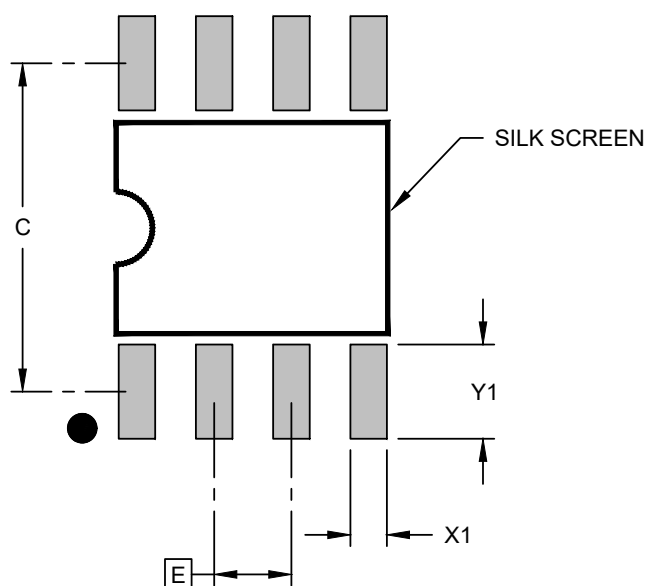
Notes:

1. The Pin 1 visual index feature may vary, but it must be located within the hatched area.
2. § Significant Characteristic
3. Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed 0.15mm per side.
4. Dimensioning and tolerancing per ASME Y14.5M
BSC: Basic Dimension. Theoretically exact value shown without tolerances.
REF: Reference Dimension, usually without tolerance, for information purposes only.
5. Datums A & B to be determined at Datum H.

Microchip Technology Drawing No. C04-00057-3BX Rev L Sheet 2 of 2

8-Lead Plastic Small Outline (3BX) - Narrow, 3.90 mm (.150 In.) Body [SOIC]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at <http://www.microchip.com/packaging>

**RECOMMENDED LAND PATTERN**

Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Contact Pitch	E	1.27 BSC		
Contact Pad Spacing	C		5.40	
Contact Pad Width (X8)	X1			0.60
Contact Pad Length (X8)	Y1			1.55

Notes:

1. Dimensioning and tolerancing per ASME Y14.5M

BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing C04-02057-3BX Rev L

15. Revision History

Table 15-1. Microchip Data Sheet Revision History

Doc. Rev.	Date	Comments
DS40002661A	10/2025	<ul style="list-style-type: none">Initial version - converted to Microchip format from Atmel version 5211FRemoved PDIP package information throughout data sheetUpdated ordering codes and notesUpdated package marking drawingsAdded SOIC package drawingAdded Microchip back matter

Table 15-2. Atmel Data Sheet Revision History

Doc. Rev.	Date	Comments
5211F	03/2015	Added JEDEC SOIC tape and reel package options
5211E	02/2014	Added package marking information and updated Microchip logos and disclaimer page
5211D	12/2011	Updated template and edited ordering information
5211C	01/2010	Added MJTG module and added ordering information
5211B	01/2010	Converted to MS Word
5211A	06/2010	Initial document release

Microchip Information

Trademarks

The “Microchip” name and logo, the “M” logo, and other names, logos, and brands are registered and unregistered trademarks of Microchip Technology Incorporated or its affiliates and/or subsidiaries in the United States and/or other countries (“Microchip Trademarks”). Information regarding Microchip Trademarks can be found at <https://www.microchip.com/en-us/about/legal-information/microchip-trademarks>.

ISBN: 979-8-3371-1948-9

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

THIS INFORMATION IS PROVIDED BY MICROCHIP “AS IS”. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP’S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

Use of Microchip devices in life support and/or safety applications is entirely at the buyer’s risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip products:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip products are strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is “unbreakable”. Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.

Product Page Links

[AT88SC0104C](#), [AT88SC0204C](#), [AT88SC0404C](#), [AT88SC0808C](#), [AT88SC12816C](#), [AT88SC1616C](#),
[AT88SC25616C](#), [AT88SC3216C](#), [AT88SC6416C](#)